Santander
FINANCIAMENTOS

REF.: POLÍTICA DE SEGURANÇA DA INFORMAÇÃO PARA CORRESPONDENTE BANCÁRIO DO SANTANDER.

1. SEGURANÇA DA INFORMAÇÃO

A informação é um dos principais patrimônios do mundo dos negócios. 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.

Quando não gerenciados adequadamente, esses riscos e ameaças podem causar consideráveis danos ao Santander e prejudicar nosso crescimento e vantagem competitiva. Atentos a isso, publicamos a Política de Segurança da Informação, o alicerce dos esforços de proteção à informação do Santander.

Segurança da Informação são esforços contínuos para a proteção dos ativos de informação, auxiliando o Santander a cumprir sua missão. Para tanto, visa atingir os seguintes 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 a todas as pessoas autorizadas a tratá-las.

2. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

2.1. Proteção da Informação

A informação é um importante ativo para a operação das atividades comerciais e para manter a vantagem competitiva no mercado. Tal como os ativos do Santander, a informação deve ser adequadamente manuseada e protegida.

A informação pode estar presente em diversas formas, tais como: sistemas de informação, diretórios de rede, bancos de dados, mídia impressa, magnética ou ótica, dispositivos eletrônicos, equipamentos portáteis, microfilmes e até mesmo por meio da comunicação oral.

Toda informação relacionada às operações do Santander, gerada ou desenvolvida nas dependências do Santander ou do Correspondente, durante a execução das atividades de prestador de serviços de correspondente no país para o Santander, constitui ativo desta instituição financeira, essencial à condução de negócios, e em última análise, à sua existência.

Independentemente da forma apresentada ou do meio pelo qual é compartilhada ou armazenada, a informação deve ser utilizada unicamente para a finalidade para a qual foi autorizada.

A modificação, divulgação e destruição não autorizadas e oriundas de erros, fraudes, vandalismo, espionagem ou sabotagem causam danos aos negócios do Santander.

É diretriz que toda informação de propriedade do Santander seja protegida de riscos e ameaças que possam comprometer a confidencialidade, integridade ou disponibilidade destas.

2.2. Responsabilidades

É missão e responsabilidade de cada Correspondente, seja por meio de seu funcionário, estagiário, prestador de serviços, parceiro ou visitante, observar e seguir as políticas, padrões, procedimentos e orientações estabelecidas para o cumprimento

da presente Política de Segurança da Informação. É imprescindível que cada pessoa compreenda o papel da segurança da informação em suas atividades diárias.

Todas as atividades executadas pelo Correspondente, por meio de seus funcionários, estagiários e demais colaboradores, devem observar a legislação vigente e a normatização de órgãos e entidades reguladoras, com relação à segurança da informação.

Para auxiliar a todos os colaboradores nessa missão, o Santander criou a área de Segurança da Informação, que administra as disciplinas de conhecimento que dão suporte a essa ciência. A Superintendência de Segurança da Informação é responsável por editar as políticas e padrões que apóiam a todos na proteção dos ativos de informação, e está preparada para auxiliar na resolução de problemas relacionados ao tema. A Central de Atendimento do Correspondente/Revendedor está apta a orientar e tratar as questões relacionadas ao tema.

2.3. Informações Confidenciais

São consideradas informações confidenciais, para os fins desta Política, quaisquer informações das partes consideradas não disponível ao público ou reservadas, dados, especificações técnicas, desenhos, manuais, esboços, modelos, amostras, materiais promocionais, projetos, estudos, documentos e outros papéis de qualquer natureza, tangíveis ou em formato eletrônico, arquivos em qualquer meio, programas e documentação de computador, comunicações por escrito, verbalmente ou de outra forma reveladas pelo Santander e/ou obtidas pelo Correspondente em decorrência da execução do contrato de prestação de serviços de correspondentes no país.

São responsáveis pela observância desta Política os diretores, empregados, agentes e consultores (incluindo advogados, auditores e consultores financeiros) do Correspondente.

O Correspondente que receber as informações confidenciais deverá mantê-las e resguardá-las em caráter sigiloso, bem como limitar seu acesso, controlar quaisquer cópias de documentos, dados e reproduções que porventura sejam extraídas da mesma. Nenhuma das informações confidenciais podem ser repassadas para terceiros sem consentimento por escrito do Santander. Qualquer revelação das informações confidenciais deverá estar de acordo com os termos e condições estabelecidos pelo Santander. As informações confidenciais somente poderão ser utilizadas para fins de execução das atividades de correspondente no país.

O Correspondente deverá resguardar as informações confidenciais de forma estrita, e jamais poderá revelá-las a não ser para os seus representantes legais. A parte que receber as informações será responsável por qualquer não cumprimento desta Política porventura cometido pelos seus representantes legais.

O Correspondente deverá informar prontamente ao Santander sobre qualquer uso ou revelação indevida da informação ou qualquer outra forma que caracterize o descumprimento desta Política.

Excetuam-se da obrigação de manutenção de confidencialidade disposta nesta Política: (i) o atendimento a quaisquer determinações decorrentes de lei ou emanadas do Poder Judiciário ou Legislativo, tribunal arbitrais e de órgãos públicos administrativos; (ii) a divulgação das informações confidenciais aos agentes, representantes (incluindo, mas não se limitando, a advogados, auditores e consultores financeiros) e empregados das partes; e, (iii) as informações confidenciais que forem divulgadas após o consentimento, por escrito, do Santander.

Se a qualquer uma das partes ou seus representantes legais, que detém as informações confidenciais, for solicitado ou requerido, oralmente ou por escrito, solicitações de informações de documentos, mandados de investigações civis ou qualquer outro pedido similar, para revelar tais informações confidenciais, deverá notificar prontamente a outra parte para que esta tenha tempo hábil para verificação, inclusive, se for o caso, aplicar as ressalvas contidas nos termos desta Política.

As cláusulas de ciência, responsabilidade e confidencialidade quanto à política e diretrizes de segurança da informação visam alertar e responsabilizar o Correspondente de que o acesso e o manuseio de informação devem se restringir ao exercício da função ou processo que requer essa informação, sendo proibido o uso para qualquer outro propósito distinto do designado.

2.4. Violação da Política, Normas e Procedimentos de Segurança da Informação

As violações de segurança devem ser informadas à área de Segurança da Informação, por meio da Central de Atendimento do Revendedor. Toda violação ou desvio é investigado para a determinação das medidas necessárias, visando à correção da falha ou reestruturação de processos.

Exemplos que podem ocasionar sanções:

- uso ilegal de software;
- introdução (intencional ou não) de vírus de informática;
- tentativas de acesso não autorizado a dados e sistemas;
- compartilhamento de informações sensíveis do negócio;
- divulgação de informações de clientes e das operações contratadas;

Os princípios de segurança estabelecidos na presente política possuem total aderência da administração do Santander e devem ser observados por todos na execução de suas funções. A não-conformidade com as diretrizes desta política e a violação de normas derivadas da mesma sujeita os Correspondentes às penas de responsabilidade civil e criminal na máxima extensão que a lei permitir e a rescisão de contratos.

Em caso de dúvidas quantos aos princípios e responsabilidades descritas nesta norma, o Correspondente deve entrar em contato com a Central de Atendimento do Correspondente/Revendedor.

3. PRINCÍPIOS E DIRETIVAS DA POLÍTICA DE SEG. INFORMAÇÃO

3.1. Classificação da Informação

As informações e os sistemas de informação, diretórios de rede e bancos de dados são classificados como estritamente confidenciais.

As informações, seja no período de geração, guarda, uso, transferência e destruição devem ser tratadas em conformidade com cada etapa do ciclo.

As informações confidenciais necessitam de sigilo absoluto e devem ser protegidas pelo Correspondente de alterações não autorizadas e estarem disponíveis apenas às pessoas pertinentes e autorizadas a trabalhá-las, sempre que necessário. Cabem ao Correspondente todos os esforços necessários de segurança para protegê-las.

Falhas no sigilo da informação, integridade ou disponibilidade deste tipo de informação trazem grandes prejuízos à Organização, expressos em perdas financeiras diretas, perdas de competitividade e produtividade ou imagem do Santander, podendo levar à extinção das operações ou prejuízos graves ao crescimento.

São exemplos de informações confidenciais:

- Informações de clientes que devem ser protegidas por obrigatoriedade legal, incluindo dados cadastrais (CPF, RG etc.), situação financeira e movimentação bancária;
- Informações sobre produtos e serviços que revelem vantagens competitivas do Santander frente ao mercado;
- Todo o material estratégico do Santander (material impresso, armazenado em sistemas, em mensagens eletrônicas ou mesmo na forma de conhecimento de negócio da pessoa);
- Quaisquer informações do Santander, que não devem ser divulgadas ao meio externo antes da publicação pelas áreas competentes;
- Todos os tipos de senhas a sistemas, redes, estações de trabalho e outras informações utilizadas na autenticação de identidades. Estas informações são também pessoais e intransferíveis.

3.2. Acesso a Sistemas e Recursos de Rede

O Correspondente é totalmente responsável pela correta posse e utilização de suas senhas e autorizações de acesso a sistemas, assim como pelas ações decorrentes da utilização destes poderes.

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 explicitamente autorizadas e de acordo com a necessidade para o cumprimento de suas funções. Acessos desnecessários ou com poder excessivo devem ser imediatamente retirados. A concessão de acesso às informações e sistemas deve ser autorizada com base na regra de mínimo acesso necessário para o desempenho da função.

Periodicamente, os acessos concedidos devem ser revistos pelo Correspondente.

3.3. Utilização dos Recursos de Informação

Apenas os equipamentos e software disponibilizados e/ou homologados pelo Santander podem ser instalados e conectados à rede do Santander.

Todos os ativos de informação devem ser devidamente guardados, especialmente documentos em papel ou mídias removíveis. Documentos não devem ser abandonados após a sua cópia, impressão ou utilização.

3.4. Autenticação e Senha

O Correspondente é responsável por todos os atos executados com seu identificador (login / sigla), que é único e acompanhado de senha exclusiva para identificação/autenticação individual no acesso à informação e aos recursos de tecnologia.

Os Correspondentes devem:

- Manter a confidencialidade, memorizar e não registrar a senha em lugar algum. Ou seja, não contá-la a ninguém e não anotá-la em papel;
- Alterar a senha sempre que existir qualquer suspeita do comprometimento dela;
- Selecionar senhas de qualidade, que sejam de difícil adivinhação;
- Impedir o uso do seu equipamento por outras pessoas, enquanto este estiver conectado/ "logado" com a sua identificação;
- Bloquear sempre o equipamento ao se ausentar (Ctrl + Alt + Del).

3.5. Direito de Acesso (Autorização)

O Correspondente é o responsável pela utilização e eventuais usos inadequados dos direitos de acesso que são atribuídos aos seus funcionários, estagiários, prestadores de serviços, parceiros e visitantes, sendo intransferíveis.

A solicitação de acesso à informação deve decorrer da necessidade funcional do Correspondente. .

3.6. Direitos de Propriedade

Todo produto resultante do trabalho dos Correspondentes (coleta de dados e documentos, sistema, metodologia, dentre outros) é propriedade do Santander.Em caso de extinção ou rescisão do contrato de prestação de serviços de correspondente no país, por qualquer motivo, deverá o Correspondente devolver todas as informações confidenciais geradas e manuseadas em decorrência da prestação dos serviços ao Santander, ou emitir declaração de que as destruiu.

3.7. Equipamentos particulares/privados

Equipamentos particulares/privados, como computadores ou qualquer dispositivo portátil que possa armazenar e/ou processar dados, não devem ser usados para armazenar ou processar informações relacionadas com o negócio, nem devem ser conectados às redes da Organização.

3.8. Mesa Limpa

Nenhuma informação confidencial deve ser deixada à vista, seja em papel ou em quaisquer dispositivos, eletrônicos ou não.

Ao usar uma impressora coletiva, recolher o documento impresso imediatamente.

3.9. Conversas em Locais Públicos e registro de informações

Não discutir ou comentar assuntos confidenciais em locais públicos ou por meio de mensagens de texto, exceto quando encaminhadas ao Santander.

3.10. Leis e Regulamentos

É de responsabilidade do Correspondente conhecer a legislação e cumprir os requisitos legais, normas e padrões locais vigentes.

Santander Financiamentos
Banco Santander (Brasil) S.A.