POLÍTICA DE

SEGURANÇA CIBERNÉTICA

Abril de 2023

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	Set 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	Mar 2022	Inclusão do item 7.16 Exclusão do item 9.3.2	Marcelo Hiroshi Larissa Horta
Última Atualização	Ago 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	Abr 2023	Inclusão da assinatura do Diretor da Corretora	Larissa Horta

Aprovação da Diretoria

Todas as aprovações da Diretoria foram enviadas por e-mail.

ANTONIO PIANUCCI:63515091815 Digitally signed by ANTONIO PIANUCCI:63515091815 Date: 2023.04.24 14:27:05 -03'00'

Antonio Pianucci
Diretor de Operações, Gerenciamento de Risco & Compliance

JAQUES MESTER:70835039749 Digitally signed by JAQUES MESTER:70835039749 Date: 2023.04.24 07:31:11 -03'00'

Jaques Mester
Diretor Financeiro

PAULO ANDRE CAMPOS BERNARDO:11810021847 Digitally signed by PAULO ANDRE CAMPOS BERNARDO:11810021847 Date: 2023.04.28 11:58:18 -03'00'

Paulo A. Bernardo
Country Head

IZABEL ELIZA DE OLIVEIRA SALVUCCI:03608582878 Digitally signed by IZABEL ELIZA DE OLIVEIRA SALVUCCI:03608582878 Date: 2023.04.28 11:45:42 -03'00'

Izabel Salvucci
Diretora, Execution

RODRIGO ALMEIDA SERGIO:30538072890 Digitally signed by RODRIGO ALMEIDA SERGIO:30538072890 Date: 2023.04.24 15:35:54 -03'00'

Rodrigo Almeida Sergio
Diretor de Operações da Corretora

ÍNDICE

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”, 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 com relação a normas gerais e princípios aplicáveis à gestão de segurança cibernética no Grupo Scotiabank Brasil. É parte integral das políticas e processos que em conjunto demonstram a maneira com a qual o Grupo Scotiabank Brasil conduz de forma efetiva a governança da área de Tecnologia.

Essa Política é um adendo que se relaciona e complementa as políticas, diretivas e procedimentos do *BNS* que se aplicam ao Grupo Scotiabank Brasil.

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. 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 DEFINIÇÕES

- **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.
- **Segurança da Informação:** conjunto de conceitos, mecanismos e estratégias que visam a proteger os ativos do Grupo Scotiabank Brasil;

- **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:** 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 alvos podem ser os clientes, fornecedores e parceiros do Grupo Scotiabank Brasil para causar impacto significante para a instituição;
- **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.

4 PRINCÍPIOS

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

- **Confidencialidade:** garantia de que somente pessoas autorizadas terão acessos 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, parceiros, 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 Scotiabank Brasil.

6 RESPONSABILIDADES

6.1 Local Information Security Officer (LISO)

O Local Information Security Officer (LISO), atualmente é exercido pelo *Senior Manager* da área de Tecnologia, e é responsável por estabelecer por meio de políticas, procedimentos e controles, a integridade, disponibilidade e confidencialidade das informações contidas nos ambientes do Grupo Scotiabank Brasil, minimizando possíveis impactos e vulnerabilidades e, reduzindo a ocorrência de incidentes de segurança que afetem os negócios do Grupo. Também é responsável por entender, gerenciar, reportar e escalar o risco de segurança cibernética em sua área (incluindo ativos relevantes, informações, sistemas e terceiros).

Demais atribuições específicas

- Governança e Gestão de Políticas de Segurança da Informação e Segurança Cibernética;
- Gestão de Acessos (definição de regras e critérios) e Segregação de Funções;
- Atendimento das Auditorias de Segurança da Informação;
- Definição de Requisitos e Análise de Segurança em Projetos;
- Gestão de Riscos e de Indicadores de Segurança da Informação;
- Gestão de Riscos de Segurança da Informação em Fornecedores;
- Gestão e Detecção de Vulnerabilidades;
- Avaliação e Validação dos Testes de Invasão;
- Gestão de Riscos e de Ameaças a Ataques Cibernéticos;
- Gestão e Resposta a Incidentes de Segurança Cibernética; e

- Segurança de Aplicações.

O Plano de Ação e de Resposta a Incidentes aborda com maiores detalhes os processos descritos acima.

6.2 Segurança da Informação

A área de Segurança da Informação é responsável por:

- Promover as Políticas de Segurança da Informação e Segurança Cibernética;
- Mitigar ou eliminar as vulnerabilidades ou ameaças cibernéticas identificadas;
- Avaliar e atuar (quando aplicável) nos incidentes de segurança da informação e segurança cibernética;
- Atuar no controle relacionado aos riscos à segurança cibernética (evento operacional);
- Gerar relatórios mediante a análise e avaliação de riscos à segurança cibernética;
- Manter as áreas de Tecnologia, Compliance e Riscos envolvidas nos trabalhos de análise e avaliação de riscos à segurança cibernética;
- Atuar nos trabalhos de gestão de continuidade de negócios;
- Direcionar às áreas do Grupo Scotiabank Brasil a quaisquer necessidades e/ou dúvidas relacionadas à segurança cibernética;
- Trabalhar em conjunto com as áreas de Tecnologia e as demais áreas na contratação de serviços e/ou sistemas de tecnologia da informação;

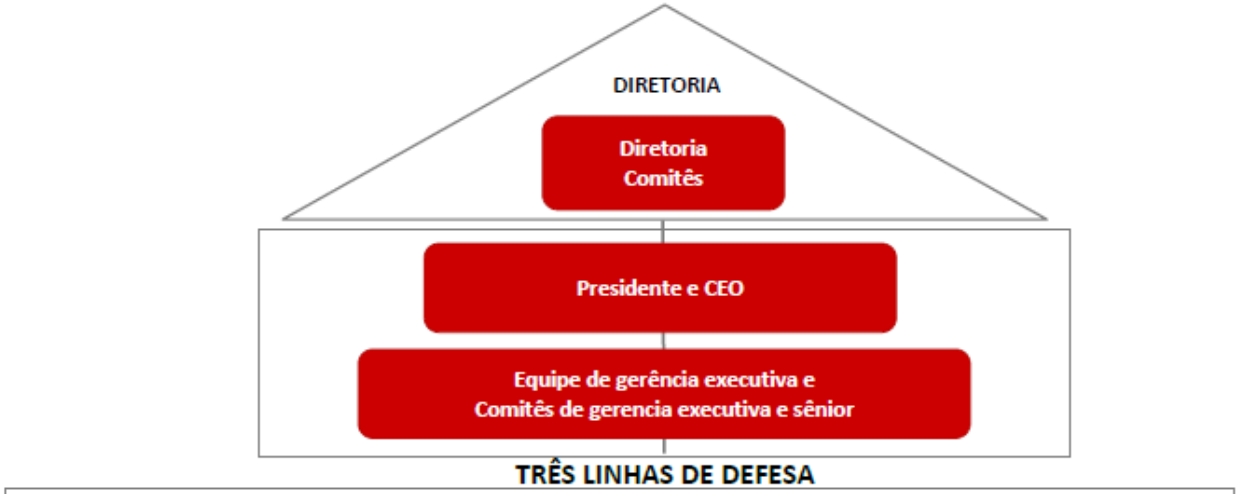
6.3 Colaboradores

- Conhecer suas responsabilidades a respeito da cibersegurança, atuando de forma segura, ética e legal na utilização dos recursos e dados, primando pela preservação da integridade, confidencialidade e disponibilidade das informações da empresa;
- Relatar a equipe de Gestão de Incidentes Local (Local Incident Management Team) qualquer situação que represente desvio ou violação desta Política bem como das normas vigentes;
- Participar ativamente dos programas de disseminação da cultura de segurança cibernética.

6.4 Três Linhas de Defesa

A Estrutura está alinhada à Estrutura Corporativa de Gerenciamento de Riscos, que implanta o

modelo Três Linhas de Defesa, conforme descrito abaixo:



TRÊS LINHAS DE DEFESA

1A Responsáveis pelos riscos

- Assumir responsabilidade pelos riscos gerados por suas atividades, os quais podem ser financeiros (por exemplo, crédito, mercado) ou não financeiros (por exemplo, operacional, reputação)
- Desenvolver e executar controles internos
- Garantir que os riscos gerados sejam identificados, avaliados, gerenciados e monitorados, estejam dentro do apetite ao risco e estejam em conformidade com as políticas, diretrizes e limites relevantes

1B Suporte dos responsáveis pelos riscos

- Auxiliar os responsáveis pelos riscos a identificar, avaliar, monitorar, reportar e responder a riscos
- Auxiliar os responsáveis pelos riscos a implementar iniciativas de gerenciamento de riscos e a estabelecer estruturas de governança de riscos, controles internos e relatórios

2 Supervisão do responsável pelo risco

- Estabelecer apetite ao risco, limites de risco, políticas e estruturas de acordo com as melhores práticas e os requisitos regulatórios
- Medir, monitorar e reportar riscos assumidos em relação aos limites e o apetite ao risco, bem como a riscos emergentes
- Deve ser independente da primeira linha para ser capaz de desempenhar sua função de maneira objetiva

3 Garantia independente

- Fornecer garantia razoável à gerencia sênior e à Diretoria de que a primeira e a segunda linhas de defesa estão efetivamente gerenciando e controlando riscos.
- Focar na estrutura de governança e sistemas de controle

Específicos de segurança da informação e segurança cibernética

Todos os funcionários, para algumas de suas atividades, são Responsáveis por riscos (1A), assim como todos os funcionários são capazes de gerar riscos à reputação e operacionais em suas atividades do dia a dia e devem ser responsabilizados por controlar e gerenciar esses riscos. Os funcionários são obrigados a:

- estar cientes dos riscos de segurança da informação e segurança cibernética que eles poderiam gerar em suas atividades do dia a dia;
- aderir às políticas e aso procedimentos pertinentes a suas atividades do dia a dia e operar dentro dos limites definidos por tais políticas e procedimentos;
- encaminhar, via cadeia de comando, qualquer preocupação referente a risco ou deficiência operacional na política ou nos procedimentos de controle interno.

		1ª linha		2ª linha	3ª linha
		1A: CIOs DO GRUPO DE TI e Serviços corporativos	1B: RISCO DE TI Governança de tecnologia	GRM + Riscos de segurança cibernética e TI	Auditoria Interna
Governança de riscos	Política e estrutura	Responsável	Responsável	Responsável	Informado
	Governança e modelo operacional	Responsável	Responsável	Responsável	Informado
	Apetite ao risco	Responsável	Consultado	Responsável	Informado
	KRIs – Métricas	Responsável	Responsável	Responsável	Informado
	Metodologia de ferramentas	Responsável	Responsável	Responsável	Informado
Identificação de riscos	Perfil de risco	Responsável	Responsável	Desafio	Consulta
Avaliação de riscos	Avaliações de riscos	Responsável	Responsável	Desafio	Informado
	Análise de cenário	Responsável	Responsável	Desafio	Informado
	Testes de controles	Responsável	Responsável	Desafio	Informado
Resposta a riscos	Incidentes de perdas	Responsável	Responsável	Desafio	Informado
	Correção de problemas	Responsável	Responsável	Desafio	Informado
	Requisitos regulatórios	Responsável	Responsável	Consulta e Desafio	Informado
Monitoramento e relatórios de riscos	Painel de risco de TI	Responsável	Responsável	Desafio	Informado
	Relatórios de risco independentes	Informado	Informado	Responsável Responsável	Informado

Como terceira linha de defesa a Auditoria Interna fornece à gerência e à Diretoria uma visão independente e objetiva relacionadas a qualidade e a efetividade dos controles internos e do grau de conformidade com as Políticas de Segurança Cibernética e de Segurança da Informação.

7 PROCESSOS E CONTROLES DE SEGURANÇA CIBERNÉTICA

A fim de assegurar que todas as diretrizes acima 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 pela instituição 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 Scotiabank Brasil 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 é responsável 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 toda infraestrutura para evitar que indivíduos não autorizados tenham acesso aos ambientes segregados e aos sistemas internos. Somente colocaboradores e prestadores de serviços autorizados possuem acesso ao ambiente do ScotiaBank.

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 de todos os 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 e mecanismos de prevenção a vazamentos de dados. Estas recomendações também são aplicadas com o acesso e o uso de sistemas de informação com terceiros e empresas parceiras.

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 instiutição. 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 Rede

O Grupo Scotiabank Brasil adota mecanismos para a segmentação de rede, sendo ambientes segregados para rede de usuarios, rede de servidores de Producão, Homologação e Disaster recovery (DR). O ambiente também possui ferramentas de Firewall, DLP e antivirus 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

O Grupo Scotiabank Brasil possui mecanismos, tais como firewall, proxy e antivirus, 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 de suas atividades.

A Política Plano de Backup, Retenção e 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 que possa causar a interrupção nos negócios. Os respectivos relatórios, em sua maioria, podem ser acessados via rede e/ou enviados regularmente pelas áreas responsáveis. Os principais testes são:

- Análise de Vulnerabilidade (Vulnerability Assessment);
- Análise de Conformidade das Configurações (Configuration Compliance Assessments);
- Penetration Testing – gerenciado pela Equipe Vermelha de Segurança Cibernética (CSRT) e cobrem as áreas que incluem:
    - Segurança de aplicativos,
    - Segurança na nuvem,
    - Segurança de rede,
    - Segurança de aplicativos móveis, e
    - Simulação de Distributed Denial of Service (DdoS).

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

7.11 Monitoramento de Incidentes ref à Fornecedores (*Cyber Vendor Incident*)

Diariamente BNS usa a ferramenta *Security Scorecard* (https://securityscorecard.com/) para monitorar globalmente atividades suspeitas referente aos fornecedores. Em caso de notificações, as quais são diárias, as mesmas são enviadas emediatamente ao Gerente do Contrato em questão.

O objetivo desse programa é aprimorar a postura de segurança de nossos fornecedores, e ao fazer isso, aperfeiçoar também a postura de segurança do Grupo Scotiabank Brasil.

7.12 Plano de Continuidade de Negócios

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

O Plano 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 *Business Continuity Plan Database*, (http://bcp.bns/UpdatePlan.aspx) monitorada pela área de *Business Continuity Management Unit* da Matriz e com supervisão local, na qual cada área descreve seus processos de continuidade de negócios de forma tempestiva e contínua, e com a inclusão de documentos comprobatórios referente aos testes realizados. Há possibilidade de gerar um PDF com todas as informações, porém em inglês, por se tratar de uma ferramenta global.

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

- Perda total do Site Principal: divisão dos times entre Site do DR, e em casa (*WFH – Working From Home*).
- Perda parcial do Site Principal: divisão dos times entre Site do DR, e em casa (*WFH – Working From Home*).
- Situações adversas como alagamentos, greves e/ou acidentes graves na região: divisão dos times entre Site do DR, e em casa (*WFH – Working From Home*).
- Pandemia: time trabalhando de casa (*WFH – Working From Home*).

A Política Plano de Continuidade de Negócios aborda com maiores detalhes os processos descritos acima.

7.13 Classificação de Relevância de Serviços

Para o Grupo Scotibank 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.

7.14 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 dela 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, tais como nome, CPF, RG, entre outros.

O gestor responsável pelo determinado sistema deve garantir que nenhum dado pessoal ou dado pessoal sensível seja classificado como informação pública.

7.15 Registro, Resposta e Tratamento de Incidentes Relevantes

O Grupo Scotiabank Brasil possui processos para gerenciar os riscos relacionados a cibersegurança, sistemas, ativos, dados, 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 Scotiabank Brasil possui uma Equipe de Gestão de Incidentes Local (Local Incident Management Team), 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.

Em se tratando de Contenção, usamos uma ferramenta global chamada *Global Event Management System - GEMS* para registrar, monitorar e fazer todo o acompanhamento dos incidentes relevantes, onde todas as equipes direta ou indiretamente envolvidas na condução e solução do caso têm acesso simultâneo a todas as ações e documentos relacionados. Nessa ferramenta são tratados os incidentes relevantes classificados nas categorias P1 e P2, conforme tabela abaixo:

Impact ⇨ / Urgency ⇩	Major	Minor	Minimal
High	P1 (High) – 911 Major Incident	P1 (High) - 911	P2 (Medium) - 411
Medium	P1 (High) - 911	P2 (Medium) - 411	P3 (Low)
Low	P2 (Medium) - 411	P3 (Low)	P4 (Minimal)

Sendo,

- **411 =** incidentes de grande impacto e que podem causar interrupção de serviços essenciais.
- **911 =** incidentes de grande impacto e que causam interrupção de serviços essenciais.

E quanto à Erradicação do problema, usamos uma ferramenta de *postmortem* chamada de *Post Incident Severity Assessment* (*PISA*) usada para avaliação de risco e impacto, quantificando

ambos. Esse processo abrange várias categorias, como por exemplo, o foco no Cliente, elementos operacionais como impacto financeiro e recorrência dos incidentes, além de impacto reputacional e regulatório.

O Plano de Ação e de Resposta a Incidentes aborda com maiores detalhes os processos descritos acima.

7.16 Monitoramento e Comunicação de Incidentes

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

7.17 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 cibernérica por meio de treinamento e campanhas de aprendizado direcionados e regulares, tais como:

- Programa de capacitação – eLearnings mandatórios e periódicos; campanhas recorrentes sobre Phishing; Portal de Treinamento (me@scotiabank), com uma biblioteca a qual oferece diversos cursos sobre o assunto;
- Informação a clientes e usuários sobre a precaução – envio das políticas e manuais de procedimentos a todos colaboradores, e acesso público aos clientes; e
- Comprometimento da alta administração quanto à segurança cibernética – lançamento de novas estratégias e treinamentos ao Board local.

Além dos treinamentos mandatórios e compulsórios, a Política é enviada a todos os colaboradores no momento de sua publicação, através de um e-mail da área de Compliance. Sendo que a mesma também fica disponível na Intranet para acesso de todos, e publicada na Internet, 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 definidas cláusulas contratuais específicas relacionadas às questões de Segurança Cibernética e LGPD.

O Manual de Procedimentos – Processo de Compras aborda com maiores detalhes os processos descritos acima.

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;
- 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;
- 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;

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 Scotiabank Brasil 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 TI.

11 COMPLIANCE

Faz-se mandatório adquir a compreensão necessária dos requisitos de segurança cibernética do Grupo Scotiabank Brasil por meio de referência constante à Política de Segurança Cibernética, além do Código de Conduta e dos materias do programa de conscientização de segurança.

Estar em conformidade com essa Política é mandatório para todas as pessoas 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 políticas da instituição.

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;
- Estrutura de Governança de Segurança da Informação – BNS;
- Política de Segurança da Informação – Grupo Scotiabank Brasil;
- Plano de Ação e de Resposta à Incidentes – Grupo Scotiabank Brasil;
- Código de Conduta – Grupo Scotiabank Brasil;
- Política de Treinamento e Desenvolvimento – Grupo Scotiabank Brasil;
- Política de Backup, Retenção e Rotação – Grupo Scotiabank Brasil;
- Manual Processo de Compras - 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 CVM Nº 35, DE 26 DE MAIO DE 2021;

15 ONDE BUSCAR AJUDA

Para maiores informações ou esclarecimentos com relação à essa Política, entrar em contato com:

- SP IT Infra através do e-mail SPITInfra@br.scotiabank.com
- SP IT Support através do e-mail SPITSUPPORT@BR.SCOTIABANK.COM
- SP IT Security através do e-mail SPITSECURITY@BR.SCOTIABANK.COM