Política de Segurança Cibernética

Código: 13.02

1. INTRODUÇÃO

A informação é um importante ativo à operação das atividades comerciais e, para manter a vantagem competitiva no mercado, é um dos principais patrimônios do mundo dos negócios. Tal como os ativos da SAM BR, a informação deve ser adequadamente manuseada e protegida. Um fluxo de informação de qualidade é capaz de decidir o sucesso de um empreendimento. Mas esse poder, somado à crescente facilidade de acesso, faz desse "ativo" um alvo de constantes ameaças internas e externas.

Segurança Cibernética é a disciplina que concentra os esforços para a proteção dos ativos de informação em um ambiente virtual, ou seja, o ambiente resultante da interação de pessoas, softwares e serviços por meio de dispositivos tecnológicos e redes conectadas a estes dispositivos.

A crescente ameaça cibernética, somada à cada vez maior dependência dos sistemas digitais faz com que a segurança da informação e segurança cibernética sejam uns dos principais riscos não financeiros para os negócios. A proteção dos sistemas e da informação, dos negócios e dos clientes, constituem prioridade de primeiro nível, sendo um componente essencial do objetivo do Grupo Santander de "contribuir para o progresso das pessoas e das empresas" e "prestar serviços digitais excelentes aos nossos clientes" e logo, da SAM BR.

2. OBJETIVO

O objetivo desta Política de Segurança da Informação e Segurança Cibernética é definir processos e controles que a Santander Brasil Gestão de Recursos LTDA. (“SAM Gestão BR”, CNPJ: 10.231.177/0001-52) e Santander Brasil Asset Management DTVM S.A. (“SAM DTVM BR”, CNPJ: 10.977.742/0001-25) - doravante designadas em conjunto como "SAM BR" estabelecem para proteção da informação e tratamento dos riscos e ameaças relacionadas à Segurança da Informação e Segurança Cibernética, com base no Marco Corporativo de Segurança Cibernética de Grupo Santander, na Política de Segurança da Informação, na Resolução nº 4.658, de 26 de abril de 2018 do Banco Central do Brasil e demais normas e disposições aplicáveis.

3. ABRANGÊNCIA

Aplica-se a todos os funcionários, executivos, diretores, estagiários e prestadores de serviços - doravante designados em conjunto como “Colaborador (es)” - da Santander Brasil Gestão de Recursos

LTDA. (“SAM Gestão BR”, CNPJ: 10.231.177/0001-52) e Santander Brasil Asset Management DTVM S.A. (“SAM DTVM BR”, CNPJ: 10.977.742/0001-25) - doravante designadas em conjunto como "SAM BR".

4. NORMAS DE REFERÊNCIA

Emissor	**Normas**
Grupo Santander	Marco Corporativo de Segurança Cibernética
BACEN	Resolução 4.658
SAM BR	Política de Segurança da Informação – Id 13-01
Banco Santander Brasil	Política de Segurança da Informação e Cyber Security: Segurança em Desenvolvimento e Manutenção de Sistemas Política de Segurança da Informação: Regras e Mecanismos de Criptografia
SAM BR	Política de Contratação de Fornecedores

5. DEFINIÇÕES/ CONCEITOS

5.1. Objetivos da Segurança da Informação

É a disciplina que concentra esforços contínuos à proteção dos ativos de informação, auxiliando a Organização a cumprir sua missão e valores. Para tanto, tem como objetivos:

Confidencialidade: garantir que as informações tratadas sejam de conhecimento exclusivo de pessoas especificamente autorizadas;

Integridade: garantir que as informações sejam mantidas íntegras, sem modificações indevidas (acidentais ou propositais);

Disponibilidade: garantir que as informações estejam disponíveis às pessoas autorizadas;

5.2. Objetivos da Segurança Cibernética

Segurança cibernética é a capacidade de identificar, prevenir, proteger, detectar, responder e recuperar rapidamente de uma ameaça cibernética, a fim de proteger a confidencialidade, integridade e disponibilidade dos ativos tecnológicos e informações. Neste contexto:

Espaço cibernético: engloba a internet, os sistemas de informação, os dispositivos móveis e as tecnologias digitais que dão suporte aos negócios, a infraestrutura e os serviços;

Incidente de segurança cibernética: todo e qualquer evento não esperado que gere algum tipo de instabilidade, quebra de política ou que possa causar danos à SAM BR;

Ataque cibernético: é a exploração por parte de um agente malicioso para tirar proveito de ponto(s) fraco(s) com a intenção de alcançar um impacto negativo no alvo. Os atacantes podem ter como alvo os clientes, fornecedores e parceiros da SAM BR para causar impacto significante para a Organização;

Risco à segurança cibernética: advêm de dentro e de fora da Organização. O impacto do risco à segurança cibernética engloba perda financeira, 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 à informação; e

Threat intelligence: consiste em todo conhecimento baseado em evidências, contexto, mecanismos e indicadores sobre ameaças existentes, correlacionando com os ativos tecnológicos que podem ser comprometidos a partir da exploração e concretização dessa ameaça.

6. RESPONSABILIDADES

6.1. Superintendência de Tecnologia e Operações – ITOP

Responsável por estabelecer, por meio da definição de políticas, padrões, procedimentos e controles, a integridade, disponibilidade e confidencialidade das informações contidas nos ambientes da Organização, minimizando possíveis impactos e vulnerabilidades e, reduzindo a ocorrência de incidentes de segurança que afetem os negócios da SAM BR. É também responsável por entender,

gerenciar, reportar e escalar o risco de Segurança Cibernética em sua área (incluindo ativos relevantes, informações, sistemas e terceiros).

As atividades abaixo descritas serão desenvolvidas por equipe interna ou por prestadores de serviço, sejam empresas do Grupo Santander ou fornecedores externos à organização. No caso de contratação de uma ou mais das atividades abaixo relacionadas, é reponsabilidade da SAM BR executar a governança dos serviços contratados.

Atribuições específicas visando a Segurança da Informação:

- Governança e Gestão de Políticas de Segurança da Informação;
- Gestão de Acessos (Definição de Regras e Critérios) e Segregação de Funções;
- Atendimento das Auditorias e Certificação de Controles Internos de Segurança da Informação;
- Definição de Requisitos e Análise de Segurança em Projetos;
- Disseminação da Cultura, Treinamento e Conscientização de Segurança da Informação, através de Netcursos disponíveis na Intranet Corporativa, conteúdos eletrônicos disponíveis no Portal da Segurança da Informação na Intranet Corporativa e demais recursos conforme disponibilidade;
- Gestão de Riscos e de Indicadores de Segurança da Informação;
- Gestão de Riscos de Segurança da Informação em Fornecedores.

Procedimentos e Controles de Segurança Cibernética:

- Autenticação e criptografia
- Proteção contra softwares maliciosos
- Gestão e Detecção de Vulnerabilidades;

- Testes de Invasão;
- Busca e Antecipação de Ameaças e Ataques Cibernéticos;
- Sistemas de Detecção e Prevenção de Ataques a Redes (IDS e IPS);
- Resposta a Incidentes de Segurança Cibernética;
- Segurança de Aplicações;
- Centro de Operações de Segurança (SOC) do Grupo Santander;
- Controles de Acesso;
- Segmentação da rede de computadores e a manutenção de cópias de segurança dos dados e das informações;
- Detalhes sobre os procedimentos para tratamento de informações de inteligência cibernética constam no ANEXO - Segurança da Informação - Procedimento para tratamento de informações de Ciber-Inteligência.

6.2. Funcionários, Prestadores de Serviços e Estagiários

Todo funcionário, prestador de serviço ou estagiário, deve observar e seguir as políticas, padrões e procedimentos estabelecidos pela Organização, sendo imprescindível a compreensão do papel da Segurança da Informação e Segurança Cibernética em suas atividades diárias. É de responsabilidade de cada funcionário, prestador de serviço ou estagiário todo prejuízo ou dano que vier a sofrer ou causar à SAM BR ou a terceiros, em decorrência da não obediência às políticas aqui referidas.

7. PRINCÍPIOS E PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

7.1. Proteção da Informação

Toda informação gerada ou desenvolvida por qualquer funcionário, prestador de serviço ou estagiário constitui ativo e propriedade intelectual desta, essencial à condução de negócios. Independentemente da forma apresentada ou do meio pelo qual é compartilhada ou armazenada, a informação deve ser utilizada unicamente à finalidade à qual foi autorizada pelo gestor da informação. É diretriz que toda informação de propriedade da SAM BR seja protegida de forma a não comprometer a sua confidencialidade, integridade ou disponibilidade.

7.2. Gestão e Controle de Acessos

O gestor de cada sistema é quem deve autorizar o acesso à informação e ao sistema, além de realizar as revisões de acesso conforme especificado. Detalhes constam na política de Segurança da Informação.

7.3. Acesso a Sistemas, Recursos de Rede e Rastreabilidade

O acesso e o uso de todos os sistemas de informação, diretórios de rede, bancos de dados e demais recursos devem ser restritos a pessoas autorizadas pelo gestor (e quando aplicável pelo proprietário da informação) responsável conforme a necessidade mínima ao cumprimento de suas funções e são rastreados através de logs fornecidos pelos Sistemas de Informação e mecanismos de prevenção a vazamentos de dados.

7.4. Autenticação e Senha

Todo funcionário, estagiário ou prestador de serviços é responsável por todos os atos executados com seu identificador (login/sigla de acesso), que é único e acompanhado de senha exclusiva para identificação/autenticação individual no acesso à informação e aos recursos de tecnologia, deve seguir os requisitos da Política de Segurança da Informação, impedir o uso de seu equipamento por outras pessoas enquanto este estiver "logado" e bloqueá-lo ao se ausentar. Detalhes constam na Política de Segurança da Informação.

7.5. Prevenção Contra Vírus, Arquivos e Softwares Maliciosos

A Organização possui controles para prevenir que vírus e outros tipos de softwares maliciosos entrem e espalhem-se nos sistemas e servidores através de arquivos e softwares não homologados cuja instalação e uso são proibidos por colocarem em risco a segurança das informações.

7.6. Manutenção e Cópias de Segurança

A SAM BR possui política e procedimentos específicos para garantir a recuperação de dados e informações. Detalhes constam no Manual de Instrução Tecnologia: Cópias de Segurança (Backup) e Recuperação (Restore) elaborado pelo Banco Santander Brasil.

7.7. Classificação dos Dados e das Informações

A Organização adota quatro categorias para efeitos de classificação da informação:

- Público;
- Interno;
- Confidencial;
- Reservado.

7.8. Desenvolvimento Seguro e Criptografia

A SAM BR, como entidade do grupo Santander, observa as políticas e procedimentos específicos relativos a prática de desenvolvimento seguro de sistemas e criptografia. Detalhes constam nas políticas de Segurança da Informação e Cyber Security: Segurança em Desenvolvimento e Manutenção de Sistemas e Segurança da Informação: Regras e Mecanismos de Criptografia, de responsabilidade do Banco Santander Brasil.

7.9. Avaliação de Fornecedores

Provedores e fornecedores que armazenam e processam dados, contratados pelo Banco Santander são avaliados sob o ponto de vista de Segurança da Informação e Segurança Cibernética e devem seguir seus papéis e responsabilidades. Detalhes constam na Política de Segurança da Informação e na Política de Contratação de Fornecedores.

8. REGISTRO, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA CIBERNÉTICA

8.1. Classificação da Relevância dos Incidentes Cibernéticos

A classificação consiste em verificar o impacto causado pelo incidente. Os impactos classificados como P0, P1, P2, são considerados incidentes cibernéticos críticos. Os impactos classificados como P3+, P3, P4 ou P5, são considerados incidentes cibernéticos não críticos. Detalhes constam no ANEXO - Cyber Security: Classificação de Cyber Incidente, elaborado pelo Banco Santander Brasil.

Devem ser seguidos, os processos de detecção, responsabilidade pelo registro e mitigação de todos os incidentes cibernéticos classificados como críticos e não críticos. Detalhes constam no ANEXO - Cyber Security: Tipos de Cyber Incidentes e Responsabilidades Envolvidas, elaborado pelo Banco Santander Brasil.

8.2. Origem e Registro dos Alertas dos Incidentes Cibernéticos

Atividades suspeitas ou incidentes identificados através do colaborador ou por qualquer área da SAM BR devem ser comunicados ao CISO do Banco Santander Brasil através da caixa jurídica Resposta a Incidentes de Segurança Cibernética Santander csirtbr@santander.com.br com cópia para o CISO da SAM BR para a caixa ASSET TECNOLOGIA assettecnologia@santanderam.com.

Os eventos originados através das ferramentas de monitoração de segurança (SOC) do Grupo Santander seguem diretrizes específicas que descreve as tarefas necessárias em cada cenário de alerta. Detalhes constam no ANEXO - Cyber Security: Tipos de Cyber Incidentes e Responsabilidades Envolvidas, elaborado pelo Banco Santander Brasil.
Provedores e fornecedores que armazenam e processam dados, contratados pela SAM BR, devem reportar os incidentes cibernéticos através do canal csirtbr@santander.com.br, com cópia para o CISO da SAM BR para a caixa ASSET TECNOLOGIA assettecnologia@santanderam.com, e seguir as diretivas descritas na política de Cyber Security - Gestão de Incidentes de Origem Cibernética.

8.3. Prevenção a Incidentes Cibernéticos

Threat Intelligence: Permite que os CISOs da SAM BR e do Banco Santander obtenham informações referentes à possíveis riscos cibernéticos, ameaças, fraudes e incidentes de segurança cibernética às instituições financeiras gerando planos de ação preventivos a partir destas informações.

8.4. Cenários de Incidentes Cibernéticos na Gestão de Continuidade de Negócios

O CISO deve comunicar a função de Gestão de Continuidade de Negócios (GCN) caso seja necessário realizar a ativação dos processos abaixo:

Planos de Continuidade de Negócios: A comunicação deve ser realizada em cenários que ofereçam impacto significativo e risco grave para as áreas de negócios da organização (P0, P1 ou P2).

Plano de Recuperação de Desastre (PRD): A comunicação deve ser realizada em cenários particularmente sensíveis que ofereçam impacto à infraestrutura tecnológica da organização e impactos as áreas de negócios (P0, P1 e P2).

Modelo de Gestão de Situações Especiais (MGSE): A comunicação deve ser realizada em cenários que ofereçam alto risco às atividades ou que possa acarretar em uma deterioração grave na situação financeira da Organização ou do Grupo, causando impactos, reputacionais, financeiros ou operacionais (P0, P1 e casos específicos P2). Detalhes constam no ANEXO - Cyber Security: Modelo de Gestão de Situações Especiais (MGSE) elaborado pelo Banco Santander Brasil.

Chief Information Security Officer (CISO): É responsável por comunicar aos demais órgãos reguladores (incluso a rede SWIFT, se aplicável) os incidentes cibernéticos ocorridos classificados como P0, P1 e P2 conforme os critérios de classificação e escalonamento de incidentes cibernéticos. Para tanto deverá seguir o modelo de "relatório" de incidentes para os casos aplicáveis. Detalhes constam no ANEXO - Cyber Security: Modelo de comunicação a demais órgãos reguladores elaborado pelo Banco Santander Brasil.

9. VIOLAÇÃO

Os princípios de Segurança da Informação e Segurança Cibernética estabelecidos nesta política possuem total aderência da Alta Administração da Organização e devem ser observados por todos na execução de suas funções.

As violações de segurança devem ser informadas ao gestor imediato e, simultaneamente, à área de Segurança da Informação da SAM BR, que deverá comunicar o CISO do Banco Santander Brasil. Toda violação ou desvio às diretrizes desta política e de outras derivadas da mesma, é investigado para determinação das medidas necessárias e sujeita funcionários e estagiários a ações disciplinares e trabalhistas e, aos prestadores de serviços e parceiros de negócios, inclui-se a rescisão de contratos e penas de responsabilidade civil e criminal na máxima extensão que a lei permitir.

O não cumprimento de algum ponto desta política, intencional ou não, pode levar o funcionário, o estagiário ou o prestador de serviço a sanções disciplinares ou legais, dependendo do caso.

10. VIGÊNCIA E REVISÕES

O presente documento entra em vigor em 08/04/2019 e será revisado no período máximo de um (01) ano ou havendo necessidade anterior, o que for menor, para que o documento permaneça sempre atualizado.

Esta Política foi aprovada por comitê virtual em 05/04/2019.

CONTROLE DE ALTERAÇÕES	
Histórico de Publicações	**Alterações**
08/04/2019	Publicação Inicial
06/05/2019	Revisão no item Origem e Registro dos Alertas

Política de Segurança Cibernética

Código: 13.02

Área	Telefone	E-mail
Tecnologia	(11) 4130-9275	assettecnologia@santanderam.com

Diretoria Responsável: Asset Management

Área Responsável: ITOP - Tecnologia