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, tem 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 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. As 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.

Visando a melhoria contínua dos processos de segurança cibernética, 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 cibernéticos

2. ESCOPO DA POLÍTICA DE SEGURANÇA CIBERNÉTICA

A Política de Segurança Cibernética do Banco Rabobank, que é revisada periodicamente, abrange a confidencialidade, a integridade e a disponibilidade das informações, assim como promover a implantação de medidas preventivas, detectivas e corretivas, voltadas ao controle do ambiente cibernético, mitigação de potenciais incidentes de segurança cibernética e redução de vulnerabilidades.

3. TERMINOLOGIA

Para a 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.
- Incidente de Segurança: Um incidente de segurança pode ser definido como qualquer evento que explora alguma brecha/vulnerabilidade, de processos, de soluções, de produtos, sistemas, infraestrutura de TI, entre outros, onde o resultado pode:
    - Causar danos à negócio e/ou aos colaboradores do Rabobank e/ou clientes, ou;
    - Afetar a habilidade do Banco de entregar serviços apropriados aos clientes, ou;

- Resultar em roubo, fraude.

- Incidente Cibernético: Também conhecido como incidente de segurança cibernética, incidente de segurança de TI e / ou um incidente de segurança da informação é definido como: Uma ocorrência que compromete a confidencialidade, integridade e/ou a disponibilidade de um sistema e/ou as informações que o sistema processa, armazena ou transmite e que portanto constitui uma violação ou ameaça iminente à informação, assim como aos regulamentos internos como às políticas, procedimentos, padrões de segurança definidos pelo Banco. Destaca-se que informações armazenadas em meio físico é parte do escopo de proteção.
- Vulnerabilidades: quaisquer condições que, quando exploradas por uma pessoa desconhecida ou não vinculada ao Rabobank (mas pode ser um funcionário também) 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 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.

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 consiste em identificar ameaças e vulnerabilidades, definir controles de segurança necessários à proteção do negócio, testar e monitorar ambientes internos e externos. O objetivo principal é evitar a concretização de ameaças cibernéticas.

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

As principais premissas aplicáveis à adoção de novas tecnologias pelo Rabobank englobam:

- O desenvolvimento de novas aplicações deve estar alinhado às melhores práticas de segurança e diretrizes do Rabobank, relacionadas com o desenvolvimento seguro;
- A adoção de novas tecnologias também deve ser submetida à 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 e depois de serem disponibilizadas no ambiente produtivo;
- A implantação de controles e mecanismos de rastreabilidade das informações;
- A realização de 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;
- A realização de testes de segurança gerais (como, por exemplo, adequação aos parâmetros de segurança); e,
- A implantação de controles que assegurem 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. 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 avaliação dos riscos associados à informação e aos ativos.

7. GESTÃO DE INFRAESTRUTURA / CONTINUIDADE DE NEGÓCIOS

Os controles adotados pelo Banco Rabobank no desenvolvimento de infraestrutura possuem como objetivo primário garantir que o Banco Rabobank se mantenha operacional frente a ameaças cibernéticas, de modo a assegurar a confidencialidade, a integridade e a disponibilidade da informação, sendo assim, garantir a continuidade dos negócios por meio de análise de cenários, monitoração e testes para a melhoria contínua azem parte deste processo.

8. GESTÃO E PLANO DE RESPOSTAS DE INCIDENTES CIBERNÉTICOS

A gestão e plano de respostas a incidentes cibernéticos para serviços relevantes do Banco Rabobank são executados considerando as análises de causa, impacto e efeito dos incidentes, bem como a identificação e o monitoramento constante de cenários e situações de risco.

9. 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.

10. 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.

11. AVISO LEGAL