POLÍTICA DE SEGURANÇA DA INFORMAÇÃO, PROTEÇÃO DE DADOS E SEGURANÇA CIBERNÉTICA

Kijani Gestora de Recursos Ltda.

Agosto/2021 – Versão 1.0

ÍNDICE

APRESENTAÇÃO

A Política de Segurança da Informação, Proteção de Dados e Segurança Cibernética ("Política") da Kijani Gestora de Recursos Ltda. ("Kijani"), aplica-se a todos os sócios, Colaboradores, prestadores de serviços e sistemas, incluindo trabalhos executados externamente ou por terceiros que utilizem o ambiente de processamento da Kijani, ou que acesse informações a ela pertencentes. Todo e qualquer usuário de recursos computadorizados da nossa instituição tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática da Kijani.

Em linha com as principais discussões e preocupações do mercado, a Política tem como base princípios e procedimentos que asseguram a confidencialidade, a integridade e a disponibilidade dos dados e sistemas de informação utilizados pela Kijani.

OBJETIVOS

Esta Política tem por objetivo contribuir para o aprimoramento da segurança, tanto informacional quanto cibernética da Kijani, estabelecendo medidas a serem tomadas para identificar e prevenir contingências que possam causar prejuízo para a consecução de suas atividades.

Em atenção aos dispositivos da Resolução CVM n.º 21/2021 e do Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros, assim como à Lei 13.709, de agosto de 2018 (Lei Geral de Proteção de Dados) a Kijani procurou identificar os eventos com maior possibilidade de ocorrência, bem como as informações de maior sensibilidade ("Informações Confidenciais"), com o propósito de mitigar os riscos à sua atividade.

Sendo assim, nenhuma informação confidencial deve, em qualquer hipótese, ser divulgada a pessoas, dentro ou fora da Kijani, que não necessitem de, ou não devam ter acesso a tais informações para desempenho de suas atividades profissionais.

Qualquer informação sobre a Kijani, ou de qualquer natureza relativa às atividades da empresa e a seus sócios e clientes, obtida em decorrência do desempenho das atividades normais do Colaborador, só poderá ser fornecida ao público, mídia ou a demais órgãos caso autorizado pelo Diretor de Risco e Compliance.

ABRANGÊNCIA

Este procedimento se aplica a Kijani, em atendimento aos requisitos do sistema de gestão de Compliance.

A efetividade desta Política depende da conscientização de todos os Colaboradores e do esforço constante para que seja feito bom uso das Informações Confidenciais e dos ativos disponibilizados pela Kijani ao Colaborador.

Esta Política deve ser conhecida e obedecida por todos os Colaboradores que utilizam os recursos de tecnologia disponibilizados pela Kijani, sendo de responsabilidade individual e coletiva o seu cumprimento.

Qualquer informação sobre a Kijani, ou de qualquer natureza relativa as atividades da empresa e a seus sócios e clientes, obtida em decorrência do desempenho das atividades normais do Colaborador, só poderá ser fornecida ao público, mídia ou a demais órgãos caso autorizado pelo Diretor de Compliance.

PREMISSAS E DEFINIÇÕES

Diante da possibilidade de vazamento, alteração, destruição e qualquer outra forma de prejuízo em relação às Informações Confidenciais, o que são de extremo valor para a Kijani, dado o princípio fundamental de confiança que a instituição trabalha para manter junto aos seus clientes, a Kijani utilizou como linha de estruturação de sua Política, o Guia de Cibersegurança, da ANBIMA, datado de dezembro de 2017.

O referido documento é um dos principais materiais sobre o tema no mercado financeiro, incluindo as melhores referências sobre proteção de dados.

Adiante, a Kijani abordará os principais mecanismos e procedimentos de prevenção as ameaças ao patrimônio, à imagem e, principalmente, aos seus negócios.

Todas as diretrizes aqui dispostas são de responsabilidade da Área de Compliance da Kijani, sob a direção do Diretor de Risco e Compliance da instituição.

Ademais, para implementação e monitoramento contínuo da presente Política, a Kijani conta com o suporte e assessoria da empresa terceirizada de TI.

PROGRAMA DE SEGURANÇA DA KIJANI

(i) Identificação de Riscos:

Os avanços tecnológicos criam facilidades e possibilitam o uso de novas ferramentas para a atuação das instituições, permitindo agilidade na construção e disponibilização de serviços, aplicação dos meios de comunicação, entre outros avanços. Por outro lado, o aumento do uso de tais ferramentas potencializa o vazamento de informações e os riscos de ataques cibernéticos, ameaçando a confidencialidade, a integralidade e a disponibilidade dos dados e/ou dos sistemas das instituições.

As ameaças cibernéticas podem variar de acordo com a natureza, vulnerabilidade, informações ou ativos de cada organização. As consequências para as instituições podem ser significativas em termos operacionais, de risco de imagem, danos financeiros ou perda de vantagem concorrencial, podendo tais danos serem irreparáveis.

Diante desse cenário, os métodos mais comuns de ataques cibernéticos são os seguintes:

- *Malware* – softwares desenvolvidos para corromper computadores e redes:
- Vírus: software que causa danos a máquina, rede, softwares e banco de dados;
- Cavalo de Troia: aparece dentro de outro software e cria uma porta para a invasão do computador;
- *Spyware*: software malicioso para coletar e monitorar o uso de informações; e
- *Ransomware*: software malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido.
- Engenharia Social – métodos de manipulação para obter informações confidenciais, como senhas, dados pessoais e número de cartão de crédito:
- *Pharming*: direciona o usuário para um site fraudulento, sem o seu conhecimento;
- *Phishing*: links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais;
- *Vishing*: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais;
- *Smishing*: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais;
- Acesso pessoal; pessoas localizadas em lugares públicos como bares, cafés e restaurantes que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.
- Ataques de DDoS (*distributed denial of services*) e *botnets* - ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição; no caso dos *botnets*, o ataque vem de um grande número de computadores infectados utilizados para criar e mandar spam ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços.
- Invasões (*advanced persistent threats*) - ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Ainda, além de ataques cibernéticos, a Kijani pode estar sujeita a mal funcionalidades dos sistemas utilizados e a atos ou omissões de seus Colaboradores, que podem acarretar no perdimento e/ou adulteração de dados e Informações Confidenciais.

(ii) Ações de Prevenção e Proteção

Para que se possam prevenir eventuais ataques cibernéticos e vazamento de informações, primeiro deve-se definir quais informações são as de maior sensibilidade para Kijani, assim como aquelas que teriam o maior impacto financeiro, operacional e reputacional para Kijani, em caso de incidente de segurança.

Deste modo, a Kijani segrega as informações geradas pela instituição, aperfeiçoando a implementação de processos e o devido manuseio, armazenamento, transporte e descarte destas informações.

Assim, classificam-se as informações digitais da instituição em 3 (três) classes diferentes, quais sejam:

a) *Green Flag:*

- Quaisquer informações e/ou dados que a Kijani teve acesso ou conhecimento por ser de domínio público ("Informação Pública");
- Quaisquer informações e/ou dados que não estejam sujeitas a compromissos ou acordos de confidencialidade; ou
- Quaisquer informações e/ou dados que tenham a obrigatoriedade de divulgação por lei ou autoridade competente.

b) *Yellow Flag:*

- Quaisquer informações que venham a ter a obrigatoriedade de divulgação por lei ou autoridade competente, mas o termo legal ainda não foi iniciado ou findado (Ex. Data de Divulgação);

c) *Red Flag:*

- Todas as Informações Confidenciais, a saber:
- *know-how*, técnicas, cópias, diagramas, modelos, amostras, programas de computador, informações técnicas, financeiras, estatísticas, logísticas ou relacionadas às estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes e/ou dos fundos geridos pela Kijani;
- operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os fundos de investimento e carteiras geridas pela Kijani; e
- estruturas, planos de ação, relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços, bem como informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades da Kijani e/ou de seus sócios e clientes.

A partir da definição acima, a Kijani se empenhará para manter controles, conforme o nível de criticidade das informações e dados, sendo certo de que a prioridade será escalonada na seguinte ordem de relevância: *Red Flag, Yellow Flag* e *Green Flag.*

A partir desse ponto, passamos a mencionar os procedimentos de prevenção e proteção adotados pela Kijani:

I. <u>Propriedade dos Recursos de TI</u>

Todos os recursos computacionais e de sistemas disponibilizados para os Colaboradores são de propriedade da Kijani. Não é permitida a utilização de notebooks, tablets ou outros hardwares para operações no âmbito da Kijani, salvo expressa permissão do Diretor de Risco e Compliance.

II. <u>Disponibilização e uso</u>

Todos os computadores disponibilizados para os Colaboradores da Kijani têm por objetivo o desempenho das atividades profissionais na Kijani, não devendo ser utilizado para quaisquer outros fins.

Conforme anteriormente citado, todo o processo de criação e exclusão de usuário, instalação de softwares e aplicativos, permissão de acesso, entre outras funcionalidades informáticas, são realizados pela área responsável, mediante aprovação do Diretor de Risco e Compliance.

A disponibilização e uso dos computadores da Kijani respeitam as seguintes regras:

- A cada novo Colaborador, o Diretor de Risco e Compliance autorizará, mediante solicitação, a criação de novo usuário e a disponibilização técnica de recursos;
- Todos os equipamentos, softwares e permissões acessos devem ser testados, homologados e autorizados pela área responsável, mediante supervisão e aprovação do Diretor de Risco e Compliance;
- O Diretor de Risco e Compliance autorizará, mediante solicitação, a retirada ou substituição do computador disponibilizado para o usuário;
- Cada computador tem o seu usuário gestor, que é responsável por esse equipamento. O controle das máquinas é de responsabilidade da área responsável, mediante supervisão e aprovação do Diretor de Risco e Compliance;
- A identificação do usuário é feita através do *login* e senha, que através do registro de *logs* utilizado pela Kijani é sua assinatura eletrônica no servidor da Kijani;
- Serão apenas permitidas senhas com no mínimo 08 (oito) caracteres alfanuméricos, maiúsculos e minúsculos. A reutilização de senhas obedecerá ao ciclo mínimo de 05 (cinco) vezes;
- Não será permitida a utilização da mesma senha para projetos e serviços diferentes realizados pela Kijani, não devendo ser criada uma senha única padrão para todos os serviços e áreas em que um mesmo Colaborador atue;
- É permitida apenas 3 tentativas máximas de autenticação de senha, sendo todas malsucedidas, será bloqueado o acesso, o qual apenas poderá ser reestabelecido através de solicitação ao Diretor de Risco e Compliance.
- A senha possui validade de 180 (cento e oitenta) dias e sua troca será solicitada automaticamente quando da sua expiração.
- Todos os eventos de *login* e alteração de senhas são auditáveis e rastreáveis, podendo ser solicitados pelo Diretor de Risco e Compliance à área responsável.

III. <u>Softwares</u>

A implantação e configuração de softwares da Kijani respeitam as seguintes regras:

- Todos os softwares, programas básicos (sistema operacional e ferramentas) e componentes físicos são implantados e configurados pela área responsável, mediante supervisão e aprovação do Diretor de Risco e Compliance;
- É desabilitado aos usuários implantar novos programas ou alterar configurações sem a permissão formalizada do Diretor de Risco e Compliance;
- É desabilitado ao usuário implantar ou alterar componentes físicos em seus computadores;
- Somente é permitido o uso de equipamentos homologados e devidamente contratados pela Kijani;
- A utilização de equipamentos pessoais por terceiros nas instalações da Kijani e a conexão destes na rede interna à Internet requer autorização prévia e expressa do Diretor de Risco e

Compliance. Os Colaboradores estão autorizados a conectar seus telefones celulares e computadores pessoais diretamente à rede interna e à Internet, desde que utilizem suas credenciais de acesso;

- A conexão de dispositivos móveis de armazenamento (e.g. *USB Drive*) somente poderá ser realizada mediante autorização prévia e expressa do Diretor de Risco e Compliance.

IV. Registros

A Kijani mantém por 5 anos todos os *logs* de sistemas, e verifica regularmente, quaisquer desvios de padrão de todos os computadores, arquivos em rede, sejam softwares, hardwares ou acessos que não sejam autorizados.

Nesse sentido, através dos *logs* realizados pela Kijani, a gestora consegue manter a integridade, autenticidade e auditabilidade das informações e sistemas, conforme Resolução CVM n.º 21/2021.

V. Responsabilidades do usuário

O Colaborador é o custodiante dos recursos disponibilizados a ele, devendo este cuidar adequadamente do equipamento.

O Colaborador também deve garantir a sua integridade física e o seu perfeito funcionamento, seguindo as regras e orientações fornecidas pela Kijani.

Ainda, o Colaborador deve adotar um comportamento seguro condizente com a Política, devendo:

- Não compartilhar nem divulgar sua senha a terceiros;
- Não transportar Informações Confidenciais da Kijani em qualquer meio (CD, DVD, *pendrive*, papel, etc.) sem as devidas autorizações e proteções;
- Assuntos confidenciais de trabalho não devem ser discutidos em ambientes públicos ou em áreas expostas (aviões, restaurantes, encontros sociais, etc.);
- Não abrir mensagens de origem desconhecida, ou links suspeitos mesmo que advindos de origem conhecida;
- Armazenar e proteger adequadamente documentos impressos e arquivos eletrônicos que contêm Informações Confidenciais; e
- Seguir corretamente a política para uso de internet e correio eletrônico estabelecida pela Kijani.

VI. Outras Proteções aos Computadores

- Proteção de tela no computador e/ou proteção de ausência (após um tempo de inatividade, o computador bloqueia o sistema, exigindo senha para ser usado novamente);
- *Log-off* automático por inatividade durante o período de 24 horas;
- Bloqueio do acesso as portas USB dos computadores para proteção contra vírus e cópia indevida dos dados contidos nos servidores;
- Bloqueio do acesso a sites de armazenamento de dados em Nuvem (*Cloud*);
- Bloqueio de sistemas de gerenciamento de computador à distância.

VII. Regras e responsabilidades do uso da Internet

O Colaborador é responsável por todo acesso realizado com a sua autenticação.

Quando o usuário se comunicar através de recursos de tecnologia da Kijani, este deve sempre resguardar a imagem da Kijani, evitando entrar em sites de fontes não seguras, assim como de abrir e-mails pessoais ou de fontes não conhecidas, salvo quando comunicado e devidamente autorizado pelo Diretor de Risco e Compliance.

O usuário é proibido de acessar endereços de internet (sites) que:

- Possam violar direitos de autor, marcas, licenças de programas (softwares) ou patentes existentes;
- Possuam conteúdo pornográfico, relacionado a sexo, exploração infantil ou ao crime de pedofilia;
- Contenham informações que não colaborem para o alcance dos objetivos da Kijani;
- Defendam atividades ilegais, menosprezem, depreciem ou incitem o preconceito a determinadas classes como sexo, raça, orientação sexual, religião, nacionalidade, local de nascimento ou deficiência física;
- Possuam origem suspeita ou que não se atenham aos padrões de segurança adequados, assim como possuírem links suspeitos.

O usuário deve garantir que está cumprindo a legislação em relação ao direito autoral, licença de uso e patentes existentes e que o uso do material foi autorizado, no mínimo, pelo gestor da sua área.

É proibido o uso de serviços de mensagem instantânea (MSN, *Skype*, etc), através dos computadores da Kijani, exceto em eventuais situações de uso profissional, sendo necessária autorização do Diretor de Risco e Compliance.

Também se faz expressamente proibido o uso de serviços de rádio, streaming, download de vídeos, filmes e músicas, através dos computadores da Kijani.

VIII. Bloqueio de endereços de Internet

Periodicamente, a Área de Compliance irá revisar e bloquear o acesso para os endereços da Internet que não estejam alinhados com esta Política e com o Código de Ética da Kijani.

IX. Uso de correio eletrônico particular

É proibido a utilização profissional de correio eletrônico particular.

A Kijani disponibiliza endereços de seu correio eletrônico para utilização do usuário no desempenho de suas funções profissionais. (ex.: usuario@kijani.com.br)

O endereço eletrônico disponibilizado para o usuário é individual, intransferível e pertence à Kijani.

O endereço eletrônico cedido para o usuário deve ser o mesmo durante todo o seu período de vínculo com a Kijani.

Se houver necessidade de troca de endereço, a alteração será realizada pela área responsável, mediante autorização e supervisão do Diretor de Risco e Compliance.

X. Endereço eletrônico de programas ou de comunicação corporativa

É permitido que um programa aplicativo ou um programa de sistema possua um endereço de correio eletrônico. Nesse caso, é obrigatória a existência de um usuário da Área de Compliance responsável por acompanhar as mensagens emitidas e recebidas por esse endereço.

É permitida a existência de endereços de correio eletrônico para o envio de mensagens tipo Comunicação Interna da Kijani, porém, é obrigatória a identificação do usuário que encaminhou a mensagem.

O endereço de correio eletrônico disponibilizado para os Colaboradores e as mensagens associadas a este correio eletrônico são de propriedade da Kijani.

XI. Acesso à distância ao e-mail

O usuário pode acessar o seu correio eletrônico cedido pela Kijani mesmo quando estiver fora do ambiente da empresa, através do serviço de correio eletrônico via Internet.

O Colaborador deve ter o mesmo zelo com a utilização do correio eletrônico à distância tal qual estivesse no ambiente físico da Kijani.

XII. Responsabilidades e forma de uso de Correio Eletrônico

O Colaborador que utiliza um endereço de correio eletrônico é responsável por todo acesso, conteúdo de mensagens e uso relativos ao seu e-mail, podendo enviar mensagens necessárias para o seu desempenho profissional na Kijani.

É proibido criar, copiar ou encaminhar mensagens ou imagens que:

- Contenham declarações difamatórias ou linguagem ofensiva de qualquer natureza;
- Façam parte de correntes de mensagens, independentemente de serem legais ou ilegais;
- Repassem propagandas ou mensagens de alerta sobre qualquer assunto. Havendo situações em que o usuário ache benéfico divulgar o assunto para a Kijani, a sugestão deve ser encaminhada para a Área de Recursos Humanos, que definirá a sua publicação ou não;
- Menosprezem, depreciem ou incitem o preconceito a determinadas classes, como sexo, raça, orientação sexual, idade, religião, nacionalidade, local de nascimento ou deficiência física;
- Possuam informação pornográfica, obscena ou imprópria para um ambiente profissional;
- Sejam suscetíveis de causar qualquer tipo de prejuízo a terceiros;
- Defendam ou possibilitem a realização de atividades ilegais;

- Sejam ou sugiram a formação ou divulgação de correntes de mensagens;
- Possam prejudicar a imagem da Kijani; e
- Sejam incoerentes com o Código de Ética Corporativa da Kijani.

É proibido reproduzir qualquer material recebido pelo correio eletrônico ou outro meio, que possa infringir direitos de autor, marca, licença de uso de programas ou patentes existentes, sem que haja autorização expressa do autor do trabalho e da organização.

O Colaborador deve estar ciente que uma mensagem de correio eletrônico da Kijani é um documento formal e, portanto, possui as mesmas responsabilidades de um documento convencional em papel timbrado da entidade.

Exceto quando especificamente autorizado para tal, é proibido emitir opinião pessoal, colocando-a em nome da Kijani.

Deve observar se o endereço do destinatário corresponde realmente ao destinatário desejado.

O Colaborador deve ser diligente em relação:

- Aos usuários que receberão a mensagem (Destinatário/To, Copiado/Cc e Copiado Oculto/Bcc);
- Ao nível de sigilo da informação contida na mensagem;
- Aos anexos da mensagem, enviando os arquivos apenas quando for imprescindível e garantindo a confidencialidade dos mesmos;
- Ao uso da opção encaminhar (*Forward*), verificando se é necessária a manutenção das diversas mensagens anteriores que estão encadeadas.

O Colaborador deve deixar mensagem de ausência quando for passar um período maior do que 24 (vinte e quatro) horas sem acessar seu correio eletrônico. Essa mensagem deve indicar o período de ausência e o endereço do substituto para quem deve ser enviada a mensagem.

XIII. Cópias de segurança do Correio Eletrônico

Para que seja possível uma gestão segura, efetiva, confiável, administrável e passível de auditoria, a cópia de segurança das mensagens de correio eletrônico é feita de forma centralizada no ambiente dos equipamentos servidores corporativos, sob a responsabilidade da área responsável, mediante supervisão do Diretor de Risco e Compliance.

XIV. Armazenamento em Nuvem (*Cloud*)

A Kijani poderá realizar o armazenamento das Informações Confidenciais e quaisquer outros dados na Nuvem (*Cloud*).

De forma a possuir um ambiente seguro de nuvem, considerando aplicações WEB, se prezará pela confiabilidade, disponibilidade e integridade do armazenamento da mesma.

XV. Contratação de Terceiros para Serviços de Armazenamento na Nuvem

Fornecedores, prestadores de serviços e parceiros ("Terceiros") podem representar uma fonte significativa de riscos para a Kijani em relação à Cibersegurança. Neste sentido, é necessário adotar certos procedimentos que devem ser realizados previamente a contratação de Terceiros para serviços de Armazenamento na Nuvem.

Necessário iniciar um devido processo de *Due diligence* do Terceiro antes da contratação, devendo-se constatar se a organização segue políticas, programas e procedimentos formais relativos à segurança da informação e Cibersegurança.

Com isto em mente, a empresa objeto de contratação deverá enviar a Kijani:

(i) Documentos que atestem a existência dos respectivos procedimentos de Cibersegurança;

(ii) Último relatório de teste/auditoria periódica;

(iii) As certificações que possam comprovar a devida capacidade técnica do prestador de serviço.

Uma vez recebidos os respectivos documentos, a Área de Compliance analisará o Terceiro, podendo negar de imediato a contratação deste ou exigir remediações para que este se encaixe nos moldes de segurança a serem aplicados pela Kijani.

Somente após a aprovação pela Área de Compliance, o Terceiro poderá ser contratado para prestar serviços de Armazenamento na Nuvem.

Em caso de qualquer incidente constatado pelo Terceiro, este deverá de imediato enviar uma notificação relatando o ocorrido à Kijani, a qual, dependendo da situação, poderá reavaliar e inclusive rescindir de imediato o contrato do Terceiro.

Outros serviços com utilização da tecnologia em Nuvem também devem ser considerados para fins das regras aqui presentes, sendo necessário aplicar os mesmos procedimentos de *Due Dilligence* aos provedores destes serviços, tal como, porém, não exclusivamente:

(i) Software *as a Service* (SaaS) – utilização do software do provedor por meio de subscrição, eliminando a necessidade de instalação e execução nos computadores;

(ii) Platform *as a Service* (PaaS) – desenvolvimento, teste, uso e controle sobre softwares próprios; e

(iii) Infrastructure *as a Service* (IaaS) – utilização e controles sobre softwares próprios e de terceiros, sistemas operacionais, servidores, unidades de armazenamento e rede – contratação de servidores virtuais.

MONITORAMENTO E TESTES PERIÓDICOS

O monitoramento dos controles existentes e estabelecidos nessa Política serão realizados e executados pela área responsável, sob supervisão do Diretor de Risco e Compliance. O referido monitoramento acontecerá de forma contínua, sem periodicidade.

Os Testes de Contingência serão realizados anualmente, de modo a permitir que a Kijani esteja preparada para a continuação de suas atividades, assim como a mitigar eventuais riscos operacionais ou reputacionais. Outras informações acerca dos Testes de Contingência estão no Plano de Continuidade de Negócios da Kijani.

Ademais, serão realizados Testes Periódicos de Segurança a Kijani, com especial enfoque em segregação lógica, testes de penetração, resposta a eventos de vazamento de dados, rastreabilidade dos logs de acessos às informações sensíveis, tratamento de dados, dentre outros, sempre objetivando a preservação dos dados mantidos pela Kijani, em especial os confidenciais. Referidos testes serão realizados, com periodicidade mínima semestral, pela empresa de TI terceirizada e o resultado será consolidado no relatório anual de controles internos da Kijani.

PLANO DE RESPOSTA

Conforme as melhores práticas de mercado, a Kijani desenvolveu um Plano de Resposta para indícios, suspeita fundamentada, vazamento de Informações Confidenciais ou outra falha de segurança.

Na hipótese de verificação de uma das hipóteses acima, inclusive em decorrência da ação de criminosos cibernéticos, as providências pertinentes deverão ser iniciadas, devendo cada área responsável agir conforme o disposto na presente Política.

Estas providências consistem em:

Empresa de TI Terceirizada (Sob Supervisão do Compliance):

a) Verificação e Auditoria dos *Logs*;
b) Criação de laudo pericial contendo as informações que foram potencialmente vazadas;
c) Execução de aplicativos externamente ou em sistemas afetados para eliminar aplicativos indesejados;
d) Desinstalação de software;
e) Execução de varreduras *offline* para descobrir quaisquer ameaças adicionais;
f) Formatação e reconstrução do sistema operacional;
g) Substituição física de dispositivos de armazenamento
h) Reconstrução de sistemas e redes;
i) Restauração de dados provenientes do backup realizado diariamente;
j) Entre outros.

Compliance ou Jurídico Contratado:

a) Criação de relatório baseado no laudo pericial elaborado pela empresa de TI Terceirizada, de forma a constar eventuais consequências reputacionais e jurídicas derivadas dos danos ocasionados pelo incidente de segurança;

b) Em caso de confirmação do incidente de segurança e eventual vazamento de informações confidenciais, elaborar notificação aos clientes afetados informando o ocorrido, se necessário.

BackOffice:

a) Análise de dados perdidos e suas influências frente ao planejamento contábil e aos ativos da Companhia;
b) Realizar planejamento de contenção de risco de liquidez frente a possibilidade de resgate de investimentos da Kijani resultantes do incidente de segurança.

Em caso de necessidade, poderá ser contratada empresa especializada no combate ao evento identificado, assim como nas respostas ao eventual dano.

Todo e qualquer incidente ocorrido, assim como os resultados do Plano de Resposta, deverão ser devidamente classificados por nível de severidade, arquivados e documentados pela Área de Compliance, bem como ser formalizado no Relatório de Controles Internos da Kijani.

A Kijani deverá realizar, em caso de incidente que afetem os dados pessoais que realize tratamento, a comunicação tempestiva às partes afetadas, bem como à Autoridade Nacional de Proteção de Dados ("ANPD")

Caso o evento tenha sido causado por algum Colaborador, deverá ser avaliada a sua culpabilidade, nos termos do Código de Ética da Kijani.

PROTEÇÃO DE DADOS PESSOAIS

Escopo e Abrangência:

A Kijani está comprometida em preservar a privacidade de dados pessoais e de dados sensíveis que forem coletados ou aos quais tiver acesso em função do uso do site ou por conta do desempenho de suas atividades, e com o cumprimento das leis e regulamentos em vigor.

Por conta disso, estabeleceu, as diretrizes, princípios e regras previstas nesta Política, as quais servirão de guia para a coleta, registro, processamento, armazenamento, uso, compartilhamento e eliminação de dados pessoais, fornecendo o arcabouço para o correto tratamento e proteção dos dados pessoais em seu poder.

Essas diretrizes, princípios e regras se aplicam a todos os Colaboradores da Kijani, e englobam os dados pessoais que se encontrem armazenados em qualquer meio, e abrangem toda e qualquer forma de tratamento que possa ser empregada e esteja disponível para a Kijani.

Importante observar que o escopo da proteção de dados pessoais no âmbito da Kijani está, em grande parte, limitado aos dados pessoais de seus Colaboradores e de pessoas físicas e jurídicas com as quais tiver estabelecido relações jurídicas, com especial menção ao cumprimento da regulação aplicável à gestão de recursos de terceiros. Também estão abrangidos por esta proteção os dados de candidatos às vagas na Kijani, de fornecedores e outros com os quais a Kijani manteve contato para atender alguma demanda relevante e específica.

Vale ressaltar que todo o tratamento de dados pessoais feito pela Kijani está pautado nos requisitos do artigo 7º da Lei 13.709/2018 ("LGPD"), assim como nas premissas do artigo 11 da mesma Lei, quando aplicável.

Princípios Norteadores:

A Kijani compromete-se a obter dados pessoais de maneira justa e legal, e suas ações serão norteadas no princípio da boa-fé e nos princípios abaixo, os quais estão elencados no art. 6º da LGPD:

I - Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - Qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX – Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X – responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Direitos:

Em respeito aos direitos fundamentais de liberdade, de intimidade e de privacidade, e, ainda, ao disposto no art. 18 da LGPD, o titular dos dados pessoais tem direito de solicitar à Kijani, em relação aos seus dados, a qualquer momento e mediante requerimento expresso o que se segue.

a) confirmação de existência de tratamento;

b) acesso aos dados;

c) correção de dados incompletos, inexatos ou desatualizado;

d) anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei 13.709/2018;

e) portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;

f) eliminação dos dados pessoais tratados com o consentimento do titular, exceto em determinadas situações e respeitados os limites técnicos das atividades, conforme determinado na Lei;

g) informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

h) informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; e

i) revogação do consentimento, nos termos da Lei.

A Kijani disponibiliza canal de comunicação, através do endereço kijani@kijani.com.br, por meio do qual o seu Encarregado pelo Tratamento de Dados Pessoais, é o responsável por auxiliar os controladores de dados pessoais em relação ao cumprimento de suas obrigações legais referentes à privacidade. Dessa forma, o DPO atua como uma ponte entre a Kijani, os titulares dos dados (pessoas físicas) e a ANPD.

Período de Armazenamento dos Dados Pessoais:

Os dados pessoais serão armazenados pela Kijani durante tempo necessário para o atingimento dos objetivos para os quais foram coletados. De todo modo, este período poderá ser ampliado para o cumprimento de obrigação legal, regulatória ou contratual, pelo que, nestas hipóteses o prazo mínimo de armazenamento será de 5 (cinco) anos.

Cooperação com Autoridades:

A divulgação de dados pessoais para o cumprimento de lei, determinação judicial, regulatória ou de órgão competente ao qual a Kijani estiver sujeita somente ocorrerá nos estritos termos e nos limites requeridos para o cumprimento da obrigação, sendo que os titulares dos dados, na medida do possível e desde que não configure infração, inadimplemento ou cause prejuízo à Kijani, serão notificados sobre tal divulgação, para que tomem as medidas apropriadas.

Adicionalmente, a Kijani cooperará com a ANPD em qualquer problema em relação à proteção de dados e dentro dos limites previstos na LGPD e nas demais regulamentações sobre a matéria, porém sem renunciar a quaisquer defesas e/ou recursos disponíveis.

Governança:

As matérias relacionadas aos dados pessoais, dados sigilosos e aos tratamentos destes serão apresentadas pelo Encarregado pelo Tratamento de Dados Pessoais para deliberação no Comitê de Gestão de Riscos e de Compliance.

Obrigação de Reporte:

Os Colaboradores estão obrigados a comunicar imediatamente ao Encarregado pelo Tratamento de Dados Pessoais sobre toda e qualquer suspeita ou indício de evento que possa ter comprometido os dados pessoais de posse da Kijani para a devida apuração. Caso necessário, o Encarregado pelo Tratamento de Dados Pessoais notificará, em prazo compatível com a severidade do evento, a ANPD, bem como todos os que porventura possam ter sido afetados pelo referido evento.

Registro de Eventos:

Os eventos reportados que tenham sido apurados e tiverem resultado no comprometimento de dados pessoais serão registrados no Relatório de Controles Internos e no Relatório de Impacto à Proteção de Dados Pessoais, inclusive de dados sensíveis, nos termos do artigo 38 da LGPD.

Treinamento:

A Kijani treinará seus Colaboradores sobre a proteção de dados pessoais e de dados sigilosos de acordo com a sua Política de Treinamento e Reciclagem de Colaboradores.

MEDIDAS DISCLIPLINARES

Caso o Colaborador não cumpra as regras desta Política, ele estará sujeito à aplicação de medidas disciplinares que serão determinadas pela direção da Kijani de acordo com o grau de gravidade da conduta praticada pelo Colaborador, podendo variar entre:

(i) **Advertência verbal**: no caso de infrações consideradas leves;

(ii) **Advertência escrita ou suspensão**: no caso de infrações consideradas graves ou quando for constatada a reincidência de uma conduta classificada leve; e

(iii) **encerramento do contrato**: no caso de infrações consideradas gravíssimas ou quando for constatada reincidência de uma conduta considerada grave. Tratando-se de Colaborador empregado, isso significa o desligamento do Colaborador e a rescisão de seu contrato de trabalho por justa causa. Tratando-se de Colaborador não empregado, isso significa a rescisão de contrato com a Kijani, que será realizada de acordo com as disposições do contrato firmado e com a legislação vigente.

Os Colaboradores que cometerem infração às regras desta PSI serão comunicados por escrito. Tal comunicação conterá a regra violada, a conduta praticada pelo Colaborador e a medida disciplinar aplicada pela Kijani, sem prejuízo de eventual indenização paga pelo Colaborador, a ser apurada judicialmente.

VIGÊNCIA E ATUALIZAÇÃO

Esta Política será revisada periodicamente, pelo menos 01 (uma) vez ao ano, e sua alteração acontecerá caso seja constatada necessidade de atualização do seu conteúdo. Poderá, ainda, ser alterada a qualquer tempo em razão de circunstâncias que demandem tal providência.

O objetivo principal do processo de revisão dessa Política é manter sempre atualiza a metodologia de avaliação de risco, as implementações de proteção e prevenção, os monitoramentos e testes e os planos de resposta.

CONTROLE DE VERSÕES	DATA	MODIFICADO POR	DESCRIÇÃO DA MUDANÇA
1	Agosto/2021	RRZ Consultoria	Versão inicial

ANEXO I - TERMO DE CIÊNCIA SOBRE A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

Nesta data, eu, _____, inscrito no CPF/ME sob o nº _____ , declaro que li e estou plenamente ciente das disposições da Política de Segurança da Informações e Segurança Cibernética da Kijani Gestora de Recursos Ltda.. Comprometo-me a cumprir com os termos dispostos na mesma, preservando a confidencialidade das informações as quais terei acesso.

Londrina, [Data]

_____

[Assinatura]

ANEXO II – PROCEDIMENTOS PARA A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO, PROTEÇÃO DE DADOS E SEGURANÇA CIBERNÉTICA DA KIJANI

CLASSIFICAÇÃO DAS INFORMAÇÕES PROTEGIDAS

Para além da classificação de informações em *Green Flag*, *Yellow Flag*, e *Red Flag*, de forma a assegurar a proteção adequada das Informações Protegidas, é necessário que sejam classificadas de acordo com a importância que representam para os negócios da Kijani, aplicando-se o grau de sigilo conforme sua classificação:

(i) **Informação Interna:** informação que guarde assuntos exclusivamente pertinentes à esfera interna da Kijani, cujo acesso é liberado apenas às pessoas internas da Kijani designadas para tal. Embora a Kijani não tenha interesse em divulgá-la a indivíduos externos, a disponibilização dessa informação não tem o potencial de causar danos sérios à Kijani;

(ii) **Informação Confidencial:** informação sigilosa que não deve ser divulgada. Seu uso é restrito a um determinado número de pessoas para desempenharem as suas atividades vinculadas à Kijani. A sua divulgação não autorizada pode causar prejuízos para a Kijani (tais como perda de clientes, danos financeiros, depreciação da imagem etc.), propiciando vantagens aos seus concorrentes e clientes, bem como revelando estratégias e resultados de negócios; e

(iii) **Informação Secreta**: informação sigilosa, com acesso controlado e liberado apenas às pessoas nomeadas para tanto, que contém matérias de ordem vital para a Kijani ou seus clientes, cuja divulgação, inexatidão e indisponibilidade (total ou parcial) podem causar danos morais ou patrimoniais graves à Kijani. **Devem ser consideradas Informações Secretas** as informações de saúde (p. ex., exames médicos de Colaboradores), os procedimentos de segurança e as outras informações de notável criticidade para os negócios da Kijani.

Além das Informações Protegidas, há também a **Informação Pública**, destinada ao público em geral e já divulgada pela Kijani, cuja utilização por quaisquer indivíduos independe de autorização e não gera prejuízos para a Kijani ou para terceiros.

Caso o Colaborador receba uma informação que não esteja classificada, ele deve considerar, obrigatoriamente, essa informação como sendo, no mínimo, uma Informação Confidencial. Se o Colaborador tiver conhecimento de que Informações Internas, Confidenciais ou Secretas estejam sendo tratadas inadequadamente, tal Colaborador deverá comunicar os responsáveis pela Área de Compliance pelo e-mail compliance@kijani.com.br.

PRIVACIDADE E PROTEÇÃO DE DADOS

A PSI e este procedimento aplicam-se a todos os dados tratados pela Kijani, incluindo Dados Pessoais e Sensíveis, que podem ser coletados sobre os clientes, os Colaboradores e demais pessoas naturais que se relacionam com a Kijani. É vedado, sem a prévia autorização da Kijani, o uso destes dados para finalidades diversas das que lastrearam a coleta, o uso, o armazenamento e qualquer outra hipótese de tratamento dos dados, nos termos deste Procedimento.

A Kijani usa provedores de serviços externos. Se os Dados que estão sendo tratados são Pessoais ou Sensíveis, devem ser firmados acordos contratuais apropriados e medidas organizacionais devem ser implementadas de acordo com a legislação aplicável para assegurar a proteção dos dados.

O Colaborador deve atuar para que todos os Dados Pessoais a que tiver acesso não sejam divulgados ou compartilhados sem autorização expressa da Kijani, bem como não sejam transmitidos ou acessados por terceiros não autorizados. O Colaborador deve adotar as melhores práticas de segurança da informação durante todo o ciclo de vida dos dados dentro da Kijani.

MONITORAMENTO E AUDITORIA DO AMBIENTE

TODO AMBIENTE FÍSICO E DIGITAL DA KIJANI É OU PODERÁ SER MONITORADO, RESPEITADOS OS LIMITES PREVISTOS NA LEGISLAÇÃO VIGENTE, INCLUINDO O ACESSO, USO OU TRÁFEGO DE INFORMAÇÕES EM TAL AMBIENTE POR QUALQUER MEIO (TAL QUAL, POR EXEMPLO, E-MAIL) COM O OBJETIVO DE APURAR O CUMPRIMENTO DAS NORMAS DE SEGURANÇA E PROTEÇÃO DE DADOS DA KIJANI.

OS COLABORADORES DEVEM ESTAR CIENTES DE QUE A KIJANI PODERÁ:

(i) MONITORAR TODOS OS SERVIDORES, REDES, CONEXÕES DE INTERNET, SOFTWARES, EQUIPAMENTOS E DISPOSITIVOS CORPORATIVOS, MÓVEIS OU NÃO, CONECTADOS À REDE CORPORATIVA;

(ii) REALIZAR INSPEÇÕES FÍSICAS NOS EQUIPAMENTOS E NAS ESTAÇÕES DE TRABALHO DO COLABORADOR, PERIODICAMENTE OU SOB FUNDADA SUSPEITA DE INFRAÇÃO ÀS NORMAS INTERNAS DA KIJANI.

O Colaborador também está ciente de que o monitoramento poderá identificá-lo e apresentar dados sobre o seu uso da infraestrutura técnica da Kijani e do material e conteúdo manipulado pelo Colaborador, sendo certo que todas as informações coletadas no curso do monitoramento são retidas pela Kijani para fins de auditoria e poderão ser utilizadas como provas de eventual violação das regras e condições estabelecidas pela Kijani ou pela legislação em vigor. Caso solicitado pelos órgãos

competentes, essas informações poderão ser divulgadas na medida em que houver razão legal ou determinação judicial para tanto.

O Colaborador entende que o monitoramento é realizado para resguardar a segurança não só dos sistemas da Kijani e das Informações Protegidas, como também do próprio Colaborador. Os dados e as informações monitoradas somente poderão ser acessadas pelos departamentos competentes e para finalidades legítimas, como a apuração de denúncias e condução de investigações no ambiente laboral. Todo e qualquer tratamento de dados para estes fins será fundamentado no relatório de auditoria ou em outro instrumento apropriado para tanto, e cumprirá as normas específicas sobre privacidade e proteção de Dados Pessoais, descritas mais detalhadamente na Política de Privacidade de Colaboradores da Kijani.

MANUSEIO DAS INFORMAÇÕES PROTEGIDAS

O Colaborador é responsável pelo uso que fizer das Informações Protegidas. Assim, as regras abaixo deverão ser observadas para garantir um nível mínimo de Segurança da Informação.

- Cuidados com impressoras e copiadoras

Os Colaboradores estão cientes de que todo e qualquer uso dos equipamentos, como copiadoras e impressoras, deve ser feito exclusivamente no âmbito das suas atividades profissionais, sendo vedado o uso para fins pessoais. Deve-se evitar imprimir documentos contendo Informações Secretas e, para todos os tipos de informação, os documentos impressos ou copiados devem ser retirados imediatamente dos equipamentos.

- Uso de Informações Protegidas

O Colaborador deve tomar o máximo de cuidado com o uso que faz das Informações Protegidas, atentando-se para não deixar anotações ou manipular documentos que contenham Informações Protegidas em locais de circulação, como salas de reunião ou espaços públicos, como cafés e aviões. É proibida a reutilização de papéis que contenham Informação Protegida para rascunho.

Nos casos envolvendo a contratação de serviços de terceiros que justifiquem a necessidade de compartilhamento de Informações Protegidas pelo Colaborador, estas somente poderão ser compartilhadas após a assinatura de instrumentos contratuais dispondo sobre o dever de sigilo e, se aplicável, de uso adequado dos Dados Pessoais.

- Comunicação Verbal

Sempre que Informações Protegidas forem transmitidas por meio de comunicação verbal, o Colaborador deverá respeitar as regras dispostas abaixo, de acordo com o meio de transferência da informação:

(i) Presencial. Informações Internas, Confidenciais e Secretas somente podem ser discutidas em locais privados de acesso controlado, para impedir que terceiros não autorizados escutem a conversa e tenham acesso a tais informações. Quando não for possível a comunicação em ambiente privado, o Colaborador deverá tomar, no mínimo, as seguintes cautelas: (a) sempre verificar se alguém está escutando a conversa; e (b) nunca identificar a Kijani ou o Cliente durante o diálogo.

(ii) Telefones, Celulares e Rádios. É vedada a transmissão de Informações Confidenciais e Secretas por rádio ou telefone (fixo ou móvel). Caso o Colaborador não possa evitar que tais informações sejam transmitidas por ligações telefônicas ou pelos outros meios de transmissão, o Colaborador deve redobrar o cuidado, sendo objetivo e discreto ao transmitir tais informações. Da mesma forma, o Colaborador também não deve fornecer informações como senhas, telefones, endereços (físicos e eletrônicos) ou outras informações de acesso restrito por telefone ou outros meios de transmissão e deve estar atento para não repetir em voz alta essas informações quando forem lhe passadas por terceiros. Ainda, o Colaborador entende e concorda que é vedada a gravação de Informações Confidenciais e Secretas em equipamentos eletrônicos, como caixa postal, secretária eletrônica, áudios em aplicativos de conversa etc.

- Recebimento, envio e compartilhamento de arquivos

O Colaborador é responsável pelos arquivos que recebe, envia e compartilha por meio eletrônico e pela infraestrutura tecnológica da Kijani, seja ela equipamentos de propriedade da Kijani disponibilizados para o uso do Colaborador, equipamentos do próprio Colaborador (quando autorizado pela Kijani, conforme as regras do item *Dispositivos*), ou ainda, serviços de *cloud* (nuvem).

Para garantir níveis mínimos de segurança da infraestrutura tecnológica da Kijani é vedado ao Colaborador:

(i) receber, enviar e compartilhar arquivos que: (a) tenham finalidades diversas e não relacionadas às atividades de interesse da Kijani ou relativas aos seus negócios; (b) contenham pornografia ou conteúdo de cunho racista, discriminatório ou qualquer outro que viole a legislação em vigor, a moral e os bons costumes; (c) violem direitos de terceiros, em especial direitos de propriedade intelectual, direitos autorais, direitos de imagem, entre outros; (d) caracterizem infração civil ou penal ou possam causar prejuízos à Kijani e a terceiros; e (e) configurem concorrência desleal ou quebra de sigilo profissional; e

(ii) enviar, compartilhar e baixar: (a) arquivos que contenham malware, como vírus ou outros códigos maliciosos; (b) Informações Internas, Confidenciais ou Secretas em ambiente externo; e (c) qualquer arquivo executável (.exe) que não seja autorizado pela Kijani.

- Guarda e deslocamento de informações

Todas as Informações Protegidas que devam ser armazenadas em suporte físico ou digital, quando da sua guarda pelo Colaborador, devem respeitar regras de ciclo de vida dos dados da Kijani, bem como os seguintes cuidados, de acordo com a classificação da informação:

(i) Suporte físico. Todos os documentos contendo Informações Internas, Confidenciais e Secretas devem ser armazenados em arquivos físicos próprios indicados pela Kijani, de acordo com os métodos de identificação do conteúdo, também indicados pela Kijani, incluindo sua data de arquivamento. Documentos utilizados pelo Colaborador em sua estação de trabalho, quando não estiverem sendo utilizados, devem sempre ser guardados em gaveta ou armário, garantindo que tais gavetas e armários permaneçam trancados quando se tratar de Informações Secretas. Nenhuma anotação relacionada às Informações Protegidas deve ser deixada à mostra, seja em cima da mesa, do computador ou em divisórias, mesmo quando o Colaborador estiver presente. Quando o Colaborador não estiver nas dependências da Kijani, os documentos contendo Informações Internas, Confidenciais e Secretas também não devem ficar expostos, inclusive no regime de teletrabalho.

(ii) Suporte digital. Todo e qualquer arquivo que contenha Informação Interna, Confidencial ou Secreta deve ser salvo na rede corporativa da Kijani, em diretório específico, que inviabilize o acesso por Colaboradores não autorizados. Caso o arquivo deva ser armazenado em dispositivo móvel (como, por exemplo, em notebooks, por conta de reuniões externas), é indispensável que o Colaborador remova o arquivo do dispositivo após a sua utilização.

Todo e qualquer documento ou arquivo que contenha Informações Confidenciais ou Secretas somente poderá ser alterado, copiado ou movimentado se houver a possibilidade de recuperação, controle de versão ou análise dos registros de tal arquivo ou documento em caso de falhas de segurança que acarretem a perda ou o extravio das Informações Protegidas.

- Descarte de informações

O descarte de um documento físico ou a exclusão de um arquivo digital que contenha Informações Protegidas deverá seguir as seguintes regras de descarte:

(i) Suporte físico: os documentos que tiverem Informações Públicas poderão ser descartados no lixo comum; já aqueles que possuírem Informações Internas, Confidenciais e Secretas devem ser destruídos manualmente ou, preferencialmente, por um aparelho fragmentador antes do descarte. No caso de Informações Secretas, o uso de aparelho fragmentador é obrigatório e, na ausência de tal aparelho, o Colaborador deverá acionar o gestor responsável para que este tome as medidas cabíveis.

(ii) Suporte digital: arquivos que contenham Informações Protegidas e estejam armazenados em suporte digital flexível, tais como CD ou DVD, deverão ser destruídos por meio de aparelho fragmentador e, na ausência de tal aparelho, o Colaborador deverá acionar o gestor responsável para que sejam tomadas as medidas necessárias. Já aqueles arquivos armazenados em suporte digital rígido, como disco rígido (HD) e pen drive, devem ser encaminhados à Área de Compliance/Tecnologia da Informação, em caixa lacrada, para destruição adequada, conforme o procedimento interno adotado.

Somente o responsável pela geração ou pelo armazenamento do arquivo, ou documento a ser descartado, tem competência para descartá-lo ou deletá-lo, salvo quando este conferir expressa autorização para que terceiro o faça. Ainda, todo descarte deve ser registrado, a fim de manter um histórico que possibilite a realização de auditorias, caso necessário. No caso de informações que envolvam dados pessoais, o Colaborador seguirá os procedimentos descritos na Política de Retenção e Descarte de Dados da Kijani.

REDES SOCIAIS E E-MAIL PESSOAIS

A Kijani poderá suspender, sem aviso prévio e a seu exclusivo critério, o uso e o acesso a redes sociais, e-mails pessoais e serviços de mensagens para fins pessoais, nas dependências físicas e nos dispositivos da Kijani, por questões de governança e de segurança da informação.

DISPOSITIVOS

Os dispositivos físicos capazes de armazenar Informações Protegidas, como computadores, celulares, notebooks, tablets e outros, disponibilizados aos Colaboradores para a execução de suas atividades, são de propriedade da Kijani, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da Kijani, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pela Área de Compliance.

Os equipamentos devem ser identificados de forma individual, inventariados e protegidos de acessos indevidos. Os computadores devem ter o recurso de atualizações automáticas do sistema operacional habilitada por padrão e software antivírus instalado, ativado e atualizado frequentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar a Área de Compliance.

Arquivos pessoais e/ou não pertinentes ao negócio da Kijani (fotos, músicas, vídeos etc.) não deverão ser copiados/movidos para os drives de rede, pois podem sobrecarregar o armazenamento no disco do computador. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente por meio de comunicação prévia ao usuário.

Documentos imprescindíveis para as atividades dos Colaboradores da instituição deverão ser salvos em diretório sincronizado com nosso serviço de *cloud* garantindo o backup e a disponibilidade por meio de qualquer computador. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio Colaborador.

O Colaborador entende que é o responsável por todo e qualquer dano que causar nos equipamentos, por dolo ou culpa, e está ciente e concorda em observar as seguintes regras:

- O Colaborador é responsável pelos equipamentos e se compromete a empregar todos os cuidados necessários, como se o dispositivo fosse seu;
- Todos os computadores de uso individual deverão ter senha de BIOS para restringir o acesso de Colaboradores não autorizados. Tais senhas serão definidas pela Área de Compliance/Tecnologia da Informação da Kijani, que terá acesso a elas para manutenção dos equipamentos;
- Os dispositivos devem estar sempre a seu alcance e não podem ser deixados em locais públicos, em veículos ou em qualquer outro local, fora das dependências da Kijani, em que possa haver acesso do equipamento por pessoas não autorizadas, a fim de evitar o furto e/ou

roubo destes equipamentos, bem como o vazamento das Informações Protegidas nele contidas;

- Os Colaboradores devem informar à Área de Compliance/Tecnologia da Informação qualquer identificação de dispositivo estranho conectado ao seu computador;
- É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por terceiros devidamente contratados para o serviço;
- O Colaborador deverá manter a configuração do equipamento disponibilizado pela Kijani, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e pelas normas específicas da instituição, assumindo a responsabilidade como custodiante de informações;
- É expressamente proibido o fumo na mesa de trabalho e próximo aos equipamentos;
- Deverão ser protegidos por senha (bloqueados) todos os terminais de computador e impressoras quando não estiverem sendo utilizados;
- Todos os recursos tecnológicos adquiridos pela Kijani devem ter imediatamente suas senhas padrões (*default*) alteradas;
- Quando o Colaborador usar um dispositivo em um local público, deve utilizar película protetora em tal dispositivo, a fim de impedir a visualização de conteúdo por terceiros;
- Todos os dispositivos devem ser protegidos por senha e não devem ficar logados quando o Colaborador não estiver presente;
- Se, no decorrer do uso do dispositivo, o Colaborador tiver dúvidas sobre o seu manuseio ou constatar falhas que impliquem a necessidade de sua substituição ou manutenção, o Colaborador deverá abrir um chamado junto à Área de Compliance/Tecnologia da Informação que, por sua vez, além de fornecer os esclarecimentos necessários, deverá orientá-lo a entregar o equipamento no local indicado para sua substituição ou conserto;
- Caso o uso de um dispositivo seja esporádico, o Colaborador deverá devolvê-lo à Área de Compliance/Tecnologia da Informação em perfeitas condições de uso, juntamente com eventuais acessórios que lhe tenham sido entregues, como bolsas, *cases*, películas etc., tão logo termine o período necessário para o uso. Em caso de não devolução do equipamento, no prazo e local determinado, o Colaborador será responsável por restituir os custos de tal equipamento à Kijani, sem prejuízo de outras medidas legais e administrativas a serem tomadas pela Kijani; e
- No caso de perda, furto, roubo ou dano ao equipamento, o Colaborador deve comunicar imediatamente a Área de Compliance/Tecnologia da Informação, que procederá com a remoção do conteúdo corporativo contido no dispositivo. O Colaborador também deverá procurar as autoridades policiais e realizar um boletim de ocorrência, que deverá ser apresentado à Área de Compliance/Tecnologia da Informação quando da comunicação do incidente.

O uso indevido dos dispositivos da Kijani sujeitará o Colaborador às sanções aplicáveis, a depender da gravidade da conduta praticada. São algumas hipóteses de uso indevido:

- Tentar ou obter acesso não autorizado a outro computador, servidor ou rede;
- Burlar quaisquer sistemas de segurança;
- Acessar informações confidenciais sem a explícita autorização do proprietário;

- Vigiar secretamente outrem por dispositivos eletrônicos ou software, como, por exemplo, analisadores de pacotes (*sniffers*);
- Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;
- Hospedar pornografia, material racista ou qualquer outro conteúdo que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública; e
- Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

É proibida a utilização, pelo Colaborador, de dispositivos móveis particulares ou de terceiros (tais como celulares, smartphones, notebook, tablets, entre outros) para o desenvolvimento das atividades profissionais vinculadas à Kijani. Excepcionalmente, a Kijani poderá permitir que determinados Colaboradores possam configurar sua conta de e-mail corporativa em dispositivos pessoais móveis, o que deverá ser previamente aprovado pela Kijani e feito com o auxílio deste.

IDENTIFICAÇÃO E SENHAS

Todos os Colaboradores têm determinados privilégios de acesso a Informações Protegidas, de acordo com seu cargo e as suas atribuições. Alguns exemplos de privilégio são acesso externo ao e-mail, liberações no acesso à Internet e no acesso lógico, utilização externa de determinados equipamentos da Kijani, liberação de espaço em disco rígido, utilização de dispositivos móveis, entre outros.

O Colaborador receberá um login e uma senha, de acordo com o perfil que lhe for atribuído, que lhe permitirá ser identificado quando do acesso à infraestrutura da Kijani. Assim, o Colaborador somente terá acesso às áreas da infraestrutura da Kijani que forem autorizadas considerando o seu perfil. A Kijani reserva-se o direito de revisar, a qualquer momento e sem aviso prévio, por meio dos Departamentos competentes, os privilégios de qualquer Colaborador, a fim de resguardar os níveis de segurança da informação da Kijani.

O login e a senha do Colaborador são pessoais e, consequentemente, o Colaborador é o responsável pelo sigilo e pela manutenção segura da sua senha vinculada ao login, sendo proibido o compartilhamento de login e senha com terceiros, inclusive outros Colaboradores, sob pena de arcar com as sanções não só previstas neste Procedimento, mas também as penalidades civis, criminais e trabalhistas, respondendo, inclusive, por todo e qualquer dano que causar à Kijani.

Além do login do Colaborador, ele também receberá uma identificação física que lhe concederá acesso a determinadas áreas físicas da Kijani. Tal identificação será feita por meio de um crachá, cujo uso é pessoal e intransferível, e terá por finalidade registrar a entrada e saída das dependências da Kijani.

DESLIGAMENTO OU MOVIMENTAÇÃO DO COLABORADOR

Ao término do vínculo do Colaborador com a Kijani, o seu acesso à infraestrutura tecnológica da Kijani será revogado de forma imediata. O Colaborador deverá devolver todos e quaisquer dispositivos de propriedade da Kijani que estejam em sua posse, em perfeitas condições de uso, juntamente com eventuais acessórios lhe tenham sido entregues. As obrigações de sigilo e não reprodução das Informações Protegidas, assumidas pelo Colaborador nessa PSI, permanecerão em vigor mesmo após o desligamento do Colaborador.

Em caso de não devolução do equipamento, no prazo e local determinado, o Colaborador será responsável por restituir os custos de tal equipamento à Kijani. Em caso de perda, furto ou roubo de equipamentos, as regras previstas no item *Dispositivos* serão aplicadas.

Caso o Colaborador tenha acesso à conta de e-mail corporativa ou a qualquer outro software instalado em um dispositivo pessoal, deverá apresentar esse dispositivo para a Área de Compliance, que procederá à desinstalação correspondente.

Caso o Colaborador mude de área ou de função dentro da Kijani, este também deverá ter seus acessos revistos, passando a visualizar apenas os sistemas e pastas de rede necessários ao desempenho de sua nova função.

REPORTE DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Para evitar a exposição indevida das Informações Protegidas, a Kijani emprega medidas de segurança, tanto internas quanto externas, as quais atendem as obrigações legais vigentes. Porém, essas medidas somente serão eficazes se o Colaborador cumprir com as obrigações de segurança assumidas neste Procedimento, uma vez que tais incidentes podem ocorrer em razão de falhas humanas, tecnológicas ou sistêmicas.

Caso o Colaborador tome conhecimento ou suspeite de qualquer acontecimento que viole as regras deste Procedimento ou coloque em risco a segurança das informações da Kijani, ele deverá imediatamente comunicar a Kijani, que disponibilizará um canal de reporte anônimo. A Kijani, por meio da sua Área de Compliance, irá apurar as causas e os efeitos do incidente ocorrido, para então tomar as medidas de contenção, avaliação de impacto e necessidade de comunicação sobre o incidente ao órgão competente e/ou aos titulares das Informações Protegidas, conforme o Plano de Resposta a Incidentes da Kijani.

Para que seja realizada uma auditoria sobre o incidente, a Kijani analisará toda e qualquer informação, bem como as evidências disponíveis que possam identificar a causa do problema. As informações e evidências serão compiladas e anexadas a um relatório para formalização do ocorrido e avaliação da gravidade do incidente e necessidade de comunicação de fato relevante.

DISPOSIÇÕES FINAIS

As exceções às regras estabelecidas por esta norma específica para atender alguma demanda específica devem ser apresentadas à Área de Compliance da Kijani para avaliação e aprovação.

Esse Procedimento poderá ser revisto, atualizado e alterado anualmente ou a qualquer tempo, a exclusivo critério da Kijani, sempre que algum fato relevante ou evento motive sua revisão antecipada.

Em caso de dúvidas, comentários ou sugestões relacionadas a PSI ou a este Procedimento, entre em contato com o Encarregado da Kijani, que está à disposição nos seguintes endereços de contato:

Encarregado: André Adanya Katsumi
E-mail para contato: aka@kijani.com.br