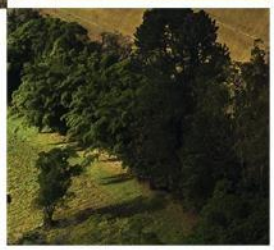
raizz
asset management







RAIZZ GESTÃO DE RECURSOS LTDA

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO, SEGURANÇA CIBERNÉTICA E CONTINUIDADE DE NEGÓCIOS

DEZEMBRO DE 2024

SUMÁRIO

INTRODUÇÃO

A presente Política de Segurança da Informação e Segurança Cibernética e Continuidade de Negócios da Raizz Asset (“Política” e “Gestora”, respectivamente) foi elaborada com o objetivo de identificar e definir os princípios, conceitos e diretrizes relacionados à segurança da informação, à segurança cibernética e à continuidade de negócios, os quais devem ser adotados por todos os funcionários e sócios da Gestora, bem como terceirizados que possuam acesso a suasinformações confidenciais (“Colaboradores”).

Os Colaboradores devem obrigatoriamente aderir a esta Política ao ingressar na Gestora, bem como concordar com suas posteriores e eventuais alterações mediante a assinatura do Termo de Compromisso anexo a esta Política, manifestando sua concordância com esta Política, bem como o caráter confidencial das informações confiadas aos Colaboradores.

Esta Política foi elaborada e deve ser interpretada em consonância com os demais manuais e políticas da Gestora, e deve ser revisada e atualizada anualmente pela área de compliance, PLDFT e gestão de riscos (“Área de Compliance, PLDFT e Gestão de Riscos”), a fim de incorporar medidas relacionadas a eventuais atividades e riscos novos ou anteriormente não abordados.

A estrutura da presente Política tem início nos princípios norteadores e diretrizes gerais que igualmente regem a segurança cibernética, a segurança da informação e a continuidade de negócios, e se desenvolve a partir da identificação e definição de contingências e procedimentos de engajamento direcionados especificamente os respectivos objetos desta Política.

A Área de Compliance, PLDFT e Gestão de Riscos realizará a revisão e atualização desta Política periodicamente ou sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão do Diretor de Compliance, PLDFT e Gestão de Riscos .

1.1. Princípios Norteadores

Em linha com as melhores práticas atinentes à segurança da informação, à segurança cibernética e à

continuidade de negócios, a presente Política considera que seus princípios norteadores básicos consistem em (i) confidencialidade, (ii) integridade, (iii) disponibilidade e continuidade e (iv) acesso controlado. Como será detalhadamente abordado nos itens seguintes, sua observância reflete em benefícios evidentes ao reduzir os riscos com vazamentos, fraudes, erros, uso indevido, sabotagens, roubo de informações e diversos outros problemas que possam comprometer os objetos específicos desta Política.

(i) Confidencialidade: Proteção compartilhada contra acessos não autorizados. Ameaça à segurança acontece quando há uma quebra de sigilo, permitindo que sejam expostas voluntaria ou involuntariamentedados restritos e que deveriam ser acessíveis apenas por um determinado grupo de usuários.

(ii) Integridade: Garantia da veracidade de dados, pois estes não devem ser alterados enquanto estão sendo transferidos ou armazenados. Ameaça à segurança acontece quando um determinado dado (físico ounão) fica exposto ao manuseio por uma pessoa não autorizada, que efetua alterações não aprovadas e sem o controle de seu proprietário (corporativo ou privado).

(iii) Disponibilidade e Continuidade: Prevenção contra as interrupções das operações da empresa como um todo. Os métodos para garantir a disponibilidade incluem um controle físico e técnico das funções dossistemas de dados, assim como a proteção dos arquivos, seu correto armazenamento e a realização de cópiasde segurança. As ameaças à segurança acontecem quando a informação deixa de estar acessível para quemnecessita dela.

(iv) Acesso controlado: O acesso dos usuários a dados é restrito e controlado, significando que só as pessoas que devem ter acesso a uma determinada informação, tenham esse acesso. Ameaça à segurança acontece quando há descuido ou possível quebra da confidencialidade das senhas de acesso à rede.

1.2. Diretrizes Gerais

Em consonância com os princípios norteadores acima expostos e com as funções usualmente designadas aos mecanismos de controles internos que tenham como objeto a segurança cibernética, a segurança da informação e a continuidade de negócios, identificamos abaixo as diretrizes gerais que devem permear os procedimentos de engajamento definidos nesta Política:

(i) Identificação/avaliação de riscos (risk assessment): Identificar os riscos internos e externos, os

ativos de hardware e software e processos que precisam de proteção.

(ii) Ações de prevenção e proteção: Estabelecer um conjunto de medidas cujo objetivo é mitigar e minimizar a concretização dos riscos identificados no item anterior, ou seja, buscar impedir previamente a ocorrência de um ataque cibernético, incluindo a programação e implementação de controles.

(iii) Monitoramento e testes: Detectar as ameaças em tempo hábil, reforçando os controles, caso necessário, e identificar possíveis anomalias no ambiente tecnológico, incluindo a presença de usuários, componentes ou dispositivos não autorizados.

(iv) Criação do plano de resposta: Ter um plano de resposta, tratamento e recuperação de incidentes, incluindo um plano de comunicação interna e externa, caso necessário.

(v) Reciclagem e revisão: Manter o programa de segurança cibernética continuamente atualizado, identificando novos riscos, ativos e processos e reavaliando os riscos residuais.

2. SEGURANÇA DA INFORMAÇÃO

2.1. Conceitos Específicos

As regras e procedimentos de controle da segurança da informação da Gestora estão estruturadas a partir dos seguintes conceitos específicos:

(i) Ambiente físico: dependências físicas da empresa, que inclui sua sede e filial;

(ii) Ambiente lógico: ambiente controlado, eletrônico, onde circulam e são armazenadas informações edocumentos confidenciais, softwares e sistemas;

(iii) Segregação: garante que a informação, por meio de ambiente lógico ou físico, esteja disponível apenas para as pessoas que necessitam do acesso àquela informação para a realização de suas atividades – conceito “need to know”.

2.2. Responsabilidades

De forma geral, cabe a todos os Colaboradores e prestadores de serviço da Gestora:

(i) Conhecer e cumprir fielmente esta Política e outros documentos normativos que venham a ser divulgados;

(ii) Evitar situações que possam caracterizar negligência ou que estejam diretamente violando o Códigode Ética e Conduta, as demais políticas e diretrizes internas da Gestora, ou qualquer lei ou regulamento, sob pena de sofrer sanções;

(iii) Assegurar que os recursos tecnológicos e informações disponibilizados pela Gestora sejam utilizados em conformidade às políticas internas;

(iv) Proteger as informações contra acessos, modificação, destruição ou divulgação não autorizadas pelaGestora;

(v) Procurar a Área de Compliance, PLDFT e Gestão de Riscos e/ou a área de tecnologia e informação
("Área de TI"), quando julgar necessário.

2.3. Comportamento Seguro e Confidencialidade

A Gestora se compromete a adotar ferramentas e tecnologias de segurança da informação com o objetivo de garantir a integridade das informações e impedir: (i) acesso e transmissão de informações e arquivos confidenciais a pessoas não autorizadas; (ii) liberação de senhas e códigos de identificação de usuários; e (iii) ocorrência de ataques cibernéticos. A Gestora disponibiliza aos Colaboradores as ferramentas tecnológicas necessárias para o exercício de suas funções incluindo rede interna de arquivos com backup diário e sistema proprietário em cloud.

2.4. Classificação de Informações

A Gestora classifica suas informações de acordo com o grau de confidencialidade e criticidade para seus negócios. Todas as informações precisam estar protegidas durante seu ciclo de vida, conforme aplicável: geração, manuseio, armazenamento, transporte e descarte.

(i) Informações Públicas: são aquelas destinadas ao público em geral, que podem ser de caráter informativo. Exemplos: informações disponíveis no website da Gestora; comunicados e apresentações institucionais destinadas aos clientes e parceiros; informações genéricas sobre as classes de fundos geridas;etc.

(ii) Informações Internas: são aquelas destinadas ao uso dos Colaboradores da Gestora, que só devem circular e ser compartilhadas internamente a que tem necessidade de ter acesso (need to know). A divulgação externa não intencional não causaria danos à Gestora, a seus clientes ou Colaboradores. Exemplos: atas de comitês internos; relatórios internos; cartas e notificações de órgãos reguladores e autorreguladores; etc.

(iii) Informações Confidenciais: correspondem a mais alta classificação de segurança para as informaçõesque transitam na Gestora. Refere-se a informações cuja divulgação não autorizada poderia potencialmentecausar danos substanciais, constrangimentos ou penalidades à Gestora, seus investidores, Colaboradores, companhias investidas ou mesmo companhias alvo dos fundos geridos. São também as informações cuja divulgação só é permitida a órgãos reguladores ou autorreguladores, Receita Federal, advogados, contadores, consultores especializados, sócios ou investidores. As pessoas que tratarem essas informações têm a responsabilidade de protegê-las e, sempre que possível, somente divulgá-las mediante assinatura deacordos de confidencialidade. Exemplos: informação antecipada e não autorizada de operações, tais como fusões e aquisições; novos produtos e/ou serviços; informações protegidas por sigilo legal; informações relativas às classes de fundos; informações societárias e/ou de remuneração dos Colaboradores; etc.

Apenas Colaboladores autorizados terão acesso a informação confidencial, e apenas na medida do necessário para a execução de suas atividades. Caso um detentor de informação confidencial mude de função dentro da Gestora na qual o acesso a tal informação não seja mais necessário, então o acesso do Colaborador será restringido pelo responsável da Área de TI.

Da mesma forma, ato contínuo ao desligamento de um Colaborador, o acesso deste a todos os sistemas, informações e documentos da Gestora será bloqueado.

Os Colaboradores deverão comunicar à Área de Compliance, PLDFT e Gestão de Riscos quaisquer casos de violações às normas de segurança da informação que tenham conhecimento. Toda violação ou desvio é investigado para a determinação das medidas necessárias, visando à correção da falha ou reestruturação de processos. Em caso de vazamento de informação confidencial, o Diretor de Compliance, PLDFT e Gestão de Riscos discutirá com o Comitê de Compliance, PLDFT e Gestão de Riscos (ou, se for o caso, com a Área de TI, qual o melhor plano efetivo de recuperação e medidas para minimizar e prevenir danos.

2.5. Política de Acesso (Físico e Lógico)

A Gestora possui sistema de controle de acesso de pessoas autorizadas às dependências do

escritório por meio de senha pessoal, individual e intransferível com possibilidade de utilização de logs e histórico de acesso.

No ambiente lógico, a Gestora conta com infraestrutura tecnológica que permite acesso por perfil de usuário com base no princípio da necessidade da informação para execução das atividades do Colaborador. Além disso, cada Colaborador possui um identificador (ID de Colaborador) registrado de forma a assegurar a responsabilidade por suas ações. O sistema proprietário está integrado e conta com ferramenta de gerenciamento de controle de acesso.

A Área de Compliance, PLDFT e Gestão de Riscos é responsável por aprovar a liberação e restrição de acesso aos Sistemas de Informação e a outros ambientes lógicos. Os acessos são periodicamente revisados pelo time da Área de Compliance, PLDFT e Gestão de Riscos. A qualquer momento, o Colaborador que precisar ter acesso à informação ou à sistema restrito, incluindo as hipóteses de alteração de posição ou função, deverá solicitar a aprovação da Área de Compliance, PLDFT e Gestão de Riscos.

2.5.1 Diretriz de Controle de Acesso

Cada Colaborador é responsável pelo uso adequado das informações que possui acesso, o que inclui as senhas de acesso aos sistemas de informações e crachás de identificação.

O acesso ao Centro de Processamento de Dados (CPD) da Gestora é restrito às Áreas de TI, Risco e Compliance e Administrativo.

2.5.2. Diretriz para Senha

A senha é a chave de acesso pessoal que garante que somente pessoas autorizadas utilizem determinados dispositivos ou recursos. Por isso, cabe aos usuários alguns procedimentos de segurança.

(i) Não compartilhar senha, não anotar em arquivos físicos ou de fácil acesso;

(ii) Não utilizar códigos comuns, como próprio nome, data de nascimento, nomes de parentes,números telefônicos, palavras existentes no dicionário ou números sequenciais;

(iii) As senhas precisam ser diferentes entre si, como as de sites de administradores, bancos, sistemasinternos e externos;

(iv) Utilizar preferencialmente senhas distintas para uso corporativo e para uso pessoal; e

(v) Trocar as senhas periodicamente e sempre que suspeitar de algo.

2.6. Política de Backup

Todos os registros eletrônicos realizados pela Gestora deverão ser mantidos e estar disponíveis para atender os prazos legais e regulatórios praticados pelos órgãos reguladores locais e de jurisdições que a Gestora atue em mercado regulado.

As informações mantidas em meios eletrônicos devem possuir polícias de backup periódicas e devem permanecer íntegras e acessíveis por prazo não inferior a 5 (cinco) anos. O acesso a essas bases deve ser limitado somente a pessoas autorizadas pela Área de Compliance, PLDFT e Gestão de Riscos.

2.7. Privacidade

2.7.1. Diretriz de Utilização de E-mail

A Gestora possui servidores de e-mail configurados com camadas de proteção de segurança para prevenir vírus ou a execução de códigos maliciosos. Os usuários são frequentemente orientados a utilizar o serviço de e-mail de forma segura. Seguem diretrizes para utilização de e-mail na Gestora.

(i) O usuário deve estar conectado ao e-mail corporativo sempre que estiver trabalhando nocomputador.

(ii) Não utilizar contas de e-mail pessoal para enviar qualquer tipo de informação confidencial ouinterna.

(iii) Ao receber e-mails com links, verificar se o mesmo corresponde ao endereço que aparece na tela.Para tanto, posicionar o ponteiro do mouse sobre o link (não clicar).

(iv) Não abrir, em hipótese alguma, caso não tenha certeza da procedência do envio e da legitimidadedo e-mail, evitando o phising.

2.7.2. Diretriz de Utilização de Telefone

Responsabilidades e forma de uso: O usuário que utiliza um telefone em seu meio de trabalho,

utilizando aplicativos para tanto, é responsável por todo conteúdo da conversa e só deverá utilizar o telefone para o seu desempenho profissional na empresa.

2.7.3. Diretriz de Utilização de Internet

(i) A Área de TI deve manter os acessos à internet configurados conforme uma política de bloqueios a ser estabelecida pela Área de Compliance, PLDFT e Gestão de Riscos.

A Área de TI deve manter bloqueados os cloud services (como Dropbox, OneDrive e Google Drive), por não ser permitido o uso desse tipo de serviço pelos Colaboradores. O compartilhamento de documentospor meio de cloud services, quando necessário, deve ser realizado pela Área de TI, com anuência da Área de Compliance, PLDFT e Gestão de Riscos.

(ii) A instalação de softwares é de responsabilidade da Área de TI e bloqueada por senha.

(iii) É proibido fazer upload ou download de softwares ou dados ilegais (“piratas”).

(iv) Não é permitido enviar ou fazer download de músicas, vídeos ou quaisquer outros arquivos que possam comprometer o bom funcionamento da infraestrutura local ou que violem as leis de direitos autorais.

(v) Não é permitido o uso de compartilhadores de informações como redes Peer-to-Peer, também conhecidas como redes P2P dentro da Gestora, sendo as mesmas bloqueadas pelos serviços de firewall.

(vi) A internet disponibilizada aos visitantes é acessível somente por uma rede de visitantes. Essa redeé totalmente segregada da rede interna da Gestora e não tem acesso aos servidores da Gestora.

(vii) No caso de perda ou roubo de dispositivos móveis que contenham acesso ao e-mail corporativo, a Área de TI juntamente com a Área de Compliance, PLDFT e Gestão de Riscos devem ser comunicados imediatamente para fins de bloqueio imediato.

Em caráter excepcional, e em função de suas atividades, alguns Colaboradores poderão ter acessos especiais para utilização de programas específicos na internet. Nessas hipóteses, o Colaborador deverá fundamentar as razões pela qual entende ser necessário acesso especial à internet. Adicionalmente o Colaborador deverá assinar termo de responsabilidade se comprometendo a manter todas as informações que tiver acesso sob sigilo e se responsabilizando no caso de eventual

vazamento.

Esse termo de responsabilidade também deverá ser assinado pelo responsável da área e encaminhado à Área de Compliance, PLDFT e Gestão de Riscos que, depois de verificar suas informações, irá solicitar o desbloqueio das ferramentas de internet necessárias para o Colaborador, junto à Área de TI.

2.7.4. Diretriz de Utilização da Rede Interna

(i) A Gestora possui segregação de pastas na rede interna. Cada área possui um perfil de acesso e cadaColaborador somente terá acesso a arquivos e informações relacionados às suas respectivas atividades, como nível de segurança. Acesso a outros documentos e arquivos dependem de autorização expressa da Gestorada área detentora da informação.

(ii) É proibido armazenar na rede arquivos de música, vídeos e fotos que não sejam de propriedade daempresa.

(iii) O usuário não deverá obter ou tentar obter acesso não autorizado a outros sistemas ou redes de computadores conectados à rede interna.

2.7.5. Outras Diretrizes

(i) Não deixar papeis ou mídias removíveis da empresa contendo informações confidenciais sem o devido armazenamento quando estiver fora do local de trabalho (política de mesa limpa). Essas informaçõesprecisam estar guardadas em armários/gavetas com chave.

(ii) Informações confidenciais, quando impressas, devem ser imediatamente retiradas da impressora.

2.8. Ações em Caso de Não Conformidade

Os descumprimentos a esta Política serão submetidos à Área de Compliance, PLDFT e Gestão de Riscos, que endereçará o referido descumprimento e suas eventuais consequências à Alta Administração.

A violação comprovada a esta Política constituirá justa causa para possível aplicação de sanção disciplinar, independente das funções exercidas, e sem prejuízo das penalidades legais cabíveis, observadas as regras constantes do contrato/estatuto social, acordo de acionistas/sócios e/ou contrato de trabalho/estágio.

A omissão diante da violação conhecida da lei ou de qualquer disposição desta Política não é uma atitude correta e constitui uma violação ao Código de Ética da Gestora. No caso de conhecimento sobre o descumprimento a esta Política, o Colaborador deve informar tal descumprimento a qualquer membro da Área de Compliance, PLDFT e Gestão de Riscos, que tem o dever de analisar e recomendar as respectivas ações corretivas para a Alta Administração.

2.9. Gestão de Incidentes de Segurança

Qualquer suspeita de um incidente de segurança deve ser imediatamente reportada à Área de TI e à Área de Compliance, PLDFT e Gestão de Riscos. Nenhum Colaborador deverá investigar por conta própria, ou tomar ações para se defender do ataque, a não ser que seja instruído de tal forma pela Área de TI, que está capacitada para conter as exposições, analisar os impactos e conduzir investigações, coletando evidências para possíveis ações jurídicas.

Incidentes relevantes que possam causar prejuízos financeiros ou materiais precisam ser reportados à Alta Administração para que delibere quais ações corretivas precisam ser tomadas.

2.10. Testes Periódicos de Segurança

A Área de TI é responsável pela realização de testes periódicos e ações preventivas para detectar falhas de segurança e vulnerabilidades. A Área de Compliance, PLDFT e Gestão de Riscos deverá monitorar os resultados desses testes e manter os registros em caso de falhas e violações desta Política.

Nesse sentido, caberá à Área de TI realizar:

(a) testes periódicos de segurança para os sistemas de informações, em especial os mantidos em meios eletrônicos;

(b) o efetivo monitoramento do trancamento de mesas das estações de trabalho e os processos de backup de informações pelos Colaboradores. Sempre que solicitado algum desvio, cabe ao Diretor de Compliance instruir o Colaborador infrator a respeito das boas práticas de conduta; e

(c) a verificação de eventual esquecimento de documentos em cima das mesas e/ou nas impressoras, instruindo os Colaboradores sobre a necessidade de preservação das informações.

Em relação aos testes periódicos para os sistemas de segurança de informação, especificamente para os mantidos em meio eletrônico, a Gestora realiza, por meio dos Colaboradores da Equipe de Compliance, testes semestrais que são formalizados por meio de relatórios encaminhados ao Diretor de Compliance. Os relatórios mencionados deverão conter:

(a) A lista de todos os sistemas e quais os Colaboradores possuem acesso a cada um; e

(b) Eventuais inconsistências detectadas em cada um dos sistemas/ferramentas/softwares.

Incumbe ao Diretor de Compliance revisar a lista de atribuições, confirmando a adequação dos acessos de cada Colaborador aos seus respectivos cargos e prerrogativas, além de adotar medidas cabíveis para corrigir eventuais inconsistências constatadas no relatório.

Ademais, a Gestora compromete-se a adotar medidas que incluem, mas não se limitam a (a) verificar os logins dos Colaboradores; (b) alterar a senha dos Colaboradores anualmente; (c) realizar testes no firewall e nas restrições impostas aos diretórios; e (d) realizar testes no back-up rotineiro.

Sempre que houver a ocorrência de descumprimento ou suspeita ou indício de descumprimento de quaisquer das regras estabelecidas em quaisquer dos manuais, códigos e políticas internas da Gestora, bem como quaisquer outras aplicáveis às atividades da Gestora, de acordo com os procedimentos estabelecidos nos referidos códigos e políticas internas, o Diretor de Compliance poderá se utilizar dos registros e sistemas de monitoramento eletrônico e telefônico disponíveis para verificar a conduta dos Colaboradores envolvidos, sendo facultado o acesso pela Gestora a quaisquer informações, contatos, documentos e arquivos gerados pelas atividades profissionais desenvolvidas na Gestora, ou que transitem pela sua infraestrutura de tecnologia

2.11. Treinamento

A Área de TI, com apoio da Área de Compliance, PLDFT e Gestão de Riscos, é responsável por difundir as melhores práticas dentro da Gestora, por meio de treinamentos, sempre que houver uma atualização nas diretrizes de segurança.

3. SEGURANÇA CIBERNÉTICA

Em consonância com as Diretrizes Gerais apresentadas no item 1.2. acima, a Gestora adota procedimentos de Segurança Cibernética, listados abaixo, sendo certo que a supervisão desses

procedimentos e desta Política cabem à Área de TI, com o apoio da Área de Compliance, PLDFT e Gestão de Riscos. A Área de Compliance, PLDFT e Gestão de Riscos deverá apresentar o resultado dos testes e monitoramento periódicos realizados com base nessa Política à Alta Administração e ao Comitê de Compliance, PLDFT e Gestão de Riscos. A Alta Administração e a Comitê de Compliance, PLDFT e Gestão de Riscos, com base nesses relatórios, poderão propor (i) ajustes na presente Política, assim como (ii) planos de ação específicos.

3.1. Identificação e Avaliação de Riscos (Risk Assessment)

A Gestora deverá identificar e avaliar os principais riscos cibernéticos aos quais está exposta. O Guia de Cibersegurança da Anbima[1] informa que os ataques mais comuns de criminosos cibernéticos (cybercriminals) são os seguintes:

(i) Malware (e.g. vírus, cavalo de troia, spyware e ransomware);

(ii) Engenharia Social;

(iii) Pharming;

(iv) Phishing;

(v) Vishing;

(vi) Smishing;

(vii) Acesso pessoal;

(viii) Ataques de DDoS e botnets; e

(ix) Invasões (advanced persistent threats).

3.2. Ações de Prevenção e Proteção

Em complemento aos procedimentos de Segurança da Informação previstos acima, ao incluir novos equipamentos e sistemas em produção, a Gestora conta com recursos anti-malware em estações e servidores de rede, como antivírus e firewall. Da mesma maneira, monitora o acesso a websites e restringe a execução de softwares e/ou aplicações não autorizadas.

[1] O Guia de Cibersegurança da Anbima (2021) pode ser acessado no seguinte link: https://www.anbima.com.br/data/files/34/B3/04/8F/D96F971013C70F976B2BA2A8/Guia%20de%20Ciberseguranca%20ANBIMA.pdf.

Adicionalmente, a Gestora dispõe de recursos para (i) realizar verificação de configurações, de modo a mitigar vulnerabilidades que possam surgir em razão da inclusão de novos equipamentos e sistemas em produção, incluindo a realização de testes prévios quando novos equipamentos e sistemas forem implementados em ambientes de homologação e de prova de conceito, (ii) implementar anti-malware em estações e servidores de rede, como antivírus e firewall, permitindo, também, a verificação do acesso a websites e restrição a execução de softwares e/ou aplicações não autorizadas, bem como (iii) realizar backup das informações e dos diversos ativos da instituição, conforme as disposições do presente documento e Plano de Continuidade do Negócio descrito abaixo.

3.3. Monitoramento

Os sistemas, serviços, dados, informações disponíveis na Gestora ou por esta disponibilizados, para serem usados pelos Colaboradores, não devem ser interpretados como sendo de uso pessoal. Todos os Colaboradores devem ter ciência de que o uso está sujeito à monitoramento periódico. Esse monitoramento poderá ser realizado automaticamente (software e/ou hardware), pela Área de TI, pela Área de Compliance, PLDFT e Gestão de Riscos e/ou por prestador de serviços externo.

Os registros obtidos e o conteúdo dos arquivos poderão ser utilizados com o propósito de determinar o cumprimento do disposto nesta Política, e nos demais documentos internos da Gestora, e, conforme o caso, servir como evidência em processos administrativos, arbitrais e/ou judiciais.

A Área de TI da Gestora possui roteiro de testes indicando as ações de proteção implementadas para garantir seu bom funcionamento e efetividade. Da mesma maneira deve diligenciar de modo a manter inventários atualizados de hardware e software atualizados, bem como os sistemas operacionais e softwares de uso atualizados.

Periodicamente, a Área de TI realiza testes de segurança no seu sistema de segurança da informação e proteção de dados. Dentre as medidas, incluem-se, mas sem se limitar:

(i) Verificação dos logs dos Colaboradores;

(ii) Alteração periódica de senha de acesso dos Colaboradores;

(iii) Segregação de acessos;

(iv) Manutenção periódica de hardwares; e

(v) Backup diário, realizado com fitas locais e redundância em nuvem.

Sem prejuízo dos testes realizados, a Gestora realizará, de tempos em tempos, simulações de ataques e respostas que seriam possíveis nestes casos. As simulações deverão prever as ferramentas mais usadas pelos criminosos cibernéticos, revelando as principais vulnerabilidades dos sistemas da Gestora, o que permitirá efetuar as correções devidas a tempo de evitar ou mitigar um ataque real.

As rotinas de backup são periodicamente monitoradas.

Essa política de segurança cibernética é revisada periodicamente em prazo não superior à 24 (vinte e quatro) meses.

3.4. Plano de Resposta

Conforme as melhores práticas de mercado, a Gestora 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 do item 3.1 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.

Essas providências consistem em:

Área de TI:

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.

Área de Compliance:

a) Criação de relatório baseado no laudo pericial elaborado pela Área de TI, 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.

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 Gestora resultantes do incidente de segurança.

Em caso de necessidade, poderá ser contratada empresa especializada para combater ao evento identificado. Caso o evento tenha sido causado por algum Colaborador, deverá ser avaliada a sua culpabilidade. Eventos que envolvam a segurança das informações sigilosas ou que sejam decorrentes de quebra de segurança cibernética deverão ser formalizados em relatório pela Área de TI, para deliberação pela Alta Administração.

4. PLANO DE CONTINUIDADE DE NEGÓCIOS

4.1. Responsabilidades

A Área de Compliance, PLDFT e Gestão de Riscos deve se certificar da implementação do Plano de Continuidade de Negócios ("PCN") para garantir a continuidade dos processos críticos da Gestora em casos de eventos inesperados que afetem parcial ou integralmente a sua capacidade operacional, assegurando a realização de testes periódicos, conforme aplicáveis, que atestem sua efetividade. Esse documento que tem por objetivo informar, treinar, organizar, orientar, facilitar, agilizar e uniformizar as ações necessárias às respostas de controle e combate às ocorrências anormais.

À Área de Compliance, PLDFT e Gestão de Riscos caberá (i) manter este PCN sempre atualizado; e (ii) treinar os Colaboradores para casos de necessidade de acionamento do PCN.

Tendo em vista que a Gestora exerce exclusivamente a gestão de classes de Fundos de Investimento Imobiliáirio ("FIIs") de "Tijolos", a instituição possui uma quantidade limitada de serviços críticos. Os investimentos previstos para as classes de FIIs de "Tijolos" são predominantemente a aquisição de ativos para os quais não há negociação ativa e frequente, sendo utilizada, portanto, uma metodologia para continuidade de negócios conforme abaixo descrito.

Através da definição de hipóteses com cenários e eventos prováveis, a Gestora desenvolveu e constantemente atualiza seu PCN. Serão abordados dois aspectos diferentes sobre o PCN: (i) o primeiro está vinculado à recuperação de dados em caso de desastres, focado na recuperação de informações armazenadas em software e equipamentos eletrônicos; e (ii) o segundo explanará como é possível diagnosticar os eventos que podem afetar o funcionamento da organização e estabelecer alternativas para que as operações não sejam interrompidas.

4.2. Plano Estratégico

4.2.1 Contingência de Internet

Com o intuito de ter acesso constante à internet, a Gestora utiliza dois links de diferentes operadoras. Assim, caso um link deixe de funcionar, o segundo poderá ser utilizado de imediato.

4.2.2 Contingência de Energia

A Gestora conta com no breaks para os switches e links da internet garantindo o suprimento de energia elétrica e o trabalho desenvolvido pelos Colaboradores da instituição. Na hipótese de o suprimento de energia não ser normalizado, os colaboradores poderão utilizar a funcionalidade de trabalho remoto, de modo que o trabalho desenvolvido não será interrompido.

4.2.3 Sistema de Backup

Os e-mails e as informações que constam no servidor contratado pela Gestora (rede de arquivos) são mantidas em backup por até 7 (sete) anos, com monitoramento constante e testes periódicos de restauração.

4.2.4 Acesso Remoto

Em caso de impossibilidade de utilização das instalações da Gestora, todos os Colaboradores possuem a funcionalidade do acesso remoto, desde que por meio de um link de internet seguro, de modo que esses tenham acesso às suas estações de trabalho remotamente, com as permissões e restrições de acesso.

4.2.5 Desastres em Geral

Em caso de algum incêndio, desastre natural ou qualquer outra hipótese que impossibilite o acesso físico aos seus escritórios, ficarão servidor da Gestora estará localizado fora da sede da instituição, e os Colaboradores acessarão as informações e efetuarão seu trabalho por acesso remoto.

4.3. Testes de Contingência

A Área de TI, com auxílio da Área de Compliance, PLDFT e Gestão de Riscos, é responsável por organizar, coordenar e supervisionar testes de contingência anuais. Em cada teste deverá ser avaliado se o PCN é capaz de suportar, de modo satisfatório, os processos operacionais críticos para a continuidade dos negócios da Gestora e manter a integridade, a segurança e a consistênciados bancos de dados, e se tais planos podem ser ativados tempestivamente.

4.4. Acionamento do PCN

Qualquer Colaborador, assim que verificar uma situação de contingência, deve informar imediatamente os responsáveis pelas Áreas de TI e de Risco e Compliance da Gestora, as quais caberá:

(i) Verificar e confirmar a situação de contingência;

(ii) Informar aos Colaboradores da Gestora sobre o acionamento do PCN;

(iii) Acionar os eventuais prestadores de serviço envolvidos na contingência; e

(iv) Acompanhar a situação até a sua normalização.

A Área de TI deverá informar os Colaboradores que a normalidade foi reestabelecida por meio de comunicados por e-mail e aviso no site, caso seja necessário. A Área de Compliance, PLDFT e Gestão de Riscos registrará as ações que foram tomadas na contingência, o que as motivou, e se houve responsáveis pelo problema. Após o evento é necessário rever o PCN no intuito de validar a execução do plano e se o PCN precisa ser atualizado.

4.5. Considerações Finais

O desconhecimento em relação a qualquer das obrigações e compromissos decorrentes deste documento não justifica desvios, portanto, em caso de dúvidas ou necessidade de esclarecimentos adicionais sobre seu conteúdo, favor consultar a Área de Compliance, PLDFT e Gestão de Riscos e/ou a Área de TI.

O descumprimento dos preceitos deste documento ou de outros relacionados pode acarretar medidas disciplinares, medidas administrativas ou judiciais cabíveis, podendo levar à demissão, desassociação, desligamento ou outras sanções, inclusive decorrentes da legislação, autorregulação ou regulamentação aplicável.

A expectativa da Alta Administração da Gestora é que em até 6 (seis) meses a contar da última revisão deste documento, todos os controles e estruturas aqui citados já estejam em vigor em caráter efetivo, sendo certo que alguns deles já estão em pleno funcionamento nesta data.

5. APROVAÇÕES E VERSÕES DA POLÍTICA

Data	Versão	Responsável
Julho de 2024	1ª	Diretor de Compliance, PLDFT e Gestão de Riscos
Dezembro de 2024	2ª e atual	Diretor de Compliance, PLDFT e Gestão de Riscos

ANEXO I

TERMO DE ADESÃO À POLÍTICA DE SEGURANÇA DA INFORMAÇÃO, DE SEGURANÇA CIBERNÉTICA E CONTINUIDADE DE NEGÓCIOS

Eu, [nome], [nacionalidade], [estado civil], [profissão], inscrito no CPF/ME sob o nº [●], declaro que tomei conhecimento dos termos e condições da "Política de Segurança da Informação, de Segurança Cibernética e Continuidade de Negócios" da Raizz Asset ("Gestora"), tendo recebido uma cópia do "Política de Segurança da Informação, de Segurança Cibernética e Continuidade de Negócios" da Gestora.

Subscrevendo o presente formalizo a minha adesão ao "Política de Segurança da Informação, de Segurança Cibernética e Continuidade de Negócios", comprometendo-me a cumprir com todos os seus termos e condições, incluindo a obrigação de manter em confidencialidade as informações confidenciais, reservadas ou privilegiadas que lhe tenha sido confiado em virtude do exercício de suas atividades profissionais.

[cidade], [data]

_____

[nome]