SL TOOLS

MANUAL DE GERENCIAMENTO DE RISCOS OPERACIONAIS E CONTROLES INTERNOS

Setembro de 2023

SL TOOLS S.A.

O acesso e manuseio do presente Manual está restrito aos Colaboradores da SL Tools e terceiros autorizados.

ÍNDICE

1. INTRODUÇÃO 2
2. RESPONSABILIDADES 2
3. GERENCIAMENTO DE RISCOS OPERACIONAIS 3
4. EVENTOS DE RISCOS OPERACIONAIS 4
5. LINHAS DE DEFESA 4
6. TRATAMENTO DE INCIDENTES 5
7. TRATAMENTO E PREVENÇÃO DE EVENTOS DE FRAUDE 5
8. RELATÓRIO ANUAL CONTROLES INTERNOS E RISCOS OPERACIONAIS 7
9. CONSIDERAÇÕES FINAIS 8

1. INTRODUÇÃO

O presente Manual de Gerenciamento de Riscos Operacionais e Controles Internos ("Manual") visa estabelecer procedimentos de gerenciamento de riscos operacionais e controles internos na **SL Tools S.A.** ("SL Tools") de acordo com as leis, regulamentos e instruções existentes acerca deste assunto, conforme aplicável ao caso concreto.

O modelo de gestão de riscos operacionais e controles internos adotado pela SL Tools tem por objetivo identificar, mensurar, avaliar, monitorar, reportar, controlar e mitigar as exposições aos riscos operacionais de produtos, processos e serviços, além de estabelecer camadas de gestão de riscos com a implementação de linhas de defesa com atribuições de responsabilidades e monitoramentos eficazes.

Conceitua-se como risco operacional a possibilidade de ocorrência de perdas resultantes de falha, deficiência ou inadequação de processos internos, pessoas e ambiente tecnológico, ou de eventos externos. Tal conceito inclui ainda o risco legal, associado à inadequação ou deficiência em contratos firmados pela SL Tools, bem como a sanções em razão de descumprimento de dispositivos legais e/ou regulatórios e a indenizações por danos a terceiros decorrentes das atividades desenvolvidas pela SL Tools.

Entre os eventos de risco operacional, incluem-se:

(i) Erros operacionais;
(ii) Mal funcionamento do sistema;
(iii) Problemas com provedores,
(iv) Fraudes internas e externas.

2. RESPONSABILIDADES

A aprovação do presente Manual incumbe à Diretoria da SL Tools.

As responsabilidades descritas neste Manual referem-se àquelas relacionadas ao gerenciamento de riscos operacionais e de controles internos.

Este Manual será periodicamente revisado, no mínimo anualmente, ou extraordinariamente, a qualquer tempo, conforme necessário.

Cada funcionário, individualmente, é responsável por adotar postura proativa no sentido de mitigar os riscos operacionais envolvidos nas tarefas sob sua responsabilidade, manifestando sua ciência dos termos do presente Manual por meio do Termo de Ciência ao presente Manual.

3. GERENCIAMENTO DE RISCOS OPERACIONAIS

A gestão de riscos operacionais da SL Tools está submetida ao presente Manual, o qual encontra-se devidamente aprovado por sua Diretoria.

Premissas e princípios. A SL Tools entende que a boa governança de riscos envolve, entre outros, os seguintes princípios: (i) envolvimento da alta direção; (ii) responsabilidades claramente definidas; (iii) rotinas adequadas de auditoria; e (iv) implementação de linhas de defesa. Nesse sentido, a SL Tools estabelece como premissas as melhores práticas na gestão de seus riscos operacionais visando, dentre outros: (a) estruturar sua área de riscos operacionais com ferramentas adequadas; (b) assegurar a efetividade do gerenciamento de riscos operacionais; e (c) disseminar os termos deste Manual para toda a instituição, com a finalidade de estabelecer ssa cultura a todos os seus funcionários, inclusive aos terceiros contratados.

Identificação. Consiste em identificar e classificar os eventos de riscos operacionais a que a SL Tools está exposta, indicando áreas de incidência, causas e potenciais impactos financeiros e reputacionais associados aos processos, produtos e serviços da organização.

Assim, as seguintes ações são tomadas pela SL Tools, a fim de assegurar a devida e proporcional gestão de seus riscos operacionais:

1.1. Avaliação, Mensuração e Controle. É a quantificação ou dimensionamento da exposição ao risco operacional, com o objetivo de avaliar o impacto nos negócios da SL Tools. Consiste em avaliar quais são os riscos operacionais que corremos, nossos limites de tolerância, estabelecer indicadores de prevenção, a avaliação de eventos que levem a uma perda operacional e a mensuração da perda potencial em si assim como implementar mecanismos de forma a garantir que os limites e indicadores de prevenção de risco operacional permaneçam dentro dos níveis desejados e evitem a incorrência dos riscos.

1.2. Mitigação. Consiste em criar e implementar mecanismos para mitigar o risco buscando reduzir as perdas operacionais por meio da remoção da causa do risco, alteração da probabilidade de ocorrência ou alteração das consequências do evento de risco. Após a conclusão do mapeamento, e identificados os riscos operacionais, a Diretoria sugere ações com o intuito de mitigá-los. Essas ações, que são de responsabilidade e decisão do gestor, devem ser acompanhadas periodicamente para verificação quanto à sua implementação.

1.3. Monitoramento e Reporte. Monitoramento é a ação que tem por objetivo identificar as deficiências do processo de gestão de riscos operacionais, de forma que as fragilidades detectadas sejam levadas ao conhecimento da alta administração. É a fase de retroalimentação do processo de gerenciamento de riscos operacionais, onde é possível

detectar fragilidades nas fases anteriores. O reporte se dá por meio das informações de riscos operacionais prestadas à diretoria da SL Tools.

4. EVENTOS DE RISCOS OPERACIONAIS

Eventos de riscos operacionais são aqueles decorrentes de falhas ou inadequações de Pessoas, Processos, Sistemas e Eventos Externos, e podem provocar impactos indesejáveis no resultado da SL Tools, seja por meio de despesas incorridas ou pela diminuição de receita.

- O fator **Pessoas** está ligado a falhas, deficiências ou inadequações no desempenho das atribuições pelos funcionários e contratados, envolvendo os aspectos referentes à conduta (postura ética, honestidade, negligência), competências (habilidades, conhecimentos e experiência) e ambiente de trabalho (cultura organizacional e motivação).

- O fator **Processos** está ligado a falhas, deficiências ou inadequações nos processos internos. Adequação à legislação, pontos de controle, comunicação interna e segurança física são aspectos que devem ser observados na modelagem de processos, para evitar riscos operacionais.

- O fator **Sistemas** está ligado a falhas, deficiências ou inadequações nos sistemas desenvolvidos e/ou utilizados pela SL Tools envolvendo aspectos de hardware, software, rede de comunicação, segurança lógica, análise e programação.

- O fator **Eventos Externos** considera situações de força maior, ambiente externo e agente externo. Envolvem, sem se limitar a, desastres naturais e catástrofes, criação/alteração de legislação, uso indevido ou incorreto dos sistemas da SL Tools, ações criminosas, fraudes e demais eventos relacionados ou praticados por fornecedores, terceirizados e/ou clientes.

5. LINHAS DE DEFESA

A SL Tools adota as melhores práticas de Autoavaliação de PFMI com a implementação das três linhas de defesa descritas abaixo.
Para um entendimento completo da Autoavaliação de PFMI, favor se referir ao documento específico disponível no site da SL Tools www.sltools.com.br .

Primeira Linha de Defesa: é composta pelos procedimentos de controles internos e gerenciamento de riscos previstos nos Normativos Internos e implementados pelos gestores de negócios, de suporte e operacionais da SL Tools, que devem ser os responsáveis primários por

identificar, avaliar, tratar, controlar e reportar os riscos de suas áreas, de forma alinhada aos Normativos Internos.

Segunda Linha de Defesa: é composta pelas funções de gerenciamento de riscos e compliance, desempenhadas pelas áreas conduzidas pelos Diretores de Gerenciamento de Riscos e Controles Internos e de Compliance e PLD/FTP, respectivamente. Esta linha também é responsável por testar e avaliar a conformidade à regulamentação, políticas e procedimentos, mantendo padrões de integridade alinhados aos princípios e diretrizes adotados pela SL Tools, bem como reportando sistemática e tempestivamente à administração os resultados de suas análises.

Terceira Linha de Defesa: função desempenhada por meio da auditoria, que tem o papel de fornecer aos órgãos de governança e à alta administração avaliações abrangentes, independentes e objetivas relativas aos riscos da SL Tools. Atuando de forma independente, a auditoria revisa de modo sistemático a eficácia das duas primeiras linhas de defesa, contribuindo para o seu constante aprimoramento.

6. TRATAMENTO DE INCIDENTES

Comunicação de um Risco Operacional. Uma vez identificado um incidente, a comunicação deve ser detalhada porém ágil e envolver a Diretoria de gerenciamento de riscos e controles internos. Como forma de monitoramento e controle da efetiva disseminação da cultura de riscos operacionais prevista neste Manual, a SL Tools adota mecanismos que certificam a leitura, por parte dos funcionários, dos Informes de Riscos Operacionais, bem como do Manual de Políticas e Procedimentos de Segurança da Informação.

Tratamento do Risco Operacional. Membros do Diretoria de gerenciamento de riscos e controles internos da SL Tools devem necessariamente estar envolvidos desde o descobrimento até a solução do eventual incidente identificado.

Incidentes devem ser controlados, mitigados e monitorados, conforme o disposto na parte de “Gerenciamento de Riscos Operacionais” deste Manual.

7. TRATAMENTO E PREVENÇÃO DE EVENTOS DE FRAUDE

Para os fins do presente Manual, considera-se fraude a prática de ardil ou conduta com emprego de artifício destinado a induzir ou manter terceiros em erro, com o propósito de dissimular fatos ou obter vantagem indevida, para si ou para outrem.

Imediatamente após a verificação de um evento de fraude, o colaborador da SL Tools que o tiver identificado deverá reportá-lo no mesmo instante ao Diretoria de gerenciamento de riscos e controles internos da SL Tools, por meio do endereço de e-mail compliance@sltools.com.br ,

que, no prazo máximo de 24 horas contadas da identificação do evento de fraude em questão, informará sua ocorrência aos clientes da SL Tools e às autoridades competentes para apurá-lo, incluindo, mas não se limitando, conforme o caso, a Comissão de Valores Mobiliários ("CVM").

Adicionalmente, a SL Tools manterá canais de comunicação disponíveis durante o horário de negociações (de Segunda a Sexta-feira entre as 9:00 e 18:00 horas) para que terceiros, como clientes e outros participantes de sua plataforma de negociação, possam reportar a ocorrência de um evento de fraude caso identifiquem a sua ocorrência ou indícios de sua ocorrência. Para tanto, o interessado poderá comunicar a SL Tools por meio do endereço de e-mail compliance@sltools.com.br, ou, alternativamente, por telefone, por meio do número (11) 4118–3137.

Como métodos de prevenção a diferentes modalidades de fraude, a SL Tools adota as seguintes medidas:

(i) **Controle duplo de posições**: controle duplo e segregado das operações conduzidas e posições detidas por cada participante nos ativos negociados na SL Tools, realizado pela SL Tools e pela Câmara de Compensação e Liquidação ("Clearing") na qual as operações realizadas na SL Tools serão liquidadas, respectivamente, tanto durante a etapa de negociação quanto na etapa de pós-negociação;

(ii) **Conexão criptografada**: tunelamento de dados e conexão criptografada de ponta a ponta entre a plataforma de negociação da SL Tools ou integrações de sistemas de clientes e seus servidores, dificultando a possibilidade de acesso por terceiros não autorizados;

(iii) **Banco de dados criptografados**: as informações relativas às operações cursadas na plataforma de negociação SL Tools, bem como aos seus sistemas e softwares, além de outras informações cujo arquivamento é exigido por lei e/ou pela regulamentação aplicável, são armazenadas em banco de dados criptografado;

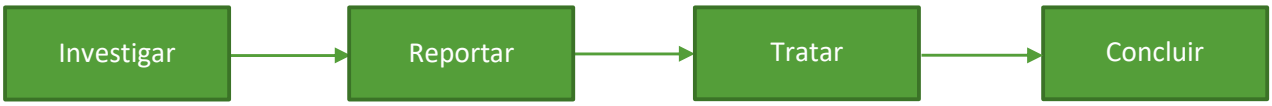
(iv) **Requisitos mínimos para senhas adotadas na SL Tools**: os colaboradores, participantes e clientes da SL Tools devem observar os requisitos mínimos previstos no Manual de Políticas e Procedimentos de Segurança da Informação no que se refere às senhas que irão adotar;

(v) **Senhas criptografadas**: criptografia de todas as senhas de acesso à plataforma de negociação da SL Tools; e

(vi) **Alteração de senha de participantes**: a alteração de senhas dos participantes da plataforma de negociação da SL Tools somente poderá se dar por meio de seu usuário administrador/usuário master, apontado nos termos do Regulamento da SL

Tools. O requerimento do usuário administrador/usuário master deve ser feito por e-mail para comercial@sltools.com.br .

Fases do tratamento a partir da identificação de evento de fraude reportado à SL Tools por meio de seus canais de comunicação:



(a) **Investigar**: Assim que um evento de fraude ou indícios que possam configurar um evento de fraude seja percebido pela área de controle ou informado à SL Tools por meio de algum de seus canais de comunicação, a área responsável da SL Tools deverá analisar os fatos relacionados à denúncia para se certificar se trata-se de fraude ou não;

(b) **Reportar**: Caso o evento identificado configure fraude, o responsável pela sua análise deverá reportá-lo à alta administração da SL Tools por meio de Informe de Risco Operacional, a qual informará sua ocorrência aos clientes e às autoridades competentes no prazo máximo de 24 horas contadas da identificação do evento de fraude;

(c) **Tratar**: Caso o evento de fraude ou eventuais prejuízos que dele tenham decorrido possam ser solucionados pela SL Tools (como, por exemplo, a inserção de informações falsas em seus sistemas ou cadastro), então a SL Tools tomará as providências cabíveis para cessar a fraude e/ou mitigar os danos que dela tenham decorrido. Caso o evento de fraude ou eventuais prejuízos que dele tenham decorrido não possam ser solucionados pela SL Tools, então os Diretores responsáveis deverão buscar terceiros capacitados a solucioná-lo; e

(d) **Concluir**: Após o devido reporte aos clientes e as autoridades competentes, e, concluído o tratamento da fraude com a mitigação ou eliminação de seus danos, caso possível, toda a documentação relativa ao processo de tratamento da fraude identificada é arquivada, permanecendo, contudo, à disposição das autoridades públicas para caso de investigações e/ou processos administrativos ou judiciais.

8. RELATÓRIO ANUAL CONTROLES INTERNOS E RISCOS OPERACIONAIS

Anualmente é elaborado o relatório de Riscos Operacionais e Controles Internos que consolida as atividades de avaliação sobre os ambientes de controles internos realizadas pelas áreas negócio e tecnologia da SL Tools, contendo seus respectivos resultados, as recomendações a respeito de eventuais deficiências com estabelecimento de prazo para regularização e manifestações dos responsáveis, assim como os critérios, metodologias e procedimentos aplicados pela entidade nas avaliações.

A data limite para emissão do relatório e envio para aprovação do Conselho de Administração até o último dia do mês de abril de cada ano. O relatório será enviado à SMI no prazo de 5 (cinco) dias úteis após sua aprovação.

Os documentos gerados durantes os trabalhos, resultados, após todas as validações, serão armazenados em local restrito, por período mínimo de 10 anos, ou maior se requerido por regulamentação ou legislação vigente.

9. CONSIDERAÇÕES FINAIS

A disseminação da cultura de riscos operacionais é feita através de informes, divulgação de treinamentos e orientação aos funcionários quanto aos princípios éticos.

A SL Tools consulta, periodicamente, as diversas fontes, internas e externas, no sentido de identificar a publicação de novas regras e/ou atualização nas matérias e normas relativas a riscos operacionais.

Compliance SL Tools.

HISTÓRICO DE REVISÕES
Elaborado em agosto de 2018
Atualizado em setembro de 2019
Atualizado em agosto de 2022
Atualizado em setembro de 2023

ANEXO I

INFORME DE RISCO OPERACIONAL

Nome Completo:	
Data:	
Ambiente de negociação no qual o evento ocorreu:	
Descrição do Evento:	