POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA RESUMIDA

Elaboração:	Data / Assinatura:
Campos Thomaz e Meirelles Advogados **Sócio** **CAMPOS THOMAZ E MEIRELLES ADVOGADOS**	**30/03/2022**
Revisão:	**Data / Assinatura:**
Fernando Paixão de Sousa **Diretor Jurídico** **2GOFINTECH**	**24/05/2022**
Revisão:	**Data / Assinatura:**
Barcellos, Tucunduva – Advogados **Sócio**	**23/09/2022**
Revisão:	**Data / Assinatura:**
Fernando Paixão de Sousa **Diretor Jurídico** **2GOFINTECH**	**10/10/2022**
Revisão:	**Data / Assinatura:**
Cauã Pastore **Diretor de Segurança da Informação** **2GOFINTECH**	**15/10/2022**
Aprovação:	**Data / Assinatura:**
Cyllas Salerno Elia Junior **CEO** **2GOFINTECH**	**21/20/2022**

Av Ibirapuera, 2332, 13º andar - Indianópolis/São Paulo-SP - 04028-900 www.2gobank.com.br CNPJ: 23.819.290/0001-03

HISTÓRICO DO DOCUMENTO:

Data	Versão	Autor	Motivo da Revisão
30/03/2022	1.0	Campos Thomaz e Meirelles Advogados	Versão inicial do documento
24/05/2022	2.0	Fernando Paixão	Revisão da Política
23/09/2022	2.0	Barcellos Tucunduva Advogados	Revisão da Política
10/10/2022	2.0	Fernando Paixão	Revisão da Política
15/10/2022	2.0	Cauã Pastore	Revisão Final

SUMÁRIO

1. DESCRIÇÃO 4
2. OBJETIVO ..... Erro! Indicador não definido.
3. PRINCÍPIOS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA 4
4. REGRAS GERAIS 5
5. DIRETRIZES DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA 6
6. CONTRATAÇÃO DE SERVIÇOS DE COMPUTAÇÃO EM NUVEM 8
7. CONTINUIDADE DE NEGÓCIOS 8
8. TREINAMENTO 8
9. RECOMENDAÇÕES AOS CLIENTES E USUÁRIOS 8
10. COMPROMETIMENTO DA ALTA ADMINISTRAÇÃO ..... Erro! Indicador não definido.
11. DAS RESPONSABILIDADES ESPECÍFICAS 9
12. PERIODICIDADE 12

Av Ibirapuera, 2332, 13º andar - Indianópolis/São Paulo-SP - 04028-900 www.2gobank.com.br CNPJ: 23.819.290/0001-03

1. DESCRIÇÃO

Esta Política de Segurança da Informação e Segurança Cibernética ("**Política**") aplica-se a todos sócios, diretores, profissionais, estagiários, aprendizes, parceiros de negócio e prestadores de serviços da 2GO Administração e Pagamentos Ltda. ("**2GOFintech**").

A gestão da segurança da informação necessita da participação e envolvimento de todos os profissionais da **2GOFintech** A partir disso, a segurança da informação é melhorada mediante a implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e tecnologia, os quais devem ser monitorados, analisados criticamente e constantemente melhorados a fim de garantir que os objetivos do negócio e de segurança específicos da **2GOFintech** sejam devidamente atendidos em todas as áreas.

Nesse sentido, a Política de Segurança da Informação e Segurança Cibernética consiste em um conjunto de definições e procedimentos que explicam como proteger os ativos da **2GOFintech**.

2. OBJETIVO

Os principais objetivos da segurança da informação e da segurança cibernética são a proteção das redes, computadores, sistemas e dados contra os diferentes tipos de ameaças, a fim de garantir a continuidade das operações, minimizar riscos aos quais a **2GOFintech** está exposta, evitar danos inesperados e garantir o retorno sobre os investimentos realizados na **2GOFintech**.

Dessa forma, o principal objetivo desta Política é resguardar a **2GOFintech** quanto à confidencialidade, integridade e disponibilidade das informações através da adoção de medidas de segurança e controles para reduzir a vulnerabilidade da **2GOFintech** à incidentes de segurança e desenvolvimento de planos e ações de comunicação e continuidade para prevenir, detectar e reduzir os riscos relacionados à cibersegurança.

3. PRINCÍPIOS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

A informação da **2GOFintech**, por ela produzida ou recebida, deverá ser utilizada em benefício exclusivo do negócio, com senso de responsabilidade, de modo ético e seguro, baseado nos seguintes princípios:

Av Ibirapuera, 2332, 13º andar - Indianópolis/São Paulo-SP - 04028-900 www.2gobank.com.br CNPJ: 23.819.290/0001-03

- **Confidencialidade:** Assegurar que o acesso à informação seja obtido somente por pessoas autorizadas e quando for de fato necessário;

- **Integridade:** Assegurar a exatidão e completude da informação e dos métodos de seu processamento, bem como da transparência no tratamento com os públicos envolvidos; e

- **Disponibilidade:** Assegurar que somente pessoas autorizadas tenham acesso à informação sempre que necessário.

- **Autenticidade**: garantia de identificar e autenticar usuários, entidades, sistemas ou processos com acesso à informação

4. REGRAS GERAIS

Com o objetivo de garantir os objetivos desta Política, os procedimentos de Segurança da Informação e Segurança Cibernética seguirão as seguintes diretrizes:

- Assegurar que não haja acessos indevidos, modificações, destruições ou divulgações não autorizadas das informações. Para tanto, o acesso do Colaborador deve ser pessoal, intransferível e restrito aos recursos necessários para realizar suas atribuições na **2GOFintech**.
- Cada Colaborador, quando aplicável, receberá uma senha pessoal de acesso e ficará responsável por manter sua senha em sigilo para evitar acesso indevido às informações que estão sob sua responsabilidade. A **2GOFintech** adotará mecanismos que visam a assegurar a utilização segura de senhas.

- Qualquer risco à informação deverá ser imediatamente reportado pelo Colaborador por meio dos canais e procedimentos indicados pela **2GOFintech**.

- Assegurar que todas as informações sejam tratadas de maneira ética e sigilosa e que sejam adotadas medidas capazes de evitar ou, ao menos, registrar acessos indevidos, modificações, destruições ou divulgações não autorizadas.

- Assegurar que as informações sejam utilizadas somente para a finalidade para a qual foram coletadas e que o acesso esteja condicionado à autorização.

- Assegurar o cumprimento dos procedimentos e controles adotados para reduzir a vulnerabilidade a incidentes e atender aos demais objetivos de Segurança Cibernética, tais

como, a autenticação, a criptografia, a prevenção e a detecção de intrusão, a prevenção de vazamento de informações, a realização periódica de testes e varreduras para detecção de vulnerabilidades, a proteção contra softwares maliciosos, o estabelecimento de mecanismos de rastreabilidade, os controles de acesso e de segmentação da rede de computadores e a manutenção de cópias de segurança dos dados e das informações.

- Assegurar que os controles específicos, incluindo os voltados para a rastreabilidade da informação, garantam, no melhor nível possível, a segurança das informações sensíveis.

- Assegurar o registro, análise da causa e o impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da **2GOFINTECH**, como Instituição de Pagamento.

- Assegurar a elaboração de cenários de incidentes considerados nos testes de continuidade dos serviços de pagamento prestados;

- Definir os procedimentos e controles voltados à prevenção e ao tratamento dos incidentes que devem ser adotados pelos prestadores serviços e terceiros que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da **2GOFINTECH**;

- Classificar os dados e as informações quanto à relevância;

- Definir os parâmetros a serem utilizados na avaliação da relevância dos incidentes;

- Assegurar os mecanismos para disseminação da cultura de segurança cibernética, incluindo:

    - A implementação de programas de capacitação e de avaliação periódica de pessoal;

    - A prestação de informações a usuários finais sobre precauções na utilização de produtos e serviços oferecidos.

- Estimular iniciativas para compartilhamento de informações sobre incidentes relevantes, com Instituições de Pagamento, instituições financeiras e demais instituições autorizadas a funcionar pelo Bacen.

- Manter o registro, análise da causa e do impacto, bem como o controle dos efeitos de incidentes de informações recebidas de empresas prestadoras de serviços a terceiros.

- Contemplar procedimentos e controles em níveis de complexidade, abrangência e precisão compatíveis com os utilizados pela **2GOFINTECH** e por esta Política.

5. DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA DA 2GOFINTECH

Com relação à segurança da informação e segurança cibernética da **2GOFintech**, as seguintes diretrizes se aplicam:

- A **2GOFintech** possui implementado o controle de acesso para seus profissionais, incluindo prestadores de serviço e parceiros de negócio, limitando tal acesso ao necessário para exercício de cada função. Os acessos às informações são controlados, monitorados e restringidos à menor permissão e privilégios possíveis, revistos periodicamente com a aprovação do gestor do responsável e o da informação, e cancelados tempestivamente ao término do contrato de trabalho do colaborador ou do prestador de serviço;
- Procedimento seguro de entrada no sistema e armazenamento de logs;
- Gerenciamento de criação de senha para os profissionais da **2GOFintech**;
- Revisão e revogação de acesso a cada 6 (seis) meses para garantir que os profissionais da **2GOFintech** só tenham acesso permitido para o desempenho de suas funções;
- Gerenciamento de segurança em redes e controle de redes através de controles que garantem a proteção da confidencialidade e integridade de informações e autenticação para acesso à rede da **2GOFintech**;
- Regras para transferência de informações seguindo procedimentos para proteger a informação transferida contra interceptação, cópia, modificação, desvio e destruição, e controles e restrições de acessos;
- Critérios de segurança para informações enviadas via mensagens eletrônicas (e-mail);
- Regras e restrições para acesso de redes sociais, espaços virtuais públicos e internet para garantir a segurança do ambiente da **2GOFintech**;

Av Ibirapuera, 2332, 13º andar - Indianópolis/São Paulo-SP - 04028-900 www.2gobank.com.br CNPJ: 23.819.290/0001-03

- Formalização de acordo de confidencialidade e não divulgação entre parceiros e fornecedores da **2GOFintech**;
- Gerenciamento e análise de matriz de risco para relacionamento com fornecedores;
- Regras para formalização de acordo e contrato com fornecedores com cláusulas especificando controles mínimos de segurança da informação para a relação comercial;
- Concordância de terceiros e fornecedores com a Política de Segurança da Informação e Segurança Cibernética da **2GOFintech**;
- Regras para mudanças em acordo de prestação de serviço com fornecedores referente a segurança da informação;
- Adoção de procedimentos operacionais de segurança como back-up e restore, procedimento para reinício e recuperação em caso de falha dos recursos de tecnologia da informação, gerenciamento de trilhas de auditoria e informações de registros (log) dos recursos de tecnologia da informação;
- Controles para prevenir, detectar, remover e gerenciar riscos associados a ameaças no ambiente cibernético;
- Registro e monitoramento dos recursos de tecnologia da informação para planejamento, tratamento de incidentes e, resposta às auditorias;
- Controles e procedimentos para gerenciamento das instalações de software em sistemas operacionais;
- Adoção de mecanismos de prevenção de vírus e outros tipos de softwares e condutas maliciosas, que venham a **2GOFintech** à vulnerabilidade.
- Regras e controles para acesso remoto de colaboradores à **2GOFintech** e seus sistemas;
- Uso de controles criptográficos para proteção de dados e informações;
- Gestão de ativos de tecnologia da informação da **2GOFintech**;
- Regras para classificação e tratamento de informação, informações confidenciais e sensíveis;
- Gestão de incidentes de segurança da informação, abordando avaliação e decisão sobre tomada de decisão e comunicação;

Av Ibirapuera, 2332, 13º andar - Indianópolis/São Paulo-SP - 04028-900 www.2gobank.com.br CNPJ: 23.819.290/0001-03

- Referência a plano de resposta a incidentes de segurança da informação da **2GOFintech** e orientações quanto ao aprendizado e processos de melhoria;
- Monitoramento e auditoria de uso de informações no ambiente da **2GOFintech** para redução de riscos.
- Adoção de criptografia dos ativos de informação da **2GOFintech,** conforme classificação da informação, em todo o tráfego que ocorrer em rede pública.

6. CONTRATAÇÃO DE SERVIÇOS DE COMPUTAÇÃO NA NUVEM

Conforme a Resolução 4.893/2021 do Banco Central do Brasil, que dispõe sobre a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, a **2GOFintech** deve implementar procedimentos efetivos para conformidade com as regras previstas na regulamentação em vigor. Para isto, a **2GOFintech** possui uma Política de Contratação de Serviços de Computação em Nuvem, que deverá ser observada.

7. CONTINUIDADE DE NEGÓCIOS

O processo de gestão de continuidade de negócios relativo à segurança da informação, deve ser implementado para minimizar os impactos e recuperar perdas de ativos da informação, após um incidente crítico, a um nível aceitável, através da combinação de requisitos como operações, classificação de incidentes, formação de grupo de trabalho, mapeamento de processos críticos, análise de impacto nos negócios e testes periódicos de recuperação de desastres. Incluem-se nesse processo, a continuidade de negócios relativos aos serviços contratados de nuvem e os testes previstos para os cenários de ataques cibernéticos.

8. INCIDENTES DE SEGURANÇA

a. CLASSIFICAÇÃO DE RELEVÂNCIA DOS INCIDENTES

A 2GOFINTECH classificará os incidentes de segurança segundo sua relevância e conforme a classificação das informações envolvidas e o impacto na continuidade dos negócios da2GOFINTECH.

b. GESTÃO DE INCIDENTES

Todos os incidentes ou suspeita de incidentes identificados por um Colaborador, cliente, prestador de serviços, fornecedor, provedor ou parceiro devem ser imediatamente comunicados à área

responsável. A comunicação deverá ser feita por meio dos canais indicados pela 2GOFINTECH através do e-mail seginfo@2gofintech.com.br

Os incidentes reportados serão classificados segundo o risco que representam para a 2GOFINTECH e o impacto na continuidade dos negócios da 2GOFINTECH. Além disso, devem ser devidamente registrados, tratados e comunicados.

A 2GOFINTECH adotará procedimentos para mitigar os efeitos dos incidentes relevantes e a interrupção dos serviços relevantes de processamento, armazenamento de dados e de computação em nuvem contratados.

c. PLANO DE COMPARTILHAMENTO DE INCIDENTES

Sem prejuízo do dever de sigilo e da livre concorrência, a 2GOFINTECH deve adotar iniciativas para o compartilhamento de informações sobre incidentes relevantes com as demais instituições autorizadas a funcionar pelo Bacen, por meio dos canais adotados pelas instituições.

As informações compartilhadas também estarão disponíveis ao Bacen.

Caso haja incidentes relevantes ou interrupção dos serviços relevantes, a 2GOFINTECH comunicará o Bacen e adotará medidas necessárias para que as suas atividades sejam reiniciadas, informando o prazo para reinício ou normalização das suas atividades ou dos serviços relevantes interrompidos, estabelecendo e documentando os critérios que configuraram a situação de crise.

d. PLANO DE AÇÃO E RESPOSTA A INCIDENTES

A 2GOFINTECH deve estabelecer plano de ação e de resposta a incidentes visando à implementação desta Política, que abrange, minimamente:

- As ações a serem desenvolvidas para adequar as estruturas organizacional e operacional às diretrizes desta Política;
- As rotinas, os procedimentos, os controles e as tecnologias a serem utilizados na prevenção e na resposta a incidentes.

e. RELATÓRIO ANUAL DE INCIDENTES

A 2GOFINTECH deve elaborar relatório anual sobre a implementação do plano de ação e de resposta a incidentes, com data-base de 31 de dezembro. O relatório abordará:

- A efetividade da implementação das ações de adequação suas estruturas organizacional e operacional;
- O resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e das tecnologias a serem utilizados na prevenção e na resposta a incidentes, em conformidade com as diretrizes desta Política;
- Os incidentes relevantes relacionados com o ambiente cibernético ocorridos no período;

- Os resultados dos testes de continuidade dos serviços de pagamento prestados, considerando cenários de indisponibilidade ocasionada por incidentes.

O relatório anual de incidentes deve ser apresentado à Diretoria da 2GOFINTECH até 31 de março do ano seguinte ao da data-base.

9. TREINAMENTO

A conscientização em segurança da informação e segurança cibernética à garantia dos objetivos e diretrizes definidos nesta Política é realizado adequando-se às necessidades e responsabilidades específicas de cada colaborador.

10. RECOMENDAÇÕES AOS CLIENTES E USUÁRIOS

- Padrão de senhas mais complexas;
- Alteração de senha quando suspeita de vazamento ou qualquer outro comprometimento das credenciais de acesso;
- Criação de senhas distintas para cada tipo de serviço utilizado pelo usuário;
- Habilitação de segundo fator de autenticação (se aplicável para a **2GOFintech**);
- Evitar o acesso de computadores de acesso público ou de terceiros para acesso ao sistema da **2GOFintech**;
- Manter o aplicativo constantemente atualizado;
- Não abrir e-mails sobre os nossos serviços cujo domínio não seja @2gofintech.com.br;
- Não clicar em links enviados via e-mail ou SMS desconhecidos;
- Não informar dados pessoais e dados financeiros em ligações ou em qualquer outro meio em que não seja possível determinar que a **2GOFintech** é a destinatária;
- Bloquear o dispositivo utilizado para acessar o site e aplicativo financeiro quando não estiver utilizando.

11. DO COMPROMETIMENTO DA ALTA ADMINISTRAÇÃO

A alta administração da **2GOFintech** se compromete com a segurança da informação e segurança cibernética da **2GOFintech**, implementando processos de melhoria contínua dos seus

procedimentos relacionados com a segurança cibernética e prevenção de incidentes na **2GOFintech**.

12. DAS RESPONSABILIDADES ESPECÍFICAS

a. DOS COLABORADORES EM GERAL

Os colaboradores da **2GOFintech**, estagiários e aprendizes, em qualquer nível hierárquico, serão responsáveis em cumprir e zelar pela realização eficaz das políticas e princípios da segurança da informação, no compromisso com os critérios legais e éticos que envolvem a .

É de total responsabilidade de cada colaborador qualquer prejuízo ou dano que vierem a sofrer ou causarem à **2GOFintech** e/ou a terceiros, em decorrência do não atendimento às diretrizes dessa Política e das demais políticas da **2GOFintech** aqui referidas.

Cabe a todos os colaboradores da **2GOFintech**:

- Cumprir fielmente as diretrizes estabelecidas neste documento;
- Buscar orientação do superior hierárquico, em caso de dúvidas relacionadas à segurança da informação;
- Assinar o Termo de Responsabilidade e Aceite da Política de Segurança da Informação e Segurança Cibernética, formalizando a ciência das políticas, bem como assumindo a responsabilidade pelo seu cumprimento;
- Preservar as informações contra o acesso, modificação, divulgação ou destruição não autorizada pela **2GOFintech**;
- Utilizar senha segura, devendo alterar a mesma, conforme periodicidade determinada pela **2GOFintech**;
- Garantir que os recursos tecnológicos sejam utilizados somente para fins profissionais e de interesse da **2GOFintech**; e
- Comunicar imediatamente a equipe de Segurança da Informação, qualquer descumprimento ou violação desta política.

b. DOS GESTORES

É responsabilidade de cada gestor registrar, atribuir valor, analisar quanto aos riscos e classificar, as

informações da sua área, além de ser responsável pela manutenção, revisão e cancelamento de

Av Ibirapuera, 2332, 13º andar - Indianópolis/São Paulo-SP - 04028-900 www.2gobank.com.br CNPJ: 23.819.290/0001-03

autorização à determinada informação ou conjunto de informações sob sua guarda. Além de garantir a implementação de mecanismos necessários para descarte seguro das informações.

Cabe a todo gestor de área:

- Assegurar que suas equipes possuam acesso e conhecimento desta política, bem como as instruções aqui estabelecidas;
- Ser referência da área em relação à Segurança da Informação, servindo como modelo de conduta para os profissionais sob a sua gestão;
- Cumprir e fazer cumprir esta política e demais itens aqui referenciados;
- Determinar quais áreas e cargos devem ter acesso à informação sob sua responsabilidade;
- Manter devidamente atualizados os registros e controles de todas as autorizações de acesso concedidas, determinando sempre que necessário a pronta suspensão do acesso ou alteração da autorização concedida;
- Revisar as autorizações de acesso sempre que necessário ou solicitado, cancelando aquelas que não se fizerem mais necessárias;
- Durante a contratação de um parceiro e o mesmo tiver contato com informações confidenciais da **2GOFintech**, será necessário a inclusão de um acordo de confidencialidade (NDA) e ciência da PSI, exigindo o repasse das obrigações a seus empregados responsáveis pela prestação de serviços dentro da **2GOFintech**;
- Assegurar que os acessos dos parceiros de negócio da **2GOFintech** estejam emconformidade com as diretrizes dessa política e demais itens referenciados; e
- Apoiar a equipe de Segurança da Informação em eventuais violações da Segurança da Informação.

c. EQUIPE DE SEGURANÇA DA INFORMAÇÃO

A equipe de Segurança da Informação será responsável por:

- Gerir o uso de tecnologias necessárias ao bom andamento dos negócios, incluindo ações preventivas e tratamento de incidentes com o propósito de promover maior nível de Segurança da Informação;

Av Ibirapuera, 2332, 13º andar - Indianópolis/São Paulo-SP - 04028-900 www.2gobank.com.br CNPJ: 23.819.290/0001-03

- Submeter as versões da Política de Segurança da Informação e Segurança Cibernética, e após a aprovação, publicar e promover a divulgação da mesma na **2GOFintech**;
- Propor as metodologias e processos específicos para a Segurança da Informação;
- Propor e apoiar iniciativas que visem à segurança dos ativos de informação;
- Promover, junto ao RH, conscientizações dos profissionais e parceiros em relação à importância da Segurança da Informação, por meio de campanhas, palestras, treinamentos e outros meios;
- Apoiar a avaliação e a adequação de controles específicos de Segurança da Informação para novos sistemas ou serviços; e
- Analisar criticamente incidentes.

d. DOS RECURSOS HUMANOS

Cabe ao departamento de Recursos Humanos:

- Atribuir no momento de contratação dos profissionais, a formalização e o aceite da política, bem como colher as assinaturas e realizar o arquivamento;
- Apresentar a política e colher a assinatura do Termo de Responsabilidade e Ciência da Política de Segurança da Informação e Segurança Cibernética dos profissionais já contratados, bem como efetuar o arquivamento da mesma;
- Comunicar à equipe de Segurança da Informação formalmente e prontamente toda e qualquer alteração no quadro funcional, contratações, demissões, alterações de cargos, funções, entre outros necessários, em prazo mínimo, a fim de evitar acessos não autorizados e/ou desnecessários; e
- Aplicar sanções cabíveis mediante a um incidente de Segurança da Informação (Penalidades).

13. ARQUIVAMENTO DE INFORMAÇÕES

A **2GOFINTECH** deve armazenar em meio físico ou digital, pelo prazo de 5 anos, as seguintes informações:

- O documento relativo à política de Segurança Cibernética;

- A ata de reunião da Diretoria da **2GOFINTECH**;
- O documento relativo ao plano de ação e de resposta a incidentes;
- O relatório anual;
- A documentação sobre os procedimentos desta Política;
- A documentação no caso de serviços prestados no exterior;
- Os contratos de prestação de serviços;
- Os dados, os registros e as informações relativas aos mecanismos de acompanhamento econtrole, a partir da implementação dos mecanismos mencionados.

14. PERIODICIDADE

A equipe de Segurança da Informação é responsável pela revisão e atualização dessa política. A revisão ou atualização da Política de Segurança da Informação e Segurança Cibernética serárealizada periodicamente, no mínimo a cada 1 (um) ano, ou quando a equipe de Segurança da Informação julgar necessário, conforme análise e decisão do comitê responsável.

Esta Política está acompanhada de um Termo de Adesão à Política de Segurança da Informação e Segurança Cibernética e Termo de Adesão às Alterações da Política de Segurança da Informação e Segurança Cibernética, que deverão ser assinados por todos os Colaboradores, prestadores de serviços, fornecedores, provedores e parceiros.

Esta Política está disponível em local acessível a todos Colaboradores, em linguagem clara e acessível. É possível acessá-la no site https://politicas.2gofintech.com.br.

Última atualização: setembro de 2022.