POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

DA

SCAI GESTORA DE RECURSOS LTDA.

28 DE SETEMBRO DE 2022

ÍNDICE GERAL

1 INTRODUÇÃO

A Política de Segurança da Informação ("Política") foi criada para estabelecer os princípios, conceitos e valores que deverão pautar a segurança da informação da SCAI Gestora de Recursos Ltda. ("SCAI") na sua atuação interna e com o mercado, assim como suas relações com os diversos públicos.

A Política de segurança da informação se refere às iniciativas que asseguram a integridade e a disponibilidade das informações, garantindo ainda que estas sejam acessadas apenas por pessoas autorizadas

O seu objetivo é assegurar que as informações da organização estão sendo tratadas de forma adequada para a garantia dos critérios de Confidencialidade, Integridade e Disponibilidade, conforme abaixo definidos.

Além disso, descreve a conduta considerada adequada para o manuseio, controle e proteção das informações contra destruição, modificação, divulgação indevida e acessos não autorizados, acidentais ou intencionais.

2 APLICAÇÃO

Os princípios e regras desta Política devem ser observados por todos os sócios, diretores, empregados, *trainees*, estagiários, colaboradores e prestadores de serviços que venham, de maneira direta ou indireta, trabalhar para a SCAI (conjuntamente referidos como "Colaboradores", e individual e indistintamente como "Colaborador").

3 DISPOSIÇÕES GERAIS

3.1 Disposições Iniciais

Todas e quaisquer atividades executadas pelos Colaboradores e terceiros devem estar em acordo com a legislação vigente, com a normatização dos órgãos e entidades reguladoras e atender integralmente a esta Política.

Com esta Política, considera-se que todos os Colaboradores estão cientes de que os ambientes, sistemas, computadores e redes da SCAI são monitorados, com prévia informação, conforme previsto nas leis brasileiras. Cada Colaborador deverá se manter atualizado em relação a esta Política e aos procedimentos e normas relacionadas, buscando orientação do seu gestor sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

A segurança da informação ("Segurança da Informação") é aqui caracterizada pela preservação dos seguintes princípios:

a) **Confidencialidade:** é a garantia de que a informação é acessível somente por pessoas com acesso autorizado;

b) **Integridade:** é a salvaguarda da exatidão e completeza da informação e dos métodos de processamento;

c) **Disponibilidade:** é a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes, sempre que necessário.

Para tornar a gestão da Segurança da Informação efetiva, a Diretoria da SCAI deve coordenar as ações necessárias para a implantação do modelo de gestão de Segurança da Informação e avaliar periodicamente a Segurança da Informação, por meio da análise de indicadores, bem como recomendar ações corretivas e preventivas.

A gestão da Segurança da Informação compreende as seguintes atividades:

a) Identificar necessidades específicas de Segurança da Informação e propor implementações necessárias;

b) Elaborar documentos necessários à Segurança da Informação;

c) Elaborar e manter indicadores de Segurança da Informação;

d) Fazer a gestão do Plano de Continuidade dos Negócios;

e) Elaborar programas de treinamento e de conscientização em Segurança da Informação;

f) Analisar os incidentes de segurança da informação e recomendar correções necessárias.

Compete ao Diretor de *Compliance* verificar o cumprimento da Política de Segurança da Informação da SCAI e recomendar as ações corretivas necessárias;

Esta Política deve ser revisada na ocorrência de alterações materiais nas atividades, infraestrutura ou operações da SCAI. Entretanto, uma revisão mínima deve ocorrer a cada 2 (dois) anos com o intuito de verificar a eventual necessidade de produzir uma versão atualizada, a ser aprovada pela Diretoria da SCAI.

3.2 Políticas

As seguintes diretrizes integram a Política de Segurança da Informação:

a) **A informação pertence à organização:** Toda informação gerada, adquirida ou processada pela SCAI é de sua exclusiva propriedade. Deve-se obter prévia autorização da gerência imediata para a saída de documentos em meios físicos ou

eletrônicos da instituição, bem como *notebooks* ou qualquer outro equipamento eletrônico que contenha informações críticas da SCAI.

b) Segurança orientada ao negócio: As ações de segurança serão planejadas e aplicadas de acordo com a avaliação dos riscos para o negócio da SCAI. A disponibilidade, uso, acesso e proteção das informações e seus recursos devem ocorrer sempre de forma a preservar a continuidade e a competitividade do negócio da SCAI.

c) Propriedade da informação: Toda informação armazenada nas dependências da SCAI é considerada patrimônio da SCAI, sendo usada exclusivamente em seu interesse e devendo estar adequadamente protegida, em qualquer que seja o meio de armazenamento, contra violação, alteração, destruição, acesso não autorizado e divulgação indevida. Os responsáveis por seu armazenamento, guarda e manuseamento responderão por sua integridade, uso ou divulgação.

d) Classificação da informação: Cada Colaborador terá acesso às informações necessárias ao seu trabalho, respeitando os conceitos de Confidencialidade, Integridade e Disponibilidade.

e) Responsabilidade: Cada Colaborador é responsável pela segurança dos ativos e das informações que estejam sob sua custódia e por todos os atos executados com sua identificação de acesso. Qualquer que seja sua forma, a identificação será pessoal, intransferível e permitirá de maneira clara e indiscutível o seu reconhecimento.

f) Menor privilégio: O Colaborador terá acesso somente a ativos de informação que componham o imprescindível para o total desenvolvimento do seu trabalho.

g) Cultura de segurança: O conteúdo desta Política e das demais normas será amplamente divulgado na SCAI.

h) Recursos computacionais: Os recursos computacionais disponibilizados pela SCAI devem ser utilizados apenas para o desenvolvimento de atividades relacionadas ao negócio da organização, sendo vedada a sua utilização para qualquer outra finalidade.

i) Treinamento em Segurança da Informação: Os Colaboradores devem conhecer e respeitar a Política de Segurança da Informação da organização. Deve ser realizado, anualmente, programa de treinamento para garantir a disseminação das informações desta Política.

3.3 Classificação da Informação

O gestor de cada área deverá estabelecer critérios quanto ao nível de confidencialidade

da informação (lógica ou física) gerada por sua área. Dessa forma, ele terá a responsabilidade de averiguar se informações confidenciais estão sendo indevidamente circuladas pelos seus subordinados, bem como orientá-os a não fazê-lo.

Ele guiará suas condutas norteado pelo conceito de "mesa limpa", ou seja, sempre verificar se há relatórios nas impressoras, mídias em locais de fácil acesso, procurando não deixar qualquer material confidencial exposto. Nenhuma informação confidencial poderá ser repassada para terceiros sem o consentimento do Departamento Técnico e do Diretor de Risco e Compliance.

A devida compreensão desta Política perpassa pelo conceito de "informações confidenciais", que deve ser entendido como: todas as informações confidenciais, reservadas ou privilegiadas, independentemente destas informações estarem contidas em discos, disquetes, pen-drives, fitas, outros tipos de mídia ou em documentos físicos, ou serem escritas, verbais ou apresentadas de modo tangível ou intangível, qualquer informação sobre a SCAI, seus sócios e clientes, aqui também contemplados os próprios fundos de investimento, incluindo:

(i) Know-how, técnicas, cópias, diagramas, modelos, amostras, programas de computador;

(ii) Informações técnicas, financeiras ou relacionadas a estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes e dos fundos de investimento administrados e/ou geridos pela SCAI;

(iii) Operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os fundos de investimento geridos pela SCAI;

(iv) Informações estratégicas ou mercadológicas e outras, de qualquer natureza, obtidas junto a sócios, sócios-diretores, funcionários, trainees ou estagiários da SCAI ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral, incluindo alterações societárias (fusões, cisões e incorporações), informações sobre compra e venda de empresas, títulos ou valores mobiliários, inclusive ofertas iniciais de ações (IPO), projetos e qualquer outro fato que seja de conhecimento em decorrência do âmbito de atuação da SCAI e que ainda não foi devidamente levado à público;

(v) Informações a respeito de resultados financeiros antes da publicação dos balanços e balancetes dos fundos e das companhias investidas pelos fundos;

(vi) Transações realizadas e que ainda não tenham sido divulgadas publicamente;

(vii) Informações de clientes que devam ser protegidas por obrigatoriedade legal, incluindo dados pessoais (CPF, RG etc.), que identificam ou podem identificar uma pessoa física, situação financeira e movimentação bancária;

(viii) Informações sobre produtos e serviços que revelem vantagens competitivas da SCAI frente

ao mercado;

(ix) Todo o material estratégico da SCAI (material impresso, armazenado em sistemas, em mensagens eletrônicas ou mesmo na forma de conhecimento de negócio da pessoa);

(x) Quaisquer informações da SCAI, que não devem ser divulgadas ao meio externo antes da publicação pelas áreas competentes; e

(xi) Todos os tipos de senhas a sistemas, redes, estações de trabalho e outras informações utilizadas na autenticação de identidades. Estas informações são também pessoais e intransferíveis.

3.4 Procedimentos e Princípios

3.4.1 Gestão de Acessos

(i) Concessão de Acessos

Acessos apenas podem acontecer mediante solicitação devidamente formalizada ao e aprovada pelo RH via e-mail, informando os dados do Colaborador, a área de atuação e o seu gestor. Após receber a aprovação, a área de TI irá conceder um acesso padrão à rede e e-mail corporativo. Havendo necessidade de acessos específicos à rede e às aplicações, o gestor terá de formalizar a solicitação destes acessos via e-mail para o Diretor responsável.

Em caso de mudança de departamento e/ou cargo, a área de negócios deve informar a área de TI, através de ticket na ferramenta de ITSM, sobre as possíveis mudanças de acessos do Colaborador, e portanto, solicitar os ajustes necessários.

(ii) Revogação de Acessos

Quando houver desligamento de um Colaborador ou terceiro, o RH deverá encaminhar a revogação do acesso imediatamente, formalizada por e-mail ao Diretor responsável e ao TI para efetuar os desligamentos do login nos sistemas de uso do colaborador.

(iii) Revisão de Acessos

As revisões visam identificar acessos indevidos. Elas devem ser solicitadas pela área de negocio para que a área de TI, envie a relação de usuários de cada área para seu respectivo gestor, solicitando que ele valide os acessos recebidos. Após tais avaliações, o gestor deverá formalizar a aprovação via e-mail para o Diretor de Compliance.

(iv) Uso da Internet

As regras da SCAI visam o desenvolvimento de um comportamento eminentemente ético e profissional do uso da internet. Com isso em mente, a internet da SCAI deve ser utilizada para atividades da SCAI. O uso para atividades pessoais não deve impactar o

desempenho das funções dos Colaboradores ou terceiros.

O uso indevido da rede de internet da SCAI abre a porta para riscos significativos para os ativos de informação. Dito isso, a SCAI, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela, de forma que a área de TI poderá saber qual usuário está conectado, o tempo em que acessou a internet e em quais páginas navegou.

Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet pela SCAI são de sua propriedade. Dessa forma, ela poderá analisar e, quando julgar necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento desta Política.

O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a SCAI cooperará ativamente com as autoridades competentes.

Os Colaboradores não poderão em hipótese alguma utilizar os recursos da SCAI para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

(v) Usuários Visitantes

Os visitantes que necessitem ter acesso a rede Wi-Fi se sujeitarão às mesmas regras que os Colaboradores da SCAI, tendo que cumprir os mesmos procedimentos de segurança. Os usuários visitantes receberão uma senha de acesso provisória para conexão via Wi-Fi.

(vi) Uso de E-mail

O correio eletrônico corporativo fornecido pela SCAI (e-mail) é um instrumento de comunicação interna e externa para a realização do negócio da SCAI. As mensagens devem ser escritas em linguagem profissional, não devendo comprometer a imagem da SCAI, assim como observar a legislação vigente e o Código de Ética da SCAI.

O Colaborador é responsável por todas as mensagens enviadas pelo seu endereço de e-mail. Visando a proteger a rede interna da SCAI de vírus e malwares, a área de TI poderá bloquear o recebimento de e-mails provenientes de domínio público.

Os Colaboradores deverão desconfiar de todos os e-mails com assuntos estranhos e não reenviar e-mails do tipo corrente, aviso de vírus, avisos da Microsoft/AOL/Symantec, descontos, promoções, etc. Deve-se utilizar o e-mail para qualquer comunicação interna que não necessite do meio físico, diminuindo o custo com impressão e aumentando a agilidade na entrega e leitura.

Em hipótese alguma, usuários que não sejam Colaboradores ou terceiros da SCAI terão acesso às contas de correio eletrônico da SCAI. A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso, não prejudique a SCAI e não cause impacto no tráfego da rede.

(vii) Segurança Física

Apenas Colaboradores de TI ("Departamento de TI") terão acesso às áreas exclusivas deste setor, como à sala destinada ao servidor e outras dependências especificadas pelo Departamento de TI.

Além disso, O usuário deverá fechar qualquer documento que esteja manipulando ou redigindo quando necessitar ausentar-se de sua mesa, deixando a proteção de tela ativada no modo de login. Papéis referentes a assuntos confidenciais que não sejam mais necessários, antes de serem levados ao lixo, devem ser processados em máquina fragmentadora. As impressões de documentos deverão ser apenas referentes aos assuntos da SCAI, não sendo autorizada a utilização de impressões de cunho pessoal. O uso de telefone da SCAI deverá ser exclusivo para uso a serviço da SCAI, não devendo ser utilizado para fins pessoais.

(viii) Monitoramento e Auditoria do Ambiente

Para garantir as regras mencionadas nesta Política, a SCAI poderá:

(i) implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede – a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;

(ii) tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior) ou por determinação do Departamento Técnico;

(iii) realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;

(iv) instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

3.4.2 Identificação

Todos os dispositivos de identificação utilizados na SCAI, como o número de registro do Colaborador, o crachá, as identificações de acesso aos sistemas, certificados e assinaturas digitais devem estar associados a uma pessoa física e atrelados inequivocamente aos seus

documentos oficiais reconhecidos pela legislação brasileira. O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a instituição e a legislação.

Portanto, nenhum dispositivo de identificação poderá ser compartilhado com outras pessoas em nenhuma hipótese. A responsabilidade do uso de login compartilhado será dos usuários que dele se utilizarem.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários, o que ocorre no caso de Colaboradores cujo contrato ou prestação de serviços tenha se encerrado, bem como aos usuários de testes e outras situações similares.

3.4.3 Computadores e Recursos

Os equipamentos disponíveis aos Colaboradores são de propriedade da SCAI, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da instituição, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelas gerências responsáveis.

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um técnico do Departamento de TI da SCAI, ou de quem este determinar. As gerências que necessitarem fazer testes deverão solicitá-los previamente à Departamento de TI, ficando responsáveis jurídica e tecnicamente pelas ações realizadas.

Todas as atualizações e correções de segurança do sistema operacional ou aplicativos somente poderão ser feitas após a devida validação no respectivo ambiente de homologação, e depois de sua disponibilização pelo fabricante ou fornecedor.

No uso dos computadores, equipamentos e recursos de informática, algumas regras devem ser atendidas como:

(i) todos os computadores de uso individual deverão ter senha para restringir o acesso de Colaboradores não autorizados;

(ii) os Colaboradores devem informar ao departamento técnico qualquer identificação de dispositivo estranho conectado ao seu computador;

(iii) é vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por um técnico da Departamento de TI da SCAI ou por terceiros devidamente contratados para o serviço;

(iv) é expressamente proibido o consumo de alimentos, bebidas ou fumo na

mesa de trabalho e próximo aos equipamentos;

(v) o Colaborador deverá manter a configuração do equipamento disponibilizado pela SCAI, 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;

(vi) deverão ser protegidos por senha (bloqueados), todos os terminais de computador e impressoras quando não estiverem sendo utilizados;

(vii) todos os recursos tecnológicos adquiridos pela SCAI devem ter imediatamente suas senhas padrões (default) alteradas;

(viii) os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos Colaboradores, datas e horários de acesso;

(ix) é proibido tentar ou obter acesso não autorizado a outro computador, servidor ou rede;

(x) é proibido burlar quaisquer sistemas de segurança;

(xi) é proibido acessar informações confidenciais sem explícita autorização do proprietário;

(xii) é proibido vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers);

(xiii) é proibido interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;

(xiv) é proibido 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;

(xv) é proibido hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública; e

(xvi) é proibido utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

3.4.4 Autonomia do Departamento de TI

O Departamento de TI tem total autonomia para atuar sobre os equipamentos de informática disponibilizados pela SCAI. Os procedimentos abaixo poderão ser realizados sem prévio aviso aos usuários:

(i) Realização de auditoria (local ou remota);

(ii) Definição dos perfis de usuários cujos privilégios não permitam a realização deatividades tidas como nocivas ao sistema operacional ou à rede como um todo;

(iii) Instalação de software de monitoramento;

(iv) Desinstalação de qualquer software considerado nocivos à integridade da rede; e

(v) Credenciamento/descredenciamento de usuários.

4 DISPOSIÇÕES FINAIS

Todos os Colaboradores receberão esta Política, devendo assinar um termo de adesão na forma do Anexo I, confirmando sua ciência e compreensão das Políticas e procedimentos aqui instituídos. Sempre que as Políticas e procedimentos forem atualizados, uma nova versão deve ser encaminhada para todos. Uma versão eletrônica atualizada do documento será disponibilizada no diretório da rede da SCAI.

4.1 Consequências do Descumprimento

O descumprimento das Políticas e procedimentos estabelecidos na presente Política implicará nas seguintes medidas, segundo o entendimento do Diretor de *Compliance* (ou, caso o Diretor de *Compliance* esteja envolvido, de qualquer outro Diretor):

(i) demissão dos Colaboradores envolvidos no descumprimento em questão, incluindo aqueles que tinham conhecimento do descumprimento em questão e foram omissos em reportá-lo a seus superiores; e/ou

(ii) responsabilização dos Colaboradores envolvidos no descumprimento por eventuais danos que a SCAI venha a sofrer em razão de sua conduta.

A aplicação das penalidades acima não isenta, dispensa ou atenua a responsabilidade civil, administrativa e/ou criminal, pelos prejuízos resultantes de seus atos dolosos ou culposos resultantes da infração da legislação em vigor e das Políticas e procedimentos estabelecidos nesta Política.

ANEXO I – MODELO DE TERMO DE ADESÃO

TERMO DE ADESÃO À POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA SCAI GESTORA DE RECURSOS LTDA.

Eu, [nome], [qualificação], declaro que tomei conhecimento dos termos e condições da Política de Segurança da Informação da SCAI Gestora de Recursos Ltda. ("Política" e "SCAI", respectivamente), tendo, ao final, recebido uma cópia da referida Política.

Subscrevendo o presente formalizo a minha adesão à Política, comprometendo-me a cumprir com todos os seus termos e condições, adotando, nas situações de dúvida, a posição mais conservadora possível, submetendo as dúvidas a respeito do cumprimento da Política e da legislação e regulamentação em vigor ao Diretor de *Compliance*.

Rio de Janeiro, [=] de [=] de [=].

_____

[=]

Testemunhas:

1. _____	2. _____
Nome:	Nome:
RG:	RG:
CPF:	CPF: