**INFORMAÇÕES SOBRE A POLÍTICA DE SEGURANÇA CIBERNÉTICA DO BANCO RABOBANK**

## 1. INTRODUÇÃO

Este documento consiste em uma versão simplificada da Política de Segurança Cibernética do Banco Rabobank International do Brasil, doravante Banco Rabobank, e possui como objetivo demonstrar, em linhas gerais, os controles adotados pelo Banco Rabobank para prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético.

Os objetivos principais de referida Política são: (i) garantir a confidencialidade, integridade e disponibilidade das informações dos clientes, empregados e fornecedores do Banco Rabobank (ii) proteger adequadamente os sistemas e informações do Banco, (iii) garantir a continuidade dos negócios do Banco, protegendo os processos críticos de interrupções, e (iv) garantir que sejam respeitadas as finalidades aprovadas pelo Banco durante a prestação de serviços de terceiros quando da contratação de serviços de processamento e/ou armazenamento de dados.

Nesse contexto, o Banco Rabobank possui um aparato para governança de segurança da informação, incluindo políticas, controles e processos de gerenciamento de riscos que asseguram a confiabilidade de seus sistemas e a continuidade dos serviços relevantes para a prestação de serviços bancários.. Referidas políticas, controles e processos de segurança estão alinhados às melhores práticas e padrões internacionais de mercado e também buscam garantir a conformidade do Banco com as leis e regulamentos aplicáveis à segurança da informação, privacidade e proteção de dados.

A alta direção do Banco Rabobank está comprometida com sua Política de Segurança Cibernética e com a melhoria contínua dos processos de segurança cibernética, tendo designado um diretor responsável pela política e pela execução do plano de ação e de resposta a incidentes.

## 2. TERMINOLOGIA

Para fins deste documento e da Política de Segurança Cibernética do Banco Rabobank, os termos abaixo possuem as seguintes definições:

- Segurança Cibernética: conjunto de práticas, políticas, conceitos de segurança, abordagens de gestão de risco, treinamentos e tecnologias utilizados para proteger o ambiente cibernético, a organização, a continuidade dos negócios e os dados dos clientes, funcionários, fornecedores ou parceiros de negócios do Banco Rabobank.
- Incidentes Cibernéticos: quaisquer incidentes de segurança ou técnicos que possam ocorrer no ambiente tecnológico do Banco Rabobank ou de terceiros prestadores de serviços, que possam resultar na violação de quaisquer políticas de privacidade e segurança da informações do Banco Rabobank, na interrupção de processos críticos para as atividades do Banco Rabobank ou, ainda, no acesso não autorizado a dados do Rabobank, de seus clientes, funcionários, fornecedores ou parceiros de negócios.
- Vulnerabilidades: quaisquer condições que, quando exploradas por um terceiro mal intencionado, possam resultar em violações de segurança, tais como falhas no projeto, na implementação ou na configuração de programas, serviços ou equipamentos de rede, desatualização ou ausência de mecanismos de segurança cibernética. Um ataque de exploração de vulnerabilidades ocorre quando um terceiro atacante tenta executar ações maliciosas,

como por exemplo invadir um sistema, acessar informações confidenciais, disparar ataques contra outros computadores ou tornar uma aplicação ou serviço indisponível.

## 3. ESCOPO DA POLÍTICA DE SEGURANÇA CIBERNÉTICA

A Política de Segurança Cibernética do Banco Rabobank, que é revisada anualmente, abrange controles para assegurar a confidencialidade, integridade e disponibilidade de informações, assim como medidas preventivas, detectivas/de rastreabilidade, corretivas, voltadas ao controle do ambiente cibernético, mitigação de potenciais incidentes de segurança cibernética e redução de pontos de vulnerabilidades. Entre os principais controles adotados pelo Banco Rabobank, estão:

- Autenticação;
- Criptografia;
- Prevenção e detecção de invasão;
- Prevenção de vazamento de informações;
- Realização periódica de testes e varreduras para detecção de vulnerabilidades;
- Proteção contra softwares maliciosos;
- Estabelecimento de mecanismos de rastreabilidade da informação;
- Controles de acesso e de segmentação da rede de computadores;
- Manutenção de cópias de segurança dos dados e das informações;
- Desenvolvimento seguro;
- Implementação de novas tecnologias;
- Gestão de incidentes; e
- Conscientização de usuários, clientes e fornecedores:
  - Iniciativas de conscientização da cultura de segurança cibernética, incluindo a implementação de programas de treinamento e de avaliação periódica da conscientização de colaboradores; e
  - Iniciativas de conscientização sobre segurança cibernética para clientes, empresas terceiras e prestadores de serviços relevantes.

## 4. MONITORAMENTO DE SEGURANÇA DA INFORMAÇÃO E PREVENÇÃO CONTRA CIBERATAQUES

O processo de monitoramento de segurança da informação e prevenção contra ciberataques do Banco Rabobank consistem em um conjunto de controles detectivos e corretivos, com o objetivo de evitar a concretização de ameaças cibernéticas, dentre os quais destacam-se:

- Aplicação de atualizações e correções de segurança;
- Monitoramento contra ataques cibernéticos e prevenção contra invasões, efetuado pela equipe global do Banco Rabobank;
- Verificação de conformidade de requisitos de segurança;
- Verificação periódica e gestão de tratamento de vulnerabilidades ;
- Realização periódica de testes e varredura de vulnerabilidades;
- Monitoramento de status das ferramentas de anti-vírus e de alertas gerados;
- Proteção contra softwares maliciosos; e
- Prevenção de vazamento de informações.

## 5. GESTÃO DE SEGURANÇA DAS APLICAÇÕES E ADOÇÃO DE NOVAS TECNOLOGIAS

As principais premissas aplicáveis à gestão de segurança das aplicações e adoção de novas tecnologias pelo Rabobank englobam:

- O desenvolvimento de novas aplicações de serviços relevantes deve estar alinhado com as melhores práticas de segurança recomendadas por padrões internacionais e pelas políticas do Rabobank, específicas para desenvolvimento seguro;
- A adoção de novas tecnologias também deve ser submetida a controles de segurança proporcionais à classificação de criticidade do ativo, sendo que estas passam por processos de classificação, avaliação de riscos e implementação de correções ou adequações antes de serem disponibilizadas no ambiente produtivo;
- Controles e mecanismos de rastreabilidade das informações;
- Testes de segurança, como teste de penetração e teste de código seguro, também devem ser executados para os serviços relevantes antes da implementação no ambiente de produção;
- Testes de segurança gerais (como, por exemplo, parâmetros de segurança); e
- Controles para assegurar a segregação entre os ambientes de desenvolvimento, teste e produção, com o objetivo de reduzir os riscos de acessos não autorizados ou alterações indevidas no ambiente operacional, banco de dados e/ou aplicações.

## 6. TESTES DE SEGURANÇA DA INFORMAÇÃO

A gestão de testes de segurança da informação do Bank Rabobank inclui os seguintes mecanismos de controle:

- Testes de segurança para novas aplicações;
- Testes de segurança para aplicações existentes;
- Acompanhamento de correções de falhas identificadas em testes; e
- Execução de novos testes para confirmação de que as falhas foram corrigidas.

## 7. GESTÃO DE CONTROLE DE ACESSOS

Os níveis de controles aplicados na gestão de controle de acessos de recursos lógicos do Banco Rabobank variam de acordo com a classificação do ativo, incluindo, dentre outros, os seguintes mecanismos de controle:

- Controles de autenticação;
- Criptografia;
- Controles de autorização;
- Segregação de funções; e
- Revisão periódica de acessos.

## 8. GESTÃO DE INFRAESTRUTURA / CONTINUIDADE DE NEGÓCIOS

Os controles adotados pelo Banco Rabobank na gestão de infraestrutura possuem como objetivo primário garantir que o Banco Rabobank se mantenha operacional frente a ameaças cibernéticas, de modo a assegurar a confidencialidade, integridade e disponibilidade da informação. No mínimo, os seguintes controles devem ser adotados:

- Backup (cópias de segurança) dos dados e das informações;
- Elaboração de cenários de incidentes considerados nos testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes cibernéticos; e
- Os resultados dos testes de continuidade de negócios devem ser informados para a confecção do relatório anual sobre o plano de ação e de resposta a incidentes.

## 9. GESTÃO E PLANO DE RESPOSTAS DE INCIDENTES CIBERNÉTICOS

A gestão e plano de respostas a incidentes cibernéticos para serviços relevantes do Banco Rabobank deve ser executada considerando as análises de causa, impacto e efeito dos incidentes, bem como deve incluir, dentre outros, os seguintes controles:

- Plano de Ações de Resposta a Incidentes;
- Medidas preventivas, detectivas e mitigantes de incidentes relacionados com o ambiente cibernético;
- Processos e ferramentas utilizados na prevenção e resposta a incidentes;
- Designação de área responsável pelo registro e controle dos efeitos de incidentes relevantes;
- Registro de incidentes, com informações sobre papéis e responsabilidades;
- Classificação do incidente cibernético;
- Análise de causa e impacto;
- Recebimento de informações de fornecedores, relacionadas com incidentes com impacto na prestação de serviços relevantes;
- Definição de mecanismos para prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético;
- Elaboração do relatório anual sobre o plano de ação e de resposta para incidentes;
- Iniciativas para compartilhamento de informações sobre os incidentes relevantes com outras instituições financeiras autorizadas pelo Banco Central do Brasil ocorridos no Banco Rabobank e/ou comunicados pelos prestadores de serviços relevantes do Banco Rabobank; e
- Comunicação tempestiva ao Banco Central das ocorrências de incidentes relevantes e das interrupções de serviços relevantes.

## 10. GESTÃO DE EMPRESAS PRESTADORAS DE SERVIÇOS RELEVANTES

O Banco Rabobank adota procedimentos para contratação de fornecedores de serviços de processamento e armazenamento de dados e de computação em nuvem compatíveis com o disposto na Resolução nº. 4.658/2018 do Conselho Monetário Nacional.

Na gestão de seus fornecedores, o Banco Rabobank busca principalmente garantir a execução de controles para prevenção de incidentes a serem adotados por fornecedores que manuseiam dados sensíveis ou que sejam relevantes

para as atividades do Rabobank. Referidos controles devem ser compatíveis com os processos e mecanismos de segurança cibernética adotados pelo próprio Banco Rabobank.

## 11. CONTATO

Em caso de dúvidas sobre este documento ou sobre a Política de Segurança Cibernética do Banco Rabobank, entre em contato com a divisão do Rabobank a qual você possui negócios, pelo nosso website institucional (http://www.rabobank.com.br/en/contact/index.html) ou por meio do e-mail csirt.sa@rabobank.com.

## 12. AVISO LEGAL

Este documento foi elaborado pelo Banco Rabobank apenas para fins informativos. Este documento não pode ser reproduzido (no todo ou em parte) para qualquer pessoa, para quaisquer finalidades, sem a prévia expressa autorização do Banco Rabobank. Eventuais violações estarão sujeitas às penas da lei.