1. SEGURANÇA DA INFORMAÇÃO

A informação é um ativo essencial para o desenvolvimento dos negócios e da **SOLAS** e, consequentemente, necessita ser adequadamente protegida em suas diversas formas, quais sejam, o formato físico, eletrônico e verbal. A segurança da informação visa à preservação da confidencialidade, integridade, disponibilidade, autenticidade e o não repúdio da informação, bem como a sua proteção dos vários tipos de ameaças e vulnerabilidades para garantir a continuidade do negócio em situações adversas.

2. DEFINIÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

A Política de Segurança da Informação e Privacidade (PSIP) define o conjunto de normas, métodos, instruções e procedimentos utilizados na proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. A Política de Segurança da Informação e Privacidade deve ser formalizada e divulgada a todos os usuários que fazem uso dos ativos de informação da **Solas**.

3. OBJETIVO

A Política de Segurança da Informação e Privacidade (PSIP) visa à: (i) proteção da **Solas** das ameaças internas e externas; (ii) promoção da gestão do risco com vistas a mitigá-lo; (iii) padronização das ações para o uso consciente, correto e seguro das informações em si e dos recursos de processamento que lhe dão suporte; (iv) garantir que a **Solas** atenda à legislação vigente; (v) assegurar a disponibilidade, integridade, confidencialidade e a autenticidade da informação necessária para a realização do negócio; (vi) a estabelecer os processos para permitir a rastreabilidade da informação para fins judiciais e de auditoria; (vii) definição dos procedimentos para que as informações geradas no ambiente eletrônico sejam corretamente armazenadas e a forma como elas serão coletadas para que possam atender aos requisitos legais; (viii) assegurar a proteção dos dados pessoais em qualquer operação realizada pela **Solas** e seus agentes e (ix) garantir a privacidade dos titulares dos dados pessoais.

4. DOCUMENTOS DE REFERÊNCIA

- Contrato Social;
- Contrato de Constituição da Empresa;
- Código de Ética;

- Regulamento Interno;
- Contrato de Trabalho;
- Demais Políticas e normas internas;
- Termo de Privacidade

5. PROCEDIMENTOS

5.1 DA GESTÃO DE RISCOS

A gestão de riscos é um importante instrumento de apoio para garantir que os eventos identificados com potencial impacto negativo sob a atividade ou processos sejam tratados de forma apropriada e em prazo estabelecido pela **Solas** de modo a não prejudicar que os objetivos ou metas institucionais sejam alcançados. Portanto, a gestão de risco deve ser aplicada a toda estrutura da **Solas**.

5.2 DO CONTEÚDO, NORMAS E INSTRUÇÕES

Por meio da análise e avaliação de risco será possível selecionar e implementar as opções de segurança personalizados, doravante denominados de "Controles", para tratamento dos riscos.
A Política de Segurança da Informação e Privacidade (PSIP) conterá as orientações básicas que indicam o que se quer. As Normas conterão as regras básicas de como deve ser implementado o controle (ou conjunto de controles) que foi definido na PSIP. As instruções conterão a descrição de maneira detalhada como será realizada uma atividade, implantando um controle.

5.3 DO CICLO DE VIDA

A política será formalmente aprovada pela alta administração da **Solas**, publicada e todos os usuários internos e externos serão comunicados sobre os requisitos de segurança da informação, por meio de um programa de capacitação. Ao final da capacitação, todos os usuários receberão um certificado de participação.
Além disso, a manutenção, análise crítica e melhoria da política, normas e instruções deve ser um processo contínuo, haja vista o surgimento quase que diário de novas ameaças e vulnerabilidades, necessidades contratuais e obrigações e responsabilidades decorrentes de leis.

5.4 DA REVISÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

A política deve ser analisada criticamente a intervalos planejados ou quando mudanças significativas ocorrerem para assegurar a sua contínua pertinência, adequação e eficácia

5.5 ABRANGÊNCIA

A Política de Segurança da Informação e Privacidade aplica-se à alta direção, empregados independentes do cargo, estagiários, aprendizes, prestadores de serviços, fornecedores, tanto internos quanto externos e terceiros que utilizem os recursos de processamento das informações da **Solas;**

5.6 ATRIBUIÇÃO DE RESPONSABILIDADES

Atividade		Responsável
Deliberar sobre assuntos relacionados à Política de Segurança da Informação		Comitê de Segurança da Informação
Cumprimento dos itens desta política.		Todos que se relacionam com a **Solas**, direta ou indiretamente, desde colaboradores e associados, até terceiros, podendo ser Contratantes na Compra de Equipamentos e Serviços, subcontratados e prestadores de serviços
Incidentes	Dados Pessoais	Comunicação imediata ao encarregado pelo tratamento de dados pessoais (*Data Protection Officer* – DPO) que acionará o Comitê de Segurança da Informação e Respostas a Incidentes e ao Gestor da área onde ocorreu o incidente.
	Informações	Gestor de Segurança da Informação e Resposta a Incidentes que acionará o Comitê de Segurança da Informação e Respostas a Incidentes e ao Gestor da área onde ocorreu o incidente.
Plano de contingência e a continuidade dos principais sistemas e serviços.		Comitê de Segurança da Informação e Respostas a Incidentes, os quais deverão ser testados, no mínimo, anualmente.
Análise de riscos.		Comitê de Segurança da Informação e Respostas a Incidentes, os quais deverão ser testados, no mínimo, anualmente.

Controles apropriados, trilhas de auditoria ou registros de atividades	Comitê de Segurança da Informação e Respostas a Incidentes e o Gestor de área de TI.
Uso correto e responsável dos recursos de TI	Todos os usuários da **Solas**, inclusive externos, associados, parceiros, clientes e prestadores de serviço, que utilizam esses recursos e a infraestrutura disponível

5.6.2 RESPONSABILIDADES ESPECÍFICAS

a) Comitê de segurança da informação e respostas a incidentes (CSIRI): é formado, por um membro representante das áreas Jurídica, Recursos Humanos, Tecnologia da Informação e Marketing e tem como atribuições, sem prejuízo de outras especificadas nas normas e instruções, conforme especificado no *Regimento Interno do Comitê de Segurança da Informação e Resposta a Incidentes*.

b) Gestores das áreas: Para garantir o alinhamento da segurança da informação ao negócio da empresa é preciso estruturar o sistema a partir das principais áreas de negócio considerando o organograma. As áreas irão formar a estrutura organizacional sob a qual os riscos de segurança serão gerenciados. Cada área deve possuir um responsável. Este responsável deve ser o diretor, gerente ou coordenador da área em questão. Isto auxilia na comunicação adequada dos riscos e na responsabilização gerencial sobre a segurança de cada área. O gestor poderá designar uma pessoa de sua confiança para executar as ações abaixo listadas; entretanto, a pessoa designada pelo gestor não terá poder de decisão. O gestor de área deve, sem prejuízo de outras atribuições especificadas nas normas e instruções:

• Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob sua gestão;

• Gerenciar o cumprimento da PSIP, normas e instruções por parte dos usuários que lhe são subordinados;

• Receber documentos e qualquer comunicação relativos à segurança da informação dos usuários de sua área;

• Identificar as ameaças significativas e a exposição da informação na sua área;

• Promover a conscientização pela segurança da informação na sua área;

• Monitorar os controles de segurança da informação e realizar uma análise crítica dos incidentes de segurança da informação na sua área;

• Reportar qualquer sugestão para melhoria e/ou correção à PSIP ao GSIRI;

• Reportar ao Gestor de Segurança da Informação e Respostas a Incidentes ameaças e/ou violações a PSIP que tomar conhecimento;

• Solicitar o auxílio do GSIRI quando necessário;

• Dar ciência, na fase de contratação e formalização dos contratos individuais de trabalho, à responsabilidade do cumprimento dessa Política e demais normas internas;

• Cumprir e fazer cumprir esta PSPI;

• Exigir de parceiros, prestadores de serviços e outras entidades externas, a assinatura de, no mínimo, o termo de confidencialidade referente às informações às quais terão acesso, caso não haja previsão contratual nesse sentido;

• Elaborar, com o apoio GSIRI, os procedimentos de segurança da informação relacionados às suas áreas, fornecendo as informações necessárias e mantendo-os atualizados;

• Informar, sempre que necessário, atualizações referentes a processos e/ou cadastros de colaboradores para que as permissões possam ser concedidas ou revogadas de acordo com a necessidade;

• Tomar as decisões administrativas referentes aos descumprimentos dessa PSIP

Caso o gestor verifique a possibilidade do envolvimento do Gestor de Segurança da Informação e Respostas a Incidentes em um evento de segurança da informação de qualquer natureza na sua área, deverá reportá-lo para qualquer membro do Comitê de Segurança da Informação e Respostas a Incidentes. As mesmas medidas se aplicam no caso de envolvimento da figura do Encarregado.

c) Gestor de Tecnologia da Informação (GTI): Além de outras atribuições definidas pela **Solas**, o gestor de TI deve estar alinhado com os objetivos e negócios da empresa e ao mesmo tempo deve estar preocupado com os aspectos técnicos para alcançar esses objetivos.

• Se comunicar com todos os usuários, seja com a equipe interna, composta pelo pessoal da própria área de TI e outros setores da empresa, como também com os agentes externos, sendo representados pelos *stakeholders* (as partes interessadas) e fornecedores;

• Se necessário, atuar em conjunto com o GSIRI para auxiliar o Gestor de Área na elaboração dos procedimentos de segurança da informação relacionados às suas áreas, fornecendo as informações necessárias e mantendo-os atualizados;

- Estar sempre alinhado com o GSIRI e o CSIRI, bem como lhes assegurar todo o suporte necessário para a execução dessa PSIP;
- Garantir que a informação e/ou recurso esteja acessível sempre que necessário, após a devida autorização para seu acesso e/ou uso;
- Preservar as informações com valor comprobatório para fins de auditorias legais e judiciais, na forma e pelo prazo correto;
- Administrar a infraestrutura física e lógica dos locais informatizados;
- Gerenciar os recursos humanos participantes das tecnologias da informação;
- Controlar os serviços de sistemas operacionais e de banco de dados;
- Estudar e buscar reduzir os impactos tanto sociais, quanto econômicos e ambientais das tecnologias da informação na **Solas**.
- Executar as ações e solicitações operacionais previstas nas normas e instruções;
- Propor melhorias, alterações e ajustes dessa Política;
- Propor investimentos relacionados à segurança da informação com o intuito de minimizar os riscos;
- Classificar e reclassificar o nível de acesso às informações sempre que necessário;
- Apoiar o CSIRI e/ou o GSIRI na avaliação de incidentes de segurança e propor ações corretivas;
- Apoiar o GSIRI na homologação dos equipamentos pessoais (smartphones e notebooks) para uso na rede da **Solas;**
- Apoiar o GSIRI no monitoramento dos acessos às informações e aos ativos de tecnologia como sistemas, bancos de dados, recursos de rede, entre outros, tendo como referência a Política e as Normas de Segurança da Informação;
- Manter registro e controle atualizados de todas as liberações de acesso concedidas, providenciando, sempre que demandado formalmente, a pronta suspensão ou alteração de tais liberações;

- Propor as metodologias e processos referentes à segurança da informação, como, classificação da informação, avaliação de risco, análise de vulnerabilidades, entre outros;

- Promover, com o envolvimento do CSIRI e o área de RH, palestras de conscientização dos colaboradores em relação à importância da segurança da informação para o negócio da **Solas**.

d) Usuário: são todos os, sem limitação, empregados, estagiários, aprendizes, prestadores de serviços, fornecedores e terceirizados, partes externas que utilizam os recursos de processamento da informação da **Solas**. As atribuições dos usuários, sem prejuízo de outras especificadas nas normas e instruções, são:

- Ler, compreender e cumprir integralmente os termos da PSIP, bem como as demais normas e procedimentos de segurança aplicáveis;

- Participar obrigatoriamente de todos os treinamentos relativos à segurança da informação;

- Reportar ao gestor de sua área as melhorias e sugestões a PSIP, bem como efetuar a entrega de documentos;

- Comunicar ao gestor de sua área qualquer evento que viole esta Política ou coloque/possa vir a colocar em risco a segurança das informações ou dos recursos computacionais da **Solas**;

- Assinar o "Termo de Ciência e Concordância" no ato de recebimento da Política de Segurança da Informação e Privacidade da **Solas**, formalizando a conhecimento e o aceite integral das disposições estabelecidas no referido instrumento, bem como as demais normas e procedimentos de segurança, assumindo responsabilidade pelo seu cumprimento;

- Responder pela inobservância da Política de Segurança da Informação e Privacidade, normas e procedimentos de segurança, conforme definido no item sanções e punições;

- Buscar o GSIRI para esclarecimentos de dúvidas referentes à essa Política;

- Proteger as informações e dados pessoais contra acesso, divulgação, modificação ou destruição não autorizados pela **Solas**;

- Garantir que equipamentos e recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pela **Solas**;
- Efetuar o descarte adequado de documentos, independente do suporte e sua natureza, de acordo com seu grau de classificação;
- Comunicar prontamente ao seu gestor de área imediato qualquer violação a esta política, suas normas e procedimentos.

Caso o usuário verifique a possibilidade do envolvimento do gestor da sua área em um evento de segurança da informação de qualquer natureza, deverá reportá-lo para o Gestor de Segurança da Informação e Respostas a Incidentes. No caso de existir indícios de envolvimento do CSIRI em conjunto com o gestor em um evento de segurança da informação de qualquer natureza, o usuário deverá reportá-lo para a direção que tomará

as medidas necessárias, inclusive por meio da contratação de consultoria externa para apurar o evento. As mesmas medidas se aplicam no caso de envolvimento da figura do Encarregado.

e) Dos Colaboradores em Regime de Exceção (Temporários): Devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto no aceite concedido pelo Comitê de Segurança da Informação e Respostas a Incidentes. O acesso a estes colaboradores se dá por meio da abertura de um chamado no "Fluxo de Trabalho no Tools" para o departamento "GRH" Selecionando a opção "Outros", inserindo no campo Descrição: "Liberação de Acesso", onde o gestor de área para quem esse colaborador responderá deverá informar o que deve ser liberado, de forma que fique tudo registrado/documentado, sendo o mesmo procedimento para um simples acesso a relatório até criação completa de um usuário no, sistema, e-mail, internet, pastas, servidor, dentre outros.

5.7 COMUNICAÇÃO DOS ATOS:

A concessão poderá ser revogada a qualquer tempo se for verificado que a justificativa de motivo de negócio não mais compensa o risco relacionado ao regime de exceção ou se o colaborador que o recebeu não estiver cumprindo as condições definidas no aceite.

A comunicação dos atos previstos nesta PSIP deve ser realizada de modo expresso e inequívoco e pode ser utilizado o meio eletrônico ou físico. A **Solas** adotará, preferencialmente, o meio eletrônico na comunicação dos atos. Cabe ao destinatário respeitar a escolha da **Solas** e utilizar o meio eleito para responder a mensagem. Ou seja, se a comunicação for feita por correio eletrônico, assim deverá ser a resposta.

Os seguintes canais deverão ser utilizados pelos usuários:

a) E-mail LGPD: lgpd@solasrepresentacoes.com.br

Para a comunicação de eventos relacionados a Dados Pessoais, os usuários deverão utilizar os seguintes canais, conforme definido na norma X32:

b) E-mail LGPD: lgpd@solasrepresentacoes.com.br

5.8 CONTROLES:

Controle	Diretrizes Globais	Norma
SEGREGAÇÃO DE FUNÇÃO	Definir a forma como a **Solas** a efetuará a separação das atribuições e responsabilidades; principalmente em processos decisórios.	1
CONTATO COM AUTORIDADES	Estabelecer os procedimentos para entrar em contato com as autoridades (Ex.: concessionárias de energia, autoridade policial) relevantes que apoiarão a gestão da segurança da informação.	2
CONTATO COM GRUPOS ESPECIAIS	Definir como o contato com grupos especiais, associações profissionais e fóruns especializados em segurança da informação deve ser realizado.	3
SEGURANÇA DA INFORMAÇÃO NO GERENCIAMENTO DE PROJETOS	Estabelecer os requisitos necessários para garantir a proteção das informações e dados pessoais durante a execução de um projeto	4
DISPOSITIVOS MÓVEIS	Estabelecer os procedimentos para o uso seguro de dispositivos móveis pelos usuários da **Solas**	5
TRABALHO REMOTO	Estabelecer os requisitos para garantir a proteção das informações da **Solas** e dados pessoais pelo usuário que executará suas atividades na modalidade de trabalho remoto.	6
SEGURANÇA EM RECURSOS HUMANOS	Definir a forma como as informações e dados pessoais serão protegidas desde a contratação do usuário até o término do seu contrato com a **Solas** os procedimentos para o caso de descumprimento de qualquer uma das diretrizes da **Solas**.	7

GESTÃO DE ATIVOS	Estabelecer as regras para identificar e inventariar os ativos da **Solas**.	8
CLASSIFICAÇÃO DA INFORMAÇÃO	Definir as regras para classificar a informação da **Solas** e dados pessoais.	9
RÓTULOS E TRATAMENTO DA INFORMAÇÃO	Estabelecer como a informação e dados pessoais será rotulada e receber o tratamento de acordo com sua classificação.	10
CONTROLE DE ACESSOS	Estabelecer as regras para liberar o acesso à equipamentos e aplicações da Solas.	11
CONTROLE CRIPTOGRÁFICO	Definir como a **Solas** utilizará a criptografia para proteger a informação e os dados pessoais	12
SEGURANÇA FÍSICA E DO AMBIENTE	Definir as regras de acesso dos usuários às dependências da **Solas** e das instalações que abrigam seus equipamentos.	13
LOCALIZAÇÃO E PROTEÇÃO DOS EQUIPAMENTOS	Definir as regras para garantir a proteção dos equipamentos da **Solas**.	14
CONTRATAÇÃO, AQUISIÇÃO E MANUTENÇÃO DOS EQUIPAMENTOS	Estabelecer as regras para efetuar a contratação de serviços, bem como para a aquisição de equipamentos e a respectiva manutenção.	15
REUTILIZAÇÃO E DESCARTE SEGURO DE EQUIPAMENTOS E DOCUMENTOS	Estabelecer as regras para a reutilização e o descarte seguro dos equipamentos e documentos.	16
EQUIPAMENTO E INFORMAÇÃO SEM SUPERVISÃO	Definir as regras para o momento no qual os equipamentos, a informação e/ou dados pessoais ficarão sem a supervisão do seu respectivo usuário	17
PROTEÇÃO CONTRA AMEAÇAS	Definir as regras para o uso de software e hardware para proteger a informação, dados pessoais e os equipamentos da **Solas** contra as ameaças.	18
CÓPIAS DE SEGURANÇA	Determinar os procedimentos para a **Solas** realizar a cópia de suas informações e dados pessoais com o objetivo de garantir a sua proteção.	19
REGISTROS E MONITORAMENTO	Estabelecer as regras para que os registros (*logs*) gerados durante, mas não se limitando, o uso dos equipamentos, informações e dados pessoais sejam produzidos, documentados e devidamente protegidos.	20

CONTROLE DE INSTALAÇÃO DE SOFTWARE EM SISTEMA OPERACIONAL	Definir as regras para a instalação segura de *softwares* nos sistemas operacionais.	21
SEGURANÇA NAS COMUNICAÇÕES	Estabelecer os procedimentos para garantir a proteção das redes utilizadas pela **Solas** na comunicação	22
TRANSFERÊNCIA DA INFORMAÇÃO	Definir como os usurários irão transferir as informações da **Solas** e dados pessoais por meio, sem limitação, da internet, intranet, extranet, ou ferramentas de envio de mensagens eletrônicas (Ex.: E-mail, WhatsApp).	23
GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO	Definir os procedimentos de como os usuários responderão a um incidente na **Solas.**	24
CONTINUIDADE DA SEGURANÇA DA INFORMAÇÃO	Estabelecer os procedimentos a serem tomados para manter a **Solas** em atividade na ocorrência de um incidente.	25
REDUNDÂNCIA	Estabelecer as regras para garantir a redundância dos equipamentos e/ou utilidades como luz, internet, com o objetivo de atender ao requisito de disponibilidade, mas não se limitando.	26
CONFORMIDADE COM REQUISITOS LEGAIS E CONTRATUAIS	Estabelecer os procedimentos para que a **Solas** siga os requisitos estabelecidos em contrato e a legislação vigente aplicável ao negócio.	27
ANÁLISE CRÍTICA DA SEGURANÇA DA INFORMAÇÃO	Definir os procedimentos para que a Política de Segurança da Informação e Privacidade seja monitorada constantemente, analisada criticamente e melhorada sempre que necessário.	28
TRATAMENTO DAS ALTERAÇÕES E EXCEÇÕES À POLÍTICA	Estabelecer os processos para que os usuários possam propor alterações, sugestões ou exceções à esta Política de Segurança da Informação e Privacidade.	29
PROTEÇÃO DE DADOS PESSOAIS	Estabelecer as diretrizes para assegurar a privacidade dos titulares e a proteção de seus dados pessoais.	30

5.9 DO DESCUMPRIMENTO DA PSIP:

As violações, mesmo que por mera omissão ou tentativa não consumada, desta política, bem como as demais normas e procedimentos de segurança, serão passíveis de penalidades que incluem advertência verbal, advertência por escrito, suspensão não remunerada e a demissão por justa causa.

A aplicação de sanções e punições será realizada conforme a análise do Comitê de segurança da informação e respostas a incidentes (CSIRI), devendo-se considerar a gravidade da infração, efeito alcançado, recorrência e as hipóteses previstas no artigo 482 da Consolidação das Leis do Trabalho, podendo o CSIRI, no uso de suas atribuições e do poder disciplinar que lhe é atribuído, aplicar a pena que entender cabível quando tipificada a falta grave.

No caso de terceiros contratados ou prestadores de serviço, o CSIRI deve analisar a ocorrência e deliberar sobre a efetivação das sanções e punições conforme termos previstos em contrato.

Para o caso de violações que impliquem em atividades ilegais, ou que possam incorrer em dano a **Solas**, o infrator será responsabilizado pelos prejuízos, cabendo aplicação das medidas judiciais pertinentes.

5.9.1 Da Quebra de Sigilo de Informação

O CSIRI poderá realizar a quebra de sigilo de informação quando solicitado por, mas não se limitando, Auditoria Interna, Comitê de Ética e por órgãos públicos, doravante simplesmente "órgãos", como, por exemplo, Ministério Público, Poder Judiciário, Autoridade Policial, Ministério do Trabalho e Autoridade Nacional de Proteção de Dados.

O solicitante deverá encaminhar o Formulário de Solicitação de Abertura de Informações, que se encontra disponível no Canal LGPD conforme especificado no item 5.7 item a, com a descrição detalhada da informação que deseja ter acesso com a cópia do ato emitido pelo respectivo órgão e encaminhar para GSIRI que levará para deliberação do CSIRI. O formulário deverá observar o que segue:

Auditoria Interna: Autorização pelos Sócios da Empresa;
Comitê de Ética: Autorização Sócios da Empresa;
Órgão público: Autorização por meio de ofício e o responsável pelo recebimento deste, deve comunicar a Diretoria/Superintendência e o GSI.

A quebra de sigilo de informação poderá ser realizada, mas não se limitando, sobre os seguintes recursos: E-mail, pasta corporativa, acessos à internet, ferramenta de comunicação (ex.: Skype for Business, Microsoft Teams), armazenamento em nuvem (ex.: One Drive) e Sistema Integrado **Solas**. O acesso será concedido apenas para a visualização do conteúdo, sendo proibido a alteração de qualquer natureza dos registros

5.10 CASOS OMISSOS:

Os casos omissos serão avaliados pelo Comitê de Segurança da Informação e Respostas a Incidentes para posterior deliberação.

As diretrizes estabelecidas nesta política e nas demais normas e procedimentos de segurança, não se esgotam em razão da contínua evolução tecnológica e constante surgimento de novas ameaças. Desta forma, não se constitui rol enumerativo, sendo obrigação do usuário da informação da **Solas**, adotar sempre que possível, outras medidas de segurança além das aqui previstas, com o objetivo de garantir proteção as informações da **Solas.**

5.11 DO PLANO DE AUDITORIA

A **Solas** se reserva ao direito de realizar auditorias, a qualquer momento, para verificar a conformidade das regras estabelecidas nesta política. **POLÍTICA DE SISTEMA** Nº: **SL-PS-CSI-001.**

5.12 VIGÊNCIA

Esta política terá a vigência de 12 (doze) meses e começa a vigorar na data de sua publicação;

5.13 REVISÕES:

Esta política será revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação

5.14 TERMOS E DEFINIÇÕES:

Para a correta compreensão desta Política de Segurança da Informação e Privacidade, serão considerados estes termos e definições:

Agentes de tratamento: o controlador e o operador.
Alta administração (AA): significa Sócio-Administrador.
Aplicação: ou software de aplicação, consiste em instruções que orientam um sistema de computação a realizar atividades especificas de processamento de informação e que

oferecem funcionalidades para os usuários; compreende as aplicações web e os programas de computador instalados nos equipamentos da **Solas**.

Área: considera-se qualquer estrutura física ou divisão organizacional existente na **Solas**: Também pode ser conceituado como setor ou área.

Ameaça: causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou para a **Solas**.

Antivírus: controle de detecção, prevenção e recuperação para proteção contra códigos maliciosos.

Add-Ons: são semelhantes a aplicativos. Porém, o seu uso está vinculado diretamente à execução de um outro software. Em outras palavras, os add-ons são aplicativos que são instalados ao lado de um programa já existente para aumentar as suas funcionalidades.

Ativo: qualquer coisa que tenha valor para a **Solas**.

Auditabilidade: o acesso e o uso da informação devem ser registrados, possibilitando a identificação de quem fez o acesso e o que foi feito com a informação;

Autenticidade: Consiste na garantia da veracidade da fonte das informações. Por meio da autenticação é possível confirmar a identidade da pessoa ou entidade que presta as informações.

Autoridade Nacional de Proteção de Dados (ANPD): órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

Banco de dados: conjunto estruturado de dados pessoais ou informações, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

Certificado digital: É um arquivo eletrônico que funciona como se fosse uma assinatura digital, com validade jurídica, e que garante proteção às transações eletrônicas e outros serviços via internet, de maneira que pessoas (físicas e jurídicas) se identifiquem e assinem digitalmente, de qualquer lugar do mundo, com mais segurança e agilidade.

Código Malicioso: termo genérico usado para se referir a programas desenvolvidos para executar ações danosas e atividades maliciosas em um computador ou dispositivo móvel. Tipos específicos de códigos maliciosos são sem limitação: vírus, *worm*, *boot*, *spyware*, *backdoor*, cavalo de tróia e *rootkit*.

Confidencialidade: garantia de que a informação é acessível somente por pessoas autorizadas.

Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

Controle: forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal.

Criptografia Forte: significa o uso de tecnologias de criptografia com comprimentos mínimos de chave de 256 bits para criptografia simétrica e 1024 bits para criptografia assimétrica cuja força fornece garantia razoável de que protegerá as informações criptografadas contra acesso não autorizado e é adequada para proteger a confidencialidade e privacidade das informações criptografadas, e que incorpora uma

política documentada para o gerenciamento das chaves de criptografia e processos associados adequada para proteger a confidencialidade e privacidade das chaves e senhas usadas como entradas para o algoritmo de criptografia.

Dado anonimizado: dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

Dados de Gravação de Chamadas: significam todos os dados que são gravados e/ou armazenados relacionados às chamadas de voz de interação de empregados e clientes da **Solas**, incluindo chamadas por meio de voip, espera, teleconferências, chamadas realizadas e recebidas.

Dado pessoal: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

Dado pessoal crítico: é o dado classificado como crítico pela **Solas** que em decorrência, mas não se limitando, do seu valor, importância e um nível alto de risco. Quando mencionado "dado pessoal" considera-se englobado o "dado pessoal crítico".

Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a **Solas** de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Diretriz: descrição que orienta o que deve ser feito e como, para se alcançarem os objetivos estabelecidos nas políticas.

Disponibilidade: garantia de que a informação estará disponível sempre que necessário.

Documento: unidade de registro de informações, independentemente do formato, do suporte ou da natureza.

Documento digital: informação registrada, codificada em dígitos binários, acessível e interpretável por meio de sistema computacional, podendo ser: a) documento nato-digital: documento criado originariamente em meio eletrônico; ou b) documento digitalizado: documento obtido a partir da conversão de um documento não digital, gerando uma fiel representação em código digital

Encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Equipamento: consideram-se todas as formas armazenamento e processamento da informação como, sem limitação, computadores (pessoais ou corporativos), telefones celulares, smartphones, *tablets*, *phablets*, pendrive, hd externo, servidores e outros equipamentos semelhantes utilizados dentro ou fora da **Solas**.

Evento de segurança da informação: ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da Política de Segurança da Informação e Privacidade ou falha nos controles, ou uma situação previamente desconhecida que possa ser relevante para a segurança da informação.

Extensões: são programas feitos para funcionar junto com o navegador para o qual elas são desenvolvidas. As extensões conseguem manipular o conteúdo em uma página e conectar-se a outros serviços para compartilhamento e acesso a dados úteis ao usuário.

Ao contrário de um plugin, extensões não impedem o acesso a um conteúdo: elas ampliam as funcionalidades de um navegador web.
Extranet: é o ambiente com o mesmo conteúdo da intranet, porém acessível pela internet.
Ferramenta de envio de mensagem eletrônica: considera-se a conta de email, *chat*, aplicativos de mensagens multiplataforma (*whatsapp*) e outras aplicações semelhantes utilizadas dentro ou fora da **Solas**.
Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.
Gateway de Segurança: significa um conjunto de mecanismos de controle entre duas ou mais redes com diferentes níveis de confiança que filtram e registram o tráfego que passa ou tenta passar entre redes e os servidores administrativos e de gerenciamento associados. Exemplos de Gateways de Segurança incluem firewalls, servidores de gerenciamento de firewall, caixas hop, controladores de borda de sessão, servidores proxy e dispositivos de prevenção de intrusões.
Incidente de segurança da informação: um incidente de segurança da informação é indicado por um simples ou por uma série de eventos de segurança da informação indesejados ou inesperados, que acarrete o comprometimento das operações do negócio e/ou ameace a segurança da informação.
Integridade: garantir que a informação não será alterada.
Internet: o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes.
Intranet: é um ambiente semelhante ao da internet, porém restrito ao recinto da **Solas**.
Legalidade: o uso da informação deve estar de acordo com as leis aplicáveis, regulamentos, normativas, licenças e contratos.
Log: o mesmo que registro.
Meio eletrônico: qualquer forma de armazenamento ou tráfego de documentos e arquivos digitais.
Mídia removível: suporte que permite o armazenamento e confere portabilidade das informações que carrega. Exemplos: pen drive, cd, hd externo.
Não repúdio: o usuário que gerou ou alterou a informação não pode negar o fato, pois existem mecanismos que garantem sua autoria.
Norma: regras básicas de como deve ser implementado o controle, ou o seu conjunto, que foi definido na política. As normas têm caráter tático, detalham situações, ambientes, processos específicos e fornecem orientação para o uso adequado das informações.
Nuvem Pública: série de serviços de computação oferecidos por terceiros, os quais são disponibilizados pela internet.
Nuvem Privada: serviços de computação em nuvem oferecidos pela Internet ou por uma rede interna privada somente a usuários selecionados e autorizados previamente e não ao público geral.
Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

Plugins: são programas instalados em um navegador ou página web que permitem a utilização de recursos que não estão disponíveis nativamente por meio do HTML. Esse é o caso, por exemplo, do Adobe Flash Player e do Java. Ambos são utilizados para a exibição de conteúdo multimídia e a execução de web apps.
Política: contém as diretrizes que devem ser seguidas. São orientações básicas que indicam o que se quer. Não definem a maneira como deve ser feita nem como deve ser a implantação.
Possuidores de dados: São responsáveis pela classificação da informação. Podem também ser responsabilizados pela exatidão e integridade das informações
Procedimentos: contém atividades que detalham como deve ser implantado o controle ou o seu conjunto. A característica deste documento é a descrição de maneira detalhada de como deve ser feita uma atividade.
Recursos: são os meios necessários para assegurar a disponibilidade da informação como, sem limitação, equipamentos, energia elétrica, internet.
Recurso(s) de Informações: significam sistemas, aplicativos, redes, elementos de rede e outros dispositivos de armazenamento de informações e computação, incluindo smartphones, tablets e pen drives USB.
Recursos de Informações Interno: significa os Recursos de Informações aos quais o acesso é restrito e não pode ser obtido sem a devida autorização e identificação.
Relatório de Impacto à Proteção de Dados Pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.
Sistema: ou software de sistema, é a classe de programas que controla e apoia um sistema de computação e suas atividades de processamento de informação. Ele também facilita a programação, o teste e a depuração dos programas de computador. Os programas de software de sistema apoiam o software de aplicação direcionando as funções básicas do computador. Por exemplo, quando o computador é ligado, o programa de inicialização (um software de sistema) prepara todos os dispositivos para o processamento O principal programa de controle do sistema é o sistema operacional, pois supervisiona a operação geral do computador.
Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.
Transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro.
Transmissão eletrônica: toda forma de comunicação a distância com a utilização de redes de comunicação, preferencialmente a rede mundial de computadores.
Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.
Usuário: compreende todas as pessoas, jurídicas e naturais, internas e externas, que irão utilizar os recursos de processamento da informação e/ou realização qualquer operação

com dados pessoais. Divide-se em usuário interno que são todas as pessoas que fazem parte da estrutura organizacional da **Solas**, como aprendizes, estagiários, colaboradores, diretores, presidentes e usuário externo que são, sem limitação, as partes externas, prestadores de serviço terceirizados, parceiros da **Solas**.

Uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais entre entes privados.

Utilidades: consideram-se, sem limitação, suprimento de energia elétrica, telecomunicações, suprimento de água, gás e esgoto, calefação/ventilação e ar-condicionado.

VPN: Do inglês Virtual Private Network, significa uma rede de comunicação privada, onde o usuário acessa o conteúdo da rede de maneira remota como se estivesse nas instalações da empresa.

Vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

"Zona Desmilitarizada" ou "DMZ": significa uma rede ou sub-rede que fica entre uma rede interna confiável, como uma rede local privada (LAN) corporativa e uma rede externa não confiável, como a Internet pública. Uma DMZ ajuda a impedir que usuários externos obtenham acesso direto aos Recursos de Informações internos.

Os canais de comunicação abaixo serão utilizados pelos usuários para encaminhar suas dúvidas quanto a PSIP, normas e/ou instruções para o Comitê de Segurança da Informação e Respostas a Incidentes:

E-mail: lgpd@solasrepresentacoes.com.br
Fone: (21) 3701-1960

Casos omissos e situações excepcionais devem ser discutidas e aprovadas em reunião específica.

5.15 DISPOSIÇÕES FINAIS:

5.16 DO COMPROMETIMENTO DA ALTA DIREÇÃO:

A alta direção da **Solas** está totalmente comprometida com a segurança da informação. Por esta razão, cumprirá fielmente todas as diretrizes previstas na Política de Segurança da Informação e Privacidade e exigirá que todos desempenhem suas responsabilidades com o mesmo rigor para proteger as informações da **Solas;**

6. RELAÇÃO DE ANEXOS

A alta direção da **Solas** está totalmente comprometida com a segurança da informação. Por esta razão, cumprirá fielmente todas as diretrizes previstas na Política de Segurança da Informação e Privacidade e exigirá que todos desempenhem suas responsabilidades com o mesmo rigor para proteger as informações da **Solas**.

6. RELAÇÃO DE ANEXOS

Anexo I – Termo de Ciência e Concordância:

https://www.solas.com.br/anexos/Anexo_I_-Termo_de_ciencia_e_concordancia.docx

7. ELABORADOR

Advoga Direito - Consultoria Jurídica e Empresarial

8. REVISORES

Cleide Souza – Analista Jurídico
Maurício Olivares – Gerente Comercial
Rafael Bonnard – Analista de Tecnologia da Informação
Lara Bravo S. Olivares – Consultoria de Marketing

9. RESPONSÁVEL

CSI – Comitê de Segurança da Informação