1. OBJETIVOS

Esta política tem como objetivo definir as diretrizes de segurança da informação e privacidade do SEEVISSP.

2. DOCUMENTO DE REFERÊNCIA

1.1. ABNT NBR ISO/IEC 27001
1.2. ABNT NBR ISO/IEC 27701
1.3. Lei n° 13.709/2018 – Lei Geral de Proteção de Dados Pessoais
1.4. Lei n° 12 965/2014 – Marco Civil da Internet

2. ABRANGÊNCIA

Abrange todas as unidades de negócios, colaboradores, terceiros, prestadores de serviços, parceiros e fornecedores do SEEVISSP.

3. PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para o SEEVISSP ou seus filiados. Ela pode estar guardada para uso restrito ou exposta ao filiado para consulta ou manuseio. Pode estar impressa ou escrita, pode ser falada, transmitidas por e-mails ou meios eletrônicos.

Independentemente da forma apresentada ou o meio pelo qual a informação é compartilhada ou armazenada, a informação é um dos principais ativos do SEEVISSP e de seus filiados, e, por isso, essencial ao negócio. Por esses motivos, deverá ser devidamente protegida e utilizada de modo ético e seguro, garantindo **confiabilidade** através da proteção da:

3.1. **CONFIDENCIALIDADE**: Garantir que a informação não seja revelada ou esteja disponível para indivíduos, entidades e processos não autorizados;

3.2. **INTEGRIDADE**: Garantir a salvaguarda da exatidão e totalidade da informação e dos métodos de processamento;

3.3. **DISPONIBILIDADE**: Garantir que a informação esteja sempre acessível e disponível quando necessário.

4. PRINCÍPIOS DA PRIVACIDADE DE DADOS PESSOAIS

O SEEVISSP dispõe na presente Política o compromisso de respeitar a segurança e privacidade de todos os titulares de dados pessoais, adotando medidas possíveis para assegurar de maneira razoável a proteção das informações coletadas, para o tratamento de acordo com as leis e regulamentações de privacidade e proteção de dados.

Para se assegurar ao tratamento de dados pessoais o SEEVISSP utiliza de procedimentos técnicos e organizacionais, como a constituição de Comitês de Gestor de Segurança da Informação e Privacidade, regular avaliação dos riscos e medidas de melhorias aos procedimentos de coleta, armazenamento e

tratamento dos dados pessoais, além dos rotineiros treinamentos para conscientização e desenvolvimento de sua equipe de colaboradores.

À luz das regras e normas da segurança da informação e privacidade, especialmente a Lei Geral de Proteção de Dados Pessoais ("LGPD"), Lei n. 13.709, de 14 de agosto de 2018, a presente Política dispõe sobre regras gerais de coleta, manutenção, exclusão e de outras formas de tratamento dos dados pessoais dos Usuários, relativos ao presente site, aplicativos e todos os demais banco de dados sob seu domínio.

5. DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO

Para endereçar todo o esforço e manutenção necessária para a Segurança da informação e privacidade, o SEEVISSP estabelece as seguintes diretrizes:

5.1. Uma estrutura de Gestão da Segurança da informação e privacidade deve ser estabelecida e mantida com apoio da Alta Administração, através de um Sistema de Gestão de Segurança da informação e privacidade (SGSIP);

5.2. Toda informação deve ser utilizada com senso de responsabilidade e de modo ético e seguro por todos, em benefício exclusivo dos negócios corporativos;

5.3. Todos os ativos de informação devem estar devidamente identificados, classificados e monitorados;

5.4. A identificação de cada colaborador do SEEVISSP é única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas;

5.5. Todos os riscos deverão ser analisados, classificados e apresentados a um comitê que deliberará sobre o tratamento adequado para tais;

5.6. Todos os incidentes de segurança devem ser reportados para a área de Segurança da informação e privacidade para que sejam analisados, avaliados e tratados;

5.7. O SEEVISSP identifica, segue, documenta e mantém atualizadas as leis relacionadas à segurança da informação e privacidade que regulamentam suas atividades, bem como dos aspectos de propriedade intelectual;

5.8. O SEEVISSP, através de sua alta administração deve definir os Objetivos Estratégicos de Segurança da informação e privacidade considerando esta política, os requisitos de Segurança da informação e privacidade aplicáveis e os resultados da Gestão de Riscos;

5.9. Todos os colaboradores, prestadores de serviços, parceiros e fornecedores que tenham acesso a informações do SEEVISSP, bem como de seus filiados e parceiros, devem aderir formalmente ao "Termo de Uso de Sistemas de Informação", comprometendo-se a respeitar esta política e as normas que a suportam de forma integral.

6. GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Para manter um nível satisfatório de segurança constitui-se o Comitê de Gestão de Segurança da Informação e Privacidade (CGSIP), que adota Políticas e Normas de Segurança para sustentar as diretrizes apresentadas:

6.1. O controle de acesso dos colaboradores, prestadores de serviços, parceiros e fornecedores aos ativos de informação deve ser devidamente aprovado pelo responsável pela informação (gestor, diretoria ou responsável conforme definido nos documentos da informação), a qual o acesso permitirá a manipulação, quer seja para simples consulta ou para alteração;

6.2. O uso do e-mail sob o domínio "@seevissp.org.br" será permitido apenas para colaboradores internos e externos, e para terceiros de acordo com o processo de contratação de terceiros, sendo a utilização do correio eletrônico regida por uma norma de segurança específica para esse propósito;

6.3. Cópias de segurança (backup) devem ser realizadas através de mídias específicas de informações, obrigatoriamente para as informações que são consideradas vitais para os sistemas do SEEVISSP e para a retomada das atividades da área em caso de contingência;

6.4. Regras para o desenvolvimento seguro de sistemas e software devem ser estabelecidas e aplicadas aos desenvolvimentos realizados dentro do SEEVISSP;

6.5. Concessão de acesso remoto para os colaboradores e prestadores de serviços deve ser previamente solicitada e autorizada pela área responsável;

6.6. Dispositivos móveis corporativos devem ser destinados ao uso em serviço para realização das atividades de trabalho dos colaboradores e para comunicação com o SEEVISSP, fornecedores ou filiados, devendo ser utilizado somente para essa finalidade;

6.7. As informações devem ser classificadas e manuseadas de acordo com os níveis de confidencialidade estabelecidos, respeitando as proteções necessárias, da seguinte forma: Pública, Interna e Confidencial, e devem ser tratadas, armazenadas e descartadas de maneira correta para garantir os aspectos de segurança da informação e privacidade no negócio do SEEVISSP e nas informações dos seus filiados;

6.8. Os ativos tangíveis e intangíveis de informação devem estar identificados de forma individual, inventariados, protegidos e monitorados de acessos indevidos. As mídias devem ser gerenciadas de forma adequada, conforme os requisitos de segurança da informação e privacidade;

6.9. Um conjunto de regras deve garantir a padronização das técnicas criptográficas, a aplicação adequada das mesmas e responsabilidades para manter a segurança no transporte ou armazenamento das informações, independentemente do meio utilizado. Quanto à transmissão de informações, esse recurso deve ser utilizado para garantir a segurança na comunicação dos dados do SEEVISSP e de seus filiados;

6.10. Um processo de gestão de mudanças deve ser aplicado para garantir que controles e modificações nos sistemas ou recursos de processamento da informação sejam realizados com planejamento, a fim de não ocasionar falhas operacionais ou de segurança no ambiente produtivo do SEEVISSP;

6.11. Para garantir a proteção das informações de maneira eficaz e reduzir os riscos de acesso físico não autorizado, perda ou dano à informação durante e fora do horário normal de trabalho, devem ser adotadas medidas (controles) de segurança;

6.12. Os riscos devem ser identificados por meio de um processo estabelecido para análise de vulnerabilidades, ameaças e impactos sobre os processos nos aspectos de segurança da informação (Confidencialidade, Integridade e Disponibilidade);

6.13. Todos os incidentes que afetem a segurança da informação e privacidade devem ser reportados à área de Segurança da informação e privacidade através do HelpDesk para a área de Segurança da informação e privacidade, que analisará o incidente e tomará as ações devidas, repassando a tratativa às áreas responsáveis;

6.14. As responsabilidades de Segurança da informação e privacidade e restrições do uso de ativos no SEEVISSP devem ser definidas;

6.15. Deve-se garantir a melhoria contínua do Sistema de Gestão da Segurança da informação e privacidade (SGSIP), com base na norma ISO/IEC 27001:2013, contendo todos os indicadores e métricas para monitorar-se o ciclo PDCA;

6.16. Deve-se definir regras para garantir que não ocorram violações jurídicas, regulamentares ou contratuais nos requisitos de segurança da informação e privacidade no SEEVISSP;

6.17. Para garantir que o acesso físico às instalações onde os ativos de TI e informações críticas à continuidade do negócio estejam armazenados, o ambiente deve ser controlado de forma a garantir a sua proteção, disponibilidade, integridade e confidencialidade.

Quando por razões tecnológicas ou determinações superiores, tornarem impossível a aplicação dos requisitos previstos nesta política, o responsável e/ou solicitante deverá reportá-las imediatamente à área de Segurança da informação e privacidade para que possibilite a adoção de medidas alternativas que minimizem os riscos, bem como um plano de ação para corrigi-los, monitorá-los ou eliminá-los.

7. MONITORAMENTO E AUDITORIA

O SEEVISSP reserva-se ao direito de monitorar e registrar todo o uso das informações geradas, armazenadas ou veiculadas no SEEVISSP. Para tanto o SEEVISSP mantém controles apropriados e trilhas de auditoria ou registros de atividades em todos os pontos e sistemas que o SEEVISSP julgou necessário para reduzir os riscos, e reserva-se o direito de:

7.1. Implantar outros sistemas de monitoramento de acesso às estações de trabalho, servidores internos e externos, correios eletrônicos, navegação, internet, dispositivos móveis ou wireless e outros componentes da rede. A informação gerada por esses sistemas de monitoramento poderá ser usada para identificar usuários e respectivos acessos efetuados;

7.2. Inspecionar qualquer arquivo que esteja na rede, no disco local da estação de trabalho ou qualquer outro ambiente, visando assegurar o rígido cumprimento desta política;

7.3. Instalar outros sistemas de proteção e detecção de invasão para garantir a segurança das informações e dos perímetros de acesso.

8. DIREITOS DO TITULAR DE DADOS PESSOAIS

A LGPD assegura aos titulares de dados pessoais direitos e princípios a serem seguidos daqueles a quem está das informações cadastrais pessoais. Assim, o SEEVISSP é comprometido no cumprimento destes direitos e princípio, esclarecendo que:

DIREITO DO TITULAR	OBRIGAÇÃO DO CONTROLADOR
Confirmação da existência de tratamento	Confirmar a existência de tratamento caso haja;
Acesso aos dados	Disponibilizar o acesso aos dados pessoais existentes sob o seu domínio, quando solicitado pelos titulares;
Correção de dados pessoais	Proceder com a correção de dados pessoais incompletos, inexatos ou desatualizados, sob orientação do titular;
Anonimização, bloqueio e eliminação	Possibilitar aos titulares a: **(i)** anonimização dados pessoais, que implica na desvinculação das informações à sua pessoa; **(ii)** bloqueio dos dados pessoais existentes, como com a suspensão temporária no tratamento; e **(iii)** eliminação definitiva;
Portabilidade	Obrigação do controlador em atender pedido de transferência de dados pessoais à terceiros;
Compartilhamento	Apresentar quando for requisitada as informações e registros a respeito com quem o controlador compartilhou seus dados pessoais;
Possibilidade de não consentir	Ao titular dos dados é informado e esclarecido sobre a possibilidade de não dar consentimento ao tratamento dos seus dados pessoais, contudo nesses casos poderá haver consequências as quais serão alertado o titular;
Revogar seu consentimento	Em caso de haver o consentimento pelo titular, este poderá manifestar o desejo pela revogação das finalidades a que foram consentidas;
Autodeterminação informativa	O titular tem o direito de escolher quais de seus dados pessoais serão usados, bem como os limites e o prazo dessa utilização desses dados.

Caso o TITULAR opte por não fornecer o consentimento para quaisquer dados, ou então decida por optar (autodeterminação informativa) pelo tratamento dos seus dados pessoais em limites, prazos e tratamentos diversos dos almejados pelo SEEVISSP, alguns serviços e atividades poderão ser prejudicados e seu acesso poderá ser restrito.

Além disso é importante ressaltar que em alguns casos o SEEVISSP poderá fazer o uso de razões e justificativas legais, diversos do consentimento, para manter o tratamento dos dados pessoais, como por exemplo no caso em que possa resultar na violação de direitos do SEEVISSP ou de terceiros, bem como em casos em que o pedido de anonimização, bloqueio ou eliminação não serão viáveis em decorrência da obrigação do SEEVISSP de manter os dados, por razão da sua atividade e para possiblidade a defesa de direitos em disputas administravas ou judiciais de qualquer natureza. Contudo, se for o caso de algumas destas inviabilidades para atendimento da solicitação, haverá o esclarecimento pertinente, sempre se assegurando a privacidade e segurança aos dados sob seu domínio.

9. FINALIDADE DOS DADOS PESSOAIS TRATADOS E LOCAIS DE COLETA

Conforme “PSIP 001 - Anexo 01”

10. DURAÇÃO DO TRATAMENTO

Geralmente armazenamos seus dados pessoais pelo tempo necessário para a entrega de nossos produtos e serviços e para fins de segurança. Em alguns casos, serão armazenados por mais tempo, por exemplo, para

possiblidade a defesa de direitos em disputas administravas ou judiciais de qualquer natureza (art. 7º, inciso VI, LGPD) ou ainda quando se fizer necessário ao cumprimento de obrigações legais (art. 7º, inciso II da LGPD).

Se uma associação/conta for encerrada, o SEEVISSP manterá as informações da conta armazenadas, após a data de encerramento, por tempo determinado conforme legislação e bases legais aplicáveis, para as finalidades determinadas conforme o mapeamento de dados pessoais.

11. COMPARTILHAMENTO DOS DADOS PESSOAIS

O SEEVISSP atua em parceria com diversas organizações, tanto para viabilidade como para o desenvolvimento das atividades, no interesse de melhor atender e prestar serviços aos Usuários. Por estas razões, alguns dos dados pessoais poderão ser compartilhados com entidades públicas e privadas ou ainda com autoridades competentes.

Fornecedores e Parceiros: Há vários fornecedores e parceiros contratados em razão da nossa atividade e para fornecimento dos nossos produtos e serviços. Alguns podem solicitar e tratar parte os dados pessoais de nossos Usuários, a exemplo, instituições financeiras ou demais organizações que atual nos sistemas de pagamento, que licenciam o direito de uso de plataformas digitais, que prestam serviços de hospedagem de dados, entre outros. Importante salientar que em todos os casos avaliamos e regularmente fiscalizamos o comprometimento destes com a segurança e privacidade da informação, bem como a regularidade e atendimento das previsões da LGPD, julgando também se estão alinhados aos princípios e valores do SEEVISSP, sempre o interesse de preservar a privacidade e segurança, minimizando riscos à proteção de dados pessoais.

Autoridades Públicas: Nossa obrigação de cumprir os termos da lei impõe a sujeição de algumas obrigações legais e regulatórias em que há determinação ao fornecimento de dados pessoais à alguma Autoridade Pública. Tanto nos casos de ordem judicial ou de autoridades competentes que exigirem a apresentação dos dados pessoais, o SEEVISSP precisará atender a obrigação do compartilhamento, contudo, sempre avaliará se a ordem expedida seja abusiva ou excessiva, de modo que providenciará a defesa dos direitos à segurança e a privacidade dos dados sob nosso domínio.

Anúncios: O SEEVISSP poderá também compartilhar dados relacionados à sua interação com nossas plataformas digitais com anunciantes e outros parceiros comerciais em que possibilitará o direcionamento de publicidade. Todavia, esses anúncios estarão limitados aos interesses e perfis de nossos usuários e, sempre que tecnicamente viável, os dados serão anonimizados ou pseudonimizados.

12. MEDIDAS E REGRAS DE SEGURANÇA

Temos a responsabilidade de preservar e manter a segurança e privacidade dos dados pessoais dos Usuários e utilizá-los de acordo com as finalidades descritas nessa Política. Para garantir a sua privacidade e a proteção dos seus dados pessoais, adotamos os recursos técnicos para garantir a segurança de todos os dados tratados pelo SEEVISSP.

Nossos esforços são para garantir a proteção e privacidade dos dados pessoais dos Usuários, porém são impossíveis de serem atendidos sem a sua colaboração e atuação. Entrada de terceiros não autorizados com informações suas, falhas de hardware ou software e outros motivos que estejam fora do controle do SEEVISSP. Assim, solicitamos a sua atenção para manter ambiente seguro, sendo que se identificar qualquer caso ou situação que possa comprometer a segurança dos seus dados nos ambientes e bancos de dados do SEEVISSP, não hesite em nos contatar por meio dos canais de atendimentos disponibilizados abaixo.

13. CANAIS DE ATENDIMENTO / FALE CONOSCO:

Em caso de dúvidas, solicitações em relação à Lei Geral de Proteção de Dados (LGPD) ou sobre a nossa Política de Privacidade, entre em contato pelos canais oficiais de comunicação, gratuitamente, nos nossos pontos de atendimento (sede ou filiais).

Salientemos que para sua própria segurança, em alguns casos poderemos requisitar informações, além de outras informações ou documentos complementares para verificação e confirmação da identidade. O processo de verificação pode variar de acordo com a natureza da solicitação, medida necessária para impedir fraudes ou fornecimento de dados para partes não autorizadas.

14. CONTATO COM O ENCARREGADO DE PROTEÇÃO DE DADOS (DPO)

Dispomos também de Encarregado de Proteção de Dados, conforme previsão do artigo 41 da LGPD, sendo esse colaborador técnico preparado e responsável por questões exclusivamente relacionados à LGPD, o qual você poderá nos contatar pelo seguinte endereço:

e-Mail: dpo@seevissp.org.br

15. SANÇÕES E PUNIÇÕES

Para toda e qualquer infração à Política de Segurança da informação e privacidade e às demais Normas de Segurança da informação e privacidade que a suportam, deverá ser aberto um incidente de segurança da informação e privacidade, tratado de acordo com o processo de gestão de incidentes de segurança da informação e privacidade e informado ao CGSIP e, por conseguinte, apurada através de procedimentos internos, que devem ser conduzidos pelo responsável da área em que se encontra alocado o profissional que cometeu a infração, em conjunto com a área de Recursos Humanos e o departamento Jurídico do SEEVISSP.

Caso o Comitê Gestor de Segurança da informação e Privacidade (CGSIP) julgue cabível, o colaborador ou terceiro envolvido poderá, enquanto durar o processo de apuração interna, ter a recomendação de afastamento da função ou suspensão.

Ao colaborador ou terceiro suspeito de cometer violações à Política e/ou Normas de Segurança da informação e privacidade, deverá ser assegurado tratamento justo e correto, sendo que toda e qualquer medida resultante de sua infração deverá ser aplicada com proporcionalidade à ocorrência com base no Código de Ética e Conduta, Termo de Confidencialidade, Política e Normas de Segurança da informação e privacidade do SEEVISSP e legislações vigentes.

O SEEVISSP exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus colaboradores, terceiros, parceiros e fornecedores reservando-se o direito de punir os infratores, analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios e adotar as medidas legais cabíveis.

16. APROVAÇÃO DO DOCUMENTO

Nome do Aprovador	Assinatura	Data
Pedro Francisco Araújo		

Leandro Scorcio		
Luiz Claudio Souza		
Maurício Olaia		
Ricardo Becker		

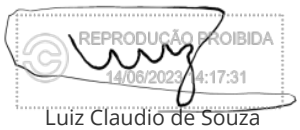
PSIP 001 - Política de Segurança da Informação e privacidade.docx

Documento número #4145790b-f13f-48b9-94ca-d35bf61afe43

Hash do documento original (SHA256): 37879852ad873bc9f8098afeab3523321043230923e75fe7c3aa2f57dfd63d2f

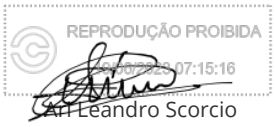
Assinaturas

Luiz Claudio de Souza
CPF: 272.523.388-78
Assinou em 14 jun 2023 às 14:17:31



Luiz Claudio de Souza

Ari Leandro Scorcio
CPF: 226.442.138-00
Assinou em 19 jun 2023 às 07:15:16

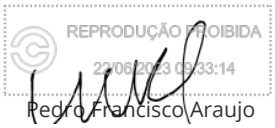


Ari Leandro Scorcio

Mauricio Olaia
CPF: 272.233.648-07
Assinou em 15 jun 2023 às 13:15:57

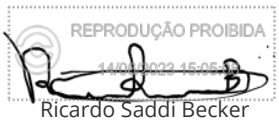
Mauricio Olaia

Pedro Francisco Araujo
CPF: 948.705.948-20
Assinou em 22 jun 2023 às 09:33:13



Pedro Francisco Araujo

Ricardo Saddi Becker
CPF: 914.056.371-53
Assinou em 14 jun 2023 às 15:05:08



Ricardo Saddi Becker

Log

14 jun 2023, 14:11:53	Operador com email pedro@fetravesp.org.br na Conta 5212964f-d413-4432-968a-70873d77deae criou este documento número 4145790b-f13f-48b9-94ca-d35bf61afe43. Data limite para assinatura do documento: 14 de julho de 2023 (14:09). Finalização automática após a última assinatura: habilitada. Idioma: Português brasileiro.

14 jun 2023, 14:11:57	Operador com email pedro@fetravesp.org.br na Conta 5212964f-d413-4432-968a-70873d77deae adicionou à Lista de Assinatura: lcsouza@datatech.com.br para assinar, via E-mail, com os pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP; Assinatura manuscrita. Dados informados pelo Operador para validação do signatário: nome completo Luiz Claudio de Souza.
14 jun 2023, 14:11:57	Operador com email pedro@fetravesp.org.br na Conta 5212964f-d413-4432-968a-70873d77deae adicionou à Lista de Assinatura: leandro@jundlaser.com.br para assinar, via E-mail, com os pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP; Assinatura manuscrita. Dados informados pelo Operador para validação do signatário: nome completo Ari Leandro Scorcio e CPF 226.442.138-00.
14 jun 2023, 14:11:57	Operador com email pedro@fetravesp.org.br na Conta 5212964f-d413-4432-968a-70873d77deae adicionou à Lista de Assinatura: mauricio@bipconsultoria.com.br para assinar, via E-mail, com os pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP; Assinatura manuscrita. Dados informados pelo Operador para validação do signatário: nome completo Mauricio Olaia e CPF 272.233.648-07.
14 jun 2023, 14:11:57	Operador com email pedro@fetravesp.org.br na Conta 5212964f-d413-4432-968a-70873d77deae adicionou à Lista de Assinatura: pedro@fetravesp.org.br para assinar, via E-mail, com os pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP; Assinatura manuscrita. Dados informados pelo Operador para validação do signatário: nome completo Pedro Francisco Araujo e CPF 948.705.948-20.
14 jun 2023, 14:11:57	Operador com email pedro@fetravesp.org.br na Conta 5212964f-d413-4432-968a-70873d77deae adicionou à Lista de Assinatura: ricardo@bipconsultoria.com.br para assinar, via E-mail, com os pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP; Assinatura manuscrita. Dados informados pelo Operador para validação do signatário: nome completo Ricardo Saddi Becker e CPF 914.056.371-53.
14 jun 2023, 14:17:32	Luiz Claudio de Souza assinou. Pontos de autenticação: Token via E-mail lcsouza@datatech.com.br. CPF informado: 272.523.388-78. Assinatura manuscrita com hash SHA256 prefixo cdaf2a(...), vide anexo 14 jun 2023, 14-17-31.png. IP: 191.183.116.71. Localização compartilhada pelo dispositivo eletrônico: latitude -23.396352 e longitude -46.7173376. URL para abrir a localização no mapa: https://app.clicksign.com/location. Componente de assinatura versão 1.513.0 disponibilizado em https://app.clicksign.com.
14 jun 2023, 15:05:09	Ricardo Saddi Becker assinou. Pontos de autenticação: Token via E-mail ricardo@bipconsultoria.com.br. CPF informado: 914.056.371-53. Assinatura manuscrita com hash SHA256 prefixo 3b4b4d(...), vide anexo 14 jun 2023, 15-05-08.png. IP: 201.68.240.158. Componente de assinatura versão 1.513.0 disponibilizado em https://app.clicksign.com.
15 jun 2023, 13:15:58	Mauricio Olaia assinou. Pontos de autenticação: Token via E-mail mauricio@bipconsultoria.com.br. CPF informado: 272.233.648-07. Assinatura manuscrita com hash SHA256 prefixo 7a32c1(...), vide anexo 15 jun 2023, 13-15-57.png. IP: 179.225.193.45. Componente de assinatura versão 1.515.0 disponibilizado em https://app.clicksign.com.
19 jun 2023, 07:15:16	Ari Leandro Scorcio assinou. Pontos de autenticação: Token via E-mail leandro@jundlaser.com.br. CPF informado: 226.442.138-00. Assinatura manuscrita com hash SHA256 prefixo 07713b(...), vide anexo 19 jun 2023, 07-15-16.png. IP: 187.90.220.84. Localização compartilhada pelo dispositivo eletrônico: latitude -23.165112532983912 e longitude -46.87441279185999. URL para abrir a localização no mapa: https://app.clicksign.com/location. Componente de assinatura versão 1.516.0 disponibilizado em https://app.clicksign.com.

22 jun 2023, 09:33:15	Pedro Francisco Araujo assinou. Pontos de autenticação: Token via E-mail pedro@fetravesp.org.br. CPF informado: 948.705.948-20. Assinatura manuscrita com hash SHA256 prefixo af09ba(...), vide anexo 22 jun 2023, 09-33-14.png. IP: 200.171.40.181. Componente de assinatura versão 1.524.0 disponibilizado em https://app.clicksign.com.
22 jun 2023, 09:33:15	Processo de assinatura finalizado automaticamente. Motivo: finalização automática após a última assinatura habilitada. Processo de assinatura concluído para o documento número 4145790b-f13f-48b9-94ca-d35bf61afe43.

ICP Brasil

Documento assinado com validade jurídica.
Para conferir a validade, acesse https://validador.clicksign.com e utilize a senha gerada pelos signatários ou envie este arquivo em PDF.
As assinaturas digitais e eletrônicas têm validade jurídica prevista na Medida Provisória nº. 2200-2 / 2001

Este Log é exclusivo e deve ser considerado parte do documento nº 4145790b-f13f-48b9-94ca-d35bf61afe43, com os efeitos prescritos nos Termos de Uso da Clicksign, disponível em www.clicksign.com.

Anexos

Luiz Claudio de Souza

Assinou o documento em 14 jun 2023 às 14:17:31

ASSINATURA MANUSCRITA

Assinatura manuscrita com hash SHA256 prefixo cdaf2a(...)

Luiz Claudio de Souza
14 jun 2023, 14-17-31.png

Ari Leandro Scorcio

Assinou o documento em 19 jun 2023 às 07:15:16

ASSINATURA MANUSCRITA

Assinatura manuscrita com hash SHA256 prefixo 07713b(...)

Ari Leandro Scorcio
19 jun 2023, 07-15-16.png

Mauricio Olaia

Assinou o documento em 15 jun 2023 às 13:15:57

ASSINATURA MANUSCRITA

Assinatura manuscrita com hash SHA256 prefixo 7a32c1(...)

Mauricio Olaia
15 jun 2023, 13-15-57.png

Pedro Francisco Araujo

Assinou o documento em 22 jun 2023 às 09:33:13

ASSINATURA MANUSCRITA

Assinatura manuscrita com hash SHA256 prefixo af09ba(...)

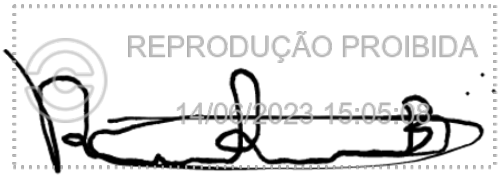
Pedro Francisco Araujo
22 jun 2023, 09-33-14.png

Ricardo Saddi Becker

Assinou o documento em 14 jun 2023 às 15:05:08

ASSINATURA MANUSCRITA

Assinatura manuscrita com hash SHA256 prefixo 3b4b4d(...)



Ricardo Saddi Becker
14 jun 2023, 15-05-08.png