STRIVO GESTÃO DE RECURSOS S.A.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Versão 2.0
Vigência Maio / 2025

Atividade	Área
Elaboração	Direção de Compliance
Revisão	Comitê de Compliance
Aprovação	Comitê de Compliance

Classificação das Informações:
Uso Interno/Uso Público

1. Introdução

A Segurança da Informação pode ser sumarizada como a proteção contra o uso ou acesso não-autorizado à informação, bem como a proteção contra a negação do serviço a usuários autorizados, enquanto a integridade e a confidencialidade dessa informação são preservadas.

A Segurança da Informação não está confinada a sistemas de computação, nem à informação em formato eletrônico. Ela se aplica a todos os aspectos de proteção da informação ou dados, em qualquer forma. O nível de proteção deve, em qualquer situação, corresponder ao valor dessa informação e aos prejuízos que poderiam decorrer do uso impróprio dela. A Segurança da Informação também cobre toda a infraestrutura que permite o seu uso, como processos, sistemas, serviços, tecnologias e outros.

A Segurança da Informação refere-se à proteção existente sobre as informações de uma determinada empresa ou pessoa, isto é, aplica-se tanto às informações corporativas quanto pessoais. Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa. Ela pode estar guardada para uso restrito ou exposta ao público para consulta ou aquisição.

Os atributos básicos da Segurança da Informação são os seguintes: (i) Confidencialidade: propriedade que limita o acesso à informação tão somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação; (ii) Integridade: propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (Corrente, intermediária e permanente); (iii) Disponibilidade: propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação; e (iv) Autenticidade: propriedade que garante que a informação é proveniente da fonte anunciada e que não foi alvo de mutações ao longo de um processo.

2. Objetivos

Esta Política de Segurança da Informação tem como objetivo definir as diretrizes e responsabilidades que norteiam a proteção dos ativos de informação da Strivo Gestora de Recursos S.A. (“Strivo”, “Gestora”), estabelecendo normas e procedimentos para o preservar a confidencialidade, integridade e disponibilidade das informações, de forma que atenda as disposições regulatórias, bem como as melhores práticas de governança.

3. Abrangência e Aplicabilidade

Esta Política se aplica a todos os acionistas, diretores, empregados, funcionários, *trainees*, estagiários, prestadores de serviços e fornecedores que venham, de maneira direta ou indireta, trabalhar para a Strivo, bem como todos que, de alguma forma, auxiliam o desenvolvimento das atividades da Gestora (“Membros”).

Sempre que pertinente, será exigido a formalização do compromisso com a Política de Segurança da Informação, seja através de um termo de ciência e responsabilidade com usuários, ou contratualmente quando por ocasião de contratação de pessoas, serviços e fornecedores.

4. Diretrizes

São diretrizes da Política de Segurança da Informação da Strivo:

a) Segurança da Informação: Processos e metodologias que são projetados, implementados, mantidos e atualizados para assegurar a confidencialidade, integridade e disponibilidade das informações através da tecnologia, pessoas e processos a fim de detectar, prevenir e responder às ameaças.

b) Usuários: Indivíduo, ou processo (sistema) agindo em nome de um indivíduo autorizado pelo proprietário do ativo da informação para os respectivos acessos.

c) Confidencialidade: É a propriedade da informação com o fim de assegurar que as informações não serão divulgadas a pessoas, processos ou tecnologias não autorizadas.

d) Disponibilidade: É a propriedade da informação com o fim de assegurar o acesso estável às informações sempre que necessário para usuários autorizados.

e) Integridade: É a propriedade da informação com o fim de assegurar que as informações não tenham sido alteradas acidental ou deliberadamente e que sejam precisas e completas.

f) Proprietário de Ativos de Informação: É o usuário com responsabilidade direta sobre determinados ativos de informação da Strivo.

g) Dados Pessoais: Informação relacionada a pessoa natural identificada ou identificável.

h) Dados Pessoais Sensíveis: Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

5. Definições

A Política de Segurança da Informação da Strivo, descrita neste documento, é caracterizada, principalmente, pela preservação dos seguintes conceitos:

a) Confidencialidade: garantia de que a informação seja acessível somente pelas pessoas autorizadas, pelo período necessário;
b) Disponibilidade: garantia de que a informação esteja disponível para as pessoas autorizadas sempre que houver a real necessidade;

c) Integridade: garantia de que a informação esteja completa e integra e que não tenha sido modificada ou destruída de maneira não autorizada ou acidental durante o seu ciclo de vida.

6. Papéis e Responsabilidades

A gestão de Segurança da Informação da Strivo é atribuída à Diretoria de Compliance, Risco & PLDFT e sua equipe. Não obstante a designação, é papel e responsabilidade de todos os Membros observar e seguir as políticas, padrões, procedimentos e orientações estabelecidas para o cumprimento da presente Política.

Seguem indicações não exaustivas destas responsabilidades:

a) Diretoria de Compliance, Risco & PLDFT e Equipe:

i) Conduzir os esforços estratégicos para cumprimento dos objetivos de Segurança da Informação da Strivo;

ii) Estabelecer mecanismos de proteção com vistas a prevenir, detectar, reduzir, e mitigar as vulnerabilidades nos ativos de informação;

iii)Realizar ações com a finalidade de prevenir a ocorrência de incidentes de segurança;

iv) Orquestrar rotinas e procedimentos necessários para a resposta de incidentes;

v) Realizar o monitoramento contínuo e detecção de ataques cibernéticos;

vi) Certificar o controle de acesso adequado dos usuários, impedindo acessos indevidos e/ou em demasia e liberando apenas os acessos devidamente autorizados;

vii) Garantir que os prestadores de serviços terceirizados e relevantes cumpram com nossas políticas e normas de segurança, bem como as obrigações regulamentares aplicáveis;

viii) Garantir a conscientização da equipe através de treinamentos mandatórios e avaliações periódicas;

ix) Revisar, anualmente, esta Política;

x) Divulgar e garantir que a presente Política seja cumprida integralmente; e

xi) Aprovar a Política de Segurança da Informação, assim como suas revisões, no Comitê de Compliance.

b) Usuários/Membros:

i) Comprometer-se a seguir as regras do Termo de Uso da Rede Corporativa, Computadores, Internet e E-mail;

ii) O usuário deve zelar pela segurança de suas credenciais de acesso (senha, múltiplo fator de autenticação, e chaves privadas) da rede corporativa, computadores, internet, e-mail corporativo e sistemas internos, não compartilhando com outras pessoas, utilizando senhas fortes e complexas, e habilitando o múltiplo fator de autenticação (MFA) sempre que suportado pelo sistema em questão;

iii) Ao se conectar em redes de computadores públicas (exemplo: aeroportos, cafeterias, entre outros) ou redes não corporativas, deve-se utilizar a solução de VPN com o objetivo de trafegar as informações de forma criptografada para evitar exposições indevidas do tráfego;

iv) Utilizar o e-mail corporativo apenas para fins estritamente profissionais, sendo proibida a comunicação pessoal e o envio de spam ou conteúdos não permitidos;

vi) Responder pela utilização inadequada de sistemas, internet, correio eletrônico, inclusive de outros usuários que estão sob sua gestão e/ou responsabilidade; e

vii) Participar de eventuais campanhas de conscientização de segurança da informação e treinamento.

c) Proprietários de Ativos de Informação

Resguardadas situações de excepcionalidade, os gestores das áreas da Strivo são os proprietários dos ativos de informação sob responsabilidade da sua área de atuação, razão pela qual devem:

i) Cumprir e transmitir as suas equipes as disposições estabelecidas pela Política e Normas de Segurança da Informação a fim de que elas tenham ampla divulgação no ambiente de trabalho;

ii) Garantir que as inconformidades ocorridas em suas áreas sejam identificadas e reportadas, e que sejam adotadas as medidas corretivas apropriadas conforme controles de segurança da informação;

iii) Realizar os procedimentos adequados para desligamento e encerramentos contratuais vigentes;

iv) Proteger os ativos de sua área (físico e lógico), de acordo com os critérios de classificação das informações definidos pela Instituição;

v) Aplicar sanções àqueles que deliberadamente violarem as determinações desta Política, suas Normas e Instruções, mediante orientação da área de Segurança da Informação;
vi) Avaliar as solicitações de acesso considerando a premissa de privilégio mínimo, que consiste em aprovar apenas os acessos essenciais com o fim de evitar permissões em demasia e desnecessárias.

É imprescindível que cada Membro compreenda o papel da segurança da informação em suas atividades. Todas as atividades executadas pelos Membros, devem observar a legislação vigente, a normatização de órgãos e entidades reguladoras, as regras internas da Strivo e as regras específicas aos quais os Membros estejam vinculados.

A equipe de *Compliance*, responsável por editar as políticas e padrões que apoiam a todos na proteção dos ativos de informação, está preparado para auxiliar na resolução de problemas relacionados ao tema. Em caso de dúvidas, as mesmas poderão ser esclarecidas pela área de *Compliance*, liderada pela Diretora de *Compliance,* Risco & PLDFT, conforme definido no estatuto societário vigente da Gestora.

7. Considerações Pertinentes

a) A informação é um ativo que possui extremo valor e importância para a Strivo e seus negócios;

b) A direção da Strivo está comprometida e apoia as metas e princípios de segurança da informação;

c) As informações da Strivo, dos seus clientes, e parceiros de negócios são tratadas e protegidas de forma ética e transparente, de acordo com as leis vigentes, regulações aplicáveis, e normas internas, apenas para a finalidade de negócio;

d) Os acessos às informações e recursos serão concedidos apenas se houver a devida autorização da pessoa proprietária do ativo de informação em questão e do(a) líder da pessoa que solicitou o acesso;

e) Para a concessão de acessos deve ser aplicado o conceito de privilégio mínimo, com acesso apenas aos recursos e informações imprescindíveis para a execução das atividades profissionais pertinentes à Strivo;

f) Cada usuário deve possuir uma identificação única (login de acesso), pessoal e intransferível, com garantia de rastreabilidade e não repúdio das ações executadas em recursos e informações da Strivo, de seus clientes e parceiros de negócios;

g) Qualquer informação ou produto resultante do trabalho dos usuários, no escopo de suas atividades contratadas, é de propriedade da Strivo. Ao término do contrato de trabalho, os usuários devem manter as informações privadas e produtos gerados, salvo por cláusula contratual prevista, sob posse da Strivo;

h) A Strivo se reserva ao direito de monitorar, inspecionar ou auditar o acesso e o uso de aplicativos e informações de sua propriedade ou sob sua guarda com ou sem o consentimento, presença ou conhecimento dos usuários, mas respeitando aspectos legais;

i) Nenhum software utilizado pela Strivo para controle e proteção de suas informações pode ser alterado ou desabilitado pelos Usuários.

8. Classificação da Informação

As informações da Strivo devem ser classificadas em níveis, de acordo com a sua criticidade. Devem ser consideradas as necessidades de negócio e de compartilhamento ou restrição de acesso, com análise de impactos em relação ao uso indevido das informações. Os níveis de classificação da informação são:

a) Confidencial: *Nível de classificação mais alto*. São informações que podem comprometer as operações da organização, tanto em nível financeiro como em competitividade ou reputação e exige aprovação do(a) proprietário(a) do ativo de informação.

b) Restrita: *Nível de confidencialidade médio*. São informações estratégicas que devem ficar disponíveis apenas para determinados grupos de pessoas que obtiveram o acesso aprovado pelo(a) proprietário(a) do ativo da informação.

c) Interna: *Nível de confidencialidade baixo*. São informações que podem ser compartilhadas entre todos colaboradores e parceiros da Strivo, mas não devem ser compartilhadas publicamente.

d) Pública: *Nível de confidencialidade inexistente*. São informações que não exigem sigilo e podem ser divulgadas para o público em geral, sem impacto ao negócio.

9. Confidencialidade

Nenhuma informação confidencial deve, em qualquer hipótese, ser divulgada a pessoas, dentro ou fora da Strivo, que não necessitem de, ou não devam ter acesso a tais informações para desempenho de suas atividades profissionais. Incluem-se aqui, por exemplo, posições compradas ou vendidas, estratégias e conselhos de investimento ou de desinvestimento, relatórios, analises e opiniões sobre ativos financeiros, dados a respeito de resultados financeiros antes da publicação dos balanços e balancetes das empresas integrantes da Strivo e dos veículos de investimento cujas carteiras sejam geridas pela Gestora, transações efetuadas e que ainda não foram publicadas, informações oriundas de estudos efetuados pelas áreas da sociedade etc.

Qualquer informação sobre a STRIVO, ou de qualquer natureza relativa às atividades desempenhadas pela Gestora, aos Membros e clientes, obtida em decorrência do desempenho das atividades normais do Membro na Strivo, só poderá ser fornecida ao público, mídia ou a demais órgãos caso autorizado expressamente pelo Diretor de Compliance, Risco & PLDFT. A solicitação e a concessão da autorização devem ser registradas por e-mail, que deverá ser armazenado por prazo não inferior a 5 (cinco) anos.

Não obstante o acima descrito, a Diretora de Compliance, Risco & PLDFT e o Diretor de Gestão, conforme definido no estatuto social vigente da Strivo, serão os únicos responsáveis diretos pela obtenção das informações relativas a análises de investimentos provenientes da empresa contratada pela Gestora. Tais informações não serão compartilhadas por nenhuma outra pessoa (Membro ou não), o que impossibilita a utilização destas informações por pessoas não habilitadas em processo de decisão de investimento.

É terminantemente proibido que os Membros façam cópias ou imprimam os arquivos utilizados, gerados ou disponíveis na rede da(s) Gestora(s) a que tiver acesso e circulem em ambientes externos com estes arquivos, uma vez que tais arquivos contém informações que são consideradas informações confidenciais.

A proibição acima referida não se aplica quando as cópias ou a impressão dos arquivos forem em prol da execução e do desenvolvimento dos negócios e dos interesses da Strivo. Nestes casos, o Membro que estiver na posse e guarda da cópia ou da impressão do arquivo que contenha a informação confidencial será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade.

Ainda, qualquer impressão de documentos deve ser imediatamente retirada da máquina impressora, pois podem conter informações restritas e confidenciais, mesmo no ambiente interno da Strivo.

O descarte de informações confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação. Todos os arquivos digitalizados em pastas temporárias serão apagados semanalmente, de modo que nenhum arquivo deverá ali permanecer. A desobediência a esta regra será considerada uma infração, sendo tratada de maneira análoga à daquele que esquece material na área de impressão. As possíveis penalidades aplicáveis por descumprimento das regras internas da Strivo estão descritas nesta Política e no Código de Ética e Manual de Compliance da Gestora.

O descarte de documentos físicos que contenham informações confidenciais ou de suas cópias deverá ser realizado imediatamente após seu uso, de maneira a evitar sua recuperação. Adicionalmente, os Membros devem se abster de utilizar pen-drives, disquetes, fitas, discos ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na Strivo.

Os Membros, quando de sua contratação, devem assinar o Termo de Compromisso com o Código de Ética da STRIVO, presente no Anexo I ao Código de Ética e Manual de Compliance da Gestora, pelo qual se obrigam, entre outras coisas, a proteger a confidencialidade das informações a que tiverem acesso enquanto estiverem trabalhando na Strivo, ou lhe prestando serviço.

Sem prejuízo dos procedimentos dispostos nesta seção, a Strivo orienta os seus Membros a tratar as informações adiante da seguinte forma:

a) Informação Privilegiada

Pode-se considerar como informação privilegiada qualquer informação importante a respeito de alguma empresa, que não tenha sido publicada e que seja conseguida de maneira privilegiada, em consequência da ligação profissional ou pessoal mantida com um cliente, com colaboradores de empresas estudadas ou investidas ou com terceiros, ou em razão da condição de Membro.

São exemplos de informações privilegiadas: informações verbais ou documentadas referentes a resultados operacionais de empresa, alterações societárias (fusões, cisões e incorporações),

informações sobre compra e venda de empresas, títulos ou valores mobiliários, e qualquer outro acontecimento que seja motivo de um acordo de confidencialidade fixado por uma empresa com a Strivo ou com terceiros.

As informações privilegiadas precisam ser mantidas em sigilo por todos que a acessarem, seja em função da prática da atividade profissional ou do relacionamento pessoal. Quem tiver acesso a uma informação privilegiada deverá transmiti-la rapidamente à área de compliance, não podendo comunicá-la a ninguém, nem mesmo a outros Membros, profissionais de mercado, amigos e parentes, e nem usá-la, seja em seu próprio benefício ou de terceiros. Se não houver certeza quanto ao caráter privilegiado da informação, deve-se rapidamente relatar o ocorrido ao *Compliance Officer*.

Quem tiver acesso a uma informação privilegiada deverá reduzir ao máximo a circulação de documentos e arquivos com tal informação, mitigando assim o seu uso indevido.

b) Insider Trading e "Dicas"

Insider trading baseia-se na compra e venda de títulos ou valores mobiliários com base no uso de informação privilegiada, com o objetivo de conseguir benefício próprio ou de terceiros (compreendendo a própria Strivo e seus Membros).

"Dica" é a transmissão, a qualquer terceiro, de informação privilegiada que possa ser usada com benefício na compra e venda de títulos ou valores mobiliários.

É proibida a prática dos casos mencionados anteriormente por qualquer Membro, seja agindo em benefício próprio, da Strivo ou de terceiros.

É de responsabilidade do *Compliance Officer* verificar e processar, trimestralmente, as notificações recebidas a respeito do uso pelos Membros de informações privilegiadas, *Insider trading* e "dicas". Casos envolvendo o uso de informação privilegiada, *insider trading* e "dicas" devem ser analisadas não só durante a vigência do relacionamento profissional do Membro com a Strivo, mas mesmo após o término do vínculo, com a comunicação do ocorrido às autoridades competentes, conforme o caso.

A Política de Segurança Cibernética visa prover a metodologia necessária para instituir processos e controles para prevenir e reduzir as vulnerabilidades e atender aos demais objetivos relacionados à segurança cibernética, garantindo a proteção dos ativos associados aos negócios críticos, definindo processos para o tratamento de incidentes cibernéticos e para avaliação de contratação de serviços de processamento e armazenamento de dados e de computação em nuvem para garantir a segurança das operações.

A crescente ameaça cibernética, somada à cada vez maior dependência dos sistemas digitais faz com que a segurança cibernética seja uns dos principais riscos não financeiros para os negócios. A proteção dos sistemas e da informação, dos negócios e dos clientes, constituem prioridade de primeiro nível, sendo um componente essencial da Strivo na condução de suas atividades.

10. Procedimentos Internos para Tratar Eventual Vazamento de Informações

Não obstante todos os procedimentos e aparatos tecnológicos robustos adotados pela Strivo para preservar o sigilo das informações confidenciais, reservadas ou privilegiadas, conforme definições trazidas pelas políticas internas da Gestora ("Informações" ou "Informação"), na eventualidade de ocorrer o vazamento de quaisquer Informações, ainda que de forma voluntaria, a Diretora de Compliance, Risco & PLDFT deverá tomar ciência do fato tão logo seja possível.

De posse da Informação, a Diretoria de Compliance, Risco & PLDFT, primeiramente, identificará se a Informação vazada se refere ao fundo de investimento gerido ou aos dados pessoais de cotistas.

Realizada a identificação, a Diretoria de Compliance, Risco & PLDFT procederá da seguinte forma:

a) No caso de vazamento de Informações relativas aos fundos de investimento geridos:

Imediatamente, seguirá com o rito para publicação de fato relevante, nos termos da regulamentação vigente, a fim de garantir a ampla disseminação e tratamento equânime da Informação. Esse procedimento visa assegurar que nenhuma pessoa seja beneficiada pela detenção ou uso da informação confidencial, reservada ou privilegiada atinente ao fundo de investimento.

b) No caso de vazamento de Informações relativas aos cotistas:

Neste caso, a Diretoria de *Compliance*, Risco & PLDFT procederá com o tanto necessário para cessar a disseminação da Informação ou atenuar os seus impactos, conforme o caso. Para tanto, poderá, dentre outras medidas: (i) autorizar a contratação de empresa especializada em consultoria para proteção de dados; (ii) autorizar a contratação de advogados especializados na matéria; (iii) entrar em contato com os responsáveis pelo(s) veículo(s) disseminador(es) da Informação. Sem prejuízo, a Diretoria de *Compliance*, Risco & PLDFT ficará à inteira disposição para auxiliar na solução da questão.

11. Segurança de Informação

A conexão de equipamentos na rede da Gestora que não estejam previamente habilitados, não terão acesso aos servidores e arquivos. Somente será possível em ambiente externo à rede.

Cada Membro é responsável por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade.

O envio ou repasse por e-mail de material que contenha conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo é também terminantemente proibido, conforme acima aventado, bem como o envio ou repasse de e-mails com opiniões, comentários ou mensagens que possam difamar a imagem e/ou afetar a reputação da Strivo.

A Diretoria de *Compliance* será avisada por e-mail em caso de tentativa de acesso aos diretórios e *logins* virtuais no servidor protegidos por senha. O *compliance officer* elucidará as circunstâncias da

ocorrência deste fato e comunicará ao Diretor de Compliance, Risco & PLDFT a fim de se estudar eventual aplicação de sanções.

Em nenhuma hipótese um Membro pode emitir opinião por e-mail em nome da Strivo, ou utilizar material, sua marca e logotipos para assuntos não corporativos ou após o rompimento do seu vínculo com este, salvo se expressamente autorizado pela Diretoria de Compliance, Risco & PLDFT para tanto.

Programas instalados nos computadores, principalmente via internet (downloads), sejam de utilização profissional ou para fins pessoais devem obter autorização previa, por e-mail, do responsável pela área de informática. Não é permitida a instalação de nenhum software ilegal ou que possua direitos autorais protegidos. A instalação de novos softwares, com a respectiva licença, deve também ser comunicada previamente, por e-mail, ao responsável pela informática. Este deverá aprovar ou vetar, por e-mail, a instalação e utilização dos softwares dos Membros para aspectos profissionais e pessoais. A área de compliance deverá ser mantida em cópia na troca de e-mails ora referida.

A Gestora se reserva no direito de gravar qualquer ligação telefônica dos seus respectivos Membros realizada ou recebida por meio das linhas telefônicas disponibilizadas para a atividade profissional de cada Membro. A Diretoria de Compliance é encarregada de, quinzenalmente, escutar, por amostragem, as ligações realizadas pelos Membros. Qualquer informação suspeita encontrada será esclarecida imediatamente. As gravações poderão ser arquivadas pelo prazo de 180 (cento e oitenta) dias.

Todas as informações do servidor da Strivo são segregadas por área, com restrições de acesso e transformadas em pacotes criptografados para backup.

11.1. Definição de Perfis de Acesso

Inicialmente, conforme detalhado adiante nesta Política, é importante pontuar que a Gestora possui ambientes de acesso segregado para área de gestão de recursos, de modo que as diferentes áreas da Gestora terão suas estruturas fisicamente segregadas. Em questões de armazenamento de informações, estas são logicamente segregadas das demais para garantir que apenas os Membros autorizados e necessários para o desempenho de determinada atividade tenham acesso às informações dela.

Desta forma, fica assegurado que somente Membros de uma determinada área possuam acesso às informações de tal área, evitando a disseminação de informações sigilosas, sem prejuízo de eventual compartilhamento de informações necessárias à consecução das atividades da Gestora.

A definição dos perfis de acesso ao sistema, rede, base de dados e servidores, são concedidos em razão da designação de função e atividades, a fim de evitar o contato com informações indevidas e/ou irrelevantes para o desempenho das funções profissionais do Membro.

Assim, fica vedado o compartilhamento de documentos e informações por pessoas não autorizadas a terceiros ou outros Membros, salvo se houver aprovação expressa, por e-mail, da Diretoria de Compliance, Risco & PLDFT nesse sentido. Qualquer conduta não autorizada na transferência de informações estará sob pena de aplicação de sanções disciplinares e legais.

É importante ressaltar que os acessos acima referidos são imediatamente cancelados em caso de desligamento do Membro da Strivo, ou em caso de redesignação de função ou atribuição de atividade que implique em alteração da necessidade de acessos.

11.2. Acesso Físico

É vedado aos Membros que não tenham autorização o acesso ao ambiente físico designado ao setor de gestão, bem como aos equipamentos de informática e demais equipamentos e sistemas utilizados que somente serão acessíveis através de senha pessoal aos Membros autorizados.

11.3. Definição e Alteração de Senhas

Como medida de segurança, o cadastramento ou alteração de senhas deve satisfazer a requisitos de complexidade, reduzindo assim riscos de acesso ou invasão de pessoas não autorizadas às informações internas. Este conceito se aplica aos acessos via Office 365.

As senhas deverão atender os seguintes requisitos:

i) Não conter partes significativas do nome da conta do usuário ou o nome todo;

ii) Ter pelo menos oito caracteres de comprimento;

iii) Conter caracteres de três das quatro categorias a seguir:

- Caracteres maiúsculos (A-Z);

- Caracteres minúsculos (a-z);

- Dígitos básicos (0-9);

- Caracteres não alfabéticos (por exemplo, !, $, #, %);

11.4. Regras Para Uso da Internet

O acesso à Internet deverá ser utilizado apenas para desenvolvimento das atividades profissionais pertinentes a área e função de cada Membro, não sendo permitidos acessos para outros fins, exceto em casos específicos, desde que com autorização da Diretoria de Compliance, Risco & PLDFT.

Não é permitido aos usuários o acesso a páginas da impróprias, com conteúdo pornográfico ou material relacionado, qualquer outro aspecto ilegal ou em desacordo com as diretrizes internas da Strivo.

11.5. Regras de Download

Não é permitido o "download" ou cópia de material da Internet, sem a devida necessidade e autorização previa da Diretoria de Compliance, Risco & PLDFT. Nos casos em que haja a autorização, deverá ser assegurada a propriedade intelectual e os direitos autorais do seu proprietário.

11.6. Regras de Upload

Os usuários não deverão divulgar na internet qualquer material que possa ser considerado impróprio, ofensivo ou desrespeitoso, ou que de alguma maneira, possam comprometer a imagem da Strivo, devendo cada Membro estar ciente e em conformidade com as diretrizes internas da Gestora.

11.7. Utilização de E-mail Corporativo

O uso do e-mail corporativo será exclusivo para questões profissionais de cada Membro, não sendo permitido a utilização do mesmo para questões pessoais, devendo todos seguirem as seguintes regras:

i) Utilizar o e-mail coorporativo, somente com autorização (usuário/senha), por necessidade de serviço ou por determinação expressa de superior hierárquico, realizando as tarefas e operações em estrita observância aos procedimentos, política e normas vigentes;

ii) Não revelar, fora do âmbito profissional, fato ou informação de qualquer natureza de que tenha conhecimento por força de suas atribuições, salvo em decorrência de decisão competente na esfera legal ou judicial;

iii) Não enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legitimo da instituição;

iv) Não se ausentar da estação de trabalho sem bloquear a máquina, garantindo assim a impossibilidade de acesso indevido por terceiros;

v) Não revelar a senha de acesso à rede corporativa, computadores, Internet e/ou de sua caixa postal (e-mail) coorporativo a ninguém e tomar o máximo de cuidado para que ela permaneça somente sob seu conhecimento;

vi) Não enviar mensagens por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;

vii) Alterar sua senha, sempre que obrigatório ou que tenha suspeição de descoberta por terceiros, não usando combinações simples que possam ser facilmente descobertas, com base na seção "Regras para definição/alteração de senha" presente nesta Política;

viii) Não apagar mensagens pertinentes de correio eletrônico quando a STRIVO estiver sujeita a algum tipo de investigação; e

ix) Responder, em todas as instâncias, pelas consequências das ações ou omissões de própria parte que possam pôr em risco ou comprometer a exclusividade de conhecimento de sua senha ou das transações a que tenha acesso.

11.8. Tratamento do Espaço Disponível em Rede

É de responsabilidade do Membro a manutenção de sua pasta de rede, bem como área de trabalho, devendo fazer a exclusão ou o arquivamento dos arquivos em outro local apropriado com intuito de manter espaço livre. Recomenda-se a utilização da pasta própria criada com o nome do Membro na aba "Este Computador", já que os arquivos salvos na área de trabalho podem ser perdidos em eventual pane no computador ou em eventual limpeza de rede para liberação de espaço.

A pasta de Rede "STRIVO" deverá ser acompanhada pela área de compliance, devendo esta monitorar o espaço livre, impedindo que o diretório fique completamente cheio e cause problemas no fluxo de trabalho das áreas. Sempre que o espaço livre for inferior à 5 Giga, será realizada uma limpeza das pastas, de modo a otimizar o espaço disponível, ou será promovida a contratação de espaço adicional com o provedor do serviço de rede.

11.9. Metodologia de Backup

Todas as informações da rede de acesso da STRIVO são enviadas para o servidor interno diariamente. Nesse servidor, as informações são segregadas por pastas, sendo armazenadas com backup realizado por empresa terceirizada, em tempo real, em serviço de backup na nuvem com acesso somente ao administrador de rede.

11.10. Testes Periódicos

Periodicamente, a Strivo realiza testes de segurança em todo o seu sistema de informação. Dentre as medidas, incluem-se, mas não se limitam:

(i) Verificação esporádica do login dos Membros;

(ii) Alteração periódica da senha de acesso dos Membros;

(iii) Testes semestrais no firewall;

(iv) Testes semestrais nas restrições impostas aos diretórios;

(v) Manutenção periódica dos equipamentos de “hardware” conforme necessidade;

(vi) Testes no backup (salvamento de informações) na periodicidade estabelecida no item “Metodologia de Backup” acima.

11.11. Violações

As violações de segurança devem ser informadas à área de compliance, por meio de e-mail, com todas as informações relativas ao fato ocorrido. Toda violação ou desvio é investigado para a determinação das medidas necessárias, visando à correção da falha ou reestruturação de processos.

Exemplos que podem ocasionar riscos operacionais ou sanções:

a) Uso ilegal de software;

b) Introdução (intencional ou não) de vírus de informática;

c) Tentativas de acesso não autorizado a dados e sistemas;

d) Compartilhamento de informações sensíveis do negócio;

e) Divulgação de informações de clientes e das operações contratadas.

Os princípios de segurança estabelecidos na presente Política possuem total aderência da Diretoria da strivo e devem ser observados por todos na execução de suas funções. A não conformidade com as diretrizes desta Política e a violação de normas derivadas da mesma sujeita os Membros às penas de responsabilidade civil e criminal na máxima extensão que a lei permitir e a rescisão de contratos. Em caso de dúvidas quanto aos princípios e responsabilidades descritas nesta Política, os Membros devem entrar em contato com a aérea de compliance.

12. Propriedade Intelectual

A propriedade intelectual é composta por bens imateriais, tais como: marcas, sinais distintivos, slogans publicitários, nomes de domínio, nomes empresariais, indicações geográficas, desenhos industriais, patentes de invenção e de modelo de utilidade, obras intelectuais (tais como obras literárias, artísticas e cientificas, base de dados, fotografias, desenhos, ilustrações, projetos de arquitetura, obras musicais, obras audiovisuais, textos e etc.), programas de computador e segredos empresariais (inclusive segredos de indústria e comércio).

Quaisquer informações e propriedade intelectual que pertenciam à Strivo, ou por ela disponibilizadas, não devem ser utilizadas para fins particulares, nem repassadas a outrem, ainda que tenham sido obtidas, inferidas ou desenvolvidas pelo próprio colaborador em seu ambiente de trabalho.

13. Procedimentos de Segurança Cibernética

Informado de forma detalhada na Política de Segurança Cibernética da Strivo.

14. Segregação de Atividades

Inicialmente, cumpre esclarecer que a Strivo atua exclusivamente como administradora de carteiras de valores mobiliários, na categoria de gestão de recursos de terceiros, não prestando, portanto, quaisquer outros serviços no mercado de capitais.

A Diretoria de Compliance, Risco & PLDFT possui total autonomia e independência em suas decisões para questionar os riscos assumidos nas operações realizadas, sendo possível a aplicação das ações disciplinares cabíveis, independente de nível hierárquico, sem que seja necessária a validação prévia dos administradores ou sócios da STRIVO, salvo se for de competência do Comitê de Compliance, Risco & PLDFT.

15. Vigência e Revisões

Esta política entra em vigor em **01/05/2025**, revoga todas as versões anteriores, devendo ser revisada anualmente ou, havendo necessidade anterior, o que for menor, para que o documento permaneça atualizado e aderente à legislação e regulação aplicável.

A aérea de compliance informará oportunamente aos Membros sobre a entrada em vigor de nova versão deste documento e a disponibilizará na página da Gestora na rede mundial de computadores.

16. Disposições Finais

A STRIVO armazenará as evidências descritas nesta Política, incluindo, sem se limitar, o fluxo de e-mails, por prazo não inferior a 5 (cinco anos.

Essa Política é parte integrante de outras Políticas e Manuais da Gestora, devendo ser interpretada dentro deste conjunto, o qual representa as diretrizes da Strivo de forma ampla.