the source laboratory

Política de Segurança de Informação e Cibernética

Emitente	Vigência	Versão
Operações	**15/05/2020 a 15/05/2022**	**1.1**

Política de Segurança de Informação e Cibernética

Aos Colaboradores, Parceiros e Clientes:

Como fator crítico de sucesso, a SourceLab considera extremamente importante garantir a segurança das informações sob sua responsabilidade.

Desta forma, a SourceLab torna pública a sua POLÍTICA CORPORATIVA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA adequada aos princípios e valores da Companhia.

Este documento consiste em um conjunto de orientações que valorizam e definem o uso adequado das informações, possibilitando ambientes de TI seguros, confiáveis e íntegros.

O comprometimento de todos em conhecer e vivenciar esta política é de extrema importância para alcançarmos um padrão de excelência na gestão de segurança, proporcionando a evolução dos nossos negócios de forma cada vez mais transparente e segura.

1. Introdução

A adoção de políticas, normas e procedimentos que visem garantir a segurança da informação deve ser uma das prioridades do *Compliance*, reduzindo-se os riscos de falhas, danos e/ou prejuízos que possam comprometer a imagem e os objetivos da organização.

A informação pode existir e ser manipulada de diversas formas, ou seja, por meio de arquivos eletrônicos, mensagens eletrônicas, internet, bancos de dados, em meio impresso, verbalmente em mídias de áudio e de vídeo etc.

Por princípio, a segurança da informação deve abranger três aspectos básicos, destacados a seguir:

● **Confidencialidade:** somente pessoas devidamente autorizadas pela organização devem ter acesso à informação e as pessoas que tiverem acesso à informação devem tratá-la com dever de sigilo, cuidado e nos limites e para os fins a que teve acesso à informação;

● **Integridade**: somente alterações, supressões e adições autorizadas pela organização devem ser realizadas nas informações;

● **Disponibilidade**: a informação deve estar disponível para as pessoas autorizadas sempre que necessário ou demandado.

Para assegurar esses três itens mencionados, a informação deve ser adequadamente gerenciada e protegida contra roubo, fraude, espionagem, perda não intencional, acidentes e outras ameaças.

Em geral, o sucesso da Política de Segurança da Informação adotada pela SourceLab depende da combinação de diversos elementos, dentre eles, a estrutura organizacional da empresa, as normas e os procedimentos relacionados à segurança da informação e à maneira pela qual são implantados e monitorados, os sistemas tecnológicos utilizados, os mecanismos de controle desenvolvidos, assim como o comportamento de colaboradores, parceiros e sócios.

1.1 Eventos de Segurança

Todos os colaboradores e demais partes interessadas podem registrar a suspeita de um evento de fragilidade de segurança cibernética através do e-mail "escudo@sourcelab.com.br".

2. Classificação de Informação

Todos os colaboradores devem seguir as diretrizes e procedimentos de classificação e proteção das informações de propriedade da SourceLab, manipuladas e armazenadas no ambiente físico e lógico existente, a fim de preservar a integridade, confidencialidade e disponibilidade das informações.

2.1 Níveis de Classificação

As informações são classificadas nos seguintes níveis:

● **Público** - todo o conteúdo de todos os arquivos físicos e digitais classificados dessa forma podem ser acessados, estar e ser mantidos em posse de qualquer pessoa, sendo colaborador da SourceLab ou não. Informação públicas são identificadas da seguinte maneira:

- Toda informação física e digital coletada pela ou da Sourcelab, de forma proativa utilizando meios lícitos e que são comprovadamente de domínio público no momento da coleta;

- Toda informação física e digital enviada ou recebida pela SourceLab classificada pelo emissor como "Pública";

- Qualquer dado/informação recebida ou enviada que não exponha, comprometa ou cause qualquer dano material ou moral ao que diretamente ou indiretamente se faça referência;

● **Restrito** – todo o conteúdo de todos os arquivos físicos e digitais classificados dessa forma podem ser acessados apenas por colaboradores da SourceLab mediante acesso permissivo designado e monitorado, provido e gerido por sócios, diretores e administradores. Informação restritas são identificadas da seguinte maneira:

- Toda informação física e digital enviada ou recebida pela SourceLab que seja sensível de acordo com LGPD e que seu dono e emissor expresse claramente o consentimento de envio;

- Toda informação física e digital enviada ou recebida pela SourceLab em que se contenha premissas para tratativas comerciais, de precificação ou de prospecção;

- Toda informação física e digital enviada ou recebida pela SourceLab que defina o formato, a execução e a entrega de um dado projeto ou objeto de prestação de serviço;

- Toda informação física e digital enviada ou recebida pela SourceLab para ser consumida como base fundamental para o desenvolvimento de soluções de objeto de prestação de serviço (exceto dados de conexão e senhas)

- Toda informação física e digital enviada ou recebida pela SourceLab em que se contenha premissas para realização de entrevistas de emprego, dados relevantes para imprensa ou campanhas de marketing;

- Toda informação física e digital enviada ou recebida pela SourceLab que se refira, aborde ou contemple treinamentos gerais, direcionados e específicos;

- Toda informação física e digital enviada ou recebida pela SourceLab classificada pelo emissor como "Restrita";

● **Sigiloso** - todo o conteúdo de todos os arquivos físicos e digitais classificados dessa forma podem ser acessados exclusivamente por pessoas com credenciais especiais atribuídas, mediante acesso restritivo e expressa autorização que contemple segurança jurídica; Informação sigilosas são identificadas da seguinte maneira:

- Toda informação física e digital enviada ou recebida pela SourceLab em que se contenha referências diretas ou indiretas às tratativas jurídicas;

- Toda informação física e digital enviada ou recebida pela SourceLab em que se contenha referências diretas ou indiretas à dados de colaboradores que possam ser identificados e localizados sem devido consentimento;

- Toda informação física e digital enviada ou recebida pela SourceLab que exponha modelos de operação, estratégias de marketing, segredos de negócio, salários, volume de faturamento ou dimensão patrimonial;

- Toda informação física e digital enviada ou recebida pela SourceLab que exponha senhas para conexões remotas à serviços, APIs ou bancos de dados utilizados para o desenvolvimento de soluções de objeto de prestação de serviço;

- Toda informação física e digital enviada ou recebida pela SourceLab classificada pelo emissor como "Sigilosa";

3. Diretrizes

A seguir, são apresentadas as diretrizes da Política de Segurança da Informação da SourceLab. Tais diretrizes constituem os principais pilares da Gestão de Segurança da Informação da SourceLab, norteando a elaboração das normas e dos procedimentos.

3.1 Leis e Regulamentações

Cabe à área de Gestão de Engenharia e desenvolvimento:

● Manter as demais áreas da SourceLab informadas sobre eventuais alterações legais e/ou regulatórias que impliquem responsabilidade e/ou ações envolvendo a gestão de segurança da informação;

● Incluir, na análise e na elaboração de contratos, sempre que necessárias, cláusulas específicas relacionadas à segurança da informação e proteção de dados, com o objetivo de proteger os interesses da SourceLab e de seus clientes;

● Avaliar, quando solicitado, as Normas e os Procedimentos de Segurança da Informação elaborados pelas diversas áreas da SourceLab.

3.2 Identificação e Autenticação

Todas as plataformas de tecnologia e operações da SourceLab devem autenticar a identidade de usuários (incluindo outros sistemas que acessam estas plataformas) antes de iniciar uma sessão ou transação, a menos que o usuário tenha direitos de acesso limitados à leitura de dados.

Todo usuário deve possuir uma identidade e ser identificado para cada plataforma de tecnologia e operações por:

● Um ID (login) de usuário não compartilhado;

● Um método de autenticação que possibilite a identificação do usuário, por exemplo: senha única, chave privada, dados biométricos ou outro mecanismo de autenticação homologado e que atenda as melhores práticas de segurança;

● Cada usuário é responsável por toda atividade associada com o login de usuário associado à sua identidade ou sob sua custódia.

Os usuários devem seguir as seguintes práticas para proteção de senhas estáticas:

● As senhas devem ser pessoais e intransferíveis e é expressamente proibida a sua armazenagem lógica em qualquer tipo de formato.

● Nunca podem ser apresentadas/escritas fisicamente em clara compreensão.

4. Integridade

Os gestores devem informar a todos os colaboradores da SourceLab, bem como a clientes, fornecedores e usuários em geral que todas as informações armazenadas, transmitidas ou manuseadas nos sistemas e processos são de propriedade da SourceLab, de seus clientes ou licenciados por terceiros. Sempre que permitido pela legislação, a SourceLab reserva-se o direito de revisar e monitorar estas informações para fins administrativos, de segurança ou legais.

Informações confidenciais da SourceLab, independentemente da mídia ou ambiente onde estejam sendo mantidas, devem ser protegidas contra acessos não autorizados e com as devidas aprovações.

Para a proteção adequada das informações custodiadas pela SourceLab, que estão sendo manuseadas nas estações de trabalho, sempre que o colaborador se ausentar do ambiente, em particular fora do horário de trabalho, é sua responsabilidade bloquear a estação de trabalho, solicitar e utilizar os recursos disponibilizados pela SourceLab para proteger as informações de acessos não autorizados. Para a proteção adequada das informações custodiadas pela SourceLab,que estão sendo manuseadas em equipamentos portáteis (notebook), todos os usuários devem cumprir os requerimentos definidos por esta política de segurança da informação.

É importante e necessário que a Gestão de Engenharia e Desenvolvimento da SourceLab atue diretamente nos seguintes pontos:

● Monitorando a atividade de todos os colaboradores que armazenam, processam, gerenciam ou acessam as informações da SourceLab ou têm conexão com os recursos de rede da SourceLab, para que cumpram os padrões aqui definidos;

● Realizando avaliações de segurança da informação nos colaboradores de acordo com os procedimentos aprovados pelo Comitê Corporativo;

● Formalizando acordos de confidencialidade NDA – "Non Disclosure Agreement" ou disposições equivalentes, aprovados pela área jurídica da SourceLab, com os colaboradores que armazenem, processem, gerenciem ou acessem informações custodiadas pela SourceLab (exceto informação classificadas como PÚBLICA).

4.1 Adoção de Comportamento Seguro

Independentemente do meio ou da forma em que exista, a informação está presente no trabalho de todos os profissionais. Portanto, é fundamental para a proteção e salvaguarda das informações que os profissionais adotem comportamento seguro e consistente com o objetivo de proteção das informações da SourceLab, com destaque para os seguintes itens:

● Sócios, colaboradores e prestadores de serviços devem assumir atitude proativa e engajada no que diz respeito à proteção das informações da SourceLab;

● Todos na SourceLab devem compreender as ameaças externas que podem afetar a segurança das informações da empresa, tais como vírus de computador, interceptação de mensagens eletrônicas, grampos telefônicos etc., bem como fraudes destinadas a roubar senhas de acesso aos sistemas de informação;

● Todo tipo de acesso à informação da SourceLab que não for explicitamente autorizado é proibido;

● As senhas de usuário são pessoais e intransferíveis, não podendo ser compartilhadas, divulgadas a terceiros (inclusive colaboradores da própria empresa), anotadas em papel ou em sistema visível ou de acesso não-protegido;

● Somente softwares homologados pela equipe de TI e Infraestrutura da SourceLab podem ser instalados nas estações de trabalho, o que deve ser feito, com exclusividade, pela equipe de Tecnologia e Operações da SourceLab, respeitando as questões legais de licenciamento;

● A política para uso de internet e correio eletrônico deve ser rigorosamente seguida;

● Arquivos de origem desconhecida nunca devem ser abertos e/ou executados;

● Documentos impressos e arquivos contendo informações confidenciais devem ser

adequadamente armazenados e protegidos;

● Qualquer tipo de dúvida sobre a Política de Segurança da Informação e suas Normas deve ser imediatamente esclarecida com a Gestão de Engenharia e Desenvolvimento da SourceLab;

4.2 Avaliação dos Riscos de Segurança da Informação

A Gestão de Engenharia e Desenvolvimento da SourceLab deve realizar, de forma sistemática, a avaliação dos riscos relacionados à segurança da informação da SourceLab.

A análise dos riscos deve atuar como ferramenta de orientação sobre a segurança da Informação, principalmente, no que diz respeito a:

● Identificação dos principais riscos aos quais as informações da SourceLab estão expostas;

● Priorização das ações voltadas à mitigação dos riscos apontados, tais como implantação de novos controles, criação de novas regras e procedimentos, reformulação de sistemas etc. O

escopo da análise/avaliação de riscos de segurança da informação pode ser toda a organização, partes da organização, um sistema de informação específico, componentes de um sistema específico etc.;

● O Planejamento trimestral de identificação e análise dos riscos, podendo ser alterado o ciclo de análise conforme definido pelo Comitê de Segurança da Informação;

● Implantação de ferramentas para identificação de riscos e compliance.

5. Monitoramento e Controle

Os equipamentos, os sistemas, as informações e os serviços utilizados pelos usuários são de exclusiva propriedade da SourceLab, não podendo ser interpretados como de uso pessoal. Todos os profissionais da SourceLab devem ter ciência de que o uso das informações e dos sistemas de informação da SourceLab pode ser monitorado, e que os registros assim obtidos poderão ser utilizados para detecção de violações da Política, as Normas e Procedimentos de Segurança da Informação e, conforme o caso, servir como evidência em processos administrativos e/ou legais.

5.1 Treinamento e Conscientização de Segurança da Informação

Cada gestor deve garantir que todos os colaboradores e fornecedores, ao iniciar a relação com a SourceLab ou quando tiverem alteração significativa na responsabilidade do trabalho, estejam cientes sobre aspectos de segurança da informação relacionados a sua função em até 5 (cinco) dias do início de seu relacionamento com a SourceLab.

5.2 Procedimentos de Desenvolvimento Seguro

A SourceLab utiliza um conjunto de princípios para projetar sistemas seguros, garantindo que a segurança cibernética seja projetada e implementada no ciclo de vida de desenvolvimento dos sistemas, levando a privacidade em consideração desde a sua concepção.

5.3 Descarte de Informações Sensíveis

Não atuamos com dados disponíveis em mídias físicas (ex.: pen drive, cds, dvds). Todos os dados de clientes são transferidos e trafegados entre servidores privados e serviços de nuvem, utilizando canais privados (ex.: VPN) para consulta e armazenamento.

5.4 Segurança em Recursos Humanos e Acessos

A SourceLab mantém controles de Segurança nos processos de recursos humanos nos momentos de seleção, contratação, mudança de função e encerramento do contrato de trabalho. Todas as nossas senhas são centralizadas e gerenciadas através de uma ferramenta de geração e gerenciamento de logins e senhas. Apenas os usuários do domínio sourcelab.com.br podem ter acesso.

Os acessos ao ambiente de cloud também são controlados através de permissões temporárias e específicas aos serviços e conjuntos de dados necessários.

5.5 Controles de Auditoria e Acessos

Em adição às políticas de controle de acessos e de usuários, atualmente utilizamos também logs de monitoramento e acessos às ferramentas utilizadas em cloud, por todos os usuários SourceLab. Esse tipo de solução permite a rastreabilidade das ações de usuários e geração de relatórios.

6. Revisão do documento

Este documento será revisto e atualizado a cada dois anos ou quando:

- Houver solicitação de atendimento, correção ou adição de informações;
- Existir a necessidade de atender requisitos legais, boas práticas ou recomendações de auditoria;
- Existir mudança na organização que tenha impacto relevante na atividade abordada neste documento.

São Paulo, 15 de maio de 2020

Marino Boscolo
Sócio Fundador CTO/CPO

Cristiane Bissiguini
Sócio Controlador