PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

PROCEDIMENTOS DE SEGURANÇA

DA INFORMAÇÃO

VERSÃO ATUALIZADA – OUTUBRO/2022

ÍNDICE

1. OBJETIVO

A SFI INVESTIMENTOS LTDA ("SFI"), baseada na norma NBR ISO/IEC 27.002 e na Lei nº 13.709, de 14 de agosto de 2018 ("Lei Geral de Proteção de Dados" ou "LGPD"), definiu sua Política de Segurança da Informação ("Política"), estabelecendo as normas e procedimentos necessários para a continuidade dos seus negócios e proteção da confidencialidade das informações.

A presente Política tem por objetivo estabelecer as regras de boas práticas de Tratamento de Dados, determinar as medidas de segurança, técnicas e administrativas para proteger os Dados Pessoais dos clientes, e, ainda, garantir a confidencialidade, integridade e proteção das informações da SFI. Outrossim, visa proteger os Dados e informações da SFI contra acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Os recursos da tecnologia de informação disponibilizados pela SFI são destinados exclusivamente às atividades operacionais da instituição.

A SFI entende que o sistema de segurança adotado atingirá sua eficácia com o comprometimento e a cooperação de todos os profissionais envolvidos nos processos: colaboradores da SFI e Equipe de Tecnologia de Informação ("**ETI**").

Os programas homologados e instalados nos computadores e nos servidores de rede são propriedade exclusiva da SFI, sendo vedada sua cópia parcial ou integral.

2. DEFINIÇÕES

2.1. Segurança da Informação – diz respeito à proteção de determinados dados, com a intenção de preservar seus respectivos valores para uma organização (empresa) ou um indivíduo.

Podemos entender como informação todo o conteúdo ou dado valioso para um indivíduo/organização, que consiste em qualquer conteúdo com capacidade de armazenamento ou transferência, que serve a determinado propósito e que é de utilidade do ser humano.

Atualmente, a informação digital é um dos principais produtos de nossa era e necessita ser convenientemente protegida. A segurança de determinadas informações pode ser afetada por

vários fatores, como os comportamentais e do usuário, pelo ambiente/infraestrutura em que ela se encontra e por pessoas que têm o objetivo de roubar, destruir ou modificar essas informações.

Confidencialidade, disponibilidade e integridade são algumas das características básicas da segurança da informação, e podem ser consideradas até mesmo atributos.

2.2. Tecnologia da Informação – conjunto de todas as atividades e soluções providas por recursos de computação que visam a produção, o armazenamento, a transmissão, o acesso, a segurança e o uso das informações. Na verdade, as aplicações para TI são tantas — e estão ligadas a tantas áreas — que há diversas definições para a expressão e nenhuma delas consegue determiná-la por completo. É a área da informática que trata a informação, a organização e a classificação de forma a permitir a tomada de decisão em prol de algum objetivo. A tecnologia da informação pode contribuir para alargar ou reduzir as liberdades privadas e públicas ou tornar-se um instrumento de dominação.

TI refere-se, de modo geral, à coleção de recursos de informação de uma organização, seus usuários e a gerência que os supervisiona, inclusive a infraestrutura de TI e todos os outros sistemas de informação em uma organização.

3. RESPONSABILIDADES E COMPETÊNCIAS

3.1. Da Diretoria de Risco e Compliance - DRCO

3.1.1. Definir e divulgar as medidas de Segurança da Informação;

3.1.2. Orientar e educar os funcionários sobre os preceitos atinentes à Segurança da Informação, bem como lhes assegurar treinamento para o uso correto dos recursos, visando evitar falhas e danos ao funcionamento dos sistemas informatizados;

3.1.3. Informar à empresa terceirizada de TI sobre acesso de novos usuários aos sistemas de informação, bem como atualizar nos sistemas as funções nas áreas de atuação;

3.1.4. Advertir formalmente e aplicar as sanções cabíveis quando o colaborador violar os princípios ou procedimentos de segurança;

3.1.5. Aprovar a solicitação de compra ou alteração de hardware e software, eventualmente indicados pela empresa terceirizada de TI.

3.2. De todos os colaboradores

3.2.1. Responder pela guarda e proteção dos recursos computacionais colocados à sua disposição para fins laborais;

3.2.2. Responder pelo uso exclusivo e intransferível de suas senhas de acesso;

3.2.3. Adquirir conhecimento técnico necessário para a correta utilização dos recursos de informática;

3.2.4. Relatar prontamente à DRCO qualquer fato ou ameaça à segurança dos recursos, como quebra da segurança, fragilidade, mau funcionamento, vírus, acesso indevido ou desnecessário a pastas/diretórios de rede, acesso indevido à Internet, programas instalados sem autorização etc.;

3.2.5. Assegurar que as informações e dados de propriedade da SFI não sejam disponibilizados a terceiros, a não ser com autorização por escrito;

3.2.6. Manter, obrigatoriamente, os dados críticos da empresa nos servidores de redes;

3.2.7. Relatar à DRCO a possibilidade de instalação de um novo software ou aquisição de novo hardware para a melhoria dos serviços prestados.

4. REGRAS DE UTILIZAÇÃO DE CONTAS E SENHAS DA REDE CORPORATIVA

4.1. Todos os usuários da rede de dados corporativa da SFI receberão login e senha individual exclusivos para sua utilização. É importante que os usuários não utilizem senhas de fácil identificação, tais como: data de nascimento próprio ou de parentes próximos, nomes próprios, datas comemorativas nacionais ou pessoais, iniciais de nomes próprios, números de telefones etc.

4.2. As senhas de acesso são pessoais, intransferíveis e não devem, em hipótese nenhuma, ser emprestadas ou compartilhadas com terceiros.

4.3. Não é permitida a utilização de computadores da rede sem senha ou com acesso local.

4.4. As senhas deverão ser alteradas pelo usuário, através de procedimento eletrônico e automático, utilizando o sistema de alteração de senhas disponível.

4.5. No caso do colaborador ser desligado da empresa, suas contas serão bloqueadas imediatamente, assim como suas senhas de acesso a qualquer recurso da rede ou sistemas.

4.6. Reserva-se a SFI o direito de auditar a utilização de contas de rede e sistemas fornecidos aos usuários de sua rede coorporativa, sem que se caracterize invasão de privacidade.

4.7. O acesso aos Dados Pessoais dos clientes da SFI será restrito e limitado ao estritamente necessário para o cumprimento da finalidade do Tratamento, de forma que somente os profissionais essenciais à função de administração de carteiras poderão ter o acesso permitido pela Diretoria de Risco e Compliance – DRCO.

4.8. O acesso de usuários desligados da SFI deve ser revogado imediatamente no momento da comunicação do desligamento realizado pelo Departamento de Recursos Humanos. A revogação de acesso deve ser registrada de modo que seja possível determinar a data da ocorrência, os usuários afetados, assim como os privilégios revogados.

4.9. As credenciais de acesso dos usuários que encerraram suas atividades na SFI não devem ser removidas das bases cadastrais, mas devem ser bloqueadas de forma que não seja possível utilizá-las. Devem ser mantidos registros que permitam identificar os usuários responsáveis pelas ações realizadas por meio das credenciais de acesso, mesmo depois de bloqueadas.

5. REGRAS PARA UTILIZAÇÃO DA REDE CORPORATIVA

5.1. Todos os recursos de rede de computadores deverão ser utilizados exclusivamente para fins profissionais, que envolvam atividades relacionadas ao bom andamento dos serviços e processos da SFI.

5.2. Todos os computadores da SFI devem ter antivírus instalado e atualizado periodicamente, é proibido desinstalar e utilizar computadores sem antivírus instalado.

5.3. É expressamente vedado aos usuários a instalação ou remoção de programas de computador, componente e periféricos sem prévia autorização e ciência da DRCO.

5.4. É proibido aos usuários conectar computadores pessoais ou de terceiros à rede coorporativa da SFI, exceto a utilização de notebooks e outros equipamentos portáteis através da rede sem fio "WiFi".

5.5. Os computadores e quaisquer sistemas da SFI que estejam em uso remoto por parte dos colaboradores deverão ser bloqueados por senha quando não estiverem sendo utilizados.

6. REGRAS PARA UTILIZAÇÃO DO CORREIO ELETRÔNICO (E-MAIL)

6.1. A SFI fornecerá, a seu critério, contas de correio eletrônico (@sfiinvestimentos.com.br) aos seus colaboradores. As mensagens de correio eletrônico (e-mails) internos e externos devem ser exclusivamente de caráter profissional, sendo proibido qualquer tipo de utilização particular. Isso vale para arquivos anexos.

6.2. É proibido configurar e/ou manter configuradas contas de correio eletrônico de servidores externos, isto é, diferentes de (@sfiinvestimentos.com.br), nos programas gerenciadores de correio eletrônico instalados em computadores da SFI.

6.3. O conteúdo das mensagens enviadas através de contas de correio da SFI (@sfiinvestimentos.com.br) é de inteira responsabilidade do usuário que utiliza a conta e que possui a senha com acesso exclusivo à caixa postal e para envio de mensagens.

6.4. É proibida a utilização do e-mail corporativo para fins ilegais, transmissão de material de qualquer forma censurável, que viole direitos de terceiros e leis aplicáveis.

6.5. É proibida a utilização de e-mail para transmitir mensagens conhecidas como Spam, JunkMail, correntes ou a distribuição de mensagens em massa não solicitadas.

6.6. É terminantemente proibido aos representantes da empresa terceirizada de TI, administradores de rede e/ou correio eletrônico, ler mensagens de correio eletrônico de qualquer usuário quando estiver realizando serviços de manutenção e suporte, exceto quando em cumprimento de determinações da Diretoria da SFI para efeitos de auditoria.

6.7. Reserva-se a SFI o direito de auditar a utilização de suas contas de correio eletrônico (@sfiinvestimentos.com.br) fornecidas aos usuários, sem que se caracterize invasão de privacidade.

7. REGRAS PARA UTILIZAÇÃO DA INTERNET

7.1. O acesso à Internet é disponibilizado aos colaboradores da SFI para viabilizar a busca de informações ou agilizar determinados processos exclusivamente necessários ao desenvolvimento dos trabalhos necessários à instituição.

7.2. Os usuários são responsáveis pela utilização da Internet em computadores acessados com seu login e senha. Ao se afastar do computador, o colaborador deverá encerrar a sessão através de "logoff", reiniciar ou desligar o sistema.

7.3. É proibido aos usuários configurar ou alterar as configurações de rede e de acesso à Internet dos computadores da SFI, incluindo as seguintes configurações de rede: IP, DNS, WINS, Gateway, Proxy e a instalação ou reconfiguração de clientes Proxy.

7.4. Não é permitido enviar, baixar (download) ou manter arquivos de imagens, músicas, vídeo, arquivos executáveis em geral ou quaisquer outros de caráter pessoal nas estações de trabalho da SFI.

7.5. É proibido o acesso a sites de relacionamento em geral, como Facebook, Twitter, e outros, a não ser para assuntos exclusivos ao desenvolvimento de atividades necessárias à SFI.

7.6. Não é permitido o acesso a sites de Internet com conteúdo pornográfico, jogos, bate-papo, *chat*, *blogger*, *cartoon*, relacionamento, música, *hacker* ou que contenha ferramentas ou regras para invasões de rede, quebra de criptografia, senhas ou outros eventos de segurança.

7.7. É proibido o acesso a sites, a instalação e a utilização de programas de troca de mensagens instantâneas ou arquivos do tipo: Whatsapp, Facebook Messenger, ICQ, MSN Messenger, Yahoo Messenger, Bittorrent, Imesh, AudioGalaxy, AIM, Morpheus, Kaaza, Emule, Napster e outros.

7.8. Sempre que os usuários, utilizando o Internet, tiverem acesso a materiais criminosos como pornografia infantil (arte, textos, figuras, cenas, imagens) e outros, mesmo que de maneira esporádica e involuntária, deverão entrar em contato imediatamente com a DRCO para relatar o fato ocorrido.

8. REGRAS PARA UTILIZAÇÃO DA REDE SEM FIO (WIFI)

8.1. Usuários autorizados poderão conectar computadores ou outros equipamentos portáteis e pessoais a Internet, utilizando a rede sem fio ("**WiFi**") da SFI.

8.2. O acesso à internet através da rede WiFi poderá ser controlado com a realização de auditorias nas páginas consultadas à critério da SFI.

8.3. Os usuários são responsáveis pela utilização da internet através da rede WiFi da SFI, e serão identificados e responsabilizados em caso de acesso indevido.

9. CONTROLE E RESTRIÇÃO DE USO DE MÍDIAS REMOVÍVEIS/PORTAS USB

9.1. A SFI bloqueia por padrão em todas as estações de trabalho o uso de mídias removíveis.

Quando necessário a utilização de mídias removíeis, o usuário deve abrir uma solicitação para o departamento de infraestrutura via canal de chamados (ServiceDesk), que irá solicitar aprovações necessárias para liberação temporária do recurso para o usuário específico.

10. CLASSIFICAÇÃO DA INFORMAÇÃO

10.1. O gestor de cada área deve estabelecer os critérios relativos ao nível de confidencialidade da informação gerada por sua área e classificá-las em Pública, Confidencial, Restrita ou Interna. Os dados e documentos de cunho estritamente financeiro e pessoal dos clientes, à exceção daqueles que sejam de conhecimento e domínio público, sempre serão classificados como confidenciais e restritos, recebendo tratamento especial de proteção à confidencialidade.

10.2. O processo de classificação da informação deve iniciar com a definição do grau de proteção necessário, com base nos quatro níveis de sigilo a seguir definidos:

10.3.

CONFIDENCIAL: Informação sensível que deve ser mantida em confidencialidade e manuseada apenas por pessoas autorizadas. O vazamento de informações com essa classificação gera impacto para a empresa e o negócio como um todo.

RESTRITA: Informação cujo acesso e manuseio são apenas para pessoas autorizadas. Caso sejam divulgadas erroneamente, afetam a continuidade de um ou mais processos de negócio da empresa. O vazamento de informações com essa classificação gera impacto para uma ou mais áreas da empresa.

INTERNA: Informação com baixa sensibilidade, mas que só deve circular internamente, não sendo de acesso público.

PÚBLICA: Informação que pode ser de conhecimento público e não possui restrições de divulgação.

11. DESCARTE DE MÍDIAS E DADOS

11.1. Mídias contendo informações referentes à SFI deverão ser destruídas antes de seu descarte.

11.2. CD's, DVD's, e documentos em papel deverão passar pelo triturador antes de serem encaminhadas ao lixo. HD's deverão ser encaminhados a TI para a destruição da informação antes do descarte ou reutilização.

11.3. Os dados armazenados na Base de Dados da SFI serão descartados em caso de ordem específica dos órgãos internos competentes ou em caso de término da relação contratual da SFI com os seus prestadores de serviço e colaboradores.

12. PENALIDADES

12.1. A SFI alerta todos os usuários que a instalação ou utilização de software não autorizados constitui crime contra a propriedade intelectual, de acordo com a Lei 9.609 de 19/02/98, sujeitando os infratores à pena de detenção e multa.

12.2. Todos os usuários são responsáveis pelo uso correto das ferramentas eletrônicas disponibilizadas.

12.3. Todas as práticas, que representam ameaça à segurança da informação, serão tratadas com a aplicação de ações disciplinares.

12..4. Portanto, na ocorrência de infrações a esta Norma ou às determinações constantes de comunicações externas ou internas, ou mesmo às ordens de superiores hierárquicos, quando for o caso, ficam os infratores sujeitos às seguintes penalidades: advertência verbal, advertência por escrito, suspensão, demissão sem ou com justa causa e/ou outras medidas judiciais cabíveis.

13.DISPOSIÇÕES GERAIS

13.1. Todos os usuários passam ter acesso a este manual, dando ciência de seu conteúdo. Os novos colaboradores/usuários terão acesso ao mesmo material por ocasião de sua admissão na SFI e deverão assinar o "Termo de Adesão às Políticas Internas – TAPI".

13.2. As decisões de medidas a serem adotadas quanto aos casos não tratados nesta Norma serão de responsabilidade da Diretoria de Risco e Compliance - DRCO.

13.3. Este Manual será atualizado ordinariamente a cada 24 meses e extraordinariamente quando houver alterações relacionadas à procedimentos de segurança da informação, seguindo o mesmo fluxo de aprovação e divulgação.

SFI INVESTIMENTOS LTDA.

CNPJ/MF Nº.: 04.608.141/0001-42

Rua Visconde de Pirajá, nº 152, Sala 601, Ipanema, Rio de Janeiro/RJ.

CEP: 22.410-000

Tel.: 55 21 2531.0270