Cargill / Banco Cargill	**Política de Segurança Cibernética**	**Grupo: RISCOS TECNOLOGICOS E SEGURANÇA**

INTRODUÇÃO

O Banco Cargill S.A., em consonância com a Resolução nº 4.658, de 26 de abril de 2018, descreve as diretrizes da Politica de Segurança Cibernética que buscam assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados.

De acordo com a Resolução esta Política deve ser compatível com:

I– o porte, o perfil de risco e o modelo de negócio da instituição;

II– a natureza das operações e a complexidade dos produtos, serviços, atividades e processos da instituição; e

III– a sensibilidade dos dados e das informações sob responsabilidade da instituição.

A abrangência desta politica aplica-se a todos os colaboradores e terceiros prestadores de serviço, além de caráter publico por meio do sítio do Banco Cargill na internet.

OBJETIVO

O Banco Cargill, como parte integrante do Grupo Cargill, conta com o programa global de Segurança da Informação que contém medidas preventivas, técnicas e administrativas para garantir a segurança, confidencialidade e disponibilidade das informações da Cargill.

Este programa foi criado com objetivo de:

1. Garantir a segurança e confidencialidade de todas as informações do Grupo Cargill, dos funcionários e terceiros;
2. Proteger contra ameaças e riscos previsíveis à segurança, integridade ou disponibilidade das informações;
3. Proteger contra acesso ou uso não autorizado das informações.

É de extrema importância a disseminação da cultura de segurança cibernética para manter a integridade, confiabilidade e disponibilidade das informações, e para garantir cumprimento das normas do setor, legislação governamental e seus próprios Princípios Éticos, contamos com politicas internas, comunicados corporativos e treinamentos periódicos.

ESTRATÉGIAS E GOVERNANÇA

O Banco Cargill conta com uma equipe de Controle, Risco e Governança de Tecnologia que administra as práticas e políticas de Seguranca da Informação em todo o Grupo Cargill, fornecendo orientações gerais quanto à gestão dos riscos e ativos de segurança da informação.

A equipe de Controle, Risco e Governança de Tecnologia tem especialistas que se dedicam a ajudar e proteger os negócios da Cargill contra as ameaças, sejam elas cibernéticas, humanas, naturais ou de natureza geopolítica. Esta equipe tem como foco a gestão e os recursos explicitamente atribuídos nestas áreas organizacionais abaixo:

- Risco em aplicações;
- Arquitetura, governança e conformidade;
- Resiliência dos negócios;
- Segurança da informação;
- Resposta a incidentes;
- Gestão de acesso e identidade;
- Gestão de Seguranca de operações;
- Criptografia;
- Privacidade de dados;
- Riscos de terceiros;
- Gestão de Continuidade de Negócios;

GESTÃO DE AMEAÇAS E VULNERABILIDADE

A Cargill realiza avaliações de risco periódicas para identificar ameaças e vulnerabilidades de segurança cibernética, bem como possíveis consequências para os negócios.

As avaliações são realizadas nas seguintes áreas:

- Aplicativos (incluindo os móveis);
- Segurança de rede;
- Testes de análise de código estático;
- Exercícios de simulação;
- Testes de intrusão;
- Exercícios de “red team”;
- Jogos de estratégia;
- Riscos de terceiros;
- Framework de controles gerais de computação;
- Análise do impacto na resiliência dos negócios;
- Análise do impacto na privacidade.

A Cargill implementou uma metodologia de modelagem de ameaças para identificar os ativos mais valiosos, priorizar processos críticos, avaliar a exposição desses ativos e desenvolver modelos e controles de proteção personalizados.

ATUALIZAÇÃO DA POLÍTICA

A Alta Administração deve revisar, indicar atualizações e aprovar esta politica e o plano de ação e de resposta a incidentes, além de garantir sua efetividade e prática nas atividades diárias do Banco. Deve, também, garantir transparência dos processos descritos neste plano.

Esta Política foi revisado/atualizada em 10 de junho de 2020 e deve ser atualizada anualmente.