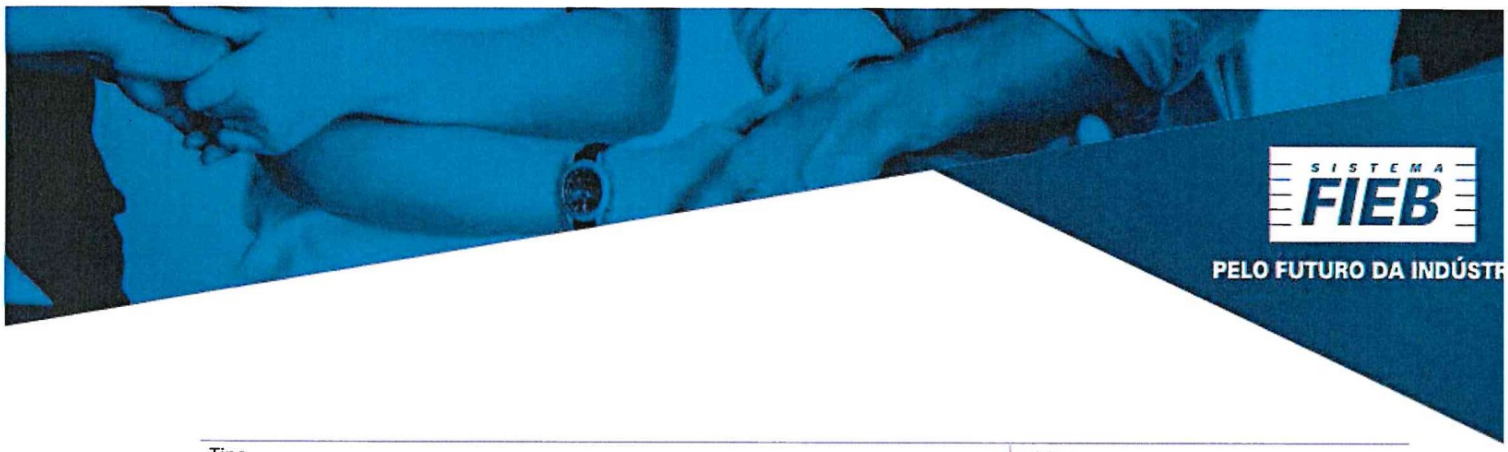

Tipo	Código
Política	**PL-CORP.001**
Título	Versão
Segurança da Informação do Sistema FIEB	**01**

1. INTRODUÇÃO

A Política de Segurança da Informação tem o compromisso com a proteção dos ativos de informação de propriedade ou sob salvaguarda das entidades que compõem o Sistema FIEB (FIEB, SESI/DR/BA, SENAI/DR/BA, IEL/BA e CIEB), preservando a confidencialidade, integridade e disponibilidade destas informações e, garantindo a transparência no tratamento dos dados. Estabelecendo um conjunto de diretrizes para implementar a Privacidade e Segurança de Dados, incluindo processos, procedimentos, estrutura organizacional e funções de software e hardware no uso dos dados do Sistema FIEB ou sob sua salvaguarda, garantindo os direitos do titular dos dados, assim como estabelecendo a padronização do uso, tratamento, e proteção das informações.

A presente Política deve ser observada por todos que mantém vínculos com as entidades do Sistema FIEB, especialmente, seus dirigentes, força de trabalho, conselhos das entidades, sindicatos associados, fornecedores, parceiros e quaisquer pessoas físicas ou jurídicas que se relacionem direta ou indiretamente com FIEB, SESI/DR/BA, SENAI/DR/BA, IEL/BA e/ou CIEB.

Foi elaborada pelas Comissões de Segurança da Informação do Sistema FIEB, observadas as normas técnicas ABNT NBR ISO/IEC 27001:2013 e 27002:2013, a legislação protetiva da privacidade e dos dados pessoais, e os requisitos de negócio das entidades.

> *A segurança da informação é alcançada pela implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, quando necessário para assegurar que os objetivos do negócio e a segurança da informação da organização sejam atendidos. (ABNT NBR ISO/IEC 27002:2013)*

2. OBJETIVOS

Objetivo geral - definir e padronizar o uso, tratamento, controle e proteção das informações que possam causar impactos no desempenho financeiro das Entidades do Sistema FIEB, na sua participação no mercado, na sua imagem, agregando valor à operação e eficiência na prestação de serviços ou no seu relacionamento com as partes interessadas.

2.1. Objetivos específicos:

- Definir o escopo da segurança da informação do Sistema FIEB;
- Definir as responsabilidades das partes interessadas na preservação da segurança da informação;
- Orientar as ações de segurança da informação das Entidades para reduzir riscos e garantir a integridade, confidencialidade e a disponibilidade das informações.

3. DEFINIÇÕES

Para compreensão deste documento, adotam-se os seguintes termos e definições:

- **Agentes de tratamento:** Controlador e Operador.
- **Ameaça:** causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.
- **Anonimização:** utilização de meios técnicos que desassociam um dado ou informação pessoal de um indivíduo, de modo que o dado não possa mais ser vinculado, direta ou indiretamente, ao seu titular.
- **ANPD:** Autoridade Nacional de Proteção de Dados, órgão da administração pública federal, responsável, dentre outras competências, por: zelar pela proteção dos dados pessoais, elaborar as diretrizes da Política Nacional de Proteção de Dados Pessoais e da Privacidade, implementar e fiscalizar o cumprimento da LGPD, e aplicar as sanções por descumprimento da legislação protetiva de dados pessoais.
- **Colaborador**: todo e qualquer empregado do Sistema FIEB.
- **Consentimento**: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

- **Controlador:** pessoa jurídica a quem compete a tomada de decisões acerca do tratamento de dados pessoais pela organização.

- **Coordenador de Segurança da Informação:** colaborador designado para operacionalizar os processos de Segurança da Informação.

- **Dado pessoal:** informação relacionada a pessoa física/natural identificada ou identificável, que poderá ser classificado como dado pessoal sensível, quando se referir a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, vinculado a uma pessoa natural.

- **Encarregado:** pessoa física ou jurídica, indicada pelo controlador, para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), sendo responsável, principalmente, por: atender as demandas dos titulares dos dados pessoais e adotar as providências, responder às notificações referentes ao tratamento de dados pela entidade, da ANPD e demais órgãos públicos competentes, e prestar as orientações aos colaboradores e terceiros quanto às boas práticas para tratamento de dados pessoais.

- **Força de trabalho do Sistema FIEB:** pessoas que compõem a organização e que contribuem para consecução de suas estratégias, objetivos e metas ou realizam atividades de aprendizagem, tais como empregados em tempo integral ou parcial, temporários, intermitentes, estagiários, autônomos que trabalham sob a coordenação direta da organização.

- **Incidente de segurança da informação:** evento ou série de eventos indesejados ou inesperados, que comprometam as operações do negócio e segurança da informação.

- **Informação ou dado pessoal anonimizado:** informação ou dado pessoal que não pode ser identificado, ou que não leve a identificação do indivíduo, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

- **Informação:** conjunto de dados, imagens, textos e quaisquer outras formas de representação dotadas de significado dentro de um contexto.

- **Líderes:** grupo formado por coordenadores, gerentes, superintendentes e diretores.

- **Monitoramento:** acompanhamento e avaliação de dados e processos com objetivo específico de proteger o negócio, seus ativos e pessoas contra ameaças, prevenindo ataques ou outras manifestações que possam resultar em prejuízo para a organização.

- **Multiplicador/Facilitador:** colaborador responsável por disseminar esta política, seus guias e apoiar no seu cumprimento.

- **Operador:** pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

- **Recursos de Tecnologia da Informação:** referem-se a qualquer sistema de armazenamento ou processamento da informação, serviço ou infraestrutura, ou às instalações físicas que os abriguem, tais como: pen drives, smartphones, tablets, e-mail, planilhas, documentos, computadores, notebooks, equipamentos de rede, dentre outros.

- **Relatório de Impacto:** documentação do Controlador que contém a descrição dos processos de tratamento de dados e informações que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de riscos.

- **Software malicioso ou *malware***: Entende-se por software malicioso qualquer software que realiza ações nocivas aos sistemas, como vírus, worm, ransonware e afins.

- **Terceiros:** grupo composto por profissionais que não são empregados do Sistema FIEB, podendo ser vinculados a empresas contratadas ou não, como, por exemplo, os fornecedores, os prestadores de serviços, parceiros e clientes que possuam acesso às informações do Sistema FIEB.

- **Titular do dado ou da informação pessoal:** pessoa física a quem se referem os dados ou informações pessoais que são objeto de tratamento.

- **Tratamento:** toda operação realizada com dados e informações, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, controle, modificação, comunicação, transferência, difusão ou extração.

- **Uso compartilhado de dados ou informações:** compartilhamento de informações com outros agentes de tratamento, para desenvolvimento de suas atividades e para cumprimento de suas determinações legais ou regulatórias.

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

4. SEGURANÇA DA INFORMAÇÃO (SI) E TRATAMENTO DOS DADOS PELAS ENTIDADES DO SISTEMA FIEB:

A informação é um ativo das organizações, ou seja, é um bem que possui valor e, portanto, deve ser protegida, independentemente de ser escrita ou falada, impressa em papel, armazenada eletronicamente, transmitida pelo correio ou através de meios eletrônicos, ou até apresentada em filmes.

A segurança da informação é alcançada através da preservação da integridade, confidencialidade e disponibilidade da informação, assim entendidos:

- **Integridade:** é a garantia da preservação da informação e consistência dos dados ao longo do seu ciclo de vida.
- **Confidencialidade:** é a garantia de sigilo, ou seja, a informação é acessível somente a pessoas autorizadas a terem acesso.
- **Disponibilidade:** é a garantia de que a informação e os ativos associados estejam disponíveis para os usuários legítimos, sempre que necessário.

Em conformidade com a legislação vigente, em especial com a Lei Federal nº 13.709/18 – Lei Geral de Proteção de Dados Pessoais (LGPD), o tratamento de dados pessoais deve observar os seguintes fundamentos:

- Respeito à privacidade;
- Autodeterminação informativa;
- Liberdade de expressão;
- Inviolabilidade da intimidade, honra e imagem;
- Desenvolvimento econômico, tecnológico e inovação;

- Livre iniciativa, livre concorrência e defesa do consumidor;
- Direitos humanos, livre desenvolvimento da personalidade, dignidade e exercício da cidadania.

As ações referentes a tratamento de dados pessoais pelas entidades do Sistema FIEB devem atentar para a finalidade e necessidade do tratamento, a adequação dos processos e tecnologias, a qualidade dos dados coletados, assegurando tratamento isonômico, livre acesso aos dados por seu titular, transparência nas ações e segurança das informações.

5. PAPÉIS E RESPONSABILIDADES

Todos que mantém relações com as entidades do Sistema FIEB (dirigentes, força de trabalho, fornecedores, parceiros, representantes de sindicatos e organizações associadas) têm responsabilidade sobre as informações que acessam e manipulam nas instalações e nos sistemas destas entidades.

A observância das diretrizes estabelecidas nesta política independe da existência de controles que, de forma total ou parcial, obriguem o seu cumprimento.

A seguir constam especificadas as principais competências dos agentes desta Política de Segurança da Informação:

5.1. Controlador:

O Controlador é o responsável por determinar as ações de tratamento de dados pela organização, podendo ser responsabilizado judicial e administrativamente em caso de incidentes de dados ou falha de segurança, ou de descumprimento à legislação protetiva da privacidade. Deste modo, constituem-se como controladores:

- FIEB;
- SESI/DR/BA;
- SENAI/DR/BA;
- IEL/BA;
- CIEB.

O Controlador possui as seguintes responsabilidades:

a) Tomar decisões referentes aos processos de gestão, atentando para as diretrizes da segurança das

informações e privacidade dos dados pessoais;

b) Adotar medidas de boas práticas para tratamento de dados pessoais pela organização, observadas as exigências legais;

c) Responsabilizar-se junto as instituições públicas e privadas acerca das decisões sobre segurança da informação da organização e tratamento de dados pessoais pela organização.

5.2. Operador:

Refere-se como Operador o terceiro, pessoa física ou jurídica, que realiza tratamento de dados pessoais em nome do Controlador, nos termos do instrumento contratual firmado. O Operador poderá ser responsabilizado solidariamente em caso de incidente de dados pessoais, devendo, portanto, adotar boas práticas de proteção de dados ao executar suas atividades.

Compete ao Operador:

a) Realizar as atividades de tratamento das informações de acordo com as orientações do controlador;

b) Responsabilizar-se pelas ações executadas, respondendo pela inobservância das orientações do Controlador e/ou da legislação vigente, para o tratamento dos dados em nome do Controlador;

5.3. Encarregado de Proteção de Dados

O Encarregado é o responsável pela execução das atividades de tratamento de dados pelo Controlador/Entidade. É a pessoa que detém conhecimento acerca de sistemas, processos e legislação sobre tratamento de dados e segurança das informações, cabendo-lhe adotar práticas condizentes com o negócio das entidades e realidade de mercado. As informações de identificação e contato do Encarregado devem ser amplamente divulgadas e inseridas em documentos relacionados ao tratamento de dados pessoais.

Compete ao Encarregado de Proteção de Dados:

a) Gerir o recebimento das solicitações, reclamações e comunicações dos titulares dos dados, prestar esclarecimentos e adotar providências;

b) Receber notificações da Autoridade Nacional de Proteção de Dados e demais órgãos públicos e adotar providências;

c) Orientar dirigentes, colaboradores e prestadores de serviços contratados pelas entidades acerca das práticas a serem executadas para a proteção de dados pessoais e segurança das informações;

d) Executar as demais atribuições determinadas pelo Controlador, ou estabelecidas em normas complementares, ou requeridas pela ANPD;

e) Acompanhar o processo de adequação das atividades de tratamento de dados às exigências legais;
f) Fiscalizar as ações de tratamento de dados pessoais pelas entidades e indicar a necessidade de melhorias em processos e sistemas, para garantia da conformidade à lei.
g) Subsidiar o Controlador acerca das ações a serem adotadas para a garantia da segurança da informação e proteção dos dados pessoais;
h) Orientar as atividades desenvolvidas pelas Comissões de Segurança da Informação e operadores do Sistema de Gestão de Segurança da Informação;

5.4. Comissões de Segurança da Informação

O Sistema de Gestão de Segurança da Informação é composto por duas Comissões coordenadas pelo Coordenador de Segurança da Informação, a Comissão Técnica e a Comissão Multidisciplinar, cujas competências encontram-se a seguir descritas:

a) Assessorar dirigentes e Encarregado sobre assuntos relativos à segurança da informação e proteção de dados pessoais;
b) Apoiar as ações do Encarregado para implementação de boas práticas para garantia da segurança das informações e proteção de dados pessoais na organização;
c) Propor revisões na Política de Segurança da Informação e documentos relacionados (guias, padrões complementares, acordo de confidencialidade, dentre outros) sempre que necessário;
d) Viabilizar que as atividades desempenhadas pelas entidades sejam executadas em conformidade com a Política de Segurança da Informação e legislação vigente;
e) Avaliar violações à Política de Segurança da Informação e informar ao Encarregado;
f) Avaliar a adequação de controles, metodologias e processos inerentes à segurança da informação, tais como análise/avaliação de riscos e classificação da informação, tabela de temporalidade de dados, dentre outros;
g) Analisar resultados de auditorias e ocorrências de incidentes de dados e falha de segurança da informação, e propor ações preventivas e/ou corretivas;
h) Propor capacitação em segurança da informação, definindo o formato, conteúdo, periodicidade e público-alvo dos treinamentos;

Obs. Para desempenhar suas atribuições, as Comissões de Segurança da Informação devem se reunir regularmente, com frequência a ser definida pelo Coordenador de Segurança da Informação, podendo, em casos excepcionais, reunir-se extraordinariamente para tratar de assuntos específicos ou

urgentes.

5.5. Coordenador de Segurança da Informação

a) Coordenar os Comitês Técnico e Multidisciplinar do Sistema de Gestão de Segurança da Informação;
b) Fornecer o embasamento técnico necessário ao Controlador e ao Encarregado para subsidiar a tomada de decisões acerca de medidas de segurança das informações e proteção de dados;
c) Supervisionar as atividades de implantação dos controles e processos de segurança da informação indicadas pelas comissões de Segurança da Informação;
d) Acompanhar os processos de Segurança da Informação, avaliando periodicamente a efetividade desta política e dos controles adotados, utilizando como subsídios os registros, resultados de auditorias, dentre outros;

5.6. Dirigentes, força de trabalho, fornecedores, membros dos conselhos das entidades, clientes e parceiros com acesso às informações corporativas

a) Cumprir as determinações desta Política de Segurança da Informação, bem como seus respectivos documentos complementares;
b) Proteger a informação contra acesso não autorizado, divulgação, modificação, destruição ou interferência, em todo o seu ciclo de vida;
c) Notificar, com a maior brevidade possível, quaisquer incidentes de dados, fragilidades ou falhas de segurança ao Coordenador de Segurança da Informação e/ou ao Encarregado, para adoção das providências.

A análise quanto a incidente de dados ou falha de segurança cabe exclusivamente ao corpo técnico competente, não devem ser testadas pelos usuários, apenas notificadas quando verificadas. Da mesma forma, ações corretivas não devem ser adotadas pelos usuários, mas, apenas, pelas pessoas autorizadas e designadas para a execução destas atividades no Sistema FIEB.

O cumprimento desta Política de Segurança da Informação faz parte das responsabilidades de trabalho e, a partir da sua publicação, deve integrar contratos de trabalho e contratos com fornecedores em que suas disposições forem aplicáveis.

5.7. Líderes

a) Difundir a Política de Segurança da Informação e viabilizar, no âmbito de sua gestão, a educação, o treinamento e a conscientização sobre segurança da informação e proteção de dados;

b) Identificar as necessidades de segurança da informação e proteção de dados nos processos sob sua responsabilidade, incluindo a classificação das informações e temporalidade dos dados, inclusive propondo novas medidas de controle, quando necessárias;
c) Validar as solicitações de acesso aos dados, informações e sistemas de interesse para processos sob sua responsabilidade, revisando os acessos periodicamente;
d) Fornecer informações a respeito dos seus processos e serviços para composição de relatório de impacto ou outra documentação necessária;
e) Atuar de forma sistêmica para garantir os direitos dos titulares em conformidade com as regras do Controlador e legislação aplicável;

5.8. Multiplicadores

a) Divulgar o conteúdo desta Política em sua Unidade/área aos atuais e novos colaboradores, através de palestras, ambientações, seminários, reuniões, campanhas educativas, mutirões, meios de comunicação, dentre outros;
b) Apoiar no cumprimento da política e suas normas, assim como esclarecer as dúvidas relacionadas a este tema;
c) Operacionalizar os processos de Segurança da Informação, avaliando periodicamente a efetividade desta política e dos controles adotados.

6. DEVER DE SIGILO E CONFIDENCIALIDADE DAS INFORMAÇÕES

As informações relacionadas a negócio são confidenciais e devem ser protegidas por todos os que tiverem acesso. O dever de sigilo e a garantia da confidencialidade das informações são diretrizes desta Política para o tratamento de dados pelas entidades do Sistema FIEB.

Apenas podem ser divulgadas informações de conhecimento público, autorizadas por seu titular, ou quando a legislação autorizar a sua publicação.

A força de trabalho deverá se submeter às diretrizes desta Política, a partir da assinatura do contrato de trabalho, devendo manter sigilo sobre as informações a que tiver acesso em decorrência da execução de suas atividades.

Deverá ser formalizado Acordo de Confidencialidade com fornecedores, prestadores de serviços e parceiros que tenham acesso a quaisquer informações consideradas confidenciais e a dados pessoais,

em decorrência do vínculo com as entidades do Sistema FIEB, a fim de que se comprometam a garantir a segurança e a confidencialidade das informações, observado o seguinte:

- Informações sensíveis e dados pessoais compartilhados devem ser protegidos, utilizando boas práticas de governança e técnicas de segurança da informação e proteção de dados, a fim de evitar vazamentos e incidentes, por toda cadeia de tratamento da informação;
- Os parceiros e fornecedores são responsáveis pelas boas práticas de governança e técnicas de segurança e proteção de dados dos seus processos;
- O acordo de confidencialidade é valido durante todo o período de vigência do contrato e adicionalmente terá duração de 10 (dez) anos após o término da vigência ou obedecerá ao prazo que tiver sido definido no instrumento firmado;
- Em quaisquer outros casos, o dever de confidencialidade e sigilo obedecerá a regulamentação que orienta a atividade específica, nas áreas de: saúde, educação, propriedade intelectual, dentre outras.

7. DO TRATAMENTO DOS DADOS PESSOAIS

O tratamento de dados pessoais consiste nas operações de coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração das informações pela organização.

Para o tratamento de dados pessoais, as entidades do Sistema FIEB deverão observar a legislação protetiva da privacidade e dos dados pessoais, em especial à Lei Federal nº 13.709/2018, e as seguintes diretrizes:

- Implementar na organização estrutura de governança de dados, visando a melhor gestão das ações de segurança da informação e privacidade de dados;
- Tratar somente os dados estritamente necessários para a execução do serviço;
- Eliminar os dados, após o tratamento concluído/finalizado, salvo, se a legislação exigir a guarda das informações por período superior;
- Sempre que possível, tratar os dados de forma anonimizada;
- Observar os fundamentos e princípios da legislação na execução de suas atividades;

- Preservar a segurança e o sigilo das Informações para o tratamento dos dados pessoais pela organização;
- Utilizar/Manter os Sistemas processuais e digitais em conformidade com as boas práticas de Segurança da Informação, quanto à disponibilidade, confidencialidade e autenticidade, adicionalmente empregando sempre que possível os princípios de *Security By Design* em seus processos, sistemas digitais e infraestrutura;
- Tratar os dados exclusivamente para as finalidades definidas nos instrumentos firmados com os titulares dos dados ou em conformidade com a legislação;
- Criar mecanismos de supervisão interna e externa para a preservação das boas práticas no tratamento das informações em seus processos e sistemas;
- Manter um canal de comunicação direto com os titulares de dados, assim como a ANPD, para interlocução com o Encarregado;
- Observar os direitos do titular dos dados e atender às suas solicitações, em conformidade com a lei;
- Manter registros das operações de tratamento de dados pessoais realizadas pela organização;
- Elaborar e disponibilizar relatório de impacto sobre a proteção de dados pessoais com os critérios mínimos determinados em conformidade com a legislação vigente;
- Comunicar à ANPD e ao titular a ocorrência de incidente de dados que possa acarretar riscos ou danos efetivos a este último;
- Elaborar e executar planos de resposta a incidentes de dados;
- Monitorar as atividades de tratamento de dados de modo contínuo e realizar avaliações periódicas;
- Observar a estrutura, escala e volume de suas operações no processo de conformidade às exigências da legislação protetiva da privacidade e dos dados pessoais.

Toda operação envolvendo dados pessoais realizada por esta organização deverá estar enquadrada nas hipóteses de tratamento previstas na legislação, e atender às finalidades legais e/ou especificadas no instrumento celebrado com o titular do dado.

8. DIREITOS DO TITULAR

O tratamento de dados pessoais pelas entidades do Sistema FIEB deve resguardar os direitos do titular dos dados especificados na lei.

Devem restar assegurados os direitos do titular de requerer, durante o período de tratamento de seus dados, as seguintes informações:

- esclarecimentos sobre a possibilidade de não fornecer o consentimento e as consequências da negativa;
- confirmação da existência do tratamento de seus dados pessoais;
- Acesso facilitado às informações sobre o tratamento de seus dados, sendo-lhe garantido conhecimento sobre: os dados existentes e suas formas de tratamento; a finalidade e duração do tratamento; o compartilhamento dos dados e sua finalidade.
- Atualização de seus dados, correção de dados incompletos, inexatos ou desatualizados.
- Anonimização, bloqueio ou eliminação de dados desnecessários; excessivos ou tratados em desconformidade com o disposto na lei;
- Eliminação dos dados – exclusão das informações pessoais dos bancos de dados e sistemas da organização - Direito ao esquecimento:
    - Quando os dados coletados não forem mais necessários para cumprimento do objeto da coleta (finalidade alcançada) e das exigências legais;
    - Fim do período de tratamento;
    - Revogação do consentimento.

9. PROCESSOS DISCIPLINARES

Violações a esta Política de Segurança da Informação e demais documentos complementares sobre segurança da informação e proteção de dados pessoais serão analisados pelo, superior imediato da área na qual ocorreu o fato, que deverá informar a ocorrência ao Coordenador de Segurança da Informação e ao encarregado, para adoção das medidas cabíveis, considerando, a natureza, gravidade e impacto causado.

Poderá ser recomendada a instauração de sindicância para averiguação dos fatos, quando houver indícios de ocorrência de infração funcional, sem prejuízo responsabilização penal e civil do suposto infrator.

Concluída a apuração, conforme normas específicas das entidades do Sistema FIEB, e comprovada a ocorrência da infração, poderão ser aplicadas as penalidades previstas na legislação vigente e nos regulamentos internos, observada a proporcionalidade entre a infração e a sanção respectiva, e respeitado os primados da ampla defesa e do contraditório.

10. CONSCIENTIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO

O Sistema FIEB se compromete a disseminar as informações da Política de Segurança da Informação as partes interessadas, parceiros, fornecedores e clientes.

11. CONTATO

Para dúvidas ou maiores informações/esclarecimentos a respeito desta política, deve-se contactar o Encarregado de Proteção de Dados através do e-mail: dpo@fieb.org.br.

12. DOCUMENTOS COMPLEMENTARES DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A Política de Segurança da Informação do Sistema FIEB é complementada por diretrizes e documentos afins, considerados como parte integrante desta política.

Esta Política está em implantação para atender aos requisitos da legislação vigente, em especial a lei 13.709/18 – Lei Geral de Proteção de Dados Pessoais – LGPD com sua conclusão prevista para 30/09/2022.

EMISSÃO	APROVAÇÃO	DATA
Superintendente Executivo de Serviços Corporativos	Antonio Ricardo A. Alban Presidente FIEB Presidente	06/11/2020