POLÍTICA DE SEGURANÇA CIBERNÉTICA

1- Aplicabilidade

Esta política se aplica a todos os usuários de Computação da RCI Brasil, bem como aos prestadores de serviços, estagiários, funcionários temporários e fornecedores. Todos esses atores devem conhecer os fundamentos e os comportamentos que devem ser adotados individualmente por todos estes atores para garantir a segurança do sistema de informação e a proteção de dados.

2- OBJETIVO

Os sistemas de informação e infra-estruturas associadas podem ser prejudicados por ameaças de todos os tipos, incluindo, mas não se limitando a, uso indevido, erro humano e ação mal-intencionada.

O objetivo desta Política de Segurança de Sistemas de Informação (doravante denominada Política) é fornecer os princípios e regras que permitem à RCI Brasil proteger sua atividade contra esse tipo de ameaça.

3- **Vocabulário e Terminologia**

TERMO	DEFINIÇÃO
CMSI	Co-responsável Métier dos Sistemas de Informação
RMSSI	Responsável Métier da Segurança dos Sistemas de Informação
CSI	Correspondente de Segurança Informática
CISO do Grupo	Diretor de segurança de informações do grupo
BCP	Plano de Continuidade dos Negócios
DRP	Plano de Recuperação de Desastre
Espaço cibernético	Compreende a Internet, os sistemas de informação, os dispositivos móveis e as tecnologias digitais que fornecem suporte aos negócios, infraestrutura e serviços
Incidentes de segurança Cibernética	Todo e qualquer evento não esperado que gere qualquer tipo de instabilidade, violação de política ou que possa causar danos ao Banco RCI
Ataque cibernético	É a exposição por um agente malicioso para tirar vantagens da (s) fraqueza (s) com a intenção de alcançar um impacto negativo no alvo. Os atacantes podem ter como alvo clientes, fornecedores e parceiros do Santander Brasil para causar um impacto significativo na Organização.
Risco para a segurança cibernética	Vem de dentro e de fora da Organização. O impacto do risco para a segurança cibernética compreendeu perdas financeiras, danos à reputação, multas regulatórias, perda de vantagem estratégica e interrupção de operações.
Ativos tecnológicos	é qualquer dispositivo físico ou digital, equipamento ou outro componente do ambiente que suporte atividades relacionadas a informações
Inteligência de Ameaça	Consiste em todo o conhecimento baseado em evidências, contexto, mecanismos e indicadores relativos às ameaças existentes, correlacionando-os com os ativos tecnológicos que podem ser comprometidos a partir da exploração e alcance dessa ameaça.

4- Fundamentos da Política

A segurança dos Sistemas de Informação do Grupo baseia-se nos principais fundamentais:

- Cada usuário age como cidadão-empresa pelo conhecimento e pela aplicação nas atividades diárias de um conjunto de regulamentos, políticas e instruções definidas dentro do Grupo.
- Todo usuário de recursos de informática deve ser identificado
- A homologação da estação de trabalho é obrigatória
- Toda conexão na rede de Informática deve ser estritamente validada
- Os aplicativos e dados devem ser protegidos devido ao seu caráter crítico
- Anexos de Segurança e Planos de Garantia de Segurança nos contratos com os Fornecedores
- Conscientização do Cliente: As informações serão disponibilizadas aos clientes e usuários com relação às precauções a serem tomadas ao usar produtos e serviços financeiros.

5- Segurança de dados

A RCI Brasil implementou uma política de classificação interna de seus documentos, descrita abaixo:

RCI SECRETO A

RCI RESTRITO B

RCI CONFIDENCIAL C

RCI INTERNO

Todos os documentos fornecidos pela RCI Brasil serão marcados de acordo com esta classificação.

6. Governança de incidentes cibernéticos

A segurança cibernética tem como fundamentos oferecer à Organização:

- A capacidade de identificar, detectar e proteger, em todo o ciberespaço, os ataques cibernéticos que possam gerar um incidente de segurança cibernética,
- A capacidade de responder rapidamente a ameaças que possam colocar em risco a RCI Brasil, afetando a confidencialidade, a disponibilidade e a integridade dos ativos e informações tecnológicas.
- Garantir a eficácia da segurança cibernética, é necessário implementar procedimentos de governança que definam os atores, as responsabilidades e a categorização de incidentes para informação e tratamento.

6.1. Plano de Ação: Avaliação e resposta a incidentes cibernéticos

O grupo CISO em conjunto com o CSI deve analisar os eventos relatados, decidir se eles devem ser classificados como incidentes de segurança da informação ou não, e avaliar o nível de criticidade.

6.1.1Definição da criticidade dos incidentes de segurança

O critério de avaliação do nível de criticidade deve ser estabelecido de acordo com o nível de exposição dos dados e pelo impacto para a continuidade dos negócios para o RCI Brasil e, dependendo da classificação, medidas devem ser tomadas considerando o tempo de reação e solução.

A primeira comunicação deve ser feita diretamente ao grupo CISO / SOC via correios eletrônicos ou outro meio rápido de contato, que assegure que as informações cheguem ao responsável pela segurança Corporativa. Todas as informações necessárias para a análise (logs, RCA e outras informações adicionais) devem ser enviadas na comunicação do evento. Deve ser levado em consideração que, como se trata de informações confidenciais, essas informações precisam ser protegidas contra acesso não autorizado e somente habilitadas ao grupo de pessoas que precisam dessas informações.

6.1.2 Operação no tratamento de incidentes relatados

Depois de receber as informações de um evento do CSI, o grupo CISO / SOC; a pessoa responsável pela Segurança local ou a pessoa designada como tal, é responsável pela sua avaliação imediata, quando o evento começou e toma a ação apropriada de acordo com os tempos de reatividade definidos pela criticidade do incidente.

6.1.3 Nível de criticidade da comunicação de incidentes de segurança

Os níveis de criticidade dos incidentes são: Crítico, Alto, Médio e Baixo. A classificação é realizada com base nos critérios definidos pelo Banco RCI.