POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

HISTÓRICO DAS ALTERAÇÕES E REVISÕES

Elaboração

Autor: Rosane Roman	
Versão: 000	**Data de início da vigência:** 28/07/2022
Ata de Aprovação: 673	

Revisão

Revisor: Julio Schaak	
Versão: 001	**Data de início da vigência:** 01/06/2025
Ata de Aprovação: 006/25	

SUMÁRIO

1. Objetivo

Estabelecer diretrizes, papéis e responsabilidades que assegurem a correta utilização dos ativos de informação da organização, baseado nos princípios de confidencialidade, integridade e disponibilidade, compatível com o modelo simplificado de negócio, natureza das operações e a complexidade dos produtos, serviços, atividades e processos da Banricoop.

2. Abrangência

O presente documento é vigente no âmbito da Banricoop e de todos os prestadores de serviços relevantes que estejam atuando em nome Cooperativa.

3. Definições

3.1 Segurança da informação

Proteção de ativos de informação, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. São propriedades básicas da segurança da informação a confidencialidade, a integridade e a disponibilidade.

3.2 Segurança cibernética

Conjunto de ações sobre pessoas, tecnologias e processos contra os ataques cibernéticos. Por vezes nomeada segurança digital ou segurança de TI, é uma ramificação da segurança da informação.

3.3 Ativo de informação

São os meios, locais, equipamentos e sistemas de armazenamento, transmissão e processamento da informação.

3.4 Incidente

Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos ativos de informação.

3.5 Malware

Proveniente do inglês *malicious software* (software malicioso), é um software destinado a infiltrar-se em um sistema de computador alheio de forma ilícita, com o intuito de causar danos, alterações ou roubo de informações.

3.6 Dado

Conjunto de informações que não foram tratadas, organizadas ou interpretadas, de forma que não tem um significado claro.

3.7 Informação

Conjunto de dados organizados, que podem ser utilizados para produção e transmissão de conhecimento, contidos em meio físico ou digital.

3.8 Vulnerabilidade

Qualquer fator que possa contribuir para gerar invasões, roubos de dados ou acessos não autorizados a ativos de informação.

4. Princípios

4.1 Confidencialidade

Garantia de que o acesso aos dados e informações estejam disponíveis apenas para pessoas autorizadas e quando eles de fato forem necessários.

4.2 Integridade

Garantia da exatidão e da completude dos dados e informações tratados pelas instituições.

4.3 Disponibilidade

Garantia de que os dados e informações estejam disponíveis para as pessoas autorizadas sempre que necessário.

5. Diretrizes

Essa política estabelece as seguintes diretrizes relacionadas à segurança da informação e cibernética:

a) Tratamento e classificação das informações da instituição, cooperados e público em geral respeitando os princípios de confidencialidade, integridade, disponibilidade de acordo com sua relevância;

b) Procedimentos e controles em conformidade com a Resolução CMN n° 4.893, de 26 de fevereiro do 2021;

c) Identificação única, pessoal e intransferível de pessoas autorizadas a acessar informações, de forma que seja possível qualificar o responsável pelas ações realizadas em ativos de informação;

d) Desenvolvimento e manutenção de controles efetivos, de forma a garantir a proteção de ativos de informação em todo o seu ciclo de vida;

e) Concessão de acessos a ativos de informação restrita aos recursos indispensáveis para o pleno desempenho das atividades da pessoa autorizada;

f) Identificação contínua dos riscos relacionados à segurança da informação e cibernética, e atuação para mantê-los em níveis considerados aceitáveis, sendo o seu gerenciamento realizado de forma integrada com os demais riscos da instituição;

g) Estabelecimento de procedimentos e controles para a redução de vulnerabilidades, gestão de incidentes, classificação de informações, rastreabilidade de informações sensíveis, entre outros, por meio de normativos específicos;

h) Aplicação dos procedimentos e controles de segurança da informação e cibernética nos ativos de informação desenvolvidos internamente e nos adquiridos de terceiros;

i) Contratação de prestadores de serviços de processamento e armazenamento de dados e de computação em nuvem, de acordo com critérios estabelecidos em normativos internos;

j) Estabelecimento de critérios mínimos de segurança através de cláusulas contratuais na relação com terceiros fornecedores de serviços e exigência de comunicação tempestiva de incidentes relevantes;

k) Exigência aos parceiros contratados de promoção de educação continuada a respeito de segurança da informação e cibernética;

l) Promoção da cultura de segurança da informação e cibernética em todos os níveis da organização, incluindo treinamentos internos e informações a cooperados e público em geral sobre precauções na utilização de produtos e serviços financeiros;

m) Definição de cenários de incidentes para realização de testes de continuidade de negócios com base na criticidade dos processos; e

n) Definição de relevância dos incidentes mediante análise da criticidade do impacto nos processos de negócio conforme legislação vigente.

6. Procedimentos e Controles

Os procedimentos e controles estabelecidos e dispostos a seguir, consideram a estrutura, o porte, o perfil de risco e o modelo de negócio da Banricoop, sendo compatíveis com a natureza

das operações e a complexidade dos produtos, serviços, atividades e processos, bem como a sensibilidade dos dados e das informações sob responsabilidade da Cooperativa.

Visando reduzir a vulnerabilidade dos ativos, prevenir o vazamento de informações e atender as diretrizes estabelecidas nesta política são adotados procedimentos e controles destacados abaixo:

a) A gestão de acessos, com tratamento das regras de controle de complexidade, de concessões e de exclusões de acessos aos ativos de informação;

b) Os ativos de informação são identificados de forma individual, inventariados e protegidos, fisicamente, nos casos aplicáveis, por meio de salas com acesso controlado, e logicamente, por meio de firewall, monitoramentos, autenticação e autorização, além de recursos para evitar a ação de malwares;

c) As informações, mantidas em meio eletrônico ou físico, são classificadas quanto à sua relevância, nos níveis Pública, Interna e Confidencial, considerando os requisitos legais, as necessidades do negócio, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida;

d) Os alertas gerados, de acordo com os critérios definidos pela estrutura, devem ser analisados, classificados, tratados como incidentes e comunicados aos canais competentes;

e) Os dados e informações são armazenados em ativos redundantes, com cópias de segurança, além de replicação para reduzir o tempo de recuperação; e

f) As comunicações por voz são gravadas e mantidas em mídias de longa retenção.

7. Rastreabilidade da Informação

A rastreabilidade é a capacidade de detalhar o histórico de um item, através de informações previamente registradas. São realizadas as seguintes ações para rastreabilidade das informações:

a) Acesso ao sistema legado: relatório de auditoria contendo as informações dos acessos dos usuários nos sistemas, que permite auditar e rastrear as alterações e os respectivos responsáveis. O relatório contempla a credencial responsável pela alteração, data e hora, tipo de ação, rotina e módulo.

b) E-mails: rastreamento por meio de ferramenta de gerenciamento de e-mails, que permite identificar origem e destino das mensagens.

c) Telefonia: a infraestrutura relacionada à telefonia é do tipo VOIP, o que permite identificar o responsável pela ligação e o seu conteúdo, que fica armazenado em backup em fita.

d) Acesso físico: monitoramento por meio de circuito fechado de TV, que permite identificar as movimentações dos colaboradores, cooperados e visitantes que acessam as dependências internas. As imagens permanecem armazenadas pelo período de 30 dias.

8. Registro e Análise da Causa e do Impacto

Os incidentes relevantes são classificados conforme os cenários previstos de acordo com a sua criticidade, que considera a probabilidade de ocorrência, a severidade e o impacto.

A partir da identificação das ocorrências, são tomadas as medidas para reestabelecimento do serviço ou plataforma, efetuando-se os respectivos registros posteriormente em Relatório de Análise de Impacto, disponibilizados sistematicamente ao Comitê de Riscos e do Conselho de Administração.

9. Contratação de serviços em nuvem

Em relação a contratação de serviços em nuvem, a Banricoop é responsável pela confiabilidade, integridade, disponibilidade, segurança e sigilo em relação aos serviços contratados, bem como pelo cumprimento da legislação e da regulamentação em vigor.

9.1 Critérios de decisão quanto a contratação de serviços em nuvem

Em relação a contratação de serviços em nuvem, tanto no Brasil como no exterior, devem ser observados os seguintes critérios:

a) Adoção de práticas de governança corporativa e de gestão proporcionais à relevância do serviço a ser contratado e aos riscos a que estejam expostos, conforme avaliação previamente realizada;

b) Verificação da capacidade do prestador de serviços em assegurar:

i. O cumprimento da legislação e da regulamentação em vigor;

ii. O acesso da instituição aos dados e às informações a serem processados ou armazenados pelo prestador de serviço;

iii. A confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados pelo prestador de serviço;

iv. A aderência quanto as certificações exigidas pela Cooperativa para a prestação do serviço a ser contratada;

v. A acesso da Banricoop aos relatórios elaborados por empresa de auditoria especializada independente contratada pelo prestador de serviço, relativos aos procedimentos e aos controles utilizados na prestação dos serviços a serem contratados;

vi. O provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;

vii. A identificação e a segregação dos dados dos cooperados por meio de controles físicos ou lógicos; e

viii. A qualidade dos controles de acesso voltados à proteção dos dados e das informações dos cooperados.

9.2 Avaliação da relevância do serviço a ser contratado

Na avaliação da relevância do serviço em nuvem a ser contratado, será considerada a criticidade do serviço e a sensibilidade dos dados e das informações a serem processados, armazenados e gerenciados pelo prestador de serviços contratado, levando em conta, inclusive, a classificação das informações, conforme item 6 - letra "c" desta política.

9.3 Disponibilidade de serviços

Os serviços de computação em nuvem devem contemplar a disponibilidade à Banricoop, seja sob demanda e de maneira virtual, de pelo menos um dos serviços destacados abaixo, quando aplicável:

a) Processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursos computacionais que permitam à instituição contratante implantar ou executar softwares, que podem incluir sistemas operacionais e aplicativos desenvolvidos pela instituição ou por ela adquiridos;

b) Implantação ou execução de aplicativos desenvolvidos pela instituição contratante, ou por ela adquiridos, utilizando recursos computacionais do prestador de serviços; ou

c) Execução, por meio da internet, de aplicativos implantados ou desenvolvidos pelo prestador de serviço, com a utilização de recursos computacionais do próprio prestador de serviços.

9.4 Contratação do serviço e comunicação ao Banco Central do Brasil

Todas as regras de contratação devem ser observadas conforme disposto no Art. 17 da Resolução CMN nº 4.893/2021.

Quanto determinada a contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem deve realizada pela Banricoop a comunicação ao Banco Central do Brasil, até dez dias após a contratação dos serviços, contendo as seguintes informações:

a) Denominação da empresa contratada;

b) Serviços relevantes contratados; e

c) Indicação dos países e das regiões em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados, no caso de contratação no exterior.

Devem também ser comunicadas as alterações contratuais que impliquem modificação das informações destacadas acima, em até dez dias após a alteração contratual.

Para a contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem prestados no exterior devem ser observados requisitos dispostos no Art. 16 da Resolução CMN n° 4.893/2021.

10. Papéis e Responsabilidades

10.1 Conselho de Administração

a) Ratificar, anualmente, as políticas e estratégias de segurança da informação e cibernética;

b) Designar o diretor responsável pela segurança da informação e cibernética; e

c) Promover a disseminação da cultura de segurança da informação e cibernética.

10.2 Diretor Responsável pela Política de Segurança da Informação e Cibernética

a) Implementar a estrutura de segurança da informação e cibernética;

b) Assegurar a aderência da instituição à política e estratégias de segurança da informação e cibernética;

c) Assegurar a disseminação da cultura de segurança da informação e cibernética; e

d) Aprovar a contratação do processamento, armazenamento de dados e de computação em nuvem.

10.3 Gerência de Infraestrutura

a) Implementar e gerenciar as soluções de segurança cibernética nos ambientes de tecnologia;

b) Conceder, revisar e excluir acessos a ativos de informações;

c) Inventariar e proteger os ativos de informações;

d) Atuar nos eventos e incidentes de segurança da informação e cibernética promovendo a solução de forma tempestiva;

e) Identificar, comunicar e monitorar os riscos relacionados à segurança da informação e cibernética;

f) Desenvolver e manter atualizada, revisando anualmente, a política e os normativos de segurança da informação e cibernética;

g) Homologar os prestadores de serviços considerados relevantes ou que manuseiem dados e informações da instituição, cooperados e público em geral;

h) Avaliar a necessidade de contratação do processamento, armazenamento de dados e de computação em nuvem; e

i) Desenvolver e manter o programa educacional em segurança da informação e cibernética.

11. Base Regulatória / Legislação Aplicável

11.1 Normas Externas

a) Resolução CMN nº 4.893/2021: Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil;

b) Resolução CMN nº 4.557/17: Dispõe sobre a estrutura de gerenciamento de riscos e a estrutura de gerenciamento de capital; e

c) Resolução CMN nº 4.553/17: Estabelece a segmentação do conjunto das instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil para fins de aplicação proporcional da regulação prudencial.

11.2 Normas Internas

a) Plano de Resposta a Incidentes de Segurança da Informação;

b) Norma para Classificação da Informação;

c) Política de Gerenciamento de Risco Operacional;

d) Plano de Continuidade de Negócios;

e) Gestão de Continuidade de Negócios.