POLÍTICA DE SEGURANÇA DA INFORMAÇÃO
FRONTEIRA GESTÃO DE INVESTIMENTOS

Março de 2019

Objetivo

A Política de Segurança da Informação da Fronteira Gestão de Investimentos Ltda. ("Fronteira" e "Política") estabelece diretrizes, mecanismos e procedimentos a serem observados pelos administradores, empregados e colaboradores da Fronteira (as "Pessoas da Fronteira") visando garantir o resguardo de informações obtidas no exercício de suas funções na Fronteira, estabelecendo mecanismos para:

I. Propiciar o controle de informações confidenciais, reservadas ou privilegiadas a que tenham acesso os seus sócios, diretores, administradores, profissionais e terceiros contratados;
II. Assegurar a existência de testes periódicos de segurança para os sistemas de informações, em especial para os mantidos em meio eletrônico, bem como assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação; e
III. Implantar e manter treinamento para os seus sócios, diretores, alta administração e profissionais que tenham acesso a informações confidenciais, reservadas ou privilegiadas e participem do processo de decisão de investimento.

Regra Fundamental

As Pessoas da Fronteira são obrigadas a empregar o devido cuidado ao receber, lidar e armazenar dados no exercício de suas funções, bem como a aderir aos padrões e procedimentos de segurança de dados pré-definidos para evitar o acesso, uso, modificação ou destruição não autorizados.

Qualquer informação obtida em decorrência da atividade profissional exercida na Fronteira não pode ser divulgada, em hipótese alguma, a terceiros que não se enquadrem no conceito de Pessoas da Fronteira ou não estejam autorizados, até que tenha sido divulgada publicamente, garantindo-se, desta forma, a confidencialidade das informações. São exemplos de informações confidenciais protegidas no âmbito desta Política: relatórios, documentos, e-mails, análises sobre ativos financeiros e/ou valores mobiliários, negócios (potenciais ou em processo de negociação), posições compradas e/ou vendidas da Fronteira e/ou de seus clientes ("Clientes"), dados cadastrais dos Clientes, entre outras de natureza semelhante.

Procedimentos – regras de acesso às informações confidenciais, reservadas ou privilegiadas

Todas as informações devem ser classificadas conforme sua necessidade de confidencialidade, integridade e disponibilidade, de acordo com as necessidades comerciais e quaisquer exigências e restrições contratuais ou regulatórias. Uma determinada informação deverá receber o mesmo nível de segurança em toda Fronteira.

Os empregados da Fronteira devem ter acesso apenas às informações ou funcionalidades necessárias ao desempenho adequado de suas funções. O acesso às informações deve ser explicitamente autorizado, sendo que a regra será a de "não acesso".

Barreiras de Informação

Barreiras de Informação são procedimentos usados para garantir que as informações confidenciais sejam comunicadas apenas às Pessoas da Fronteira que tenham necessidade legítima de saber ou ter acesso a tais informações ("política *need to know"*).

As Pessoas da Fronteira não poderão utilizar informações confidenciais para qualquer finalidade que não aquela originalmente pretendida e estritamente de acordo com as **Políticas de Controles Internos da Fronteira**, bem como com as leis, normas e regulamentos aplicáveis.

As Pessoas da Fronteira que receberem informações confidenciais acidentalmente ou que passarem informações confidenciais importantes inadvertidamente, deverão comunicar esse fato o quanto antes ao responsável pelo Departamento de *Compliance*, Jurídico e Controles Internos da Fronteira.

Acesso Restrito

Os computadores, arquivos (físicos e virtuais) e e-mails utilizados pelos profissionais de cada área da Fronteira são acessados por meio de senhas pessoais de acesso para controlar e permitir a identificação dos usuários do sistema. Bem assim, os arquivos (pastas) do sistema possuem restrições de acesso, conforme permissão individual das Pessoas da Fronteira. Nesse sentido, nos casos de mudança de atividade de qualquer Pessoa da Fronteira, dentro da Fronteira, as regras de acesso deverão ser prontamente atualizadas, conforme necessidade. Da mesma forma, na hipótese de desligamento de qualquer Pessoa da Fronteira, o acesso aos dados da Fronteira devem ser imediatamente interrompidos, mediante cancelamento de senhas e bloqueio de e-mails e acesso aos sistemas, documentos e dependências da Fronteira.

Os procedimentos de cruzamento de Barreiras de Informação também são usados para controlar o fluxo de informações confidenciais. O "cruzamento" de uma Barreira de Informação poderá ocorrer quando informações confidenciais residentes em um lado da Barreira de Informação precisam ser compartilhadas com Pessoa da Fronteira residente do outro lado da barreira (*e.g.* entre diversos departamentos). Isso só pode ocorrer quando houver necessidade comercial legítima para ter acesso a tais informações e somente mediante a aprovação dos diretores da Fronteira.

Antes de aprovar o cruzamento de uma Barreira de Informações por uma Pessoa da Fronteira, os seguintes pontos devem ser considerados:

(i) Esse é o momento adequado (por exemplo, depois do fechamento do mercado no dia anterior ao anúncio)?
(ii) Há outras normas ou regulamentações locais mais restritivas que devem ser observadas, conforme informado pelo Departamento de *Compliance*, Jurídico e Controles Internos?
(iii) As informações confidenciais em questão estão limitadas àqueles que necessitam ter conhecimento das mesmas para cumprir uma necessidade legítima (princípio *need to know*)
(iv) O efeito de fazer uma Pessoa da Fronteira cruzar um Barreira de Informação com relação às suas responsabilidades comerciais individuais e atividades diárias foi levado em consideração (potencial conflito de interesses)?
(v) Foi levado em consideração o fato de a informação fornecida provavelmente se tornar ou não pública imediatamente?

Com relação ao cruzamento de Barreiras de Informação, o Departamento de *Compliance*, Jurídico e Controles Internos deve estar envolvido de forma que sejam tomadas as medidas adequadas. A Pessoa da Fronteira que está detrás de uma Barreira de Informação será notificada sobre o cruzamento da Barreira de Informação e também sobre o momento em que tal cruzamento deverá ser encerrado.

Nenhum cruzamento de Barreira de Informação poderá ocorrer até:

a) a aprovação dos diretores da Fronteira; e
b) que tal aprovação tenha sido comunicada por escrito ao Departamento de *Compliance*, Jurídico e Controles Internos.

Se qualquer diretor da Fronteira tiver qualquer dúvida quanto à adequabilidade ou o momento do cruzamento, ele deverá consultar o Departamento de *Compliance*, Jurídico e Controles Internos. O Departamento de *Compliance*, Jurídico e Controles Internos poderá ser contrário a qualquer cruzamento. Departamento de *Compliance*, Jurídico e Controles Internos irá registrar as pessoas físicas que tiverem cruzado uma Barreira de Informação e realizará seu acompanhamento, conforme adequado.

Segurança Cibernética

Dada a relevância que os dados, de seus clientes e/ou produzidos pelas Pessoas da Fronteira, representam para Fronteira e que grande parte destes dados são mantidos em meio eletrônico, passíveis de ameaças cibernéticas, a Fronteira decidiu estabelecer Programa de Segurança Cibernética para identificar e mitigar riscos cibernéticos, assim como para recuperação de possíveis incidentes ("Programa").

Identificação de Riscos. O primeiro elemento do Programa é a identificação dos ativos de *hardware* e *software* que precisam de proteção na Fronteira em função dos riscos, internos e externos, decorrentes de ataques cibernéticos. Nesse sentido, foi identificado que os ativos mais importantes da Fronteira são as informações confidenciais que se tem acesso no desenvolvimento de suas atividades. Portanto, foi determinado que precisam de proteção os dados armazenados no servidor da Fronteira, passíveis de danos em decorrência dos riscos de *malwares* (*softwares d*esenvolvidos para corromper computadores e redes), que abrangem, entre outros:

a) vírus: *software* que causa danos a máquina, rede, *softwares* e banco de dados;
b) cavalo de troia: aparece dentro de outro *software* e cria uma porta para a invasão do computador;
c) *spyware*: *software* para coletar e monitorar o uso de informações; e
d) *ransomware*: *software* malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido.

Além dos riscos operacionais, que podem inclusive inviabilizar o funcionamento da Fronteira, tais como *ransomwares*, eventuais ataques podem gerar consequência significativas em termos de risco de imagem e danos financeiros, para Fronteira e/ou para as Pessoas da Fronteira.

Prevenção e Proteção. Identificado o principal risco cibernético a que se submete a Fronteira, as seguintes medidas são adotadas visando mitigar e minimizar sua concretização:

1. **Restrição de Acesso Físico**: A sala em que são localizados os computadores e servidor da Fronteira somente pode ser acessada por meio de sistema biométrico de acesso, restrito às Pessoas da Fronteira;
2. **Restrição de Acesso Técnico**: Os computadores, arquivos (virtuais) e e-mails utilizados pelos profissionais de cada área da Fronteira são acessados por meio de senhas pessoais de acesso (sujeitas a regras mínimas na definição de senhas de acesso) para controlar e permitir a identificação dos usuários do sistema;

3. **Armazenamento de Informações e Back-Up:** Além do armazenamento em servidor próprio, a Fronteira utiliza o Google Drive para fins armazenamento de arquivos de documentos relativos às suas atividades. Todas as Pessoas da Fronteira tem acesso ao Google Drive, sendo certo que algumas das pastas tem acesso restrito, como forma de Barreira de Informação. Ademais, a Fronteira possui sistema de HD externo remoto, no qual periodicamente (mensalmente) é realizado o arquivamento dos arquivos constantes no Google Drive, para fins de *back up*.
4. **Serviços de Segurança da Informação**: contratação de recursos anti-malware em estações e servidores de rede, como antivírus e firewalls pessoais.
5. **Restrição do acesso a sites e instalação de softwares**: os equipamentos da Fronteira impedem a instalação e execução de software e aplicações não autorizadas por meio de controles de execução de processos, bem como a sites na internet com potencial para danificar os sistemas da Fronteira.

Monitoramento e testes. Tendo em vista identificar se as medidas de proteção e prevenção listadas acima estão sendo capazes de mitigar os riscos cibernéticos a que se submete a Fronteira, o Departamento de Compliance, Jurídico e Controles Internos da Fronteira deverá:

(i) manter os sistemas operacionais e softwares de aplicação sempre atualizados, instalando as atualizações sempre que forem disponibilizadas.
(ii) deve-se monitorar as rotinas de backup, executando testes mensais de restauração dos dados, especialmente para garantir a manutenção das informações mantidas em meios eletrônicos; e
(iii) deverá contratar empresa especializada e suporte de Tecnologia da Informação, a qual deve realizar, em periodicidade pelo menos trimestral, testes de invasão externa e phishing, bem como a análise de vulnerabilidades na estrutura tecnológica da Fronteira, sugerindo melhorias, quando aplicável.

Plano de Resposta e Atualizações do Programa de Segurança Cibernético.

As áreas responsáveis pelo Programa de Segurança Cibernético da Fronteira são o Departamento de Administração de Valores Mobiliários, Departamento de Gestão de Riscos e Departamento de *Compliance*, Jurídico e Controles Internos, representados pelos respectivos Diretores, os quais deverão se reuniar anualmente, no mês de janeiro, para rever os riscos e práticas elencadas acima. Não obstante, o Diretor de Compliance, Jurídico e Controles Internos é o responsável, interna e externamente, pelas questões de segurança cibernética da Fronteira.

Na eventualidade da concretização de um ataque cibernético, os Diretores das áreas responsáveis pelo Programa de Segurança Cibernético da Fronteira deverão se reunir para definir as medidas a serem adotadas visando interromper o ataque cibernético sofrido e minimizar os seus efeitos e danos à Fronteira.

Política de Utilização de E-mail Corporativo

Os sistemas de e-mail corporativo tornaram-se ferramenta imprescindível no processo de formalização de atividades e complementação de informações visando aumentar a agilidade dos procedimentos internos e na obtenção de vantagens competitivas para assegurar maior rapidez e eficiência na concretização de negócios.

A Fronteira considera que os recursos oferecidos pelo ambiente de correio eletrônico ampliam grandemente a eficácia e a agilidade de seus procedimentos negociais destacando que, devido à sua flexibilidade, requer uma política de utilização específica, dentro das seguintes definições:

- Todas as Pessoas da Fronteira utilizarão seu endereço de e-mail corporativo exclusivamente para finalidades que envolvam os processos e/ou atividades de ordem profissional; e

- Devido ao fato do e-mail corporativo carregar a identificação da Fronteira, nenhum usuário poderá utilizar o e-mail para fins particulares ou ainda utilizar o e-mail para transferir ou endereçar informações de caráter duvidoso ou com possível conteúdo pornográfico;

Treinamento e Confidencialidade

Todas as Pessoas da Fronteira são obrigadas participar dos treinamentos específicos referentes às Barreiras de Informação e à confidencialidade das informações a serem ministrados nos termos previstos nas regras de Controles Internos da Fronteira.

As Pessoas da Fronteira assinarão, no momento de seu ingresso na Fronteira, Declaração de ciência e conformidade aos termos dessa Política, inclusive no que se refere à confidencialidade sobre as informações reservadas, privilegiadas ou confidenciais que lhes tenham sido confiadas em virtude do exercício de suas atividades profissionais, excetuadas as hipóteses permitidas em lei, nos termos do anexo A do Código de Ética da Fronteira.

Igualmente, os terceiros contratados pela Fronteira, que tiverem acesso às informações confidenciais, reservadas ou privilegiadas que lhes tenham sido confiadas no exercício de suas atividades, devem assinar Declaração de ciência e conformidade aos termos dessa Política, podendo tal documento ser excepcionado quando o contrato de prestação de serviço possuir cláusula de confidencialidade.

* * * * *