SL TOOLS

POLÍTICA DE CIBERSEGURANÇA

DEZEMBRO DE 2023

ÍNDICE

1. INTRODUÇÃO

A presente **Política de Cibersegurança** ("Política") visa a estabelecer princípios e diretrizes que busquem assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados pela **SL Tools S.A.** ("SL Tools"), assegurando a proteção adequada dos ativos e dos dados tratados por ela, garantindo, assim, a identificação, proteção, detecção, resposta e recuperação de contingências em casos de eventuais incidentes de segurança.

A SL Tools busca atingir um alto padrão de cibersegurança. Por isso, está comprometida com a segurança de todos os ativos físicos e lógicos de informação da empresa, garantindo que todos os requisitos legais, operacionais e contratuais sejam cumpridos. A preocupação com os riscos cibernéticos é comum aos diversos níveis de gestão e um compromisso individual de todos.

Nesse sentido, de modo a cumprir com os valores da SL Tools, a presente Política tem como premissa: *(i)* estabelecer diretrizes de cibersegurança, visando a proteger os ativos de tecnologia e os dados dos clientes da SL Tools; *(ii)* informar os Colaboradores da SL Tools e atribuir responsabilidades para garantia da segurança da informação, prevista em política própria; e *(iii)* garantir o cumprimento dos mais elevados padrões de ética e integridade, bem como de leis, normas, regulamentos, códigos, diretrizes e padrões aplicáveis aos negócios da SL Tools.

2. PRINCÍPIOS

A SL Tools adotará os seguintes atributos básicos de cibersegurança em conformidade com os padrões internacionais:

- Confidencialidade: a SL Tools limitará o acesso a informação tão somente às entidades legítimas, ou seja, àquelas pessoas autorizadas pelo proprietário da informação;

- Integridade: todas as informações manipuladas pela SL Tools manterão todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida.

- Disponibilidade: atributo que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pela SL Tools;

- Autenticidade: a SL Tools garante que a informação é proveniente da fonte anunciada e que não foi alvo de mutações ao longo de um processo;

- Irretratabilidade ou não repúdio: propriedade que garante a impossibilidade de negar a autoria em relação a uma transação anteriormente feita;

- Conformidade: a SL Tools seguirá as leis e regulamentos associados ao processo de segurança das informações.

3. OBJETIVO

Entre os objetivos desta Política estão: *(i)* proteger as informações e ativos de tecnologia da informação contra acesso, modificação, destruição ou divulgação não autorizados; *(ii)* assegurar a continuidade do processamento das informações críticas ao negócio; *(iii)* cumprir as leis e normas que regulamentam os aspectos de propriedade intelectual; *(iv)* determinar os mecanismos de gestão de riscos cibernéticos; e *(v)* dar ciência ao público em geral.

4. ABRANGÊNCIA

Esta Política estabelece princípios que devem nortear condutas e regras a serem observadas por todos os sócios, diretores, administradores, empregados, estagiários e, ainda, fornecedores e prestadores de serviços ("Colaboradores") que venham, direta ou indiretamente, trabalhar ou prestar serviços para a SL Tools.

As premissas definidas nesta Política são aplicáveis a todos os ambientes computacionais de processamento de dados da SL Tools, estendendo, sem limitação, a todos os servidores, bases de dados, sistemas operacionais, *hardware*, *software*, dispositivos de redes, telefonia, dispositivos móveis, além de ambientes de terceiros que, de forma física ou lógica, estejam

integrados ou conectados aos ambientes da SL Tools e seu acervo tecnológico. Assim, toda a atividade desempenhada pela SL Tools deve respeitar os princípios estabelecidos nesta Política, devendo tais princípios serem aplicados a todos os que estão acima mencionados.

Adicionalmente, todos deverão zelar pela lealdade, honestidade, transparência e o respeito mútuo nas relações profissionais e pessoais com clientes, potenciais clientes, concorrência, fornecedores, órgãos reguladores e fiscalizadores, prestadores de serviços e entre si.

Fica, portanto, vedado aos Colaboradores descumprirem as regras desta Política ou qualquer lei, regra ou regulamentação da legislação aplicável ao tema.

5. REFERÊNCIAS

A SL Tools pauta suas ações em boas práticas do mercado nacional e internacional. Dentre elas, destacam-se:

- Lei nº 13.709, de 14 de agosto de 2018, conforme alterada ("Lei Geral de Proteção de Dados Pessoais");

- Guia de Cibersegurança da Associação Brasileira das Entidades dos Mercados Financeiros e de Capitais – ANBIMA, datado de 6 de dezembro de 2017.

6. IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS – *RISK ASSESSMENT*

A SL Tools tem o compromisso de desenvolver uma cultura organizacional para gerenciar riscos de cibersegurança, sistemas, pessoas, ativos, dados e capacidades. Para tanto, visa a realizar o registro, a análise de causa e impacto e o controle dos efeitos de incidentes, incluindo informações recebidas de terceiros, utilizando como base o seguinte procedimento, a fim de mitigar riscos:

- Avaliação de Risco Inicial: deve-se identificar todos os processos e ativos relevantes da SL Tools (sejam equipamentos, sistemas ou banco de dados) expostos ao risco que se

busca mitigar, avaliando-se, por conseguinte, a vulnerabilidade dos ativos em questão e identificando-se possíveis ameaças e o seu grau de exposição. Adicionalmente, devem ser considerados os possíveis impactos financeiros, operacionais e reputacionais em caso de um incidente de segurança, bem como a expectativa de tal evento ocorrer;

- Classificação do Risco: deve-se classificar as informações geradas a partir da Avaliação de Risco Inicial de acordo com o seu grau de severidade, permitindo com isso a implementação de processos para o devido manuseio, armazenamento, transporte e descarte de informações;

- Implementação: uma vez definidos os riscos, devem ser implementadas ações de prevenção e proteção aplicáveis, de acordo com a legislação vigente.

7. AÇÕES DE PREVENÇÃO E PROTEÇÃO

Os controles internos de cibersegurança da SL Tools são desempenhados por meio da realização das seguintes ações de prevenção e proteção, sem prejuízo de outras medidas que podem vir a ser adotadas mediante a análise do caso concreto:

- Segregação de informações: o acesso às informações e o tráfego de dados tratados pela SL Tools devem estar restritos apenas aos recursos e equipamentos relevantes para o desempenho das atividades necessárias. Do mesmo modo, o acesso deve ser permitido de forma a ser revogado rapidamente assim que atingido o fim para que foi concedido.

- Controle de acesso aos ativos da SL Tools: o acesso aos ativos da SL Tools passa pela identificação, autenticação e autorização dos usuários ou Colaboradores. As regras que regem os níveis de acesso a cada informação estão dispostas no Manual de Política de Informações da SL Tools.

- Login e senha: os eventos de *login* e alteração de senhas realizados nos ambientes da SL Tools são auditáveis e rastreáveis, de modo a criar logs e trilhas de auditoria sempre que possível. Desse modo, a SL Tools busca permitir a identificação das partes responsáveis pelo

uso indevido de redes, servidores, sistemas, aplicativos e recursos em caso de incidentes. As regras que regem a utilização das senhas de acesso estão dispostas no Manual de Política de Informações da SL Tools, o qual está disponível através do *link* www.sltools.com.br.

- Configurações de Segurança: ao adquirir novos equipamentos e sistemas ou desenvolver novos *softwares* ou aplicações, a SL Tools garante que tenham sido feitas configurações seguras de seus recursos, bem como a aplicação dos últimos *patches* de segurança recomendados pelos fabricantes e processo de *hardening*. Além disso, contas "padrão" (default account), contas de "convidado" (guest account) e conta de sistema (system accounts) devem ser desabilitadas ou inativadas em todos os ambientes e equipamentos. Sempre que aplicável, a SL Tools realizará ou garantirá que sejam realizados testes de segurança em ambientes de homologação, sem o uso de informações reais de clientes, antes da utilização em definitivo do referido recurso.

- Inventário de Ativos de Tecnologia: A SL Tools mantém inventário atualizado dos ativos de tecnologia (*software e hardware*) afim de manter sua infraestrutura tecnológica atualizada, bem como realiza verificações frequentes para identificar elementos estranhos à SL Tools, como por exemplo, computadores não autorizados ou software não licenciado, ou ainda, *software* ou *hardware* que não estejam sendo suportados por seus respectivos fornecedores, ou seja, entraram em processo de *EOVS (End of Vendor Support)*.
    - *Softwares sem suporte de seus fornecedores deverão ser atualizados até 24 meses após a anúncio oficial de seus fornecedores.*
    - *O inventário de ativos de tecnologia deve conter informações relevantes para identificação dos equipamentos, tais como: nome, endereço IP, datacenter, ambiente, sistema operacional, componentes e data da última atualização.*

- Backup: como medida de segurança, a SL Tools implementa o serviço de *backup* dos diversos ativos da empresa, conforme disposto no Manual de Política de Informações da SL Tools.

- Serviços de terceiros: ao contratar serviços de terceiros, será realizada diligência nos termos previstos no Código de Ética e Conduta da SL Tools, de modo a assegurar a

confidencialidade das informações compartilhadas, bem como a adoção dos princípios previstos nesta Política pelo prestador de serviços.

- Firewalls: a SL Tools utiliza:

  (i) segurança de borda, nas redes de computadores, por meio de *firewalls* e outros mecanismos de filtros de pacotes; e;
  (ii) recursos *anti-malware* em estações e servidores de rede, como antivírus e *firewalls* pessoais;
  (iii) antivírus e *anti-malware* devem ser atualizados diariamente ou de acordo com os alertas enviados pelos próprios fornecedores sempre que houver atualização disponível;
  (iv) Ainda, como forma de prevenção e redução da superfície de ataque, as regras de *firewall*, *proxy* e roteadores serão revisadas no mínimo a cada 24 meses pela SL Tools e/ou seus provedores de infraestrutura.

- *Whitelisting:* para impedir a instalação e execução de *softwares* e aplicações não autorizadas, deverão ser utilizados controles de execução de processos tais como a aplicação de *whitelisting*.

- Treinamento de privacidade e segurança: os Colaboradores da SL Tools devem se submeter anualmente a um treinamento de cibersegurança de modo a se atualizar periodicamente quanto às melhores práticas de privacidade e segurança.

- E-mails e *links* externos: A SL Tools possuiu mecanismos de proteção de e-mails e *links* externos enviados nos mesmos, contudo os Colaboradores deverão ter atenção especial antes de clicar em *links* recebidos, mesmo vindos de pessoas conhecidas, dado que este é um dos principais vetores atuais de invasão.

- Estações de trabalho: a depender do grau de hierarquia do Colaborador, ele não deverá ter permissão para agendar tarefas em sua estação de trabalho ou alterar chaves de registro. Adicionalmente, as estações de trabalho (*e.g. desktops* e mesas de trabalho) não deverão conter arquivos ou informações confidenciais.

- Teste de penetração e vulnerabilidade: serão realizados testes de penetração e vulnerabilidade na infraestrutura tecnológica da SL Tools a fim de verificar possíveis problemas de segurança e corrigi-los preventivamente. Tais testes serão (i) realizados por empresas independentes, especializadas em segurança e escolhidas a critério da SL Tools; e (ii) pelo menos uma vez ao ano, ou sempre que houver mudança significativa na infraestrutura utilizada pela SL Tools ou seus parceiros. O prazo para correção dos problemas encontrados poderá variar dependendo da classificação de severidade dos mesmos, entretanto a SL Tools envidará todos os esforços necessários para que as correções sejam realizadas no menor tempo possível, a saber:

Severidade	**Prazo**
Baixa	120 dias
Média	90 dias
Alta	60 dias
Crítica	Imediata ou o mais breve possível

8. MONITORAMENTO E TESTES

Adicionalmente às ações de prevenção e proteção previstas acima, a SL Tools busca a estabelecer os seguintes mecanismos e sistemas de monitoramento, sem limitação, de modo a detectar possíveis ameaças e anomalias no ambiente tecnológico de maneira eficiente e em tempo hábil, reforçando os controles internos de cibersegurança existentes, caso necessário:

- Atualizações e gerenciamento de *patches*: a SL Tools mantém os sistemas operacionais e *softwares* de aplicação sempre modernizados, instalando as atualizações sempre que forem aplicáveis. Os *patches* disponíveis são gerenciados de modo a permitir o controle sobre o que deve ou não ser atualizado com o fim de rastrear e implementar melhorias necessárias, corrigindo vulnerabilidades identificadas na estrutura tecnológica para o caso de riscos classificados como críticos, médios ou altos. Os servidores de produção e contingência possuem processo automático para verificação dos últimos *patches* disponibilizados pelo fornecedor e dispara e-mail automático à Equipe de Tecnologia informando semanalmente a necessidade da aplicação dos *patches*. Dessa forma, o Time de Tecnologia planeja a aplicação dos *patches* em horários que não comprometam a operação da SL Tools no prazo máximo de até 30 dias, ou em prazos inferiores a 30 dias dependendo da criticidade da atualização em questão. Antes da aplicação dos *patches* de segurança deverá ser realizado *backup* das informações relevantes existentes nos servidores sempre que aplicável.

- Backup: a SL Tools monitora diariamente as rotinas de *backup*, executando testes regulares de restauração dos dados.

- Análise de logs: a SL Tools analisa regularmente os logs e as trilhas de auditoria criados, de forma a permitir a rápida identificação de ataques, sejam internos ou externos, utilizando-se, para tanto, de ferramentas de centralização sempre que aplicável.

- Testes de sistema: Serão testados, sempre que assim exigido, o tráfego de mensagens e informações confidenciais, o risco de vazamento de *drop copies*, a blindagem de níveis de acesso e eventuais planos de resposta a incidentes, simulando os cenários possíveis durante a sua criação. Os testes que envolvem dados considerados críticos devem ser conduzidos em padrão “caixa preta”. Esse procedimento consiste em uma validação minuciosa das informações imputadas e suas resultantes após o processamento no sistema. Essa validação, por sua vez, é feita por um programa automático ou individualmente, obrigatoriamente comprovados por logs da mensageria interna da plataforma. A SL Tools esclarece que o teste das funcionalidades informadas acima ou correções nas

funcionalidades existentes devem ser feitos sem restrição de tempo e usando excesso de recursos das equipes, dado o grau de relevância para o negócio da SL Tools.

- Testes de penetração e vulnerabilidade: Serão realizados testes de penetração e vulnerabilidade na infraestrutura tecnológica da SL Tools afim de verificar possíveis problemas de segurança e corrigi-los preventivamente. Esses testes serão realizados por empresas independentes, especializadas em cibersegurança escolhidas a critério da SL Tools, pelo menos uma vez ao ano ou sempre que houver mudança significativa na infraestrutura utilizada pela SL Tools ou seus parceiros.

9. PLANO DE RESPOSTA

Muito embora cada incidente de segurança seja inteiramente único, em caso de ocorrência de um vazamento de informações ou qualquer outra ameaça de segurança, os Colaboradores da SL Tools deverão necessariamente obedecer às seguintes etapas de identificação, tratamento e recuperação de incidentes ("Plano de Resposta"), de modo a permitir que uma resposta seja formulada rapidamente ao identificar as pessoas principais que devem ser incluídas, suas funções e seus protocolos de comunicação:

(i) Identificação: todo conjunto de atividade incomum, desde um alerta de acesso anormal a um alerta de *upload* irregular, deve ser tratado o mais rápido possível pelos Colaboradores assim que identificado. Para os fins de acionamento do Plano de Resposta, todos os acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer outra forma de tratamento inadequado ou ilícito de dados mantidos pela SL Tools ou por seus subcontratados devem ser considerados como ameaças ou incidentes;

(ii) Preparação e escalonamento interno: ao detectar uma ameaça ou incidente, os Colaboradores devem registrar e comunicar o fato, em até **30 (trinta) minutos** após a comprovação da violação de segurança, por telefone ou e-mail, aos Diretores da SL Tools, que, por sua vez, se reunirão com os encarregados pela área de segurança tecnológica, bem como o departamento ou escritórios que prestam a assessoria jurídica, responsáveis por

compliance e comunicação, para combinar seus esforços na execução do Plano de Resposta. Neste momento, deverão ser designados colaboradores ou deverá ser contratada uma empresa especializada para compor as equipes responsáveis pelas etapas de (a) contenção, (b) erradicação, (c) recuperação e (d) notificação. Se possível, já no momento da comunicação da ameaça ou incidente, o Colaborador deverá indicar, em sua notificação, a identificação do usuário responsável pela violação, a data da violação e os respectivos horários de *login* e *logoff*;

(iii) Contenção: a etapa de contenção pode ser desenvolvida tanto em curto, quanto a longo prazo. A contenção de curto prazo é uma resposta imediata que visa a impedir que a ameaça se espalhe e cause mais danos. A contenção a longo prazo inclui a devolução de todos os sistemas à produção para permitir a operação comercial padrão, mas sem as contas e *backdoors* que permitiram a intrusão. Deve-se buscar identificar todos os processos e ativos relevantes da SL Tools (sejam equipamentos, sistemas ou banco de dados) expostos ao incidente que se busca mitigar, avaliando-se, por conseguinte, a vulnerabilidade dos ativos em questão e o grau de severidade do incidente, considerando os possíveis impactos financeiros, operacionais e reputacionais;

(iv) Erradicação: nesta etapa, deve-se restaurar todos os sistemas afetados pela ameaça ou incidente, recriando ou atualizando todos os sistemas envolvidos e removendo quaisquer vestígios do incidente de segurança. Adicionalmente, deverá ser avaliada a necessidade de atualização dos sistemas vigentes e aplicação de medidas corretivas para evitar a repetição do incidente;

(v) Recuperação: a equipe responsável pela etapa de recuperação terá como principal atribuição a devolução de todo o sistema a seu funcionamento padrão. Neste momento, será preciso fazer uma varredura para verificar eventuais perdas e como recuperar possíveis dados perdidos. Para tanto, deve-se recorrer a cópias de segurança armazenadas em um sistema de *backup* para restabelecer todas as informações necessárias para o fluxo operacional;

(vi) Notificação: a SL Tools se compromete a comunicar à autoridade nacional e ao titular dos dados afetados a ocorrência de incidente de segurança que possa acarretar risco

ou dano relevante aos titulares. A comunicação aos clientes impactados pela violação de dados identificados será feita em **até 48 (quarenta e oito) horas** após a certificação da violação. Adicionalmente, a notificação à autoridade nacional será feita em prazo razoável, nos termos da Lei Geral de Proteção de Dados Pessoais, e deverá mencionar, no mínimo, (a) descrição da natureza dos dados afetados; (b) informações sobre os titulares envolvidos; (c) indicação das medidas técnicas e de segurança adotadas pela SL Tools; (d) os riscos relacionados ao incidente; (e) a justificativa para o tempo da notificação, no caso da comunicação não ter sido imediata; e (f) as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

Cumpre ressaltar que, durante a implementação do Plano de Resposta, os Colaboradores da SL Tools deverão manter toda a documentação relativa a ocorrências de incidentes e os procedimentos de resposta a eles. Com isso, busca-se criar o histórico de ocorrências contra a segurança e as devidas ações tomadas, tornando a SL Tools mais preparada para lidar com transtornos futuros. Ademais, o devido arquivamento de documentações relacionadas ao gerenciamento dos incidentes é essencial para servir como evidência em caso de eventuais questionamentos.

Por fim, será elaborado relatório de incidentes, contendo (i) as características e descrição do incidente e das medidas tomadas, informando o impacto gerado, quando aplicável e (ii) anexos relacionados as comunicações recebidas da área identificadora e demais informações pertinentes aos incidentes, conforme aplicável.

O relatório de incidentes será mantido à disposição da Superintendência de Relações com o Mercado e Intermediários (“SMI”).

10. RELATÓRIO DE TESTES NOS SISTEMAS CRÍTICOS

Anualmente é elaborado o relatório que consolida o resultado dos testes dos sistemas críticos da SL Tools, indicando às deficiências identificadas e as ações planejadas para saná-las. O relatório anual é encaminhado ao Conselho de Administração da SL Tools e a SMI.

11. RECICLAGEM E REVISÃO

A presente Política deve ser revisada periodicamente, de modo a atualizar de maneira constante o procedimento para avaliações de risco, ações de prevenção e proteção, Plano de Resposta, monitoramento e testes dos ambientes da SL Tools.

Com intuito de promover e disseminar a cultura de segurança internamente, a SL Tools busca conscientizar seus Colaboradores sobre os riscos e as melhores práticas de segurança, dar treinamentos anuais e repassar novas orientações. Os Colaboradores, por sua vez, devem manter-se atualizados acerca de novas vulnerabilidades e ameaças identificadas, de modo que possam facilmente tomar as medidas adequadas e proporcionais ao grau de exposição dos ativos da SL Tools.

Como parte dos mecanismos para conscientização sobre o assunto, a SL Tools dispõe ainda de um Manual de Políticas de Informação como parte de um conjunto de princípios, práticas e cuidados que norteiam a gestão de segurança das informações corporativas da SL Tools.

12. PROCEDIMENTOS DISCIPLINARES

As violações a esta Política estão sujeitas às ações disciplinares previstas nas normas internas da SL Tools e na legislação brasileira vigente. Sem prejuízo, eventuais acessos não autorizados ao banco de dados da SL Tools podem ser punidos mediante a rescisão do contrato firmado a qualquer título com o respectivo Colaborador infrator ou mediante a redução de eventuais bonificações, conforme o grau de severidade da violação.

A SL Tools se reserva no direito de tomar as medidas legais a respeito a quaisquer violações à confidencialidade dos dados em seu poder.

13. PROCESSO DE INVESTIGAÇÃO FORENSE

Em situações de incidentes de cibersegurança a equipe de infraestrutura ou quaisquer colaboradores devem adotar protocolos que permitam investigações forense de incidentes. Preservando dados, ambientes e hardware necessários para investigações posteriores, própria ou de terceiros contratados pela SL Tools.

Deve-se:

- Desligar cabos de rede
- Preservar e documentar a máquina alvo do ataque
- Não acessar logs
- Não desencadear comandos da máquina alvo

Será avaliada a possibilidade de análise e investigação pela equipe interna ou a contratação de peritos terceirizados para uma análise forense dos fatos e reconstrução dos acontecimentos.
O objetivo é determinar onde se localizou a vulnerabilidade, responsabilizar os envolvidos e corrigir falhas de tecnologia e processos que originaram o incidente.

14. GERENCIAMENTO DE CHAVES E CERTIFICADOS DE CRIPTOGRAFIA

O uso de chaves de criptografia e certificados digitais são mecanismos de segurança para proteção de dados e ativos sensíveis da SL Tools, possibilitando a mitigação de riscos, além de cumprir com leis e regulamentações em vigor.
Como forma de proteção, a SL Tools utiliza criptografia para dificultar a legibilidade dos dados tratados por terceiros não autorizados, a saber:

i. o canal de comunicação entre a aplicação cliente e o servidor usam criptografia assimétrica TLS 2.048 bits para criptografar as informações em trânsito;
ii. as informações em repouso que possam levar à identificação dos titulares dos dados são criptografadas usando criptografia simétrica AES 256 bits
iii. a senha dos usuários utiliza criptografia de hash (SHA-512);
iv. as chaves de criptografia utilizadas na criptografia das informações em trânsito e em repouso são únicas para cada finalidade;
v. e-mails são criptografados com criptografia assimétrica TLS;

14.1. ACESSO AS CHAVES DE CRIPTOGRAFIA

Adicionalmente, a chave para descriptografar os dados tratados pela SL Tools deverão ser mantidos em sigilo, sendo seu acesso permitido apenas aos Colaboradores autorizados pela SL Tools, de modo a impedir que qualquer pessoa possa decifrar os dados em trânsito ou em repouso.

14.2. COMPROMETIMENTO DAS CHAVES DE CRIPTOGRAFIA

No caso de suspeita ou conhecimento de que as chaves de criptografia tenham sido comprometidas, essas deverão ser substituídas o mais breve possível para evitar acessos indevidos ou vazamento de dados sensíveis.
Além disso, quando um funcionário com conhecimento das chaves de criptografia encerra suas atividades na SL Tools, as chaves que eram de conhecimento desse funcionário deverão ser substituídas o mais breve possível.

15. PROCESSO DE DILIGÊNCIA PROVEDORES DE SERVIÇO

Como parte do processo de segurança dos serviços prestados pela SL Tools aos seus clientes, a SL Tools conduz processo de diligência para avaliar e escolher seus parceiros e provedores de serviço.

O processo é conduzido aplicando um questionário técnico onde são verificados os principais itens de segurança e aderência aos padrões de segurança da informação estabelecidos pela SL Tools.

No caso específico de datacenters onde dados sensíveis possam ser armazenados pela SL Tools, é exigido que o provedor desse serviço possua certificação ISO/IEC 27001 válida e certificada por órgão independente, assegurando assim que os padrões e controles de segurança estarão nos níveis internacionais estabelecidos pelo *International Organization for Standardization (ISO).* Periodicamente, a SL Tools solicita a apresentação do certificado ISO/IEC 27001.

16. DISPOSIÇÕES GERAIS

Atualização. Esta Política será revisada, no mínimo, anualmente, considerando a data de publicação mais recente (quadro "Histórico de Revisões" abaixo), podendo ser atualizada a qualquer tempo para incorporar melhorias, corrigir erros ou atender normativos.

Direitos Autorais e Distribuição. A SL Tools possui sobre esse documento todos os direitos de elaboração, alteração, reprodução e distribuição. Este documento substitui todas as versões anteriores. A SL Tools não se responsabiliza por versões desatualizadas, modificadas, ou por quaisquer versões provenientes de outras fontes que não a fonte oficial designada para fornecer este material.

Ciência. Todos os Colaboradores devem atestar a leitura e perfeita compreensão desta Política e suas posteriores alterações.

Em caso de dúvidas ou esclarecimentos sobre o conteúdo desta Política ou sobre a aplicação da mesma em relação a algum assunto específico, a direção da SL Tools deverá ser consultada.

SL Tools S.A.

HISTÓRICO DE REVISÕES	Observações
Elaborado em 15 de maio de 2020	
Atualizado em setembro de 2020	
Atualizado em novembro de 2020	
Atualizado em abril de 2021	
Atualizado em novembro de 2021	
Atualizado em agosto de 2022	
Atualizado em dezembro de 2022	Atualização/Ajuste de textos
Atualizado em dezembro de 2023	Atualização