Política de

Segurança da Informação e Proteção de Dados

BIOINDMT

1. Objetivo

1.1. Essa política tem por objetivos instituir diretrizes estratégicas, mecanismos e controles que visam garantir atitudes adequadas para o manuseio, tratamento, controle e proteção de dados, informações, documentos e conhecimentos produzidos e armazenados, sob guarda ou transmitidos, por qualquer meio ou recurso, contra ameaças e vulnerabilidades.

1.2. Desse modo, essa política busca preservar os ativos de informação, reduzir riscos de ocorrência de perdas e alterações desses, bem como de acessos indevidos a informações da Entidade e, sobretudo, preservar a imagem institucional do BIOIND[MT]. A finalidade é preservar as informações no que diz respeito à:

a. **Confidencialidade:** garantia de que o acesso à informação seja obtido somente por pessoas autorizadas;
b. **Integridade:** garantia de fidedignidade e autenticidade das Informações. Propriedade que garante a não violação das informações com intuito de protegê-las contra alteração, gravação ou exclusão indevida, acidental ou proposital.
c. **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes, sempre que necessário.

1.3. Esta Política, dentre outras diretrizes, dá ciência a cada envolvido de que os ambientes, sistemas, recursos computacionais e redes informacionais do BIOIND[MT] poderão ser monitorados e gravados, com prévia informação, conforme previsto na legislação brasileira.

2. Abrangência

2.1. A presente política alcança todos os processos que tratam ativos de informações do BIOIND[MT], digitais e analógicos, que se relacionam com à entidade e a dados dos seus titulares.

2.2. Portanto, aplica-se a todas as pessoas que trabalham no BIOIND [MT], sejam Diretores, colaboradores (CLT), estagiários, prestadores de serviços, bem como quaisquer pessoas física ou jurídica, com que o BIOIND [MT], mantém relacionamento.

3. Referências

3.1. Esta Política foi desenvolvida tendo como suporte as seguintes normas:

- Norma ABNT NBR ISO/IEC Família 27000: Sistema de Gestão de Segurança da Informação (SGSI).
- Decreto-Lei nº 5.452, de 1º de maio de 1943: aprova a Consolidação das Leis do Trabalho (CLT).
- Lei Geral de Proteção de Dados Pessoais (LGPD): Lei nº 13.709/2018.
- Lei de Diretos Autorais: Lei nº 9.610/1998.

4. Diretrizes Gerais

4.1. Proteção da Informação

4.1.1. As diretrizes de segurança da informação e proteção de dados estabelecidas nesta política se aplicam às informações originadas em papel e em meio digital, as convertidas para papel e meio digital, faladas, armazenadas, acessadas, produzidas, utilizadas, editadas, recebidas e transmitidas pela Entidade. Essas diretrizes devem ser seguidas pelos usuários, os quais deverão atuar com responsabilidade e de acordo com o previsto nesta política.

4.1.2. Toda informação relacionada às operações do BIOINDMT, gerada ou desenvolvida nas dependências da Entidade, físicas e virtuais, constitui ativo desta, independente da forma apresentada ou do meio pelo qual é compartilhada ou armazenada.

4.1.3. A informação deve ser utilizada unicamente para a finalidade para a qual foi autorizada e estritamente para o propósito institucional.

4.1.4. É diretriz que toda informação de propriedade do BIOINDMT deva ser protegida de riscos e ameaças, que possam comprometer a confidencialidade, a integridade, a disponibilidade ou a autenticidade destas, através de medidas técnicas e administrativas tais como: perfis de acesso, controle de senhas, troca de senhas, armários com chaves, dentre outros.

4.1.5. Para consolidar a proteção da informação, garantir sua disponibilidade e segurança das informações tratadas, o BIOINDMT, por meio das respectivas áreas responsáveis pelos procedimentos, sistemas, serviços e utilização destes, deve

estabelecer, cumprir e fazer cumprir os procedimentos desta política e demais normativos internos.

4.2. Confidencialidade de Dados e Informações

5.2.1 O BIOIND MT obriga-se a preservar a confidencialidade dos dados cadastrais e pessoais dos diretores, associados, colaboradores, prestadores de serviços e parceiros, e os utilizará tão e somente para propósitos legítimos e específicos, de modo adequado e conforme as necessidades institucionais, utilizando-se das medidas técnicas e administrativas para proteger tais dados, de acordo com a presente Política e pela Lei Geral de Proteção da Dados (LGPD).

5.2.2 São consideradas informações confidenciais, para os fins desta Política, as descritas no item anterior, bem como quaisquer informações não disponíveis ao público ou reservadas, tais como dados, especificações técnicas, desenhos, manuais, esboços, modelos, amostras, projetos, estudos, documentos e outros papéis de qualquer natureza, tangíveis ou em formato eletrônico, arquivos em qualquer meio, programas e documentação de computador, comunicações por escrito, verbalmente ou de outra forma reveladas para a Entidade.

5.2.3 O usuário que receber informações confidenciais deverá mantê-las e resguardá-las em caráter sigiloso, bem como limitar seu acesso, controlar cópias de documentos, dados e reproduções que porventura sejam extraídas da mesma, sob pena de se responsabilizar pelo seu uso indevido. Dados considerados sensíveis e de menores devem ter atenção redobrada.

5.2.4 Nenhum dado ou informação confidencial pode ser compartilhado com terceiros, interna ou externamente à Entidade, sem consentimento por escrito do BIOIND MT, sob pena de aplicação das sanções disciplinares cabíveis previstas no Código de Conduta, e à eventual responsabilização civil e criminal.

5. Diretrizes Específicas

5.1. Gestão de Ativos

O usuário deve ter acesso apenas aos ativos necessários e indispensáveis ao seu trabalho ou atividade, respeitando as recomendações técnicas, comportamentais e de sigilo específicas aplicáveis, constantes nesta política.

Como condições gerais para a gestão e o uso aceitáveis dos ativos de informação e dados dos titulares, esta política considera:

5.1.1. Acessos e Recursos de Rede.

a. O acesso e o uso de todos os sistemas de informação, pastas de rede, bancos de dados e demais recursos (computadores, servidores de documentos e arquivos, impressoras, câmeras de vídeo, telefones, sistemas de videoconferência e audioconferência) devem ser restritos a pessoas expressamente autorizadas, de acordo com a necessidade para o cumprimento de suas atividades laborais e durante o exercício delas nos ambientes do BIOINDMT (físicos ou virtuais) ou externos a ele.

b. Todo acesso será monitorado e se verificada a ocorrência de acessos desnecessários ou com poder excessivo.

c. Acessos fornecidos sob a forma de login (usuário e senha), seja para acesso à rede corporativa, e-mail, sistemas, entre outros, sempre deverão ser realizados através de uso de senhas sigilosas. Senhas são de uso pessoal e intransferível, tendo sua divulgação e compartilhamento vedados sob qualquer hipótese.

d. A área técnica responsável do BIOINDMT poderá bloquear o login de qualquer usuário, no caso de suspeitas de vazamento de senhas ou de tentativas consecutivas de violação de acesso.

5.1.2. Correio Eletrônico (e-mail) e Sistemas de Mensageria e de Correspondências

a. O BIOINDMT fornecerá, a seu critério exclusivo, o acesso às plataformas digitais e correio eletrônico (e-mail) ao servidor, com o respectivo domínio, em sua admissão através de perfis de acessos previamente definidos, baseados em cargos e funções.

b. Por quaisquer meios de correio eletrônico, e-mail, mensageria e correspondência, o usuário é responsável pelas informações recebidas, enviadas e compartilhadas, bem como pela sua guarda, confidencialidade e publicidade.

c. As plataformas de colaboração, correio eletrônico e mensageria disponibilizadas pelo BIOINDMT deverão ser utilizadas para fins corporativos e relacionados às atividades dos colaboradores, enquanto se mantiver o vínculo empregatício. A utilização desses serviços para fins pessoais fica limitada ao contido no Código de Conduta.

d. As mensagens de correio eletrônico sempre deverão incluir assinatura conforme o padrão estabelecido pelo BIOIND MT.

e. É obrigatória a manutenção da caixa de e-mails pelo respectivo usuário, evitando acúmulo de e-mails e arquivos desnecessários.

f. O uso dos recursos de correio eletrônico, bem como o conteúdo das mensagens poderão ser vistoriados por amostragem, estando o BIOIND MT autorizado a ler, copiar, e/ou bloquear mensagens que violem as normas estabelecidas nesta política e no Código de Conduta, e os interesses do BIOIND MT.

g. É proibido aos diretores e colaboradores o uso do correio eletrônico do BIOIND MT para:

- Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação.
- Produzir, transmitir ou divulgar mensagem que não estejam de acordo com o Código de Conduta do BIOIND MT ou com a legislação vigente.
- Enviar mensagens contendo material protegido por direitos autorais sem a permissão do detentor dos direitos;
- Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas na legislação vigente ou ato normativo interno.
- Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo do BIOIND MT;
- Enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;
- Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou o BIOIND MT vulneráveis a ações civis ou criminais;
- Apagar mensagens pertinentes de correio eletrônico quando o BIOIND MT estiver sujeito a algum tipo de investigação;

h. É proibido aos diretores e colaboradores do BIOIND MT, produzir, transmitir ou divulgar mensagem que:

- Contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses do BIOIND MT;

- Contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador;
- Vise obter acesso não autorizado a outro computador, servidor ou rede;
- Vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- Vise burlar qualquer sistema de segurança;
- Vise vigiar secretamente ou assediar outro usuário;
- Vise acessar informações confidenciais sem explícita autorização do proprietário;
- Vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
- Inclua imagens criptografadas ou de qualquer forma mascaradas;
- Tenha conteúdo considerado impróprio, obsceno ou ilegal;
- Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
- Contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;
- Tenha fins políticos locais ou do país (propaganda política);
- Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

5.1.3. Internet (Rede Mundial)

a. Qualquer informação que for acessada, transmitida, recebida ou produzida na internet estará sujeita a divulgação e auditoria. Portanto, o BIOINDMT reserva-se o direito de monitorar e registrar todos os acessos à internet.

b. Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade do BIOINDMT, que analisará e, se necessário, bloqueará qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em unidade de armazenamento de dados local, na estação de trabalho, ou em áreas privadas da rede, visando assegurar o cumprimento desta política.

c. É proibido o acesso a sites da internet ou quaisquer arquivos digitais, bem como sua produção e propagação, que desrespeitem o Código de Conduta do BIOINDMT, possuam conteúdo ilegal, pornográfico, preconceituoso, racista, bem como objetos, fatos, imagens, conceitos, opiniões e outros que possam disseminar o ódio e a violência e influenciar atitudes alheias aos interesses da

Entidade, expondo pessoas físicas ou jurídicas, produtos, marcas ou assemelhados à exposição pública, calúnia, injúria e/ou difamação.

d. Como é do interesse do BIOIND^{MT} que seus colaboradores estejam bem-informados, o uso de sites de notícias ou de serviços, por exemplo, é aceitável, desde que não comprometa a banda da rede em horários estritamente comerciais, não perturbe o bom andamento dos trabalhos nem implique conflitos de interesse com os seus objetivos de negócio

5.1.4. Dispositivos de Acesso (Computadores, Notebooks, Smartphones e ou dispositivos similares), Móveis e Mídias Removíveis.

a. O BIOIND^{MT} deseja facilitar a mobilidade e o fluxo de informação entre seus colaboradores. Por isso, permite que eles usem equipamentos portáteis

b. Quando se descreve "dispositivo móvel" entende-se qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da instituição, ou aprovado e permitido pelo(a) Diretor(a) Executivo(a), como: notebooks, smartphones e pendrives.

c. O usuário do dispositivo mantido pelo BIOIND^{MT} e utilizado para fins corporativos é responsável por sua conservação, segurança, bloqueio de acesso por meio de senhas e/ou outros recursos, cópia de segurança dos dados.

d. É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pelo BIOIND^{MT}, notificar imediatamente seu gestor direto sobre a ocorrência. Também deverá procurar as autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO).

e. Os dispositivos móveis devem ser controlados e supervisionados pela área técnica responsável do BIOIND^{MT}, sendo ao usuário confiado o responsável e correto uso, guarda e segurança do mesmo.

f. O uso de mídias removíveis (cartões de memória, disquetes, pen drive, pen USB e similares) não é recomendado, pois trata-se de uma das maiores fontes de ameaças a vulnerabilidades, tanto no sentido de injetar ataques cibernéticos na Rede Corporativa, bem como fontes de vazamento de informações. Contudo, caso seja imprescindível a utilização das mesmas, atuar com toda a cautela possível e, quando estas não forem mais necessárias, deverão ser descartadas de forma segura e protegida.

5.1.5. Computação em Nuvem

a. O uso das "plataformas de nuvem" para transmissão e armazenamento de informações só poderá ocorrer nas plataformas formalmente contratadas pelo BIOIND^{MT} e disponibilizadas pela área técnica responsável.

5.1.6. Redes e Mídias Sociais

a. O uso das redes e mídias sociais institucionais, por parte dos colaboradores, deve ser regido pelas determinações contidas nesta política.

b. A gestão dos perfis institucionais do BIOIND^{MT} nas redes sociais deve ser realizada por colaboradores competentes e/ou por terceirizados contratados para tal, devidamente autorizados, identificados e instruídos de forma a preservar a imagem institucional, sendo vedado aos demais colaboradores a criação de perfis em nome do BIOIND^{MT}.

c. Quanto ao conteúdo das publicações nas redes e mídias sociais, fica vedado divulgar informações sigilosas e internas do BIOIND^{MT} ou da vida pessoal e profissional de qualquer pessoa física sem a devida autorização; difamar pessoas ou divulgar assuntos que venham prejudicar a imagem do BIOIND^{MT} ou de terceiros; discriminar e compartilhar temas que venham prejudicar pessoas ou grupos de pessoas, por qualquer motivo.

d. O BIOIND^{MT} detém legalmente a propriedade intelectual e os direitos autorais de suas obras e criações, composta sobretudo por bens imateriais, tais como marcas, obras intelectuais, nomes empresariais, fotografias e obras audiovisuais, as quais somente podem ser divulgadas nas redes e mídias sociais ou em quaisquer outros meios, para fins profissionais, sendo vedado o uso para fins particulares.

5.1.7. Dados e Informações

a. O BIOIND^{MT} preservará a confidencialidade dos dados cadastrais e pessoais dos seus titulares e os utilizará tão somente para propósitos legítimos e específicos, de modo adequado e conforme as necessidades institucionais, utilizando-se das medidas técnicas e administrativas aptas a proteger tais dados pessoais.

b. O BIOIND^{MT} decidirá sobre o compartilhamento ou restrição de acesso aos dados e informações, sob sua gestão, bem como adotará meios de monitoramento do uso dos seus dados.

c. Cabe ao usuário da informação tratar as informações que estejam sob seus cuidados com zelo e de acordo com os princípios desta Política e jamais, sob qualquer fundamento, tentar acessar informações e dados sem autorização para fazê-lo e sem correlação com suas funções laborais.

d. Cabe ao usuário da informação documental proceder a guarda dos documentos que estejam sob seus cuidados em locais seguros durante o expediente, enquanto estiver manuseando e ao final do dia de trabalho.

e. Cabe ao BIOINDMT estabelecer condições para transferência segura de informações a partes externas, prevendo responsabilidades aos usuários que exercerem atividades de tratamento de dados pessoais, observando os seguintes processos:

- Controle e notificação de transmissões de dados pessoais.
- Procedimentos para assegurar a rastreabilidade dos eventos e o não repúdio.
- Notificação e registro de incidentes de segurança da informação, como perda de dados.
- Utilização de um sistema acordado de identificação para informações críticas e sensíveis, garantindo que a informação esteja devidamente protegida.

5.1.8. Guarda de Informações Digitais (Backup) e Documentação Física

a. Rotinas sistemáticas de backup e guarda de informações devem ser realizadas por colaboradores da área técnica responsável do BIOINDMT.

b. Cópias dos dados de produção, backup local e backup off-site deve ser produzidas, aplicando-se as melhores práticas de mercado com relação à segurança e proteção de dados.

c. Documentos imprescindíveis para as atividades do BIOINDMT deverão ser salvos em drives de rede corporativa, viabilizando a produção de backup e guarda da informação.

d. Documentações Físicas devem ser guardadas/arquivadas de forma segura, quer seja em ambiente interno ou externo, de acordo com os prazos previstos em lei para guarda e arquivamento de referidos documentos.

e. As cópias de segurança devem ser armazenadas em uma localidade remota, a uma distância suficiente para escapar dos danos de um eventual desastre ocorrido no local principal, bem como as mídias de backup devem ser

regularmente testadas para garantir que elas são confiáveis no caso do uso emergencial.

5.1.9. Instalação de Programas (Softwares)

a. Os softwares instalados e utilizados nos equipamentos do BIOINDMT e externos devem ser legalmente adquiridos e/ou autorizados pela área técnica responsável, mesmo que supostamente de livre uso, como aqueles usualmente classificados como "freeware", "shareware", "demoware", sendo todos utilizados somente dentro do seu período de validade de licenciamento.

b. A área técnica responsável deverá realizar a gestão dos softwares instalados nas estações de trabalho e servidores da Entidade, mantendo o devido registro das licenças disponíveis.

c. O processo de homologação de software deve avaliar, sobretudo, o impacto da utilização deste na segurança da informação do BIOINDMT e o suporte para o mesmo.

d. É vedado efetuar réplicas dos softwares adquiridos pelo BIOINDMT, bem como promover esta prática com outros programas.

e. É vedado utilizar softwares que, por algum motivo, descaracterizem os propósitos da Entidade ou danifiquem de alguma forma o ambiente instalado.

f. A área técnica responsável poderá remover programa de computador instalado em estação de trabalho que não se enquadre nos critérios estabelecidos nessa norma.

g. O usuário deverá manter a configuração do equipamento disponibilizada pelo BIOINDMT seguindo os devidos controles de segurança exigidos por esta política, pelas normas específicas do BIOIND MT, assumindo a responsabilidade como custodiante de informações.

5.1.10. Antivírus

a. Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente de forma automática pela área técnica responsável.

b. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar imediatamente a área técnica responsável.

c. O usuário não pode, em hipótese alguma, desabilitar o programa de antivírus instalado no computador.

d. É proibida a instalação de outros sistemas de antivírus, que não sejam os fornecidos pela área técnica responsável.

5.1.11. Dispositivos de Impressão, Cópia e Digitalização

a. Todos os ativos de informação devem ser devidamente guardados, especialmente documentos em papel ou mídias removíveis do BIOINDMT.

b. Documentos não devem ser abandonados após a sua cópia, impressão ou utilização. Ao usar uma impressora coletiva, o usuário deverá recolher o documento impresso imediatamente.

c. As impressoras e seus respectivos suprimentos são de uso exclusivo para as atividades do BIOINDMT.

d. Os usuários devem recolher imediatamente suas impressões, sejam elas corretas ou impressões com falhas. No caso de impressões com falhas, deverão ser descartadas de forma adequada.

e. Impressões com falhas contendo informações sigilosas devem ser inutilizadas, tornando-as ilegíveis.

5.1.12. Cookies

a. Cookies são pequenos arquivos de texto baixados automaticamente em seu dispositivo quando você acessa e navega por um site. Eles servem, basicamente, para seja possível identificar dispositivos, atividades e preferências de usuários. Por meio deles são coletadas as informações como endereço de IP, localização geográfica, fonte de referência, tipo de navegador, duração da visita e quantidade de acessos.

b. Os cookies não permitem que qualquer arquivo ou informação sejam extraídos do disco rígido do usuário, não sendo possível, ainda, que, por meio deles, se tenha acesso a informações pessoais que não tenham partido do usuário ou da forma como utiliza os recursos do site.

c. As informações coletadas por meio destes cookies são utilizadas para melhorar e personalizar a experiência do usuário, sendo que alguns cookies podem, por exemplo, ser utilizados para lembrar as preferências e escolhas do usuário, bem como para o oferecimento de conteúdo personalizado.

5.1.13. Gestão de Cookies

a. O usuário poderá se opor ao registro de cookies pelo site, bastando que desative esta opção no seu próprio navegador. Mais informações sobre como fazer isso em alguns dos principais navegadores utilizados hoje podem ser acessadas a partir dos seguintes links:

- Internet Explorer: https://support.microsoft.com/pt-br/help/17442/windows-internet-explorer-delete-manage-cookies
- Safari: https://support.apple.com/pt-br/guide/safari/sfri11471/mac
- Google Chrome: https://support.google.com/chrome/answer/95647?hl=pt-BR&hlrm=pt
- Mozila Firefox: https://support.mozilla.org/pt-BR/kb/ative-e-desative-os-cookies-que-os-sites-usam
- Opera: https://www.opera.com/help/tutorials/security/privacy
- Vivaldi: https://br.vivaldi.net/cookies/
- Microsoft Edge:
- https://support.microsoft.com/pt-br/microsoft-edge/excluir-cookies-no-microsoft-edge-63947406-40ac-c3b8-57b9-2a946a29ae09

b. A desativação dos cookies, no entanto, pode afetar a disponibilidade de algumas ferramentas e funcionalidades do site, comprometendo seu uso correto e esperado funcionamento. Outra consequência possível é remoção das preferências do usuário que eventualmente tiverem sido salvas, prejudicando sua experiência.

6. Coleta de Dados

6.1. Dados a partir da sindicalização

6.1.1. A coleta de dados a partir de cadastro para fins de sindicalização inclui informações de pessoas jurídicas e pessoa física, como CNPJ e Razão Social, endereço e outros dados relativos à empresa, dados pessoais do representante da organização, assim sendo o nome completo, RG e CPF, filiação, data de

nascimento, telefone celular/WhatsApp, endereço residencial, endereço de e-mail.

6.1.2. Os dados fornecidos pelos empregadores, para cumprimento de obrigação definida em lei (atos e prerrogativas sindicais) ou em instrumentos jurídicos como Convenções Coletivas de Trabalho e Acordos Coletivos de Trabalho serão tratados como dados pessoais, respeitando as regras de sigilo e de confidencialidade. Neste caso será considerada a finalidade e a boa-fé que justifica a disponibilização dos dados.

6.2. Dados Sensíveis

6.2.1. Não serão coletados dados sensíveis de nossos usuários, assim entendidos aqueles definidos no artigo 11 e seguintes da Lei de Proteção de Dados Pessoais. Dessa forma, não haverá coleta de dados sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato laboral ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

6.3. Coleta de Dados Não Previstos Expressamente

6.3.1. Eventualmente, outros tipos de dados não previstos expressamente nesta Política poderão ser coletados, desde que sejam fornecidos com o consentimento do usuário, ou, ainda, que a coleta seja permitida com fundamento em outra base legal prevista em lei.

6.4. Compartilhamento de Dados Pessoais com Terceiros

6.4.1. O BIOIND^{MT} não compartilhará dados pessoais com terceiros, salvo nos casos em que seja compelida a cumprir alguma determinação legal ou regulatória, ou, ainda, para cumprir alguma ordem expedida por autoridade pública.

6.5. Tempo de Armazenamento dos Dados Pessoais

6.5.1. Os dados pessoais coletados são armazenados e utilizados pelo período que corresponda ao tempo necessário para atingir as finalidades do BIOIND$^{MT.}$

6.5.2. Uma vez expirados os períodos de armazenamento dos dados pessoais, eles são removidos de nossas bases de dados ou anonimizados, salvo nos casos em que houver a possibilidade ou a necessidade de armazenamento em virtude de disposição legal ou regulatória.

6.6. Destinatários e Transferências dos Dados Pessoais

6.6.1. Os dados pessoais do usuário não serão compartilhados com terceiros. Serão, portanto, tratados apenas pelo BIOIND[MT].

7. Do encarregado de proteção de dados

7.1. O encarregado de proteção de dados (DPO) é o profissional encarregado de informar, aconselhar e controlar o responsável pelo tratamento dos dados e o processador de dados subcontratado, bem como os trabalhadores que tratem os dados, a respeito das obrigações do site nos termos da Lei de Proteção de Dados Pessoais e de outras disposições de proteção de dados presentes na legislação nacional e internacional, em cooperação com a autoridade de controle competente.

7.2. O encarregado é responsável por garantir que o BIOIND[MT] esteja em conformidade com as leis e regulamentos relacionados à privacidade e proteção de dados pessoais, bem como com suas políticas e procedimentos internos relacionados ao tema;

7.3. O encarregado de proteção de dados (DPO) será designado pelo BIOIND[MT], o qual poderá ser contatado pelo e-mail.

8. Tratamento e Solicitações

8.1. Em cumprimento à regulamentação aplicável, no que diz respeito ao tratamento de dados pessoais, o BIOIND[MT] respeita e garante ao Usuário, a possibilidade de apresentação de solicitações baseadas nos seguintes direitos:

a. confirmação da existência de tratamento;
b. o acesso aos dados;
c. a correção de dados incompletos, inexatos ou desatualizados;
d. a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade;
e. a portabilidade de seus dados a outro fornecedor de serviço ou produto, mediante requisição expressa pelo Usuário;
f. a eliminação dos dados tratados com consentimento do Usuário;
g. a obtenção de informações sobre as entidades públicas ou privadas com as quais o BIOIND[MT] compartilhou seus dados;

h. a informação sobre a possibilidade de não fornecer o seu consentimento, bem como de ser informado sobre as consequências, em caso de negativa;
i. a revogação do consentimento.

9. Como o Titular Pode Exercer Seus Direitos

9.1. Para garantir que o usuário que pretende exercer seus direitos é de fato, o titular dos dados pessoais objeto da requisição, o BIOIND^{MT} solicitará documentos ou outras informações que possam auxiliar em sua correta identificação, a fim de resguardar o Sindicato e os direitos de terceiros.

9.2. Isto somente será feito, porém, se for absolutamente necessário, e o requerente receberá todas as informações relacionadas.

10. Medidas de Segurança no Tratamento de Dados Pessoais

10.1. O BIOIND^{MT} empregará medidas técnicas e organizativas aptas a proteger os dados pessoais de acessos não autorizados e de situações de destruição, perda, extravio ou alteração desses dados.

10.2. As medidas utilizadas levam em consideração a natureza dos dados, o contexto e a finalidade do tratamento, os riscos que uma eventual violação geraria para os direitos e liberdades do usuário, conforme padrões exigidos.

10.3. Medidas de segurança adotadas pelo BIOIND^{MT}:

a. Os dados de nossos usuários são armazenados em ambiente seguro;
b. Limitação do acesso aos dados de nossos usuários, de modo que terceiros não autorizados não possam acessá-los;
c. Manutenção de registros de todos aqueles que têm, de alguma forma, contato com os dados do BIOIND^{MT}.

10.4. Considerando que o BIOIND^{MT} tem adotado todas as medidas necessárias para evitar incidentes de segurança, deve ser observado pelo usuário acerca da possibilidade de ocorrência de problemas motivados exclusivamente por um terceiro - como em caso de ataques de hackers ou crackers ou, ainda, em caso de culpa exclusiva do usuário, que ocorre, por exemplo, quando ele mesmo transfere seus dados a terceiro;

10.5. Caso ocorra qualquer tipo de incidente de segurança que possa gerar risco ou dano relevante para qualquer de nossos usuários, comunicaremos os afetados e a

Autoridade Nacional de Proteção de Dados acerca do ocorrido, em conformidade como disposto na Lei Geral de Proteção de Dados.

11. Requisitos da Política de Segurança de Informações e Proteção de Dados.

11.1. Para a uniformidade da informação, a Política de Segurança de Informações e Proteção de Dados deverá ser comunicada a todos os membros do Conselho Deliberativo, Colaboradores e Terceiros contratados do BIOIND[MT], a fim de que a política seja cumprida dentro e fora do Sindicato.

11.2. Deverá constar em todos os contratos do BIOIND[MT] para com Terceiros, a ciência acerca da CONFIDENCIALIDADE DAS INFORMAÇÕES, e para os Colaboradores a assinatura de um Termo de Adesão ao Código de Conduta e Ciência da Confidencialidade, como condição imprescindível para formalização do contrato, e via de consequência, assunção de obrigações e responsabilidades.

11.3. A responsabilidade em relação à segurança da informação deve ser comunicada na fase de contratação dos colaboradores. Todos os colaboradores devem ser orientados sobre os procedimentos de segurança, bem como o uso correto das ferramentas de trabalho, a fim de reduzir possíveis riscos.

11.4. Todo incidente que afete a segurança da informação deverá ser comunicado inicialmente ao Diretor(a) Executivo(a) e ao Compliance Officer, e este deverá encaminhar posteriormente ao conhecimento do Conselho Deliberativo para análise.

11.5. O BIOIND[MT] exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus colaboradores, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

11.6. Esta Política será implementada no BIOIND[MT] de forma obrigatória para todos os Diretores e colaboradores, independentemente do nível hierárquico ou função no Sindicato, bem como de vínculo empregatício ou prestação de serviço.

11.7. O não cumprimento dos requisitos previstos nesta Política acarretará violação às regras internas do BIOIND MT e sujeitará o usuário às medidas administrativas e legais cabíveis.

12. Procedimento de Denúncia

12.1. O BIOIND MT manterá um canal de ética para o recebimento de relatos de boa-fé referentes a violações a legislações vigente, ao Código de Conduta, e demais políticas e procedimentos internos.

12.2. O BIOIND MT manterá um canal de ética através de um link disponibilizado no site do Sindicato, além de uma linha telefônica 0800-591-3457, para a recepção de qualquer tipo de denúncia, reclamação, entre outros, com garantia de absoluto sigilo e anonimato.

12.3. Uma empresa externa contratada pelo BIOIND MT será o responsável pela gestão do Canal de Ética, garantindo a confidencialidade dos denunciantes e informações apresentadas.

12.4. Os relatos serão investigados conforme a Política do Canal de Ética e Investigações Internas.

12.5. Se ainda permanecerem dúvidas acerca das condutas apropriadas nos relacionamentos com as partes interessadas do Sindicato, todos devem se dirigir ao *Compliance Officer* antes da execução da ação.

12.6. Não será permitida ou tolerada qualquer forma de retaliação contra as pessoas que porventura realizem denúncias de boa-fé.

13. Sanções

13.1. Todos os incidentes denunciados de suspeitas de infringir esta Política serão investigados. Caso se confirme a denúncia, serão tomadas as medidas corretivas imediatas.

13.2. Qualquer Diretor, colaborador, associado ou terceiro que viole as disposições desta Política estará sujeito às sanções disciplinares previstas no Código de Conduta, sejam elas: Advertência por escrito; Suspensão; Demissão sem justa causa; Demissão por justa causa; Exclusão do associado; e/ou Ação judicial cabível.

13.3. As penalidades serão aplicadas pelo Conselho Deliberativo do BIOIND[MT], nos termos da legislação em vigor, sem prejuízo, caso necessite de comunicação dos fatos às autoridades judiciais.

13.4. As sanções a serem aplicadas para os associados, deverá observar o que dispõe o Estatuto Social do BIOIND [MT] em termos hierárquicos.

14. Aplicação e Revisão da Política

14.1. Essa política passa a ser aplicada a partir da presente data e deverá ser revista trienalmente ou quando ocorrer alterações necessárias.

Registro de Versões

Elaborado por: Compliance Officer
Aprovado por: Conselho Deliberativo
Data da aprovação: 14 de fevereiro de 2022.
Data da atualização: 19 de julho de 2023.