POLÍTICA DE

SEGURANÇA CIBERNÉTICA

JULHO 2025

Histórico de Aprovações

Versão	Data da Alteração	Revisões Feitas	Responsável pela Manutenção
Criação	Maio 2019	N/A	Paulo Souza
Última Atualização	Maio 2020	Atualização	Wilma Cabral
Última Atualização	Maio 2021	Atualização do formato e conteúdo	Marcelo Hiroshi Jarbas Marcato Larissa Horta
Última Atualização	Setembro 2021	Itens 6.4; 7.10; 7.11; 7.12; 7.15; 7.16; 9.3; 10; 11	Wilma Cabral Marcelo Hiroshi Jarbas Marcato Larissa Horta
Última Atualização	Março 2022	Inclusão do item 7.16 Exclusão do item 9.3.2	Marcelo Hiroshi Larissa Horta
Última Atualização	Agosto 2022	Atualização e Inclusão de conteúdo, itens:2; 6; 6.2; 7.11; 7.14; 7.15 e 15	Marcelo Hiroshi Larissa Horta
Última Atualização	Abril 2023	Inclusão da assinatura do Diretor da Corretora	Larissa Horta
Atualização	Março 2024	Atualização da Política	Marcelo Hiroshi Larissa Horta
Revisão	Julho 2025	Revisão da Política	Marcelo Hiroshi Larissa Horta

ÍNDICE

1 INTRODUÇÃO 4
2 OBJETIVO 5
3 ESCOPO 5
4 PRINCÍPIOS 6
5 APLICABILIDADE 6
6 RESPONSABILIDADES 7
7 PROCESSOS E CONTROLES DE SEGURANÇA CIBERNÉTICA 7
8 PRESTADORES DE SERVIÇOS 16
9 CONTRATAÇÃO DE SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E COMPUTAÇÃO EM NUVEM 16
10 GOVERNANÇA 18
11 COMPLIANCE 19
12 REVISÃO E APROVAÇÃO DA POLÍTICA 19
13 POLÍTICAS E DOCUMENTOS RELACIONADOS 19
14 LEIS LOCAIS 20
15 ONDE BUSCAR AJUDA 20
16 ANEXO 20

1 INTRODUÇÃO

A Política de Segurança da Cibernética ("Política") expressa o comprometimento do Scotiabank Brasil S.A. Banco Múltiplo ("Banco") e da Scotiabank Brasil S.A. Corretora de Títulos e Valores Mobiliários ("Corretora"), definidos como Grupo Scotiabank Brasil ("Grupo"), em gerenciar os riscos relacionados à segurança cibernética de forma eficiente e efetiva, sob coordenação global e em aderência às leis aplicáveis locais.

A Política descreve as diretrizes adotadas pela área de Tecnologia da Informação com relação as normas e regulamentos locais e Políticas globais do *Bank of Nova Scotia* (BNS), seguindo os princípios aplicáveis à gestão de segurança cibernética no Grupo Scotiabank Brasil. Este documento é parte integral das Políticas e processos que em conjunto demonstram a maneira com a qual o Grupo conduz de forma efetiva a governança dos ativos do Banco e Corretora.

Segurança da Informação vs. Segurança Cibernética

Os domínios da informação e da segurança cibernética incluem, mas não estão limitados a: estruturas, políticas, padrões, conscientização, gerenciamento de ativos, operações de segurança, avaliações de ameaças e riscos, avaliações de vulnerabilidade, continuidade de negócios, backup e recuperação de desastres, segurança física, resposta a incidentes, resiliência operacional e conformidade.

Segurança da Informação

- Protege informações em qualquer formato (digital, eletrônico, físico)
- Além da Cibersegurança, protege a confidencialidade, integridade, disponibilidade e continuidade dos dados
- Lida com uma variedade de ameaças para garantir que controles, processos e procedimentos de segurança adequados estejam em vigor

Cibersegurança

- É um subconjunto da Segurança da Informação
- Protege informações em formato digital ou eletrônico
- Protege os dados no ciberespaço contra acesso digital não autorizado
- Lida com ameaças cibernéticas (por exemplo, phishing, malware etc.)

2 OBJETIVO

Esta Política tem o objetivo de estabelecer diretrizes que permitem o Grupo Scotiabank Brasil preservar e proteger as informações de seus clientes, colaboradores, prestadores de serviços, partes interessadas e da própria instituição, contra ameaças e riscos (internos e externos) relacionados à segurança cibernética, bem como implementar controles e procedimentos que visam prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético. Este documento deve ser lido em conjunto com a Política de Segurança da Informação e Plano de Ação e de Resposta a Incidentes.

O Grupo Scotiabank Brasil deve implementar e manter esta Política formulada com base em princípios e diretrizes que busquem assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados.

3 ESCOPO

Esta Política define as principais salvaguardas para informações registradas, processadas, recuperadas, compartilhadas, transmitidas ou armazenadas em formato eletrônico, sistêmico e/ou por infraestrutura tecnológica (servidores e Bando de Dados). Neste contexto, a informação inclui ficheiro de dados estruturados ou não estruturados, ficheiros de áudio ou vídeo, correio eletrônico, correio de voz ou outros tipos de mensagens, cópias de segurança ou arquivadas do original em mídia óptica, magnética ou qualquer outra.

A informação deve ser protegida durante todo o seu ciclo de vida, incluindo a sua geração, captura, retenção, processamento, armazenamento, transmissão, utilização e destruição final. As informações iniciadas pelo cliente devem ser protegidas desde o ponto de aquisição pelo Grupo Scotiabank até o ponto de entrega ao cliente.

Se uma unidade de negócios autorizar um acordo pelo qual um terceiro gera, reúne, processa, armazena ou usa, transmite ou descarta informações em seu nome, então essa unidade de negócios é responsável pela supervisão das práticas de segurança cibernética do terceiro para garantir que atendam aos requisitos desta Política e quaisquer regulamentos aplicáveis.

A Política aborda os riscos cibernéticos atuais à medida que evoluem e contribui para manter

esses riscos em um nível aceitável. O risco de segurança cibernética é um domínio de gerenciamento de riscos de Tecnologia da Informação que se concentra na identificação, proteção, detecção, resposta e recuperação de um ataque cibernético, minimizando danos e impacto para o Grupo Scotiabank Brasil.

4 PRINCÍPIOS

O Grupo tem o compromisso de garantir a segurança e tratamento adequado das informações de seus clientes, colaboradores, prestadores de serviços e do próprio Scotiabank Brasil. Para tanto, nossas atividades se baseiam nos seguintes princípios:

- **Confidencialidade:** garantia de que somente pessoas autorizadas terão acesso às informações e apenas quando houver necessidade;
- **Integridade:** garantia de que as informações permanecerão exatas e completas e não serão modificadas indevidamente;
- **Disponibilidade:** garantia de que a informação estará disponível às pessoas autorizadas sempre que for necessário.
- **Autenticidade:** garantia de que as informações sejam autenticas, isto é, de fontes confiáveis.

5 APLICABILIDADE

Esta Política destina-se a todos os colaboradores, fornecedores, prestadores de serviços e clientes do Grupo Scotiabank Brasil. Para os fins do disposto nesta Política o termo "Colaboradores" abrange todos os empregados, menores aprendizes, estagiários e os membros da alta administração do Grupo.

Os colaboradores envolvidos na gestão de fornecedores e prestadores de serviços terceirizados são responsáveis por garantir que todos os contratos e acordos de terceiros imponham obrigações suficientes aos fornecedores e prestadores de serviços para apoiar os objetivos de segurança cibernética do Grupo Scotiabank Brasil, conforme definidos nesta Política, bem como pela Política de Segurança da Informação. Tentativas deliberadas ou persistentes de violar ou violações reais desta Política levarão a medidas disciplinares de acordo com o Código de

Conduta.

6 RESPONSABILIDADES

Todos os colaboradores têm a responsabilidade de proteger as informações, sejam elas proprietárias ou confiadas ao Grupo Scotiabank Brasil por clientes, fornecedores ou outros com quem o Grupo faz negócios, cumprindo esta Política e quaisquer Políticas, Normas ou Procedimentos específicos pertinentes à sua função, sempre observando os seguintes princípios:

- Cumprimento da Lei e Requisitos Regulatórios;
- Responsabilidade;
- Uso da Tecnologia;
- Proteção de Dados;
- Privilégio de Acesso e;
- Segregação de Funções;

7 PROCESSOS E CONTROLES DE SEGURANÇA CIBERNÉTICA

A fim de assegurar que todas as diretrizes descritas nesta Política sejam cumpridas e que os princípios de segurança cibernética sejam devidamente seguidos, o Grupo Scotiabank Brasil adota políticas e procedimentos conforme os tópicos elencados a seguir.

7.1 Proteção da Informação

Toda informação gerada ou desenvolvida para ou pelo Grupo Scotiabank Brasil constitui como um ativo e propriedade intelectual desta, essencial à condução dos 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 do Grupo seja protegida de forma a não comprometer a sua confidencialidade, integridade ou disponibilidade.

7.2 Autenticação

O Grupo Scotiabank Brasil adota mecanismos para garantir que o acesso às informações e ambientes tecnológicos seja permitido apenas aos indivíduos autorizados, levando em consideração o princípio do menor privilégio, a segregação de funções e a classificação da informação.

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

7.3 Criptografia

As senhas utilizadas no acesso à informação e aos recursos de tecnologia possuem criptografia adequada, a fim de se garantir proteção da informação.

7.4 Controle de Acesso

O Grupo Scotiabank Brasil adota controles de acesso em todo o ambiente tecnológico, assim como em sua infraestrutura para evitar que indivíduos não autorizados tenham acesso aos ambientes segregados e aos sistemas internos. Somente colaboradores e prestadores de serviços autorizados possuem acesso ao ambiente do Grupo.

Desta forma, são implementados mecanismos para a autenticação de usuários, manutenção de segregação de funções e rastreabilidade de acesso, de forma a garantir procedimentos internos adequados e consistentes.

7.5 Acesso a Sistemas, Recursos de Rede e Rastreabilidade

O acesso e o uso dos sistemas de informação, diretórios de rede, bancos de dados e demais recursos devem ser restritos a pessoas autorizadas pelo gestor e *Owner* (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 local e

mecanismos de prevenção a vazamentos de dados.

7.6 Segurança Física do Ambiente

O Grupo Scotiabank Brasil implementa controles de acesso aos colaboradores, prestadores de serviços, fornecedores, provedores e parceiros aos locais físicos na instituição. Os equipamentos e instalações de processamento de informação crítica ou sensível são mantidos em áreas seguras, com níveis de controle de acesso apropriados, incluindo proteção contra ameaças físicas e ambientais.

7.7 Segmentação de Ambiente

O Grupo Scotiabank Brasil adota mecanismos para a segmentação de rede, sendo ambientes segregados para rede de usuários, rede de servidores de Produção, Homologação, Desenvolvimento e *Disaster Recovery* (DR). O ambiente também possui ferramentas de Firewall, DLP *(Data Loss Prevention)* e antivírus para proteger seus dados de ataques cibernéticos e determinar que todos os computadores conectados à rede corporativa não estejam acessíveis diretamente pela Internet.

7.8 Prevenção Contra Vírus, Arquivos e Softwares Maliciosos

O Grupo possui mecanismos tais como firewall, proxy e antivírus, para prevenir que vírus e outros tipos de software e condutas maliciosas (ex. phishing, spam etc.) se propaguem nos computadores, sistemas e servidores internos ou exponham a instituição a vulnerabilidades.

7.9 Backup

O Grupo Scotiabank Brasil possui política e procedimentos específicos para garantir as rotinas de backup e restauração de dados, para assegurar a disponibilidade das informações para o pleno funcionamento das atividades do Grupo.

A Política de Backup, Retenção & Rotação aborda com maiores detalhes os processos descritos acima.

7.10 Testes Periódicos de Segurança

Os testes de segurança são conduzidos pelo *Bank of Nova Scotia ("BNS")*, de forma periódica a fim de minimizar incidentes de segurança da informação e segurança cibernética que possam causar a interrupção nos negócios. Os resultados dos testes mencionados, em sua maioria, podem ser solicitados para as áreas responsáveis.

Os principais testes são:

- Análise de Vulnerabilidade (Vulnerability Assessment);
- Teste de Penetração (Penetration Testing): gerenciado pela Equipe Vermelha de Segurança Cibernética da matriz (CSRT);
- Programa de Conscientização sobre Phishing: Teste de conformidade e aderência do assunto.

A Política de Segurança da Informação aborda com maiores detalhes os processos descritos acima.

7.11 Continuidade de Negócios

O Grupo Scotiabank Brasil possui uma Política em vigor o qual descreve os processos necessários para evitar ou mitigar os impactos decorrentes de um evento que cause interrupção nos negócios do Grupo.

A Política visa fornecer orientações de segurança adequadas para que os sistemas que suportam os processos de negócios críticos sejam recuperados dentro do tempo aceitável de interrupção e o negócio tenha continuidade.

Além disso, há uma plataforma global chamada Fusion cuja gestão é do time de *Enterprise Crisis & Business Continuity,* com supervisão local da área de Tecnologia da Informação, na qual cada área descreve seus processos de continuidade de negócios de forma tempestiva e contínua, e com a inclusão de documentos comprobatórios, conforme e necessidade de cada área, referente aos testes realizados.

São considerados alguns cenários de incidentes em se tratando de Plano de Continuidade, tais como os eventos a seguir:

- Perda total do Site Principal: ativação do site secundário e divisão dos times entre w*ork*

area (*Kyndryl*) e trabalho remoto (*WFH – Working From Home* via VPN);

- Perda parcial do Site Principal: ativação total ou parcial do site secundário e a divisão dos times se necessário entre *work area* (*Kyndryl*) e/ou trabalho remoto (*WFH – Working From Home via VPN*), se necessário;
- Situações adversas como alagamentos, greves e/ou acidentes graves na região: divisão dos times entre *work area* (*Kyndryl*) e trabalho remoto (*WFH – Working From Home* via VPN) e;
- Pandemia: os times trabalhando remotamente (*WFH – Working From Home* via VPN) e, se necessário, divisão para o *Work Area* (*Kyndryl*).

A Política de Continuidade e Procedimentos & Contingência aborda com maiores detalhes os processos descritos acima.

7.12 Classificação de Relevância de Serviços

Para o Grupo Scotiabank Brasil, serão considerados relevantes os serviços que satisfizerem as condições a seguir:

A. Essenciais para o desempenho das funções operacionais críticas:
   a. Liquidação em reais ou em moeda estrangeira.
   b. Controle de risco de mercado e exposição.
   c. Gerenciamento de caixa.

B. Desempenhados fora do território brasileiro.

C. Serviços em nuvem ou estabelecido em data center externo necessários para operação.

D. Que tratem informações pessoais e sensíveis.

E. Cumprimento de obrigações regulatórias.

As condições de exclusão abaixo também serão aplicadas para definir serviços não relevantes:

A. Serviços relevantes que possam ser prestados por terceiros, e

B. Que possam ser operacionalizados com novo prestador em até 3 meses.

7.13 Classificação dos Dados e das Informações

As informações devem ser classificadas segundo sua criticidade e sensibilidade para o negócio e seus clientes. Portanto, o Grupo Scotiabank Brasil deve adotar a seguinte classificação:

- **Informação Pública:** aquela que pode ser acessada por todos, sem restrição.
    - São exemplos de Informação Pública: dados divulgados ao mercado.
- **Informação Interna:** aquela que pode ser acessada somente por colaboradores da instituição.
    - São exemplos de Informação Interna: normas, procedimentos e formulários.
- **Informação Restrita:** aquela que pode ser acessada somente por colaboradores que precisam da informação para desempenhar suas atribuições.
    - São exemplos de Informação Restrita: contratos e documentos estratégicos da instituição.
- **Informação Confidencial:** aquela que pode ser acessada somente por colaboradores que tenham permissão de acesso ou que necessitem dela para um propósito específico.
    - São exemplos de Informação Confidencial: plano estratégico e informações de clientes.
- **Informação Sensível:** aquela que pode ser acessada somente por colaboradores que tenham permissão de acesso ou que necessitem dela para um propósito específico.
    - São exemplos de Informação Sensível: informações que permitem identificar de forma direta ou indireta uma determinada pessoa, tendo como premissa todo e qualquer dado de cliente, seja pessoa física e/ou jurídica, colaboradores e prestadores de serviço.

O responsável pela informação deve garantir que nenhum dado pessoal ou dado sensível sejam classificados como informação pública.

7.14 Registro, Resposta e Tratamento de Incidentes Relevantes de Segurança Cibernética

O Grupo Scotiabank Brasil possui processos para gerenciar os riscos relacionados a cibersegurança, sistemas, dados e seus ativos, entre outros. A instituição visa realizar o registro, análise de causa e impacto, e controle dos efeitos de incidentes, utilizando como base os seguintes processos e recursos, a fim de mitigar riscos:

- Identificação;
- Contenção,
- Erradicação; e
- Recuperação.

O Grupo possui uma Equipe de Gestão de Incidentes Local (*Local Incident Management Team*[1]), a qual tem a responsabilidade de se reunir mediante a face de crises.

Todo o incidente relacionado a segurança cibernética é analisado pela Matriz (*BNS*), e dependendo da sua criticidade, se necessário, o *LISO* é acionado localmente para tomar as medidas necessárias.

No que diz respeito à contenção, utilizamos uma ferramenta global chamada *Global Event Management System (GEMS).* Quanto à Erradicação do problema, usamos uma ferramenta de *post-mortem* chamada de *Post Incident Severity Assessment (PISA).*

A Política de Ação e de Respostas a incidentes aborda com maiores detalhes os processos descritos acima, assim como no "*IT&S Incident Management Process And Major Incident Management Process*" (*BNS*).

7.15 Monitoramento e Comunicação de Incidentes

7.15.1 FS-ISAC (Financial Services Information Sharing and Analysis Center)

O BNS é um associado da *FS-ISAC*, seguindo a recomendação do comunicado *FB-024/2019* da Febraban. O time de Segurança da Informação do Grupo é responsável pelo monitoramento, gerenciamento e compartilhamento das informações referente a cibersegurança na plataforma *FS-ISAC*.

7.15.2 ANPD (Autoridade Nacional de Proteção de Dados)

Atendendo a lei nº 13.709, de 14 de agosto de 2018 e a resolução CD/ANPD nº 15, de 24 de abril de 2024 o Grupo Scotiabank Brasil deverá comunicar à ANPD e ao titular a ocorrência do incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

[1] Para maiores informações, consultar a Política de Ações e de Resposta a Incidentes

Considera-se como risco ou dano relevante aos titulares, quando pude afetar significativamente interesses e direitos fundamentais dos titulares e, cumulativamente, envolver, pelo menos, um dos seguintes critérios:

I - Dados pessoais sensíveis;

II - Dados de crianças, de adolescentes ou de idosos;

III - Dados financeiros;

IV - Dados de autenticação em sistemas;

V - Dados protegidos por sigilo legal, judicial ou profissional; ou

VI - Dados em larga escala.

A comunicação do incidente à ANPD deverá ser realizada no prazo de três dias úteis, esse prazo será contado a partir do conhecimento de que o incidente tenha afetado os dados pessoais do titular, ressalvada a existência de prazo para comunicação previsto em legislação específica.

A comunicação deverá ocorrer por meio de formulário eletrônico disponibilizado pela ANPD e deverá conter as seguintes informações:

I - A descrição da natureza e da categoria de dados pessoais afetados;

II - O número de titulares afetados, discriminando, quando aplicável, o número de crianças, de adolescentes ou de idosos;

III - As medidas técnicas e de segurança utilizadas para a proteção dos dados pessoais, adotadas antes e após o incidente, observados os segredos comercial e industrial;

IV - Os riscos relacionados ao incidente com identificação dos possíveis impactos aos titulares;

V - Os motivos da demora, no caso de a comunicação não ter sido realizada no prazo previsto;

VI - As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente sobre os titulares;

VII - A data da ocorrência do incidente, quando possível determiná-la, e a de seu conhecimento pelo Grupo Scotiabank Brasil;

VIII - Os dados do encarregado ou de quem represente o Grupo;

IX - A identificação do controlador;

X - A identificação do operador, quando aplicável;

XI - A descrição do incidente, incluindo a causa principal, caso seja possível identificá-la; e

XII - O total de titulares cujos dados são tratados nas atividades de tratamento afetadas pelo incidente.

A comunicação do incidente de segurança deverá ser realizada pelo controlador, por meio do encarregado, acompanhada de documento comprobatório de vínculo contratual, empregatício ou funcional, ou por meio de representante constituído, acompanhada de instrumento com poderes de representação junto à ANPD.

7.15.2.1 Titular do(s) Dado(s)

A comunicação do incidente de segurança ao titular deverá ser realizada pelo Grupo Scotiabank Brasil no prazo de três dias úteis, esse prazo será contado a partir do conhecimento de que o incidente tenha afetado os dados pessoais do titular, e deverá conter as seguintes informações:

I - A descrição da natureza e da categoria de dados pessoais afetados;
II - As medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
III - Os riscos relacionados ao incidente com identificação dos possíveis impactos aos titulares;
IV - Os motivos da demora, no caso de a comunicação não ter sido feita no prazo;
V - As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente, quando cabíveis;
VI - A data do conhecimento do incidente de segurança; e
VII - O contato para obtenção de informações e, quando aplicável, os dados de contato do encarregado.

A comunicação do incidente aos titulares de dados deverá atender aos seguintes critérios:

I - Uso de linguagem simples e de fácil entendimento; e
II - Ocorrer de forma direta e individualizada[2], caso seja possível identificá-los.

7.16 Disseminação da Cultura de Segurança Cibernética

Por meio do *BNS*, o Grupo Scotiabank Brasil faz parte de um programa global e abrangente para promover a conscientização dos funcionários e terceiros com relação à evolução das ameaças à segurança cibernética por meio de treinamento e campanhas de aprendizado direcionados e

[2] Considera-se comunicação de forma direta e individualizada aquela realizada pelos meios usualmente utilizados pelo Grupo para contatar o titular, tais como telefone, e-mail, mensagem eletrônica ou carta.

regulares, tais como:

- Programa de capacitação: *e-learnings* mandatórios e periódicos (*me@scotiabank*), Portal de Treinamento (*me@scotiabank*) com uma biblioteca a qual oferece diversos cursos sobre o assunto e campanhas recorrentes sobre *Phishing*.
- Informação a clientes e usuários sobre a precaução: envio das políticas e manuais de procedimentos a todos colaboradores, terceiros e prestadores de serviços, e acesso público aos clientes (site institucional); e
- Comprometimento da alta administração quanto à segurança cibernética.

Além dos treinamentos mandatórios e compulsórios, a Política é enviada a todos os colaboradores e terceiros no momento de sua publicação, através da área de Compliance. Sendo que a mesma também fica disponível na Intranet para acesso de todos, e publicada no site institucional (https://www.br.scotiabank.com/Regulamentos_e_Politicas.html) para acesso público.

8 PRESTADORES DE SERVIÇOS

Os prestadores de serviços que armazenam e processam dados, contratados pelo Grupo Scotiabank Brasil, são avaliados e devem seguir seus papéis e responsabilidades.

Para os principais prestadores de serviços são definidos cláusulas contratuais específicas relacionadas às questões de Segurança Cibernética e LGPD.

9 CONTRATAÇÃO DE SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E COMPUTAÇÃO EM NUVEM

Toda e qualquer alteração relacionada na infraestrutura local (inclusive contratação de serviços em nuvem), devem ser autorizados por um comitê gerenciado pela Matriz, o *ARB* (Architecture Review Board), para avaliação dos Riscos.

9.1 Contrato de Prestação de Serviços

O Grupo Scotiabank Brasil deve assegurar que os contratos de prestação de serviços de

processamento, armazenamento de dados e computação em nuvem prevejam:

- A indicação dos países e da região em cada país em que os serviços serão prestados e os dados armazenados, processados e gerenciados;
- A adoção de medidas de segurança para a transmissão e armazenamento dos dados;
- A manutenção, enquanto o contrato estiver vigente, da segregação dos dados e dos controles de acesso para proteção das informações dos clientes
- Em caso de extinção do contrato, a obrigatoriedade de transferência dos dados ao novo prestador de serviços ou ao Grupo Scotiabank Brasil, bem como a exclusão dos dados pela empresa contratada substituída, após a transferência dos dados e a confirmação da integridade e da disponibilidade dos dados recebidos;
- O acesso às informações fornecidas pela empresa contratada, bem como as informações relativas às certificações e aos relatórios de auditoria especializada e informações e recursos de gestão adequados ao monitoramento dos serviços a serem prestados;
- A obrigação da empresa contratada em notificar a instituição sobre a subcontratação de serviços relevantes;
- A permissão de acesso do Bacen aos contratos e acordos firmados para a prestação de serviços, documentação e informações referentes aos serviços prestados, dados armazenados e informações sobre seus processamentos, cópias de segurança dos dados e das informações, bem como códigos de acesso aos dados e informações;
- A obrigação de a empresa contratada manter a instituição permanentemente informada sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor.

9.2 Contratação de Serviços de Computação em Nuvem no Exterior

Em caso de contratação de serviços de processamento, armazenamento de dados e de computação em nuvem no exterior, o Grupo Scotiabank Brasil deverá observar os seguintes requisitos:

- Existência de convênio para troca de informações entre o Bacen e as autoridades supervisoras dos países onde os serviços serão prestados (acordo de cooperatividade entre os países);
- Garantia que a prestação dos serviços não irá prejudicar seu funcionamento regular nem dificulte a atuação do Banco Central do Brasil;

- Definição dos países e regiões em cada país em que os serviços serão prestados e os dados armazenados, processados e gerenciados. Essa definição deverá ocorrer antes da contratação dos serviços;
- Prevenir alternativas para a continuidade dos negócios, no caso de impossibilidade de manutenção ou extinção do contrato de prestação de serviços.

Caso não haja convênio para troca de informações entre o Bacen e as autoridades supervisoras dos países em que os serviços serão prestados, a instituição deverá solicitar uma autorização do Bacen para a contratação do serviço. O prazo para solicitar autorização é de 60 dias anteriores à contratação. Caso haja alterações contratuais que impliquem em modificação das informações, o Grupo deverá solicitar autorização 60 dias antes da alteração contratual.

A instituição deve assegurar que a legislação e a regulamentação nos países em que os serviços serão prestados não restrinjam ou impeçam o acesso do Grupo Scotiabank Brasil e do Bacen aos dados e às informações.

9.3 Comunicação ao Bacen

9.3.1 Contratação de Serviços Em Nuvem

A comunicação ao Bacen deve conter as seguintes informações:

- O nome da empresa a ser contratada;
- Os serviços relevantes a serem contratados;
- No caso de contratação no exterior, indicação dos locais onde os serviços serão prestados e os dados armazenados, processados e gerenciados.

O prazo para comunicação é de 10 dias, contados a partir da contratação dos serviços. Caso haja alterações contratuais que impliquem em modificação das informações, a comunicação ao Bacen deverá ocorrer em 10 dias contados da alteração contratual.

10 GOVERNANÇA

O Comitê de Tecnologia da Informação ocorre em períodos estipulados pelo mandato e tem por objetivo discutir, desenvolver, monitorar, atualizar e aprovar investimentos, projetos e prioridades

relativos à área.

O Presidente do comitê é o CEO do Grupo Scotiabank Brasil, e como membros integrantes temos os com direito a voto e os sem direito a voto, sendo que a delegação de autoridade está devidamente formalizada.

Todos os detalhes podem ser encontrados no Mandato do Comitê de Tecnologia da Informação.

11 COMPLIANCE

Estar em conformidade com essa Política é mandatório para todas as pessoas e processos que acessam os recursos de sistemas de informação do Grupo Scotiabank Brasil. De acordo com o Código de Conduta, todos os colaboradores e prestadores de serviços são responsáveis por manter a comunicação, os processos e as informações de forma precisa, confidencial e segura.

Os colaboradores que estão diretamente envolvidos na gestão dos prestadores de serviços são responsáveis por garantir que todos os contratos tenham cláusulas contratuais em aderência com os objetivos e diretrizes desta Política.

12 REVISÃO E APROVAÇÃO DA POLÍTICA

A Política de Segurança Cibernética deverá ser revisada, atualizada e aprovada pela Diretoria Executiva do Grupo Scotiabank Brasil anualmente, ou sempre que houver qualquer alteração de processos, por demanda dos reguladores locais ou do *Bank of Nova Scotia ("BNS")*.

13 POLÍTICAS E DOCUMENTOS RELACIONADOS

Esse documento está em conformidade com os procedimentos definidos nas seguintes políticas e documentos/procedimentos globais:

- Cybersecurity Policy – BNS;
- Information Security Policy – BNS;
- Problem Management Process – BNS;
- IT&S Incident Management Process and Major Incident Management Process – BNS;

- Política de Segurança da Informação – Grupo Scotiabank Brasil;
- Política de Ação e de Resposta à Incidentes – Grupo Scotiabank Brasil;
- Política de Continuidade e Procedimentos & Contingência
- Código de Conduta – Grupo Scotiabank Brasil;
- Manual de Treinamento e Desenvolvimento – Grupo Scotiabank Brasil;
- Política de Backup, Retenção & Rotação – Grupo Scotiabank Brasil;
- Mandato Comitê de Tecnologia da Informação - Grupo Scotiabank Brasil;

14 LEIS LOCAIS

Esse documento está em conformidade com as seguintes leis locais vigentes:

- Resolução CMN Nº 4.893, de 26 de fevereiro de 2021;
- Resolução BCB n° 85 de 8/4/2021;
- Resolução CVM Nº 35, de 26 de maio de 2021;
- Lei nº 13.709, de 14 de agosto de 2018; e
- Resolução CD/ANPD nº 15, de 24 de abril de 2024.

15 ONDE BUSCAR AJUDA

Para maiores informações ou esclarecimentos com relação à essa Política, entrar em contato com a área de Segurança da Informação através do e-mail SPITSECURITY@BR.SCOTIABANK.COM

16 ANEXO

16.1 TERMOS E SIGLAS

- **Ativos:** todas as formas de criação, processamento, armazenamento, transmissão e exclusão de informações. Os Ativos podem ser documentos impressos, sistemas, softwares, banco de dados, arquivos digitais, dispositivos móveis etc.
- **Informação:** Informação refere-se à representação de fatos, que são coletados para a realização de transações comerciais. Usado de forma intercambiável com dados, o termo inclui arquivos de dados não estruturados ou estruturados, arquivos de áudio ou vídeo; correio eletrônico, correio de voz, fax ou outros tipos de mensagens, impressões em papel,

cópias de segurança ou arquivadas do original em qualquer mídia etc.

- **Sistema da Informação:** Um conjunto discreto de recursos de informação organizados para a coleta, processamento, manutenção, uso, compartilhamento, disseminação ou disposição de informações
- **Segurança da Informação:** A proteção de informações e sistemas de informação contra acesso não autorizado, uso, divulgação, interrupção, modificação ou destruição, a fim de fornecer confidencialidade, integridade e disponibilidade.
- **Segurança Cibernética:** conjunto de tecnologias e processos desenvolvidos para proteger os sistemas internos, computadores, redes e dados do Grupo Scotiabank Brasil contra-ataques, danos, ameaças ou acesso não autorizado.
- **Incidente:** Evento que pode trazer prejuízos à organização, que pode ser classificado como interno e/ou externo, o qual pode ser uma falha na infraestrutura, queda de sistemas, ataque cibernético, destruição ou quebra na segurança de dados de clientes e/ou colaboradores, endereço de e-mail e/o senha comprometidos, ataque de vírus (Malware), intrusão nos sistemas ou rede, spam, entre outros.
- **Incidente de segurança cibernética:** todo e qualquer evento não esperado que gere algum tipo de instabilidade, quebra de política ou que possa causar danos ao Grupo Scotiabank Brasil;
- **Ataque cibernético:** um ataque cibernético, via ciberespaço, visando o uso do ciberespaço com a finalidade de interromper, desabilitar, destruir ou controlar maliciosamente um ambiente/infraestrutura computacional, ou destruir a integridade dos dados ou roubar informações controladas;
- **Ciberespaço:** Um domínio global dentro do ambiente de informação que consiste na rede interdependente de infraestrutura de sistemas da informação, incluindo a Internet, rede de telecomunicações, sistemas informáticos e processadores e controladores incorporados.
- **Cibersegurança:** A capacidade de proteger ou defender o uso do ciberespaço contra-ataques cibernéticos
- **Risco de Tecnologia da Informação:** O risco de perda financeira, interrupção ou dano à reputação devido a uma falha nos sistemas de tecnologia da informação.
- **Risco à segurança cibernética:** advêm de dentro e/ou de fora da instituição. O impacto do risco à segurança cibernética engloba perda financeira, danos à reputação, multas regulatórias, perda de vantagem estratégica e interrupção de operações
- **Backup:** é a cópia de dados de um dispositivo de armazenamento a outro para que possa ser restaurado em caso da perda dos dados originais.

- **Firewall**: é um dispositivo de segurança da rede que monitora o tráfego de rede de entrada e saída e configurado a permitir ou bloquear tráfegos específicos de acordo com um conjunto definido de regras de segurança.
- **Proprietário da informação/sistema:** é um indivíduo no nível SVP ou VP que é o guardião designado das informações. O "proprietário do sistema/informação" exerce os direitos de propriedade e/ou responsabilidades de custódia do Scotiabank para proteger e gerenciar informações.

  Para aplicações partilhadas fornecidas como "serviços", o proprietário do serviço responsável pela prestação do serviço será o "proprietário da informação/sistema" designado.