Política de Segurança da Informação e Segurança Cibernética para Fornecedores

Sumário

1. Objetivo

O objetivo desta política é estabelecer as principais diretrizes e controles de Segurança da Informação e Segurança Cibernética a serem implementados por fornecedores das sociedades controladas direta ou indiretamente, coligadas ou sob controle comum do Banco Santander (Brasil) S.A. “Grupo Santander Brasil”.

É importante observar que, o estabelecimento de diretrizes e controles na relação com os fornecedores do Grupo Santander Brasil, não se limita a esta política, podendo ser definidos novos itens e a revisão destes ao longo de toda a relação contratual.

2. Abrangência

Esta política aplica-se a todos os fornecedores do Grupo Santander Brasil.

3. Diretrizes

Todo fornecedor deve ter o conhecimento desta política e suas diretrizes, assegurando a confidencialidade, integridade e disponibilidade das informações, por meio da implantação e manutenção dos seguintes controles e princípios:

3.1. Gestão de Políticas

a) Assegurar a confidencialidade, integridade e disponibilidade das informações, por meio da definição de políticas, padrões, procedimentos e controles tecnológicos.

3.2. Segurança em Recursos Humanos

a) Realizar programas de conscientização e treinamento, assegurando que todos os seus colaboradores absorvam e se engajem com os princípios e a cultura de Segurança da Informação do Grupo Santander Brasil;

b) Garantir a aderência da instituição, seus colaboradores e prestadores de serviços à referida política e as demais derivadas da mesma;

3.3. Gestão de Ativos

a) Definir categorias para efeitos de classificação da informação e proteção através de controles e diretrizes adequados a cada categoria. O Santander adota cinco categorias:

- Público;
- Interno;
- Confidencial;
- Confidencial restrito;
- Secreto.

b) Assegurar que sejam estabelecidos padrões de configuração para softwares e equipamentos a serem disponibilizados para o uso de funcionários, prestadores de serviço e estagiários.

3.4. Gestão de Acessos

a) Assegurar que toda a informação de propriedade do Grupo Santander Brasil independentemente da forma apresentada seja protegida contra acessos indevidos, modificação, destruição não autorizada ou outros incidentes relevantes;

b) Assegurar a adoção de um processo de gestão de acesso visando controles e o registro da solicitação, autorização, concessão, manutenção e revogação de acesso;

c) Assegurar a adoção de mecanismos que visem o acesso e o uso das informações de propriedade do Grupo Santander Brasil apenas para as finalidades previamente acordadas contratualmente e por pessoas devidamente autorizadas pelo responsável pela informação, sempre através do perfil por função correspondente às suas atividades e acessos, garantindo os conceitos de mínimo privilégio de acesso e de segregação de função;

d) Assegurar que a autenticação do usuário envolva padrões correspondentes aos praticados pelo Grupo Santander Brasil quanto à complexidade, disponibilidade e uso de senha, uso de múltiplo fator de autenticação, acesso remoto através de VPN e outros controles a serem considerados a depender da criticidade do acesso;

e) Assegurar que todo funcionário, estagiário ou prestador de serviços possua apenas um identificador (login) de acesso à informação.

3.5. Segurança Física e do Ambiente

a) Assegurar a adoção de práticas orientadas aos funcionários, prestadores de serviço e estagiários para que não deixem informações à mostra e as descartem sempre que necessário, conforme sua categoria de classificação;

b) Assegurar a segregação física de áreas que atendem o Grupo Santander Brasil, quando em ambientes compartilhados com outras áreas e/ou empresas.

3.6. Segurança nas Operações

a) Assegurar a implantação de procedimentos e controles tecnológicos que previnam ações de intrusão e a exploração de vulnerabilidades;

b) Assegurar a adoção de medidas preventivas contra o vazamento e violação de dados;

c) Assegurar a adoção de controles para prevenir que vírus e outros tipos de softwares maliciosos entrem e se espalhem nos sistemas de informação por meio de arquivos e softwares não homologados cuja instalação e uso são proibidos;

d) Assegurar a adoção de procedimentos específicos para garantir a recuperação de dados e informações quando necessário;

e) Assegurar a adoção de controles e políticas que previnam o vazamento de informações estabelecendo boas práticas para uso de correio eletrônico, acesso à internet, acesso remoto, uso de telefones móveis, comportamento de toda a Equipe de Trabalho das empresas contratadas para prestarem serviços e/ou fornecerem produtos ao Grupo Santander Brasil, seja em locais públicos e na troca de informações com as empresas do Grupo Santander Brasil e/ou demais fornecedores desses.

3.7. Aquisição, Desenvolvimento e Manutenção de Sistemas

a) Garantir que os sistemas fornecidos por qualquer das empresas do Grupo Santander Brasil ao fornecedor, sejam utilizados somente para a execução das atividades inerentes ao objeto de contrato, assegurando que se mantenham íntegros e não façam parte de escopos de testes e análises ou sejam modificados ou estudados ou ainda, copiados, zelando pelos direitos de propriedade intelectual do titular do sistema;

b) Assegurar que sejam adotadas práticas de desenvolvimento seguro em sistemas de propriedade do fornecedor, bem como na prestação de serviços de desenvolvimento;

c) Garantir que, para fornecedores de desenvolvimento de software, o código fonte seja fornecido à empresa Contratante do Grupo Santander Brasil.

3.8. Relacionamento na Cadeia de Suprimento

a) Devem ser adotadas todas as medidas necessárias para assegurar a aderência dos fornecedores a todas as cláusulas contratuais, políticas e outras diretrizes estabelecidas ao longo de toda relação contratual firmada com quaisquer das empresas do Grupo Santander Brasil.

3.9. Gestão de Incidentes de Segurança da Informação

a) Garantir a adoção de mecanismos para prevenção de ameaças de origem cibernética. Todo e qualquer incidente de segurança cibernética, passa por uma análise e é classificado de acordo com o impacto causado pelo incidente, que pode ser crítico ou baixo de acordo com a classificação vigente;

b) Garantir que os incidentes de origem cibernética sejam direcionados à equipe de CSIRT do Banco Santander (Brasil) S.A., através da caixa csirtbr@santander.com.br para o devido registro e acompanhamento da resolução do mesmo.

3.10. Aspectos da segurança da informação na gestão da continuidade do negócio

a) Assegurar a implantação de um programa de GCN (Gestão de Continuidade de Negócios) que tenha por objetivo avaliar a necessidade do desenvolvimento e

implantação do PCN (Plano de Continuidade de Negócios), identificando procedimentos e infraestrutura alternativa para proteger as pessoas, a reputação, os valores e os compromissos com os públicos relacionados;

b) Garantir a implantação, manutenção e execução de testes dos mecanismos de acionamento dos planos de continuidade de negócios em caso de desastres, tanto de origem cibernética como operacional;

c) Assegurar a adoção de um programa de Gestão de Crises através de uma estrutura de acionamento e governança caso ocorra uma situação de excepcionalidade, diferente da esperada e que possa comprometer o desenvolvimento das atividades ou acarretar uma deterioração grave na situação financeira da entidade ou do grupo, por conjeturar um afastamento significativo do apetite ao risco e dos limites definidos.

3.11. Auditoria e Gestão de Riscos

a) Assegurar a disponibilidade para o atendimento a auditorias e processos de análise de riscos, por parte de quaisquer das empresas do Grupo Santander Brasil, ou empresa por ela indicada (incluindo, se for o caso, o próprio Banco Santander (Brasil) S.A.), garantindo a aderência às recomendações e implementações necessárias conforme identificação e solicitação da empresa contratante do Grupo Santander Brasil, ou do próprio Banco Santander (Brasil) S.A., em qualquer auditoria e processo de análise de riscos, dentro dos prazos previamente determinados, inclusive contratualmente.

4. Aderência à Política

Caso seja identificada uma conduta não aderente à referida política, ou o seu descumprimento, a empresa contratante do Grupo Santander Brasil, ou o próprio Banco Santander (Brasil) S.A., caso a contratante assim determinar, tomará as medidas legais, tecnológicas ou disciplinares necessárias de forma a manter a aderência a mesma.