SL TOOLS

MANUAL DE POLÍTICA DE INFORMAÇÕES E PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

AGOSTO 2024

SL TOOLS S.A.

ÍNDICE

1. INTRODUÇÃO

O presente Manual de Políticas de Informações e Procedimentos ("Manual") tem como premissa estabelecer regras de governança e melhores práticas necessárias para a proteção das informações da **SL Tools S.A.** ("SL Tools"), bem como informações disponibilizadas por terceiros e clientes que de qualquer forma venham a ser manuseadas e/ou armazenadas pela SL Tools.

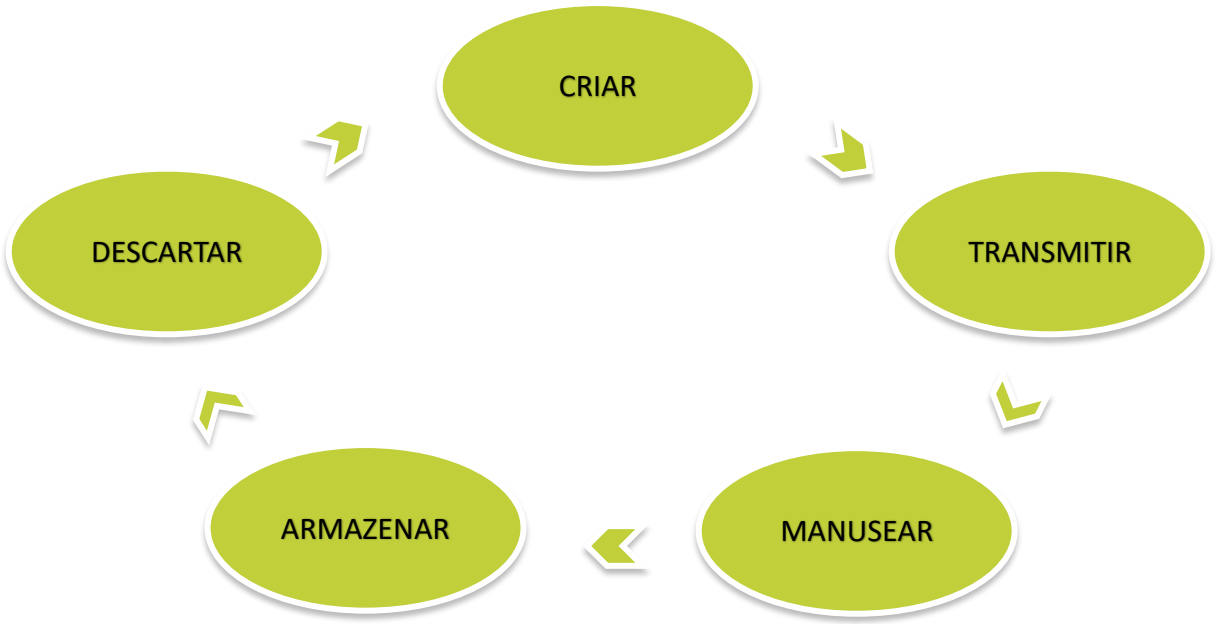
Este Manual contém um conjunto de princípios, práticas e cuidados que norteiam a gestão de segurança das informações corporativas da SL Tools.

Adicionalmente, cumpre ressaltar que este Manual deverá ser observado e integralmente cumprido por todos os colaboradores da SL Tools, incluindo estagiários, funcionários, fornecedores, prestadores de serviços e parceiros comerciais da SL Tools ("Colaboradores") e sócios, devendo ser regularmente atualizado e divulgado pelos gestores da SL Tools, os quais ficarão responsáveis por fazer com que os Colaboradores observem e cumpram o disposto neste Manual.

O objetivo deste Manual é definir regras, responsabilidades e estratégias relacionadas aos procedimentos e mecanismos de controles internos visando à mitigação de eventuais impactos e riscos que possam ser causados durante o ciclo de vida da informação, conforme será explicado no item a seguir.

2. CICLO DA INFORMAÇÃO

A aplicabilidade das regras e procedimentos dispostos neste Manual refere-se ao ciclo de vida físico e digital da informação, conforme demonstra o esquema abaixo:



- **CRIAR**: é a fase de elaboração e disponibilização de documentos, bases de dados e informações pela SL Tools.

- **TRANSMITIR**: refere-se à circulação interna ou recebimento e envio externo à SL Tools de documentos físicos e mídias móveis, seja por vias físicas ou eletrônicas.

- **MANUSEAR**: trata-se de uso e acesso a informações e dados, físicos e digitais, incluindo mídias móveis.

- **ARMAZENAR**: refere-se a criar formas de acesso e organização do armazenamento de documentos e mídias em locais físicos internos e externos ou arquivos de dados de documentos e informações eletrônicas.

- **DESCARTAR**: fase do ciclo de vida da informação em que deverá ocorrer a fragmentação de documentos físicos e mídias ou exclusão definitiva de dados e informações digitais que se encontrem armazenados junto à SL Tools.

3. CICLO DE DESENVOLVIMENTO DE SOFTWARE

Para o desenvolvimento de novos *softwares*, a SL Tools utiliza uma metodologia ágil de gestão e planejamento conhecida pelo mercado como **SCRUM**. Tal ciclo de desenvolvimento é dividido nas seguintes etapas:

- **ANÁLISE DO PROJETO E VIABILIDADE**: Corresponde à fase de planejamento e definição do escopo do projeto, na qual busca-se traçar uma estrutura de desenvolvimento. O projeto, por sua vez, pode ser separado em dois grupos *(i)* emergencial – em que são feitas correções necessárias para estabilizar o funcionamento do sistema – e *(ii)* programado – em que são desenvolvidas novas funcionalidades, melhorias e novos produtos.

- **ESPECIFICAÇÃO DE REQUISITOS**: Esta fase consiste na definição e escolha do projeto que será executado. Com base no escopo definido na etapa anterior, deverão ser propostas possíveis abordagens de design e arquitetura do produto a ser desenvolvido, as quais são elaboradas através do método de *design thinking*, investindo tempo relevante na consulta de todas as partes interessadas no projeto, em especial seus clientes, de modo a desenhar a estratégia mais adequada a ser seguida. A partir das informações coletadas de seus clientes, departamento comercial, de produtos e tecnologias, pesquisas de mercado e de especialistas que se fizerem necessários, os projetos deverão ser formalizados detalhadamente através de um *template* único da SL Tools. Nessa fase, a equipe de testes participa da definição das regras de negócio das funcionalidades a serem desenvolvidas.

- **ESTIMATIVAS**: uma vez especificados, os projetos priorizados serão direcionados aos responsáveis para a realização da estimativa de recursos, prazos e custos que deverão ser despendidos para o desenvolvimento do projeto. Baseado nessas estimativas, deverá ser dada prioridade para as etapas de desenvolvimento e alocação em *sprints*. Também nesta fase, a equipe de testes estima o desenvolvimento dos casos de testes para desenvolvimento e uso no processo de homologação.

- **DESENVOLVIMENTO:** O processo de desenvolvimento da SL Tools não cumpre determinação de prazo, mas sim de qualidade do produto desenvolvido. Nesta etapa, além do desenvolvimento da funcionalidade são desenvolvidos os casos de testes pela equipe correspondente.

Durante o ciclo de desenvolvimento, os projetos devem ser alocados com base nas prioridades definidas na etapa anterior. A área de produtos e o *Product Owner* devem definir os itens que comporão o *Product Backlog*, isto é, uma lista de tudo o que será preciso para a execução do produto ou funcionalidade, que podem incluir mais de uma especialidade de programação. A equipe de projetos, composta por analistas de desenvolvimento, de qualidade, de infraestrutura e de operação, deve analisar o *Product Backlog* a que foi dada prioridade e o alocar em uma determinada *Sprint*, a qual deverá ter duração média de 2 (duas) semanas. Estes itens deverão tornar-se, então, um *Sprint Backlog*. A supervisão do projeto, por sua vez, cabe ao *Scrum Master*. A SL Tools trabalha com *feedback* contínuo do processo de desenvolvimento. Assim, a equipe de tecnologia debate entre ela constantemente os projetos em desenvolvimento, buscando alcançar a melhor eficiência na execução do projeto. Por fim, esclarece-se, ainda, que, durante o processo de desenvolvimento, deverá ser utilizado controle de versão e repositório de código

através da ferramenta Atlassian BitBucket. Este controle de versão deverá se basear em *branches*, *issues* e *tags* para a segregação do que deve ser desenvolvido em cada *Sprint*.

- **REVISÃO DE CÓDIGO *(Code Review)*:** Durante o processo de desenvolvimento de software, a fim de garantir a qualidade e segurança do código que está sendo desenvolvido, nossos desenvolvedores enviam o código-fonte desenvolvido para ser revisado por outro desenvolvedor sênior (por meio do processo de *Pull Request* utilizando a ferramenta *BitBucket*) que verificará todos os aspectos do código-fonte, tais como complexidade, padrões de código, a "não existência" de informações sensíveis (nomes de usuários, senhas, chaves de criptografia), etc. e uma vez aprovado, o código será mesclado junto ao repositório de código mestre e poderá ser utilizado para gerar uma nova versão do sistema em questão.

- **RESTRIÇÃO DE USO DE INFORMAÇÕES SENSÍVEIS:** É estritamente proibido o uso, definição ou guarda de informações sensíveis no código fonte da aplicação, ou seja, processo de "hard coded". As informações consideradas sensíveis são nomes, senhas, chaves de usuários de rede, banco de dados, tokens de acessos e quaisquer outras informações que permitam acessos a servidores, banco de dados, áreas restritas, aplicações, etc. Além disso, dados e informações do ambiente de produção não devem ser utilizados em ambientes de desenvolvimento, testes ou qualquer outro ambiente que não seja o ambiente de produção. Para fins de desenvolvimento e testes serão utilizados somente dados e informações fictícias preparados para essa finalidade.

- **DESENVOLVIMENTO SEGURO DE CÓDIGO**: Durante o processo de desenvolvimento deverão ser realizados testes e análise de segurança no artefato desenvolvido sempre que possível, buscando elevar o nível de segurança do produto final ao mais alto nível possível. A preocupação com a segurança é de responsabilidade de todos os envolvidos no Ciclo de Desenvolvimento de Software em todas as suas fases. *Os testes de segurança durante o processo de desenvolvimento poderão ser realizados de forma manual ou automatizado via ferramentas como SonarQube, AWS Code Guru, entre outras, de acordo com as necessidades avaliadas pela Equipe de Desenvolvimento.*

- **TESTES E *QUALITY ASSURANCE***: Nesta fase, sendo uma funcionalidade nova ou uma correção de funcionalidade defeituosa, é **restrita** ao ambiente de homologação, distinto dos demais ambientes (desenvolvimento e produção). Nesta fase do ciclo de desenvolvimento, a equipe de testes e Q&A aplica testes positivos e negativos na funcionalidade. Os testes visam testar o maior número de cenários possíveis, podendo ser realizado de forma manual ou automatizada, dependendo do contexto e complexidade da funcionalidade à ser testada.

O processo de testes envolve o time de desenvolvimento para correções e posteriormente re-teste, completando o processo de homologação.

IMPLANTAÇÃO – *"GMUD"*

O processo de gestão de mudança/implantação "GMUD" é o processo que documenta a promoção de novas versões de *software* em ambiente de produção, bem como a correção de problemas e falhas previamente reportados ao time de tecnologia. As "GMUDs" podem ser classificadas em três categorias dependendo do planejamento prévio e sua criticidade:

- **Planejada**: Mudança planejada que geralmente é utilizada para promover à produção uma nova versão do software ou produto que seguiu todo o Ciclo de Desenvolvimento de Software. Também pode ser utilização para aplicar correção de problemas previamente reportados e que não tem impacto ao ambiente de negociação SL Tools.

- **Não Planejada**: Mudanças que geralmente são realizadas para atender alguma demanda regulatória não prevista ou ainda alguma correção de problema "não crítico", porém que não possa aguardar por uma mudança planejada.

- **Emergenciais**: São correções de problemas que estejam impactando o bom funcionamento do ambiente de negociação da SL Tools e se não forem corrigidos rapidamente poderão resultar em prejuízos ou impactos ainda maiores ao ambiente de negociação da SL Tools.

As "GMUDs" seguem o processo de "atualização contínua automatizada", ou seja, uma esteira que percorre o caminho de desenvolvimento, testes, aprovação e promoção ao ambiente produtivo a saber:

- Desenvolvimento: etapa onde as funcionalidades estão sendo implementadas pelos desenvolvedores;

- Testes: etapa em que as funcionalidades que foram entregues pelos desenvolvedores serão testadas pela área de qualidade de software;

- Aprovação: o processo de aprovação é realizado via ferramenta Atlassian BitBucket seguindo o processo de *merges/branches* como descrito a seguir:

- Ambiente de Desenvolvimento: Aprovação realizada pelos próprios desenvolvedores, sempre para a *Branch* de desenvolvimento;

- Ambiente de Testes: Aprovação realizada pelos próprios desenvolvedores, sempre realizando o processo de *merge* para a *Branch* de "stage";

- Ambiente de Certificação: Aprovação realizada por pelo menos um desenvolvedor sênior e CTO ou CCO, sendo obrigatória no mínimo duas aprovações para seguir para o ambiente de certificação sempre realizando o processo de *merge* para a *Branch* "demo";

- Ambiente de Produção: Aprovação realizada por pelo menos um desenvolvedor sênior e CTO ou CCO, sendo obrigatória no mínimo duas aprovações para seguir para o ambiente de produção sempre realizando o processo de *merge* para a *Branch* "master";

- A implantação de mudanças planejadas deverá ser executada após o fechamento da janela de negociação da SL Tools, preferencialmente às quintas-feiras. Mudanças emergenciais, em geral correções, devem seguir uma análise criteriosa de impactos e desencadear um fluxo de comunicação eficiente interna e com os participantes do ambiente de negociação para uma eficiente implantação e mitigação de impactos.

Após a execução da implantação em produção, o *Product Owner* que requisitou a mudança irá realizar as validações aplicáveis a fim de certificar-se que o sistema está funcionando como esperado, bem como se a mudança foi implantada como esperado. O *Product Owner* deverá coletar evidências da validação realizada e armazená-las na ferramenta *JIRA Service Management.*

4. RESPONSABILIDADES

Tendo em vista o porte, o perfil de risco e modelo de negócio da SL Tools, seguem abaixo as principais definições dos papéis e responsabilidade de seus Colaboradores e sócios no que se refere à segurança de suas informações:

- o CTO (Chief Technology Officer) é o responsável por manter e fazer cumprir de forma ampla e irrestrita todo o conteúdo disposto neste Manual, no Código de Ética e Conduta e demais políticas e diretrizes da SL Tools a todos os Colaboradores, parceiros e fornecedores que mantenham relacionamento com a SL Tools;

- ter ciência de que todas as informações geradas, acessadas, processadas, utilizadas ou armazenadas em qualquer meio ou sistema de informação, devem ser relacionadas às suas atividades profissionais e poderão ser monitorados e auditadas pela SL Tools, não cabendo nenhuma expectativa de privacidade do colaborador;

- proteger as informações contra acessos, modificações, destruições ou divulgações não autorizadas;

- cumprir as leis e as normas que regulamentam a propriedade intelectual;

- assegurar a confidencialidade de informações de terceiros e clientes;

- participar de treinamentos em geral, incluindo aqueles que versem sobre a responsabilidade no tocante ao tratamento das informações da SL Tools e de seus clientes;

- comunicar aos sócios qualquer suspeita ou violação deste Manual;

- manter-se devidamente atualizados e discutir regularmente sobre leis, normas e regulamentos referentes à segurança da informação;

- ministrar treinamento referente ao conteúdo deste Manual sempre que necessário;

- gerenciar as ações em segurança da informação física e digital;

- assegurar a existência de processo estruturado de informação e comunicação de incidentes e violações de segurança;

- designar colaboradores internos ou terceiros para verificar e testar a vulnerabilidade nos sistemas da SL Tools;

- revisar e atualizar este Manual anualmente ou quando necessário;

- divulgar este Manual a todos os Colaboradores da SL Tools;

- identificar, mensurar e controlar os diversos tipos de risco envolvidos em operações das quais a SL Tools esteja envolvida; e

- avaliar e monitorar as ações de prestadores de serviços terceirizados que desempenhem suas atividades juntamente com a equipe da SL Tools.

5. CLASSIFICAÇÃO DAS INFORMAÇÕES

A SL Tools entende ser importante dividir e classificar as informações que trafegam em seus servidores e sua plataforma. Assim, as informações são classificadas da seguinte forma:

Informações Crítica. Trata-se da informação que pode causar danos e prejuízos gravíssimos para a SL Tools e seus clientes. Deve ser totalmente preservada em seu estado original durante todo o período de necessidade de armazenamento, sendo vedada a divulgação fora da SL Tools ou mesmo internamente para pessoas que não necessitem de seu conhecimento para o exercício de suas funções.

As seguintes informações serão consideradas críticas:

a) nome dos clientes da SL Tools;
b) número da conta e corretora quando associados;
c) ponta da operação;
d) quantidade do ativo; e
e) símbolo do ativo.

Informações Confidenciais. Entende-se por informação que, se divulgada ou acessada por pessoas não autorizadas, pode acarretar danos e prejuízos moderados ou graves para a SL Tools. Deve ser totalmente preservada em seus estados originais durante todo o período de necessidade de armazenamento, podendo ser divulgada somente com autorização prévia da diretoria da SL Tools.

As seguintes informações serão consideradas confidenciais:

a) prazos;
b) datas associadas aos contratos negociados; e
c) contrapartes dos contratos negociados.

Informações Públicas. Trata-se da informação de conhecimento irrestrito e de conhecimento de todos, podendo ser divulgada fora da empresa mediante autorização da administração.

As seguintes informações serão consideradas públicas:

a) cotações do livro de ofertas não identificados; e
b) execuções de operações não identificadas.

6. SEGURANÇA DAS INFORMAÇÕES

A SL Tools adotará os seguintes atributos básicos da segurança da informação 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.

7. PREVENÇÃO CONTRA VAZAMENTO DE DADOS

A SL Tools utiliza mecanismos para monitoramento e prevenção contra vazamento de informações sensíveis *(DLP – Data Loss Prevention)* em todos os computadores corporativos da Organização.

Documentos e informações classificadas como "Confidenciais" só podem ser compartilhadas com aprovação da diretoria da SL Tools, responsável por analisar, classificar e controlar tais documentos e informações.

Para a realização do controle e monitoramento de informações sensíveis, a SL Tools utiliza a solução Microsoft 365 Compliance DLP onde todas as regras de monitoramento, classificação de informações sensíveis e demais itens a proteção contra vazamento de dados é realizada.

8. ARMAZENAMENTO, RETENÇÃO E *BACK-UP*

A SL Tools manterá os dados coletados armazenados em seus sistemas até o término de seu tratamento, no âmbito e nos limites técnicos das atividades desenvolvidas pela SL Tools, ressalvada a conservação dos mesmos pelo período adicional de 10 (dez) anos para os fins de cumprimento de obrigação legal ou regulatória e para o uso próprio da SL Tools, ressalvados os limites previstos em lei.

O back-up de seu banco de dados é realizado diariamente via replicação de dados em tempo real para um servidor independente e disponibilizado em datacenter diferente do principal, sem acesso à internet.

Adicionalmente, a SL Tools manterá em suas dependências ou garantirá que os seus Colaboradores mantenham em suas dependências, conforme aplicável, o nível de segurança e controle adequado para proteger os registros de mídia ou em papel, instalando, conforme necessário, fechaduras, alarmes, câmeras de vigilância, entre outros.

Os Colaboradores, por sua vez, deverão empreender seus melhores esforços para garantir o armazenamento e descarte seguro dos dados coletados pela SL Tools, de modo a impedir o vazamento, extravio ou a utilização de forma indevida, protegendo a confidencialidade das informações tratadas, sejam elas digitais ou impressas, sob pena de responsabilização.

9. SEGURANÇA E GUARDA DAS INFORMAÇÕES

A seguir estão dispostas regras e procedimentos para tratamento das informações de modo seguro:

- documentos críticos ou confidenciais (sobretudo de clientes da SL Tools) devem ficar armazenados em locais seguros e de acesso restrito aos Colaboradores autorizados;
- locais de armazenamento das informações citadas no item anterior devem ser rigorosamente monitorados;
- o período de armazenamento das informações antes do descarte deve respeitar o disposto neste Manual;
- informações armazenadas em computadores devem ser direcionadas à rede corporativa, sendo vedada a gravação de arquivos no disco rígido local;
- e-mail não deve ser usado para guarda de informações;
- o envio e o recebimento de informações e documentos em meio físico de/para locais externos devem ser protocolados e controlados quanto à entrada e saída da SL Tools.

10. *CLEAR DESK & CLEAR SCREEN*

Todos os Colaboradores devem manter as suas mesas limpas e organizadas, devendo toda a documentação e informação que não seja uma Informação Pública ser mantida em local com fechadura e de acesso restrito. Nenhuma Informação Confidencial deve ser deixada à vista, seja em papel ou em quaisquer dispositivos, eletrônicos ou não.

A seguir estão dispostos regras e procedimentos que deverão ser observados para reduzir o risco de acesso não autorizado, perda e dano às informações durante e fora do horário normal de trabalho ou quando os ambientes da SL Tools não estiverem sendo vigiados:

- ao usar uma impressora coletiva, o Colaborador deve recolher o documento impresso imediatamente;
- após reuniões e visitas, internas ou externas, todo o material utilizado deve ser retirado das salas de reuniões, incluindo anotações;
- computadores e *notebooks* não devem ser deixados conectados quando desacompanhados e devem ser protegidos por senha;
- o bloqueio de segurança dos computadores e *notebooks* deve ser definido para ativar quando não houver atividade por mais de cinco minutos consecutivos, devendo, ainda, ser protegido por senha para reativação;
- os Colaboradores devem bloquear os computadores caso se ausentem da estação de trabalho;
- os Colaboradores devem se certificar que não existem informações confidenciais abertas na tela caso precisem compartilhar a mesma;

- os Colaboradores devem desligar seus respectivos computadores diariamente ao final do dia de trabalho;
- ao final do expediente, todo Colaborador deve se certificar de que não há nenhum papel ou pertences deixados sobre a sua respectiva estação de trabalho;
- as áreas de trabalho (*desktops*) devem conter apenas atalhos, sendo vedado salvar arquivos ou pastas nesse local;
- as telas dos computadores devem estar posicionadas afastadas da vista de pessoas não autorizadas; e
- todas as Informações Confidenciais e de uso interno devem ser removidas da mesa e trancadas em uma gaveta ou arquivo quando a estação de trabalho estiver desacompanhada e/ou ao final do dia de trabalho.

11. ACESSO FÍSICO E LÓGICO

A credencial de acesso a qualquer meio lógico ou físico trata-se de um importante mecanismo de controle e segurança das informações da SL Tools. As áreas responsáveis, realizarão a revisão dos perfis e dos acessos físicos e lógicos no mínimo anualmente ou sempre que necessário, de acordo com o procedimento interno definido para tal e respeitando-se a segregação de funções. Não obstante, deverão ser observadas as disposições estabelecidas neste Manual.

Além da credencial supramencionada, os seguintes preceitos deverão ser observados quando do **Acesso Físico** à estrutura da SL Tools:

- O acesso aos Data Centers (se aplicável) se darão por meio de solicitação formal prévia à área responsável, a qual deverá autorizar ou não o acesso do solicitante e desde que previamente notificado aos responsáveis da SL Tools. Não obstante, se fará necessário a apresentação de documentação oficial com foto quando do efetivo acesso;

- O acesso aos *cages* e *racks* é monitorado por câmeras posicionadas para gravar imagens dos corredores de acesso. Os provedores de data centers são encarregados de contratar os referidos serviços de monitoramento e, sempre que for necessário e solicitado pela SL Tools, dará acesso às imagens gravadas;

- O crachá de acesso ao prédio e dependências internas é pessoal e intransferível;

- As demais formas de acesso físico (como por exemplo, a biometria) somente deverão ser concedidas para os Colaboradores que necessitarem para o exercício das funções e conforme orientação do gestor responsável;

- Todos os crachás possuem níveis de acesso diferenciados conforme cargo e/ou função a fim de evitar conflito de interesses e acesso não autorizado de informações;

- A recepção do condomínio onde a SL Tools encontra-se instalada deve registrar a entrada e saída de terceiros ou visitantes;

No que tange ao **Acesso Lógico**, os seguintes preceitos deverão ser observados:

- O gestor deve solicitar, no momento da contratação do novo Colaborador ou da movimentação de área do colaborador antigo, os acessos necessários aos diversos sistemas da SL Tools, conforme aplicável;

- Os Colaboradores desligados deverão ter seus acessos revogados no momento imediato do desligamento;

- Todo Colaborador que tenha acesso aos sistemas de informação da SL Tools é responsável por tomar todas as medidas necessárias a fim de impedir o acesso não autorizado de terceiros não autorizados; e

- Adicionalmente à regra lógica de bloqueio automático das estações de trabalho, todos devem travar o acesso aos seus computadores (CTRL+ALT+DEL) quando se ausentarem do local físico de trabalho, independentemente do período de ausência.

12. NÍVEIS DE ACESSO

Atribuições de níveis de acesso são determinados pelos gestores da SL Tools na contratação do Colaborador ou ocasionadas por alterações em suas funções. Os acessos são segregados por ambiente, serviços, sistemas e classificação de usuários, conforme detalhado abaixo.

Os ambientes são segregados em:

- **Ambientes Produtivos (Produção e Contingência)**
  - Acesso permitido à analistas de infraestrutura responsáveis pelo suporte, monitoramento e sustentação do ambiente de produção;
  - Acesso temporário concedido à desenvolvedores sêniores em situações específicas para identificação e resolução de problemas, sempre aprovado pelo seu gestor imediato.

- **Ambientes "Não Produtivos"**
  - Acesso permitido à desenvolvedores, analistas de qualidade e analistas de infraestrutura, podendo ser permitido à usuários da área de negócio para testes e avaliações;
  - Em nenhuma hipótese é permitida a utilização de dados de clientes de Produção nos ambientes de testes/desenvolvimento.
    Todos os dados utilizados no ambiente de desenvolvimento/testes são fictícios (fake), utilizados para desenvolvimento e testes somente.

- **Ambiente de Desenvolvimento**

- Acesso permitido à desenvolvedores, analistas de infraestrutura e analistas de qualidade;

Os acessos são classificados como:

- **Administrador:**
  - Permissão para realizar atividades de administração no serviço/sistema/ambiente em questão;
  - São criadas contas secundárias pessoais e intransferíveis (segregadas das contas primárias dos usuários) para os usuários que necessitem de acesso administrativo aos servidores;
  - A utilização de contas secundárias com privilégio administrativo deve ocorrer somente em situações em que tais privilégios sejam realmente necessários, principalmente na resolução de problemas em ambiente de produção, gerenciamento de mudanças e atualizações de sistema;
- **Regular:**
  - Acesso restrito para realização de atividades que não necessitam de elevação de permissão para administrador;
- **Somente leitura:**
  - Permissão apenas para visualização das informações referente ao serviço/sistema/ambiente em questão;
- **Sem acesso:**
  - Sem permissão para qualquer tipo de acesso ao serviço/sistema/ambiente em questão;
- **Usuário funcional ou de sistema:**
  - Usuário restrito somente para execução de serviços e sistemas nos servidores de aplicação, não pode ser utilizado para acesso direto aos servidores.
  - A senha do usuário funcional/sistema é dividida em duas partes e custodiadas por usuários distintos;

A requisição de nível de acesso deve incluir o nome do Colaborador requisitante, aprovador, serviços e softwares necessários para acessar e a respectiva classificação do acesso.

Alterações em níveis de acesso de colaboradores existentes devem ser feitas via aprovação do diretor de tecnologia – CTO ou outro diretor da SL Tools.

As contas de usuários (funcionários ou prestadores de serviço) são nomeadas e identificáveis e de uso exclusivo do funcionário/prestador de serviço. Dessa forma, todas as ações realizadas por esses usuários são de carácter irretratável e “não-repudiáveis”, o que permite a SL Tools identificar tais ações em caso de auditorias ou processos de investigação.

É proibida a utilização do mesmo nome de conta e senha utilizados no ambiente de produção nos ambientes não-produtivos (desenvolvimento e homologação), ou seja, as contas deverão ser criadas de forma individual para cada ambiente.

As contas inativas e/ou contas de funcionários que não fazem parte do quadro de colaboradores da SL Tools deverão ser desabilitadas/excluídas em todos os sistemas e equipamentos onde possam ter sido adicionadas durante vigência do contrato de trabalho, seja via processo manual ou automatizado.

O processo de revisão nos níveis de acesso dos funcionários e colaboradores da SL Tools deverá ser realizado com base semestral para usuários regulares e trimestral para usuários privilegiados, ou sempre que houver mudança de estrutura organizacional da Empresa.

13. ACESSO ÀS INFORMAÇÕES

O acesso às informações e aos ambientes tecnológicos da SL Tools é restrito às equipes de infraestrutura e segundo nível (responsáveis pela sustentação das aplicações em produção). Os acessos às informações críticas acessíveis nas plataformas são limitados apenas aos Diretores da SL Tools.

O telefone, o endereço de e-mail e demais ferramentas de comunicação corporativos disponibilizados aos Colaboradores são de propriedade da SL Tools e devem ser utilizados unicamente para atividades relacionadas ao trabalho a ser desempenhado.

14. POLÍTICAS DE SENHAS

A SL Tools implementará senhas de acesso a qualquer meio físico ou lógico por se tratar de um dos mais básicos e importantes mecanismos de segurança de suas informações. A fim de assegurar as melhores práticas relacionadas a este tema, seguem abaixo algumas diretrizes que devem ser observadas por todos os Colaboradores:

- A senha deve ser memorizada e de uso pessoal e intransferível, não devendo, portanto, ser compartilhada;
- O eventual uso ou acesso indevido é de total responsabilidade do detentor e titular da senha que deve tomar todos os cuidados necessários para salvaguardá-la;
- A senha de acesso aos sistemas internos deverá seguir os critérios definidos pela Direção da SL Tools;
- Toda e qualquer senha, de acesso físico ou lógico, deverá ser imediatamente bloqueada em casos de desligamento e/ou demissão;
- Especificamente com relação à senha de acesso aos softwares da SL Tools, os seguintes critérios deverão ser observados:

    a) Deve ter, no mínimo, 6 (seis) caracteres e atender, no mínimo, a 3 dos 4 grupos de caracteres abaixo citados:

        (i) Letras maiúsculas (de A a Z);
        (ii) Letras minúsculas (de a a z);

(iii) Algarismos (de 0 a 9); e
(iv) Caracteres não-alfabéticos (Ex. !, #, @, #, %).

b) Deverá ser alterada, compulsoriamente, a cada 45 (quarenta e cinco) dias;
c) Não pode ser igual ou similar às 3 (três) últimas utilizadas;
d) Não pode conter seu nome completo ou o de sua conta;
e) Em hipótese alguma será concedida senha de acesso a outro funcionário que não seja o próprio usuário; e
f) Ao receber a "nova" senha, o usuário deverá, obrigatoriamente, alterá-la no primeiro acesso seguindo os critérios acima citados.

15. SOLICITAÇÃO DE SENHA INICIAL E VALIDAÇÃO DE IDENTIDADE DE USUÁRIO

Para solicitação de acesso inicial ao sistema, o usuário deverá preencher um formulário eletrônico indicando o usuário *master* e seu respectivo endereço de e-mail e enviá-lo a SL Tools para que esse usuário *master* seja criado no sistema. O usuário *master* receberá um e-mail contendo seu *login* e outro e-mail contendo sua *senha* de acesso ao sistema, tendo obrigatoriamente que alterar sua senha no primeiro *logon* ao sistema.

O usuário *master* será responsável pela criação dos demais usuários de sua organização, os quais por sua vez receberão as informações para acesso ao sistema, *login* e senha, sendo um e-mail contendo somente o *login* e outro e-mail contendo somente sua tenha temporária, tendo também que alterar sua senha no primeiro *logon* ao sistema.

Para fins de validação de identidade do usuário, os e-mails contendo usuário e senha serão enviados apenas para endereços de e-mail corporativos, ou seja, e-mail pertencentes ao domínio da organização informado no formulário enviado para criação do usuário master.

16. USO DE INTERNET

O uso da internet pelos Colaboradores da SL Tools é permitido e encorajado desde que seu uso atenda os objetivos e atividades fins dos negócios da SL Tools. Acerca do uso de Internet, é estritamente proibido:

- visitar sites que contenham material obsceno;
- executar quaisquer tipos ou formas de fraudes;
- criar ou transmitir material difamatório;
- introduzir de qualquer forma um vírus de computador dentro da rede corporativa.

17. GERENCIAMENTO DE MÍDIAS REMOVÍVEIS

No que tange ao gerenciamento de mídias removíveis, os seguintes pontos serão observados pela SL Tools:

- mídias e recursos portáteis ou móveis devem ser controlados e registrados;
- informações confidenciais e críticas só são acessíveis via banco de dados ou por meio de sistemas da própria da SL Tools;
- o banco de dados da SL Tools possui proteções de acesso físico e lógico e não dispõe de acesso a mídias removíveis;
- o nível de acesso interno da SL Tools à plataforma é configurado para não permitir download de dados; e
- Nenhum dispositivo ou equipamento eletrônico para transmissão, armazenamento ou manuseio de dados, tais como: CD, DVD, máquina fotográfica, celular, HD portátil, *pen drive*, *tablet*, *memory card* ou similar deve ser conectado ou utilizado nas instalações da SL Tools sem análise e aprovação prévia da Diretoria.

18. UTILIZAÇÃO DE SOFTWARE E PROPRIEDADE INTELECTUAL

Utilização de Softwares. Toda instalação de programas e software em computadores da SL Tools deve ser feita pela área de TI e todos softwares e aplicativos devem ser homologados e licenciados. Verificada qualquer irregularidade em relação a instalação de softwares, estes poderão ser desinstalados pelo TI sem aviso prévio. A utilização de softwares não licenciados é considerada infração ao presente Manual e acarretará punições ao Colaborador, em qualquer nível da SL Tools.

Propriedade Intelectual. A Propriedade Intelectual da SL Tools é composta por bens imateriais, tais como: marcas, sinais distintivos, slogans publicitários, domínios, nomes empresariais, indicações gráficas, desenhos industriais, patentes de invenção e de modelo de utilidade, obras intelectuais, programas de computador e segredos empresariais (inclusive segredos de indústria e comércio) ("Propriedade Intelectual").

Nenhuma Propriedade Intelectual pertencente à SL Tools poderá ser repassada, alienada, transferida, cedida ou de qualquer outra forma utilizada para fins particulares dos Colaboradores, ainda que tenha sido obtida, inferida ou desenvolvida pelo próprio colaborador em seu ambiente de trabalho.

19. *HACKING* E VULNERABILIDADES

A SL Tools utiliza a infraestrutura de nuvem pública da AWS para opera sua plataforma de negociação. Para mitigar riscos de ataques cibernéticos, a SL Tools implementou um modelo de acesso

privado à sua infraestrutura na AWS. Esse modelo consiste na configuração de redes privadas (VPCs - Virtual Private Clouds), eliminando a exposição direta à internet.

Todo o acesso à infraestrutura da SL Tools na AWS é realizado por meio de uma conexão privada e dedicada entre a RTM (Rede de Telecomunicações para o Mercado Financeiro) e a AWS, sendo este o único ponto de entrada autorizado para acessos externos.

A RTM, amplamente adotada no mercado financeiro brasileiro, é responsável pela aplicação de medidas avançadas de segurança, como proteção contra ataques DoS, DDoS e synflood, utilizando os recursos de seu Centro de Operações de Segurança (SOC). Qualquer comportamento anômalo é monitorado, analisado e tratado pela equipe de segurança da RTM.

Além disso, a SL Tools utiliza a solução antivírus Microsoft 365 Defender para todos as estações de trabalho e servidores. A distribuição do antivírus, bem como de suas políticas é realizada através da ferramenta de gerenciamento Microsoft Intune para as estações de trabalho e instalada manualmente nos servidores. Os alertas de detecção de possíveis ameaças fica centralizado no painel de controle do próprio Microsoft 365 Defender no qual o time de infraestrutura e segurança pode verificar e tomar as ações necessárias.

20. DESCARTE DE INFORMAÇÕES

Toda informação que não necessite de sua manutenção em arquivos deve ser descartada através de máquinas fragmentadoras e/ou de modo que não seja possível sua reconstrução.

Informações de negociação geradas nas plataformas da SL Tools são convertidas em dados históricos e consequentemente armazenadas no banco de dados durante 10 (dez) anos ("Prazo de Armazenamento"), conforme já mencionado. Findo o Prazo de Armazenamento, os dados históricos deverão ser definitivamente apagados do banco de dados da SL Tools.

Referente equipamentos tais como servidores e laptops, quando atingirem sua vida útil ou forem descomissionados, os passos abaixo deverão ser seguidos:

i) servidores virtuais deverão ser destruídos ou apagados;
ii) laptops e equipamentos físicos deverão ser formatados e retornados ao seu estado original de fábrica, sem nenhuma informação ou identificação da SL Tools;

21. INCIDENTES DE SEGURANÇA

Em caso de ocorrência de um vazamento de informações ou qualquer outro incidente de segurança, o Colaborador deve registrar e comunicar o fato, para fins de acionamento do Plano de Resposta, conforme definido na Política de Cibersegurança da SL Tools disponível em: https://www.superliquidtools.com.br/governanca.

Uma vez detectado o incidente, deve-se analisar as informações e arquivos de logs recebidos sobre o assunto. Não obstante, deve-se analisar a abrangência, persistência e impacto do incidente, de forma que, antes de tomar qualquer medida faz se necessário analisar a dimensão do problema, o tempo de persistência e qual o impacto que tal incidente já causou ou eventualmente possa causar.

22. CONSIDERAÇÕES FINAIS

Atualização. Este Manual será revisado, no mínimo, anualmente, considerando a data de publicação mais recente (quadro "Histórico de Revisões" abaixo), podendo ser atualizado 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.

Abrangência. O presente Manual deve ser amplamente divulgado entre os Colaboradores SL Tools.

Confidencialidade. Todos os contratos que a SL Tools venha a celebrar em decorrência de prestação de serviços com parceiros, fornecedores e/ou qualquer outro tipo de contrato que de qualquer forma possibilite a outra parte a ter acesso à informações de cunho confidencial, devem conter cláusula específica de confidencialidade de todas as informações.

Comunicação Verbal. Os Colaboradores devem adotar cuidados especiais para evitar o comprometimento da segurança das informações quando da comunicação verbal. Nesse sentido, é vedo tratar sobre assuntos considerados confidenciais em locais onde estejam presentes pessoas não autorizadas. Adicionalmente, recomenda-se fortemente não gravar mensagens com conteúdo confidenciais em secretárias eletrônicas, caixas postais e afins, assim como não devem ser comunicadas por telefone.

Ciência. Todos os Colaboradores e sócios devem atestar a leitura por completo e perfeita compreensão deste Manual, assim como suas posteriores alterações.

Conformidade. O presente Manual está em conformidade com o disposto na Lei nº 13.709, de 14 de agosto de 2018, conforme alterada, e na Resolução nº 4.658, de 26 de abril de 2018 do

Banco Central do Brasil, levando-se em conta o porte, o perfil de risco e modelo de negócios da SL Tools, nos termos do Artigo 2º, §1º, Inciso 1º, da referida Resolução.

Em caso de dúvidas ou esclarecimentos sobre o conteúdo deste Manual ou sobre a aplicação do mesmo em relação a algum assunto específico, a direção da SL Tools deverá ser consultada.

O descumprimento de qualquer regra deste Manual será considerado falta grave e deverá ser objeto de análise da Diretoria.

Histórico de Revisões	**Observações**
Elaborado em 29 de agosto de 2018	
Atualizado em setembro de 2019	
Atualizado em maio de 2020	
Atualizado em agosto de 2020	
Atualizado em abril de 2021	
Atualizado em novembro de 2021	
Atualizado em agosto de 2022	
Atualizado em fevereiro 2024	Atualização de Texto – Não houve alterações relevantes em conceitos.
Atualizado em agosto 2024	Atualização de texto indicando melhorias nos processos de segurança da infraestrutura.