Política de segurança de informação e proteção de dados

Vigência: a partir de 04 de agosto de 2023

FICHÁRIO

Título	Política de segurança de informação e proteção de dados
Aprovador	Diretoria
Data da Aprovação	04.08.2023
Data da Vigência	04.08.2023
Data de Validade | Revisão	04.08.2026 | 3 anos
Área Responsável	Diretoria de Conformidade

Sumário

1. OBJETIVO

A presente Política objetiva consolidar os requisitos e procedimentos necessários à manutenção da efetividade da Segurança da Informação na Frente Corretora de Câmbio (“FRENTE”), estabelecendo um arcabouço sólido de proteção de dados, tanto internos quanto de clientes.

2. APROVAÇÃO

A Política de segurança de informação e proteção de dados foi aprovada pela Diretoria em agosto de 2023.

3. RESPONSABILIDADE E VALIDADE

A elaboração, a manutenção e a disponibilização desta Política são de responsabilidade da Diretoria de Conformidade em conjunto com a área de Tecnologia da Informação (“TI”).

3.1. PERÍODO DE REAVALIAÇÃO

Esta política será reavaliada a cada 3 anos, quando houver alterações na FRENTE ou ainda a requerimentos legais/ regulatórios que justifiquem a sua atualização.

4. ABRANGÊNCIA E PÚBLICO ALVO

Este documento é de caráter confidencial, estando disponível na rede interna da FRENTE.

A Política de segurança de informação e proteção de dados é direcionada a todos os administradores, funcionários, estagiários e prestadores de serviços, ligados de forma direta ou indiretamente com a FRENTE e empresas do grupo, se aplicando a todas as áreas.

5. DEFINIÇÕES E CONCEITOS

Para melhor entendimento desta política, apresenta-se definições e conceitos sobre o tema que será abordado neste documento.

CLIENTE: Qualquer pessoa física ou jurídica com a qual seja realizada uma transação comercial e/ou financeira, de acordo com os parâmetros estabelecidos pela regulamentação vigente e pela FRENTE.

COLABORADORES: Todos os administradores, funcionários, estagiários e prestadores de serviços, sejam eles vinculados diretamente ou indiretamente à FRENTE e às empresas do grupo.

FRENTE CORRETORA DE CÂMBIO (“FRENTE”): Corretora de Câmbio com uma abordagem inovadora, digital e contemporânea.

COOKIES: Arquivos que autorizem determinado site a registrar informações sobre visita, como preferências, configurações, histórico de navegação e outras atividades realizadas na página.

CONFIDENCIALIDADE: Significa garantir que a informação não será acessada ou conhecida por pessoas que não tenham autorização para tal.

DISPONIBILIDADE: Garante que a informação deve estar disponível para usuários autorizados quando solicitado.

INTEGRIDADE: É a garantia de que a informação utilizada é apresentada sem erros e inconformidades.

SOFTWARE: Parte intangível e não física de um computador, que permite que ele realize diversas operações, controlando o hardware e fornecendo funcionalidades úteis aos usuários.

6. SEGURANÇA DA INFORMAÇÃO

A Segurança da informação está diretamente relacionada à proteção de informações contra ações e ameaças que possam causar prejuízos à FRENTE, parceiros e clientes.

Para garantirmos a segurança das informações, são contemplados, principalmente, três conceitos. São eles: Confidencialidade, Disponibilidade e Integridade.

7. CULTURA

É fundamental que todos aqueles a quem a política é endereçada possuam fácil acesso e que a cultura da segurança cibernética seja estabelecida e solidificada

de maneira efetiva. A divulgação da presente política é pilar fundamental para garantir que seja realmente aplicada.

8. PROTEÇÃO E PREVENÇÃO

Todos os acessos ao ambiente de rede, software de apoio, sistemas e dados da FRENTE devem ser concedidos somente mediante aprovação deliberada conforme segue:

PRÁTICAS DE SEGURANÇA

Os prestadores de serviços somente podem ter acesso a informações e infraestrutura corporativas se aderirem a contratos de prestação de serviços com cláusulas de confidencialidade de informação já validadas por Compliance e aprovadas pela Diretoria.

Os funcionários somente podem ter acesso às informações e infraestrutura corporativas após a finalização do processo de admissão, o qual consta previsto em cláusula contratual a confidencialidade de informação já validada por Compliance e aprovada pela Diretoria.

CONTROLE DE ACESSOS

Será concedido aos usuários, mediante solicitação formalizada via e-mail para a área de Controles Internos ou responsável da área solicitante, que detêm, por

força das suas responsabilidades, o papel de assegurar o controle de acesso efetivo das informações. O documento de solicitação conterá obrigatoriamente todos os dados de identificação do usuário e suas necessidades, devidamente discriminadas entre acesso para entrada, alteração/exclusão ou consulta aos dados referentes aos processos e produtos sistêmicos, somente com base nas suas atribuições e responsabilidades funcionais junto à FRENTE.

CENTRAL DE PROCESSAMENTO DE DADOS (CPD)

As salas atribuídas às operações de TI são destinadas ao armazenamento de servidores (Centrais de processamento de dados – CPDs), consideradas áreas de alta segurança, e devem ter o seu acesso restrito apenas aos funcionários da área de Suporte, considerando as seguintes premissas:

- O acesso às salas é monitorado por sistema de câmera de vídeo e devidamente gravado.
- O acesso será pessoal e intransferível através de chave de segurança digital.
- É terminantemente proibida a entrada de pessoal não autorizado nas áreas de armazenamento de servidores, mesmo acompanhado de pessoal autorizado, salvo caso de funcionários que necessitem executar alguma tarefa extraordinária.
- Funcionários que porventura necessitem executar serviços extraordinários dentro das salas devem permanecer sob supervisão constante de pessoal autorizado.

REDE CORPORATIVA

Todo usuário da Rede Corporativa da FRENTE será identificado pelo nome do usuário para acesso à rede e identificação no Webmail corporativo com o seguinte formato de nomenclatura: nome.sobrenome@frentecorretora.com.br. A identificação do usuário será feita pelo primeiro nome. Havendo outro colaborador já cadastrado, será adicionada a inicial do último sobrenome (não considerados os complementos que indicam filho, júnior, por exemplo).

Podem ser criadas contas para prestadores de serviços terceirizados, mas estas deverão possuir prazo de expiração (validade) igual ou inferior à data de término de seu contrato ou quando solicitado pelas áreas de Controles Internos e Compliance.

O software de rede corporativa, os sistemas de aplicativos e utilitários terão acesso liberado somente com o fornecimento de identificação e a composição de senha pessoal, intransferível e que deve seguir os seguintes parâmetros de segurança:

- As senhas devem ter no mínimo 8 caracteres, dentre eles letras maiúsculas, minúsculas, caracteres especiais e números;
- Toda senha deverá expirar em até 90 dias;
- É proibido repetir as últimas 6 senhas;

- Contas recém-criadas ou com senhas reiniciadas deverão solicitar ao usuário a alteração da senha no primeiro logon;
- Tempo mínimo de validade de uma senha é de 1 dia;
- Bloquear senha após 4 tentativas mal sucedidas consecutivas;
- É proibido incluir a senha em processos automáticos de conexão;
- Não podem ser divulgadas; e
- Devem ser alteradas sempre que houver suspeita de que alguém tenha visto a digitação da senha ou que tenha sido descoberta.

9. REGRAS DE USO

USO DE SOFTWARE

As áreas da FRENTE não poderão receber, adquirir ou instalar qualquer tipo de software sem que haja uma autorização pontual da área de TI. Na eventualidade de real necessidade de uso de algum, quando não exista no mercado um software comercial homologado, ou seja, economicamente inviável a aquisição de um, poderão ser avaliadas possíveis exceções, e se aprovados, somente a área de TI poderá realizar a sua obtenção (por download ou outra forma) e instalação nas estações de trabalho.

USO DA INTERNET

O acesso será definido caso a caso pela área de TI e somente liberado mediante requisição dos Gestores das áreas interessadas, com a aprovação da respectiva Diretoria e da área de Conformidade.

Os usuários serão orientados quanto à negação de acesso a sites inadequados à atuação profissional no ambiente da FRENTE, além de sites que possam envolver a Corretora em atividades ou manifestações ilegais, racistas, ou contrárias às regras de civilidade.

Dada a assinatura do contrato de trabalho ou de prestação de serviços terceirizados junto à FRENTE, os colaboradores manifestarão a concordância com as regras de acesso e monitoramento contínuo de suas atividades, bem como as penalidades em que estão sujeitos em caso de violação das regras estabelecidas.

USO DE E-MAIL

Deverá ser feito exclusivamente para objetivos profissionais dos colaboradores, devendo ser evitado o uso em caráter totalmente pessoal, especialmente a circulação de correntes, mensagens de cunho ilegal ou ofensivo, envio e recebimento de anexos que possam representar violação de direitos de propriedade intelectual e disseminação de informação não autorizada ou restrita da Corretora.

Padronização de Assinaturas: Será padronizado o formato das Assinaturas de Mensagens de Correio Eletrônico, assim como será obrigatória a inserção de

uma mensagem orientando destinatários sobre a limitação de responsabilidade da Frente sobre o conteúdo das mensagens. Esta nota será inserida em modelo pela área de TI e não poderá ser removida pelos usuários, conforme o teor do Termo de Responsabilidade citado anteriormente.

REDES WIRELESS

A FRENTE possui uma rede sem fio configurada para comodidade e flexibilidade em acessos de natureza específica ou extraordinária.

O acesso a esta rede só será permitido mediante solicitação documentada ao departamento de TI com cópia para a área de Conformidade e, posterior aprovação por parte da autoridade competente.

A rede sem fio da corretora não permite acesso aos recursos de rede local, sua utilização visa exclusivamente o acesso à internet, de forma irrestrita.

O controle de acesso se dará por senha criptografada que deverá ser alterada a cada 30 dias, nunca se repetindo.

ACESSO REMOTO

A rede é de uso exclusivo de funcionários de TI e colaboradores registrados mediante contrato para fins de instalação ou manutenção de sistemas. O acesso deverá ser feito mediante conexões SSH encriptadas ou sessões de conexão remota (VNC, Remote Desktop e similares).

USO DE MÍDIAS DE ARMAZENAMENTO

As mídias de armazenamento permanente ou temporário de informações devem ter tratamento seguro para as situações de descarte, retenção, restrições e condições para outros casos, visando proteger a Corretora de exposição não autorizada de informações que tenham sido gravadas nelas, ainda que tenham sido apagadas logicamente.

Tal tratamento seguro inclui o apagamento físico de informações em mídias como Hard Disks que venham a ser enviados para reparo técnico ou outra forma de envio para locais externos.

USO DE EQUIPAMENTOS

Todos os equipamentos devem ser homologados pela área de TI, e deverá ser priorizado o uso seguro de impressoras e material impresso.

IMPORTANTE: No uso cotidiano, todos os usuários devem adotar a opção de timeout nas estações de trabalho, ou seja, ativar a Proteção de tela do Windows protegida por senha. Dessa forma, em ausência maior que 10 minutos, será ativada esta proteção, salvo exceção para mesas que possuam terminais de operações.

BACKUP

O backup dos servidores de aplicações críticas é realizado de modo dinâmico em tempo real e replicado em site backup em sua totalidade. Todos os arquivos dos usuários deverão ser mantidos em drive de rede, sendo de responsabilidade do próprio usuário a cópia e guarda do arquivo. A restauração dos arquivos salvos em rede será avaliada mediante solicitação por escrito do usuário ou supervisor.

PROCESSO DE GRAVAÇÃO DE VOZ

A solicitação para a escuta de gravações deve ser formalizada pelas gerências para diretoria de Conformidade por e-mail. Se aprovada, ela irá solicitar à área de TI a gravação em meio magnético. As gravações só poderão ser reproduzidas para os clientes na dependência da FRENTE em caso de solicitação formal da Ouvidoria, Compliance ou Controles Internos, e não poderão ser enviadas a meios externos por e-mail ou gravadas em meio magnético a fim de retirada, salvo solicitação para fins de Auditoria, Fiscalização de Órgãos reguladores, ou por solicitação da justiça.

10.GESTÃO DE SEGURANÇA DA INFORMAÇÃO

A gestão de Segurança da Informação deverá garantir, por meio de seus processos, avaliações, controles, testes e treinamento, além de controles de Segurança Cibernética aplicados para prevenir, detectar e reagir aos ataques cibernéticos, conforme requeridos na legislação aplicável ao tema.

- Devem promover regras ou processos necessários para proteger o ambiente de TI.
- Garantir a segurança e a confidencialidade das informações de clientes, colaboradores e parceiros;
- Proteger contra ameaças ou riscos à segurança das informações;
- Proibir o acesso não autorizado ou o uso de informações que possam prejudicar os clientes, colaboradores e prestadores de serviços;
- Armazenar, transportar e descartar adequadamente informações de clientes, colaboradores e prestadores de serviços;
- Informar aos empregados sobre suas responsabilidades de proteger as informações de clientes e a segurança dos sistemas da FRENTE;
- Garantir que os prestadores de serviços cumpram com nossas políticas e normas de segurança da informação, bem como as obrigações regulamentares aplicáveis;
- Identificar os riscos à segurança da informação e promover programas de proteção tecnológica aos recursos de informação, incluindo aplicativos, infraestrutura e informações confidenciais e privadas relacionadas a clientes, colaboradores e prestadores de serviço.

REGISTRO, PROTEÇÃO E REVISÃO DE REGISTRO DE EVENTOS (“LOGS”)

Os sistemas, utilitários como gerenciador de banco de dados e outras ferramentas de gestão de rede, especialmente as que acessam dados em produção, geram registro de operações sensíveis feitas pelo Suporte/Gestão de Infraestrutura, e é fundamental que este "Log" seja mantido protegido de alteração e deleção. Deverá ser feita revisão periódica dos mesmos pela Gestão de Segurança da Informação, quer diretamente, quer usando rotina de extração de operações pontuais com software de extração e análise de dados.

REGRAS PARA MANUSEIO, TROCA E ARMAZENAMENTO DE DADOS

Não será permitido aos usuários extraírem diretamente informações sem que seja formalizado um pedido, devidamente justificado pelas necessidades funcionais do requisitante e aprovado pelo seu Gestor imediato, com cópia para a área de Conformidade para controle,. Para garantir que esta restrição seja efetiva, serão bloqueados os dispositivos de leitura e gravação USB e a capacidade de gravação de Unidades de CD e DVD. Exceções serão avaliadas pelo gestor do solicitante, pelo gestor da área de TI e de Conformidade.

11. REQUISITOS DE SEGURANÇA APLICÁVEIS AOS PROGRAMAS APLICATIVOS

Os sistemas aplicativos deverão conter módulos de Segurança responsável pela autenticação dos usuários, que para acessá-los e utilizá-los, deverão ser

cadastrados associados a perfis que reflitam as suas necessidades funcionais, a partir da aprovação do respectivo gestor do produto, processo ou área.

Na eventual falta de módulo de segurança, deverão ser definidos, caso a caso, controles compensatórios suficientes que permitam efetiva validação de que foi preservada a necessária segregação de funções no lançamento e manutenção de operações nos sistemas e no desenvolvimento de aplicativos internamente ou adquiridos no mercado.

CONTROLES DE MUDANÇAS, AMBIENTES (DESENVOLVIMENTO, HOMOLOGAÇÃO E PRODUÇÃO) E IMPLEMENTAÇÃO.

Os sistemas aplicativos devem ser mantidos em Ambientes de Rede diferentes para Testes de Homologação (congelado) e de Produção, devidamente segregados e protegidos, com acessos concedidos dependendo dos papéis e direitos de acesso diferenciados para movimentação entre ambientes. A formalização da autorização desses direitos e o registro de log de acessos e ações também serão realizados.

Será formalizado um processo de homologação e controles de versão, roll back e integração com o Plano de Continuidade de Negócios. Será requerido que sejam mantidos Manuais de Sistemas para garantia de entendimento de suas funcionalidades e adequada manutenção.

Será estabelecido um processo para alterações de requisitos de segurança para software houses, através de solicitação formal, incluindo a necessidade de

utilização de perfis de acesso e manutenção da requerida segregação de funções, usando grupos para seu gerenciamento. A definição de cadastramento e manutenção de perfis e grupos será segregada da associação destes perfis aos usuários cadastrados por TI.

TESTE DE SISTEMAS

Os sistemas aplicativos deverão ser objeto de testes de suas funcionalidades e capacidade de executar as operações previstas, quando criados ou modificados, de acordo com uma rotina padronizada, com planejamento e documentação. O tratamento de falhas de testes de sistemas será realizado, e os responsáveis pelas fases de testes deverão ser devidamente registrados e identificados para garantir a rastreabilidade dos seus resultados.

12. ANTIVÍRUS

Todos os servidores e estações de trabalho serão protegidos pela instalação de software Antivírus sob responsabilidade da Área de TI.

A atualização do software será feita nos menores intervalos possíveis, dependendo somente do possível impacto na disponibilidade e no processamento, para ser definido se será em tempo real ou em períodos definidos e monitorados por TI. Não será permitido a nenhum usuário desabilitar o uso ou desinstalar o software Antivírus.

Deve ser objeto de divulgação aos usuários as melhores práticas preventivas relativas a anexos e links de mensagens de e-mail que são fonte de risco de contaminação por vírus.

13. PLANO DE AÇÃO EM CASO DE INCIDENTES

Registro da análise da causa, do impacto e das medidas tomadas para incidentes relacionados à segurança cibernética.

AVALIAÇÃO DE INCIDENTES

Será realizada uma reunião com a equipe de Conformidade, Sistemas e Suporte, a fim de caracterizar o incidente, identificar os motivos e impactos imediatos, avaliar a gravidade da situação, desenvolver estratégias para combater as ameaças cibernéticas identificadas e definir um plano de ação.

COMUNICAÇÃO

Na ocorrência de um incidente, é imprescindível a comunicação imediata à equipe de Conformidade para que o plano de ação seja executado e as medidas sejam tomadas rapidamente. E quando aplicável, comunicar os respectivos órgãos, clientes ou colaboradores afetados.

PLANO DE AÇÃO

A área de Segurança da Informação é responsável pela implementação dos planos de ação e resposta aos incidentes em que ela está envolvida.

TRATAMENTO DE INCIDENTES

Após a identificação do incidente e a definição do plano de ação, este deverá ser estruturado de acordo com a gravidade do risco de segurança cibernética. As respectivas ações cabíveis a serem tomadas deverão receber as tratativas necessárias sob a gestão da área de Segurança da Informação.

RISCO DAS INFORMAÇÕES

É importante que as informações, conforme seu grau de confidencialidade, sejam tratadas e classificadas de maneira adequada e proporcional.

AVALIAÇÃO QUANTO À TRATATIVA AOS INCIDENTES

A área de Segurança da Informação deverá avaliar os impactos causados, bem como a eficiência das medidas de prevenção adotadas relacionada à Tecnologia. Já a área de Conformidade será acionada para verificar se os controles e seguranças estão sendo executados, se os procedimentos posteriores foram seguidos e se há a necessidade de acionar a Justiça.

14. INFORMAÇÕES TRATADAS PELA FRENTE CORRETORA

A FRENTE estimula que todos leiam com atenção esta Política de Privacidade.

Buscando facilitar o entendimento, o quadro a seguir resume as informações tratadas.

INFORMAÇÕES TRATADAS PELA FRENTE CORRETORA DE CÂMBIO	
DADOS PESSOAIS TRATADOS	A FRENTE utiliza os Dados Pessoais que os clientes e usuários diretamente fornecem, como, mas não limitado à: ▪ Dados cadastrais (nome, CPF, RG, profissão, CNH, estado civil, nacionalidade, data de nascimento, RNE, filiação, nº passaporte); ▪ Dados financeiros (dados bancários e dados de rendimentos); ▪ Dados de contato (telefones, e-mail, endereço, etc.); ▪ Perfil de cliente; ▪ Dados que são coletados automaticamente de dispositivos eletrônicos (IP, data e hora de utilização no website, etc.); ▪ Dados obtidos através de Terceiros ou bases públicas.

ARMAZENAMENTO DOS DADOS	Os Dados Pessoais serão acessados, alterados, divulgados ou excluídos apenas por aqueles autorizados a fazê-lo. Nos casos de eliminação pela FRENTE quando o objetivo que motivou a coleta deles for atingido, e os dados não forem mais necessários para cumprir qualquer obrigação legal, regulatória e/ou contratual, ou quando não forem mais necessários para resguardar os direitos dos clientes ou da empresa.
TRATAMENTO DOS DADOS	Os Dados Pessoais são utilizados para identificar, responder ou manter contato com o cliente, para realização de cadastro, manutenção de histórico de operações, realizar investigação de fraude, atendimento de políticas de segurança da FRENTE, para atendimento de obrigações do Branco Central, demandas judiciais, para cadastro e acesso nas Plataformas, entre outras finalidades.
COMPARTILHAMENTO DOS DADOS PESSOAIS	Os Dados Pessoais podem, conforme legislação específica e aplicada ao tema, ser compartilhados nos seguintes casos: 1) Consentimento; 2) Cumprimento de Obrigação Legal ou Regulatória pelo Controlador; 3) Execução de Contrato; 4) Exercício de Direitos em Processos; e 5) Interesses Legítimos do Controlador ou de Terceiro.
DIREITOS DO CLIENTE	O cliente pode solicitar a confirmação de existência de Tratamento de seus Dados Pessoais, acessar os dados tratados, solicitar correções, requerer a exclusão definitiva dos dados pessoais que tiver fornecido, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas na Lei.

EXERCÍCIO DO DIREITO	Os direitos do cliente poderão ser exercidos por meio do formulário para exercício de direitos dos titulares de Dados Pessoais, disponibilizado através do website da FRENTE através de: https://frentecorretora.com.br/contato/.

15. INFORMAÇÕES TRATADAS

A depender da relação que o cliente ou usuário possua com a FRENTE e empresas do grupo, podem ser realizada a coleta de diferentes categorias de Dados Pessoais, tais quais:

- Informações que identificam o cliente ou o tornam identificável, incluindo, por exemplo, o seu nome, RG, CPF, CNH, estado civil, profissão, nacionalidade, data de nascimento, filiação, RNE, passaporte;
- Informações que auxiliem a empresa a contatá-lo, como endereço postal, CEP, telefone fixo ou celular, e-mail, etc.;
- Informações financeiras, como dados bancários, dados de rendimentos etc.;
- Informações comportamentais, como perfil de consumo ou hábitos de navegação online;
- Atributos associados aos dispositivos eletrônicos do cliente, como endereço de IP, fontes instaladas, idioma, configurações do navegador e fuso horário;

- Informações proveniente de Terceiros, como identificadores de contas bancárias,informações de rendimentos, certidões de óbito etc.

16. DADOS PESSOAIS COLETADOS

Os Dados Pessoais que a Frente possui podem ser coletados e tratados, para as finalidades abaixo indicadas:

- Quando o titular autoriza;
- Identificação e qualificação do titular;
- Verificação da adequação de produtos e serviços ao perfil do titular e oferta a estes de produtos e serviços;
- Apresentação de propostas, contratação e cumprimento de contratos;
- Avaliação e acompanhamento de situação econômico-financeira;
- Cumprimento de obrigações legais, regulatórias e de autorregulação;
- Exercício regular de direitos; e
- Prevenção e identificação de fraudes e identificação, prevenção e gerenciamento de riscos à segurança.

Quando necessário para atender aos interesses legítimos do Controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

17. UTILIZAÇÃO DAS INFORMAÇÕES

A FRENTE trata os dados pessoais para finalidades diversas. Sendo as principais:

ATENDER A FINALIDADE PARA A QUAL O DADO FOI FORNECIDO

Os dados fornecidos podem ser utilizados com propósitos informados pelo cliente no momento da coleta das informações e para outras finalidades que sejam compatíveis.

Por exemplo, para identificação, responder ou manter contato com o cliente, administrar o histórico de operações, realizar investigações de fraude, atender às políticas de segurança da FRENTE, para atendimento de obrigações do Branco Central, demandas judiciais, para cadastro e acesso nas Plataformas, entre outras finalidades.

Os Dados Pessoais ainda podem ser utilizados para fins publicitários.

CUMPRIR COM OBRIGAÇÕES LEGAIS OU REGULATÓRIAS

Os Dados Pessoais poderão ser utilizados para atender obrigações previstas em lei, em regulações de órgãos governamentais ou de autoridades fiscais, pelo Poder Judiciário e/ou por outra autoridade competente.

A depender da obrigação, este tratamento poderá incluir os dados de identificação, documentos pessoais, dados financeiros e de rendimentos, por

exemplo, para comunicações obrigatórias ao Banco Central e demais órgão reguladores e governamentais.

18. UTILIZAÇÃO DAS INFORMAÇÕES

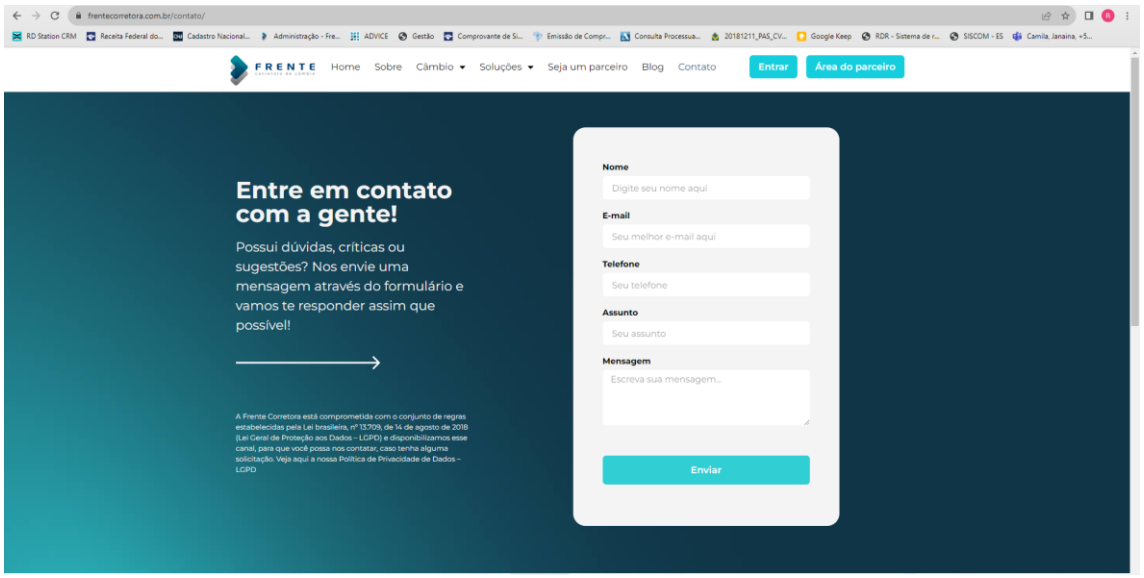
Durante vigência e até mesmo após o término da relação contratual, a FRENTE poderá tratar dados pessoais dos clientes e usuários nas situações descrita abaixo:

- **FORÇA DE LEI**

Para exercer seus direitos garantidos em lei e/ou regulamentação dos órgãos governamentais, inclusive como prova em processos judiciais, administrativos ou arbitrais.

- **AUTORIZAÇÃO DO CLIENTE**

Mediante autorização do cliente para utilização de seus dados. Caso o cliente se sinta incomodado e não deseje mais receber quaisquer contatos, é possível, a qualquer momento, contatar a FRENTE por meio do formulário disponível no website: https://frentecorretora.com.br/contato/ demonstrado abaixo, manifestando sua vontade para tal.



19. EXCLUSÃO DOS DADOS EM DEFINITIVO

O cliente pode requerer a exclusão definitiva dos dados pessoais que tiver fornecido à FRENTE, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas em Lei.

EVITAR FRAUDES E ZELAR PELA SEGURANÇA DO CLIENTE

Por fim, a FRENTE também trata os dados para comprovar que o cliente é realmente quem diz ser e, assim, evitando fraudes.

20. COOKIES

Cookies são arquivos de texto que podem ser armazenados nos dispositivos eletrônicos, quando o cliente visita um website ou utiliza um serviço online. Essa é uma prática comum de uso da internet, dado que ela ajuda aos websites a funcionarem de forma correta, além de otimizar a experiência do usuário no website.

A FRENTE utiliza cookies para diferentes finalidades, como para contar quantos visitantes recebe no seu website, possibilitar que o cliente e usuário navegue de forma personalizada para lembrar as configurações de anúncios, etc.

Todas estas finalidades podem ser agregadas em quatro categorias, conforme exposto:

TIPOS	FUNÇÕES
NECESSÁRIOS	Essenciais para viabilizar o adequado funcionamento do website, assim como para permitir que o cliente faça uso de todas as funcionalidades disponíveis.
DESEMPENHO	Ajudam a entender como os visitantes interagem com o website, fornecendo informações sobre as áreas visitadas, o tempo de visita ao site e quaisquer problemas eventualmente são encontrados.

FUNCIONAIS	Permitem que o website se lembre das escolhas anteriores, como, por exemplo idioma de navegação. Além de proporcionar uma experiência personaliza, esses cookies possibilitam que o cliente preencha campos para comentários, dentre outros.
MARKETING	Fornecem mais conteúdos relevantes e específicos para os interesses do cliente . Podem, ainda, ser utilizados para apresentar publicidade com um maior direcionamento ou limitar o número que esta é veiculada. Também, permitem a medição da eficácia de uma campanha publicitária lançada.

Destacamos que os cookies necessários são essenciais para o normal funcionamento do Website e demais Plataformas, sendo que a oposição à utilização desta ferramenta poderá implicar na inutilização dos serviços disponíveis ou na suspensão do acesso.

21. SEGURANÇA DOS DADOS

A segurança das informações pessoais dos clientes é uma prioridade. Por isso, a FRENTE dispõe de políticas e procedimentos internos que determinam como os Dados Pessoais devem ser tratados pela empresa.

A FRENTE adota medidas técnicas aptas a manter os dados pessoais seguros e protegidos de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer outra forma de

tratamento inadequado ou ilícito, sempre à luz das regras aplicáveis de proteção de dados e segurança da informação.

As principais medidas adotadas são:

- Controle estrito do tratamento de dados pessoais, incluindo limitação de acesso;
- Mecanismos de autenticação de acesso, incluindo senhas e sistemas de dupla autenticação, quando cabível, que asseguram a individualização dos registros;
- Inventário detalhado dos registros de conexão, incluindo o momento, a duração, a identidade do responsável e o arquivo acessado;
- Soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, incluindo encriptação ou medidas de proteção equivalentes, sem prejuízo da adoção de outros padrões técnicos posteriormente estipulados pelas autoridades competentes; e
- Treinamentos periódicos de funcionários e colaboradores, quanto ao tratamento de dados pessoais.

22. DIREITOS E PRERROGATIVAS DO CLIENTE

- Corrigir dados incompletos, inexatos ou desatualizados, pelos meios exigidos pela regulamentação específica, quando necessário;

- Solicitar a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou que, por ventura, tenham sido tratados em desconformidade com a lei;
- Solicitar a portabilidade dos dados a outro fornecedor de serviço ou produto, caso isso seja feito expressamente;
- Solicitar a eliminação dos dados tratados com o consentimento dele; e
- Obter informações sobre as entidades públicas ou privadas com as quais foram compartilhados seus dados.

Quando a atividade de tratamento necessitar do consentimento do cliente, ele pode se negar a consentir. Nesse caso, a FRENTE informará sobre as consequências da não realização de tal atividade. Caso seja consentido, a qualquer momento o cliente poderá revogá-lo.

O cliente poderá exercer os seus direitos por meio do formulário para exercício de direitos dos titulares de dados pessoais, disponibilizado no website: https://frentecorretora.com.br/contato/

Quando isso não for possível, o cliente e usuário poderá recorrer ao encarregado pela proteção de dados pessoais, cujo contato está disponibilizado ao final desta Política.

Informações do encarregado pela proteção de dados pessoais

Nome: Ricardo Baraçal

E-mail: compliance@frentecorretora.com.br