GOVERNO DO ESTADO DE MINAS GERAIS

[Instituto de Previdência dos Servidores Militares do Estado de Minas Gerais]

[Assessoria de Tecnologia da Informação]

PORTARIA DG Nº 1121/2023

Institui a Política de Privacidade e Proteção de Dados Pessoais , no âmbito do Instituto de Previdência dos Servidores Militares - IPSM.

O Diretor-Geral do Instituto de Previdência dos Servidores Militares do Estado de Minas Gerais (IPSM), no uso das atribuições que lhe confere art. 7º, inciso I, do Decreto 48.064, de 16 de outubro de 2020, RESOLVE:

Art. 1º Instituir a **Política de Privacidade e Proteção de Dados Pessoais** no âmbito do IPSM, conforme normas nesta Portaria.

Art. 2º **O INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES MILITARES DO ESTADO DE MINAS GERAIS – IPSM,** tem como missão, garantir o benefício previdenciário e promover a atenção à saúde por meio de ações administrativas, em prol da segurança e qualidade de vida da Família Militar Mineira. Tem como visão, ser reconhecido como Entidade de excelência na gestão do Regime Próprio de Previdência dos militares do Estado e na promoção da assistência à saúde. Tem como valores a solidariedade, legalidade, ética, transparência, pontualidade, efetividade e impessoalidade.

Art. 3º Na aplicação da Lei Geral de Proteção de Dados, serão observados os princípios da legalidade, da impessoalidade, da moralidade, da publicidade, da eficiência, da supremacia do interesse público, da igualdade, do planejamento, da transparência, da eficácia, da motivação, da vinculação da lei especifica, do tratamento objetivo, da segurança jurídica, da razoabilidade, da proporcionalidade, da celeridade, da finalidade, da adequação, da necessidade, do livre acesso, da qualidade dos dados, da transparecia, da segurança, da prevenção, da não discriminação, da prestação de contas *(Accountability)*.

I - A base legal para uso dos Dados Pessoais pelo IPSM se da com as Leis, Decretos e normas a seguir: Lei nº 12.527, de 18 de novembro de 2011, Lei nº 12.965, de 23 de abril de 2014, Lei nº 13.460, de 26 de junho de 2017, Lei nº 13.709, de 14 de agosto de 2018, Lei Federal nº 14.063, de 23 de setembro de 2020, Lei Federal nº 14.129, de 29 de março de 2021, Lei Estadual nº 24.030, de 29 de dezembro de 2021, Decreto Estadual nº 45.241, de 10 de dezembro de 2009, Decreto Estadual nº 45.969, de 24 de maio de 2012, Decreto Estadual nº 46.226, de 24 de abril de 2013, Decreto Estadual nº 46.765, de 26 de maio de 2015, Decreto Estadual nº 47.441, de 03 de julho de 2018, Decreto Estadual nº 47.974, de 05 de junho de 2020, Decreto nº 48 237, de 22 de julho de 2021, - Decreto Estadual nº 48.383, de 18 de Março de 2022, Resolução Seplag nº. 071, de 28 de novembro de 2003, Resolução Seplag 64, de 24 de novembro de 2008, Resolução Seplag n° 72, de 21 de setembro de 2009, Resolução nº 48, de 1° de julho de 2011, Resolução nº. 100, de 23 de dezembro de 2009, Resolução Seplag nº 017, de 11 de maio de 2010, Resolução Seplag nº 38, de 12 de julho de 2010, - Resolução Seplag nº 29, de 05 de julho de 2016, Resolução Seplag nº 63, de 14 de setembro de 2011 e a Resolução Seplag nº 084, DE 11 de novembro de 2022 e legislações da Tecnologia da Informação vigente, do Estado de Minas Gerais.

§1º Além das bases citadas, todo processo do IPSM pode ter sua legislação própria, sendo esta da área previdenciária, de saúde ou de atividade meio administrativa, como as áreas de contabilidade, recurso

humanos, licitação, patrimônio entre outras.

Art 4º A presente Portaria contendo a Política de Privacidade e Proteção de Dados Pessoais, ou simplesmente "política", tem como objetivo fornecer orientações sobre como gerenciar as diversas atividades e operações de tratamento de dados pessoais existentes no IPSM. Este documento faz parte do programa de Implantação da Lei Geral de Proteção de Dados (Lei nº 13.709/2018 – "LGPD") e outras leis setoriais sobre o tema, no âmbito do IPSM, pelo Grupo de Estudos da Lei Geral de Proteção de Dados Pessoais - GT-LGPD/IPSM, da Tecnologia da Informação e subsidiarias aos processos desempenhados pelo IPSM.

I - O IPSM, consciente da importância e da necessidade de adequar as suas operações de tratamento de dados pessoais a uma nova e ampla regulação sobre o tema, no caso, a LGPD, aprovada em agosto de 2018, deu início, em julho de 2019, ao seu processo de conformidade à nova Lei.

II - Nota-se que a LGPD é uma lei transversal, que perpassa diferentes agentes econômicos no Brasil, do setor público e privado; e oferece as regras e condições para que os dados pessoais possam ser utilizado.

III - Na condução das atividades previstas em Leis e Estatutos, o IPSM realiza diversas operações de tratamento de dados pessoais, buscando o melhor interesse dos titulares dos dados e respeitando os seus direitos. Podendo ser caracterizado como Controlador de Dados Pessoais, Operador de Dados Pessoais, Controlador e Operador de Dados Pessoais ou ainda Controladoria Compartilhada de Dados Pessoais, de acordo com as definições da LGPD, reforçando em todas as posições que ocupar, o seu compromisso com o cumprimento das regras de privacidade e proteção de dados pessoais aplicáveis.

IV - Essas atividades abrangem uma série de particularidades nos tratamentos de dados pessoais realizados em sua estrutura, a exemplo o atendimento des obrigações legais específicas das legislações Previdenciárias e de Saúde de seus Beneficiários, de seus Colaboradores (Servidores, Estagiários, Funcionários Terceirizados), Fornecedores, Órgãos Parceiros e outros Órgãos reguladores, às quais muitas vezes, possuem sinergia com o campo da proteção de dados, como a necessidade de guarda permanente.

V - O processo de compliance regulatório, que culminará no Programa de Conformidade da LGPD, envolve um trabalho de interpretação da Lei para definições das obrigações legais, diagnóstico dos fatos pertinentes e relevantes para a sua aplicação e levantamento de fluxos e processos, que contribuem ou não para que os fatos estejam de acordo com o documento legal.

VI - Esta Política se insere em um conjunto amplo de elementos que integram o Sistema de Controles Internos e de Conformidade IPSM cuja coordenação fica a cargo do Grupo de Estudos da Lei Geral de Proteção de Dados - GT-LGPD/IPSM e deve ser lida e interpretada a partir do conjunto de documentos e normativos que compõem a estrutura de governança da informação no Instituto.

VII - O IPSM compreende que, em seus processos onde existe tratamento de dados pessoais, essas informações passam por diferentes meios de suporte, armazenamento e comunicação, sendo estes vulneráveis a fatores externos e internos que podem comprometer a proteção de dados pessoais e afetar negativamente a privacidade dos seus titulares, conforme descriminado nesta Política de Privacidade e Proteção de Dados Pessoais.

Art 5º Para os fins desta Portaria, considera-se:

a) Agentes de tratamento: o controlador e o operador. Responsabilização (do inglês accountability), remete à obrigação de membros de um órgão administrativo ou representativo de prestar contas a instâncias controladoras ou a sociedade de seus atos realizados. Também conhecida como prestação de contas, significa que quem desempenha funções de importância na sociedade deve responder pelas suas ações tanto para órgãos controladores quando solicitado e para sociedade de forma ativa.

b) Agente público: todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da Administração Pública, direta e indireta.

c) Agentes de Estado: inclui órgãos e entidades da Administração pública, além dos seus agentes públicos. causa potencial de um incidente, que pode vir a prejudicar o IPSM; utilização de meios técnicos razoáveis

e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

d) ATI – Assessoria de Tecnologia da Informação do IPSM;

e) Ativo de informação: Patrimônio intangível do IPSM, constituído por suas informações de qualquer natureza, incluindo de caráter estratégico, técnico, administrativo, financeiro, mercadológico, de recursos humanos, legal natureza, bem como quaisquer informações criadas ou adquiridas por meio de parceria, aquisição, licenciamento, compra ou confiadas ao IPSM, por parceiros, beneficiários, empregados e terceiros, em formato escrito, verbal, físico ou digitalizado, armazenada, trafegada ou transitando pela infraestrutura computacional do IPSM ou por infraestrutura externa contratada pela organização, além dos documentos em suporte físico, ou mídias eletrônicas transitadas dentro e fora de sua estrutura física.

f) Autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

g) Autoridade Nacional de Proteção de Dados – ANPD: Autoridade Nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional. software ou sistema de computador é geralmente uma porta de acesso não documentada que permite ao administrador entrar no sistema, solucionar problemas ou fazer manutenção. Quando for acessado por hackers e agências de inteligência para obter acesso ilícito, seja escravizar o computador ou espionagem. Por isso, a expressão assume diversos significados.

h) Banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico. suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados. são aplicações autônomas que rodam na Internet enquanto desempenham algum tipo de tarefa pré-determinada. Eles podem ser úteis e inofensivos para os usuários em geral, mas também podem ser usados de forma abusiva por criminosos.

i) Códigos maliciosos: é qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores.

j) Comitê Estadual de Proteção de Dados Pessoais do Estado de Minas Gerais - CEPED: Comitê instituído pelo Decreto nº 48 237, de 22 de julho de 2021, criado no ambito de Minas Gerais, com objetivo orientar os órgãos e entidades quanto à proteção de dados pessoais e responsável pela criação de normatizações;

k) Controladoria Conjunta: quando dois ou mais responsáveis pelo tratamento determinem conjuntamente as finalidades e os meios desse tratamento, ambos são responsáveis conjuntos pelo tratamento. Estes determinam, por acordo entre si e de modo transparente, as respectivas responsabilidades pelo cumprimento do presente regulamento, nomeadamente no que diz respeito ao exercício dos direitos do titular dos dados e aos respectivos deveres de fornecer as informações referidas, a menos e na medida em que as suas responsabilidades respectivas sejam determinadas pelo direito da União ou do Estado-Membro a que se estejam sujeitos. O acordo pode designar um ponto de contato para os titulares dos dados. medida de segurança adotada pelo IPSM para o tratamento de um risco específico.

l) Dado pessoal: informação relacionada a pessoa natural identificada ou identificável.

m) Dado pessoal sensível: dado pessoal sobre 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, quando vinculado a uma pessoa natural.

n) 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. propriedade dos ativos da informação do IPSM, de serem acessíveis e utilizáveis sob demanda, por partes autorizadas. exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.

o) Encarregado de Dados: 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). - Grupo de Estudos da Lei Geral de Proteção de Dados Pessoais do IPSM.:

p) Incidente de Segurança: Um evento ou conjunto de eventos indesejados de segurança da informação que tem possibilidade significativa de afetar as operações ou ameaçar as informações e dados do IPSM.:

propriedade dos ativos da informação do IPSM, de serem exatos e completos.

q) 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. Instituto de Previdência dos Servidores Militares de Minas Gerais

r) Login: termo em inglês *logging in*, que significa se conectar. Trata-se de um conjunto de credenciais que identificam usuários em um site, rede social, e-mail etc. Através desse mecanismo, os usuários podem não apenas acessar suas contas com maior segurança como também fazer alterações nelas. termo abreviado para "software malicioso" (malicious software). Esse software foi criado especificamente para obter acesso ou danificar um computador, sem o conhecimento do seu proprietário. Existem vários tipos de malware, incluindo spyware, keyloggers, vírus verdadeiros, worms ou qualquer outro tipo de código malicioso que se infiltra em um computador. pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

s) Perimetro Seguro: linha de divisão imaginária que separa a sua rede de dados da organização e seus dispositivos de outras redes e da internet. Fazer segurança de perímetro significa controlar tudo que tenta ultrapassar esta barreira. Por exemplo, se uma pessoa que não faz parte da empresa tentar acessar a sua rede, a segurança de perímetro vai impedir que ela tenha sucesso. Efeito da incerteza sobre os objetivos de segurança da informação do IPSM. software, na maioria das vezes malicioso, criado para esconder ou camuflar a existência de certos processos ou programas de métodos normais de detecção e permitir acesso exclusivo a um computador e suas informações.

t) Segurança da informação: A preservação das propriedades de confidencialidade, integridade e disponibilidade das informações do IPSM.

u) Senha: palavra-passe, PIN (*personal identification* number ou número de identificação pessoa), ou *password* (senha em inglês), é uma palavra ou código secreto previamente convencionado entre as partes como forma de reconhecimento. Em sistemas de computação, senhas são amplamente utilizadas para autenticar usuários e conceder-lhes privilégios — para agir como administradores de um sistema, por exemplo ou permitir-lhes o acesso a informações personalizadas armazenadas no sistema.

v) Sítios e aplicativos: sítios e aplicativos por meio dos quais o usuário acessa os serviços e conteúdos disponibilizados. tipo de malware – arquivo malicioso – que fica oculto no sistema enquanto registra informações e rastreia atividades online, nos computadores ou dispositivos móveis. O spyware pode monitorar, copiar e fazer registros que são enviados ao criminoso sobre o que se digita, carrega, baixa e armazena nos dispositivos. Algumas modalidades podem ativar câmeras e microfones para assistir e ouvir o alvo sem ser detectado. pessoa ou entidade que não participa diretamente em um contrato, em um ato jurídico ou em um negócio, ou que, para além das partes envolvidas, pode ter interesse num processo jurídico. pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

w) 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.

x) Trojan: também conhecido como cavalo de Troia (em inglês Trojan horse), é um malware que executa ações em um computador criando uma porta para uma possível invasão sem a autorização do usuário. Trata-se de um programa que tem um pacote de vírus e na maioria das vezes é utilizado para se conseguir informações de outros computadores ou executar operações indevidas em diversos dispositivos. Essas instruções são pré-programadas pelos criminosos e depois enviadas como vírus para as vítimas.

y) Uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados. ou "Usuário", quando individualmente considerado, todas as pessoas naturais que utilizarem qualquer serviço do IPSM.

z) Usuário da informação: Empregados com vínculo empregatício de qualquer área do IPSM ou terceiros alocados na prestação de serviços o IPSM, indiferente do regime jurídico a que estejam submetidos, assim como outros indivíduos ou organizações devidamente autorizados a utilizar manipular qualquer ativo de

informação do IPSM para o desempenho de suas atividades profissionais;

aa) Violação de dados pessoais: é uma violação de segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso não autorizado a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento;

bb) Virus: Vírus atua se inserindo ou se anexando a um programa ou documento legítimo, que tenha suporte para macros, a fim de executar o seu código. Durante esse processo, um vírus pode potencialmente causar efeitos inesperados ou prejudiciais, como danificar o software do sistema, corrompendo ou destruindo os dados. Causa potencial de um incidente de segurança da informação, que pode vir a prejudicar as operações ou ameaçar as informações do IPSM.

cc) Transferência Internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro.

dd) Trojan: Tipo de malware mais perigoso que um vírus comum, pois sua propagação é rápida e ocorre sem controle da vítima. Assim que ele contamina um computador, o programa malicioso cria cópias de si mesmo em diferentes locais do sistema e se espalha para outras máquinas, seja por meio de Internet, mensagens, conexões locais, dispositivos USB ou arquivos. O objetivo do golpe, em geral, é roubar dados do usuário ou de empresas.

Art. 6º Esta Política se aplica - se:

a) aos Servidores, Estagiários e Funcionários Terceirizados do IPSM;

b) fornecedores que prestam serviços para o IPSM;

c) credenciados que prestam serviços de assistência à saúde aos Beneficiários do IPSM;

d) a todos os terceiros, sejam eles pessoas físicas ou jurídicas que atuam para ou em nome do IPSM em operações que envolvam tratamento de dados pessoais que sejam realizadas no escopo das atividades conduzidas pelo IPSM;

e) aos agentes de tratamento de dados pessoais externos ao IPSM que de qualquer forma, se relacionem com o Instituto;aos titulares de dados pessoais, cujos dados são tratados pelo IPSM (Beneficiários, Militares, Pensionistas, Servidores, Estagiários, Funcionários Terceirizados do IPSM entre outros);

§ 1º A adesão ao programa de conformidade do IPSM às leis de proteção de dados pessoais e aos diplomas normativos dele decorrentes, Programa de Conformidade da LGPD, incluindo a presente Política, é obrigatória a todos os destinatários acima indicados na medida em que se relacionam com o IPSM. Todas as operações que envolvam tratamento de dados pessoais que sejam realizadas no escopo das atividades conduzidas pelo IPSM estão sujeitas a tais normativas.

§ 2º A presente Política estabelece as diretrizes do IPSM para resguardo e uso de dados pessoais que venham a ser tratados em suas atividades, tendo como referência a Lei Geral de Proteção de Dados Pessoais, entre outras normas nacionais e internacionais relativas à privacidade e proteção de dados pessoais.

Art, 7º Esta Política estabelece diretrizes e regras para garantir que seus destinatários entendam e cumpram as legislações que versam sobre proteção de dados pessoais em todas as interações com atuais e futuros titulares de dados pessoais, terceiros e agentes de tratamento, externos ao IPSM no âmbito de suas atividades.

I - Para além dos conceitos definidos pelas normas que versam sobre privacidade e proteção de dados pessoais, as informações abarcadas pela presente Política incluem todos os dados detidos, usados ou transmitidos pelo ou em nome do IPSM, em qualquer tipo de mídia. Isso inclui dados pessoais registrados em papel, mantidos em sistemas de computador ou por meio de internet ou dispositivos portáteis, bem como dados pessoais transmitidos oralmente.

II - Esta política tem por propósito estabelecer diretrizes de Proteção de Dados que permitam o IPSM realizar o tratamento de dados pessoais, em conformidade com a legislação brasileira:

a) Orientar quanto à adoção de controles técnicos e administrativos para atendimento dos requisitos para

Proteção de Dados Pessoais, conforme a legislação vigente;

b) Resguardar os titulares dos dados pessoais que são tratados pelo IPSM, garantindo direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural;

c) Prevenir possíveis causas de violações de dados pessoais e incidentes de segurança da informação relacionados ao tratamento de dados pessoais;

d) Minimizar os riscos, mantendo a credibilidade e confiança dos Beneficiários, Parceiros e Colaboradores, ou de qualquer outro impacto negativo do IPSM, como resultado de violações de dados.

II - O Escopo do uso de Dados no IPSM se aplica:

a) A operação de tratamento seja realizada em território nacional brasileiro;

b) Tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional;

c) Os dados pessoais, objeto do tratamento, tenham sido coletados no território nacional;

d) Nos objetivos finalísticos do IPSM;

e) Na execução da atividade meio, para obtenção de melhores resultados nos objetivos do IPSM.

Art. 8º São objetivos da Política de Privacidade e Proteção de Dados Pessoais IPSM:

a) Estabelecer as diretrizes e responsabilidades do IPSM, que assegurem e reforcem o compromisso do Instituto com o cumprimento das legislações de proteção de dados pessoais aplicáveis;

b) Descrever as regras a serem seguidas na condução das atividades e operações de tratamento de dados pessoais realizadas pelo IPSM e pelos destinatários desta Política, no âmbito das atividades do IPSM, que garantam a sua conformidade com as legislações de proteção de dados pessoais aplicáveis e, em especial, com a LGPD.

I - A presente Política deve ser lida em conjunto com as obrigações previstas nos documentos abaixo relacionados, que versam sobre informações em geral, e a complementam, quando aplicável:

a) Contratos e documentos congêneres do IPSM e outros documentos comparáveis, que dispõem sobre obrigações de confidencialidade em relação às informações mantidas pelo Instituto;

b) Políticas e normas de procedimentos de segurança da informação, bem como termos e condições de uso, que tratem sobre confidencialidade, integridade e disponibilidade das informações do IPSM;

c) Todas as normas internas e legislações pertinentes a tecnologia da informação e a respeito da proteção de dados pessoais que vierem a ser elaboradas e atualizadas, de tempos em tempos.

Art. 9º O IPSM cumprirá com os seguintes princípios de proteção de dados pessoais quando do tratamento de dados pessoais:

a) Finalidade:realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

b) Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

c) Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

d) Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

e) Qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

f) Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e

industrial;

g) Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

h) Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

i) Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

J) Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

I Esta Política de Privacidade poderá ser atualizada em decorrência de eventual atualização normativa, razão pela qual o usuário deverá consultar o site do IPSM sempre que possível.

Art. 10 º Todas as operações de tratamento de dados pessoais no âmbito das atividades conduzidas pelo IPSM terão uma base legal que legitime a sua realização, com estipulação da finalidade e designação dos responsáveis pelo tratamento.

I - O IPSM assume, como compromisso institucional, a avaliação periódica das finalidades de suas operações de tratamento, considerando o contexto em que estas operações se inserem, os riscos e benefícios que podem ser gerados ao titular de dados pessoais e o legítimo interesse do Instituto.

II - A realização de operações de tratamento de dados pessoais pelo IPSM poderá ser realizada:

a) Pela Administração Pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres;

b) Mediante o fornecimento de consentimento pelo titular de dados pessoais;

c) Para o cumprimento de obrigação legal ou regulatória;

d) Quando necessário, para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular de dados pessoais;

e) Para a proteção da vida ou da incolumidade física do titular de dados pessoais ou de terceiro;

f) Para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

g) Quando necessário para atender aos interesses legítimos do IPSM ou de terceiros.

III - O IPSM não realiza Transferência Internacional de dados. Caso seja necessário a qualquer tempo, será realizado a atualização desta Política de Privacidade de Dados e normatizado com base na Lei Geral de Proteção de Dados.

Art. 11º O IPSM reconhece que o tratamento de dados pessoais sensíveis representa riscos mais altos ao titular de dados pessoais e por esta razão, o Instituto assume o compromisso de resguardo e cuidados especiais frente ao tratamento de dados pessoais sensíveis:

I - Este compromisso incorpora os dados pessoais sensíveis enumerados no art. 5º, inciso II da LGPD, bem, para os fins desta Política e da Implantação da Lei Geral de Proteção de Dados no IPSM, serão tratados de forma devida.

II - Os dados pessoais de crianças e adolescentes serão tratados com o mesmo nível de cuidado exigido e oferecido aos dados pessoais sensíveis, mas também estarão sujeitos às disposições próprias estabelecidas no Capítulo II, Seção III, da LGPD, e outras normas específicas aplicáveis.

III - A realização de operações de tratamento de dados pessoais sensíveis pelo IPSM somente poderá ser realizada:

a) Quando o titular de dados pessoais ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

b) Sem fornecimento de consentimento do titular de dados pessoais, nos casos em que o tratamento for indispensável, conforme legislação pertinente e normas do IPSM;

c) Pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres;

d) O cumprimento de obrigação legal ou regulatória pelo IPSM;

e) O exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral;

f) Proteção da vida ou da incolumidade física do titular de dados pessoais ou de terceiros;

g) Tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.

Art. 12 - O objetivo da Política de Proteção de Dados no IPSM é garantir a gestão sistemática e efetiva de todos os aspectos relacionados à proteção de dados pessoais e dos direitos dos seus titulares, provendo suporte as operações críticas e minimizando riscos identificados e seus eventuais impactos a organização.

I - A Diretoria Geral , a Assessoria da Tecnologia da Informação e o Grupo de Estudos de Proteção de Dados - GT-LGPD/IPSM, estão comprometidos com uma gestão efetiva da Proteção de Dados Pessoais, e desta forma, adotam todas medidas cabíveis para garantir que esta política seja adequadamente comunicada, entendida e seguida em todos os níveis da organização. Revisões periódicas serão realizadas para garantir sua contínua pertinência e adequação as necessidades do o IPSM.

II - É política de uso de dados por parte do IPSM:

a) Garantir ao titular o tratamento de seus dados pessoais, excetuando-se casos onde a lei aplicável permitir especificamente o processamento de dados pessoais;

b) Garantir que o objetivo do tratamento de dados pessoais esteja em conformidade com a legislação vigente e de acordo com uma base legal permitida;Comunicar, de forma clara e adequadamente adaptada às circunstâncias, o tratamento de dados pessoais ao titular, conforme os dados são coletados ou usados pela primeira vez, em conformidade com o Relatório de Impacto de Dados Pesoais - RIPD;

c) Sempre que necessário, fornecer ao titular explicações suficientes sobre o tratamento de seus dados pessoais, conforme previsto na legislação vigente e base legal de uso;

d) Limitar a coleta de dados pessoais estritamente ao que é permitido de acordo com a legislação vigente, e os objetivos especificados, minimizando, onde possível, a coleta dos referidos dados pessoais;Limitar o uso, retenção, divulgação e transferência de dados pessoais ao necessário para cumprir com objetivos do IPSM, conforme legislação vigente;

e) Reter dados pessoais apenas, conforme tabela de temporalidade de processos do IPSM, para cumprir os propósitos de sua atividade fim;Garantir a precisão e qualidade dos dados pessoais tratados;Fornecer aos titulares dos dados pessoais tratados, informações claras e facilmente acessíveis sobre as políticas, termos de uso, procedimentos e práticas com relação ao tratamento de dados pessoais realizado pela organização;Notificar titulares, quando necessário, quando ocorrerem alterações significativas no tratamento dos seus dados pessoais, desde que dados são gerenciados e de responsabilidade do IPSM;

f) Garantir que titulares tenham a possibilidade de acessar e revisar seus dados pessoais, desde que sua identidade seja autenticada com um nível apropriado de garantia (senhas ou similar), e que não exista nenhuma restrição legal a esse acesso ou a revisão dos dados pessoais, desde que dados são gerenciados e de responsabilidade do IPSM;Garantir prestação de contas durante todo o tratamento de dados pessoais, incluindo quando dados pessoais forem compartilhados com terceiros;

g) Tratar integralmente violações de dados, garantindo que sejam adequadamente registradas, classificadas, investigadas, corrigidas e documentadas e reportadas a ANPD para demais providências;

h) Garantir que, na ocorrência de uma violação de dados, todas as partes interessadas serão notificadas, conforme requisitos e prazos previstos na Lei de Proteção de Dados e conforme determinado pela ANPD;

i) Documentar e comunicar, conforme apropriado, todas as políticas, procedimentos e práticas relacionadas à privacidade e proteção de dados.Garantir a existência de um responsável (DPO) por documentar, implementar e comunicar políticas, procedimentos e práticas relacionadas à privacidade e proteção de dados;

j) Adotar controles de segurança da informação, tanto técnicos quanto administrativos, suficientes para garantir níveis de proteção adequados para Dados Pessoais;

k) Disponibilizar políticas, normas e procedimentos para proteção de dados pessoais a todas as partes interessadas e autorizadas, tais como: Servidores, Colaboradores, Terceiros Contratados, Empregados, Credenciados e outros que compartilhem dados com o IPSM;

l) Garantir a educação e conscientização de Servidores, Colaboradores, Terceiros Contratados, Empregados, Credenciados e outros que compartilhem dados com o IPSM, sobre as práticas de proteção de dados pessoais adotadas pelo IPSM;

m) Melhorar continuamente a Gestão de Proteção de Dados Pessoais através da definição e revisão sistemática de objetivos de privacidade e proteção de dados pessoais em todos os níveis do IPSM;

n) Garantir a não discriminação no tratamento de dados pessoais, impossibilitando que estes sejam usados para fins discriminatórios, ilícitos ou abusivos;Garantir a conformidade integral com leis e regulamentações de proteção de Dados Pessoais.

Art. 13º É direito dos titulares de dados pessoais, quais sejam:

a) Direito de confirmação e acesso (Art. 18, I e II): é o direito do usuário de obter do serviço a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento e, se for esse o caso, o direito de acessar os seus dados pessoais.

b) Direito de retificação (Art. 18, III): é o direito de solicitar a correção de dados incompletos, inexatos ou desatualizados.

c) Direito à limitação do tratamento dos dados (Art. 18, IV): é o direito do usuário de limitar o tratamento de seus dados pessoais, podendo exigir a eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei Geral de Proteção de Dados, desde que a lei não exigir o fornecimento do dado ou para atividades meios e fins.

d) Direito de oposição (Art. 18, § 2º): é o direito do usuário de, a qualquer momento, se opor ao tratamento de dados por motivos relacionados com a sua situação particular, com fundamento em uma das hipóteses de dispensa de consentimento ou em caso de descumprimento ao disposto na Lei Geral de Proteção de Dados, desde que a oposição não impeça o mesmo de obter serviços do IPSM ou seja imposto ao IPSM por força de lei.

e) Direito de não ser submetido a decisões automatizadas (Art. 20, LGPD): o titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade, desde que a desde que a decisão não impeça o mesmo de obter serviços do IPSM ou seja imposto ao IPSM por força de lei.

f) Direito do acesso à informação (Lei 12.527 - Lei de Acesso à Informação): é dever do Estado garantir o direito de acesso à informação, que será franqueada, mediante procedimentos objetivos e ágeis, de forma transparente, clara e em linguagem de fácil compreensão.

g) Direito do respeito à intimidade (Constituição Federal, Art. 5º, X) - O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.

h) Direito de portabilidade dos dados (Art. 18, V): é o direito do usuário de realizar a portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial e compatibilidade de portabilidade da Administração Publica, uma vez que, haverá impossibilidades de portabilidades entre a Administração Privada e Pública, devido a peculiaridades de tecnologia de cada organização.

I - O IPSM reitera o seu compromisso com os direitos dos titulares de dados pessoais à transparência e à informação adequada, destacando o fornecimento de:

a) Informação das entidades públicas e privadas com as quais o IPSM realizou uso compartilhado de dados;

b) Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa limitação de uso dos direitos ao exercício e quando em norma especifica impedir tal execução;

c) Informação sobre a possibilidade de não exclusão de dados e sobre as consequências, tendo em vista a limitação da temporalidade do processo e de legislação especifica, que impede sua exclusão devido as Auditorias Internas e Externas.

Art. 14º Os deveres de cuidado, atenção e uso adequado de dados pessoais se estendem a todos os destinatários desta Política no desenvolvimento de seus trabalhos e atividades no IPSM, comprometendo-se a auxiliar o Instituto a cumprir suas obrigações na implementação de sua estratégia de privacidade e proteção de dados pessoais.

I - Incumbe aos titulares de dados pessoais comunicar ao IPSM sobre quaisquer modificações em seus dados pessoais na sua relação com o Instituto (ex: mudança de endereço), notificando- a preferencialmente na seguinte ordem:

a) Por meio da plataforma disponibilizada pelo IPSM com a qual o titular se relaciona;

b) Por e-mail endereçado ao responsável da Unidade responsável do IPSM com o qual o titular se relaciona;

c) Por e-mail endereçado diretamente ao IPSM, quando necessário; e

d) Por meio físico (ex: carta) endereçado diretamente ao IPSM, quando necessário.

II - O compartilhamento de dados pessoais de titulares de dados pessoais entre as Unidades do IPSM por empregados terceirizados do IPSM é permitido, desde que respeitada a sua finalidade e base legal, observado o princípio da necessidade, ficando o tratamento de dados pessoais sempre adstrito ao desenvolvimento de atividades autorizadas pelo Instituto e estabelecido no Contrato de trabalho.

III - São deveres dos Servidores, Estagiários do IPSM, Agentes de Tratamento de dados pessoais e terceiros (fornecedores e credenciados):

a) Não disponibilizar nem garantir acesso aos dados pessoais mantidos pelo IPSM para quaisquer pessoas não autorizadas ou competentes de acordo com as normas do Instituto.

b) Obter a autorização necessária para o tratamento de dados e ter os documentos necessários que demonstrem a designação de sua competência para a realização da operação de tratamento de dados lícita, nos termos do arcabouço normativo do IPSM que será elaborado.

c) Atender aos ditames da Lei nº 13.709/2018 (LGPD), observando o cumprimento das cláusulas contratuais firmadas (fornecedores e credenciados), assegurando que os empregados e outros profissionais sob sua direção e/ou controle respeitem o uso dos dados somente para as finalidades previstas em contrato, bem como adotar medidas de segurança administrativas, tecnológicas, técnicas e operacionais necessárias a resguardar os dados pessoais que lhe serão confiados, além de evitar o repasse de senhas e logins, e comunicar de imediato, a ocorrência de transferência, remanejamento ou demissão de funcionário, para que seja providenciada a revogação de todos os privilégios de acesso aos sistemas, informações e recursos do órgão contratante.

d) Cumprir as normas, recomendações, orientações de segurança da informação e prevenção de incidentes de segurança da informação publicadas pelo Instituto (Ex: Política de Segurança da Informação, Plano de Resposta a Incidentes de Segurança da Informação, orientações de gestão de senhas, dentre outras).

IV - É responsabilidade da Assessoria de Tecnologia da Informação - ATI:

a) Garantir que políticas, normas e procedimentos de Segurança da Informação sejam ajustados de forma a atender os requisitos da Política Geral de Proteção de Dados Pessoais;

b) Adotar medidas de segurança, tanto técnicas quanto administrativas, aptas a proteger os dados pessoais

de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, conforme padrões mínimos recomendados pela autoridade nacional de proteção de dados pessoais.

c) Realizar o tratamento de incidentes de segurança da informação que envolvam o tratamento de dados pessoais, garantindo sua detecção, contenção, eliminação e recuperação dentro de um prazo razoável.

IV - É responsabilidade dos Usuários da Informação do IPSM:

a) Ler, compreender e cumprir integralmente os termos da Política Geral de Proteção de Dados Pessoais, bem como as demais normas e procedimentos de proteção de dados pessoais aplicáveis;

b) Encaminhar quaisquer dúvidas e/ou pedidos de esclarecimento sobre a Política Geral de Proteção de Dados Pessoais, suas normas e procedimentos ao Encarregado pelo Tratamento de Dados Pessoais ou, quando pertinente, ao Grupo de Estudos da Lei Geral de Proteção de Dados Pessoais- GT-LGPD/IPSM;

c) Comunicar ao Encarregado pelo Tratamento de Dados Pessoais qualquer evento que viole esta Política ou coloque/possa vir a colocar em risco Dados Pessoais tratados pelo IPSM;

d) Ter a ciência e o aceite integral das disposições da Política Geral de Proteção de Dados Pessoais, bem como as demais normas e procedimentos de segurança, assumindo responsabilidade pelo seu cumprimento;

e) Responder pela inobservância da Política Geral de Proteção de Dados Pessoais, normas e procedimentos relacionados ao tratamento de Dados Pessoais;

f) Apoiar o Encarregado pelo tratamento de dados pessoais na comunicação à autoridade nacional e ao titular dos dados pessoais em casos de ocorrência de incidente de segurança que possam acarretar risco ou dano relevante aos titulares.

V - É dever de todos os destinatários desta política:

a) Contatar o Encarregado do IPSM, quando da suspeita ou da ocorrência efetiva das seguintes ações:

b) Não realizar operação de tratamento de dados pessoais, sem base legal que a justifique;

c) Não realizar tratamento de dados pessoais sem a autorização por parte do IPSM no escopo das atividades que desenvolve;

d) Não realizar operação de tratamento de dados pessoais, desconformidade com a Política de Segurança da Informação do IPSM;

e) Realizar eliminação ou destruição não autorizada pelo IPSM de dados pessoais de plataformas digitais ou acervos físicos em todas as instalações do Instituto ou por ele utilizadas;

f) Realizar qualquer violação desta Política ou de qualquer um dos princípios de proteção de dados dispostos neste documento e na Lei Geral de Proteção de Dados.

Art.15º A LGPD estabelece que a responsabilidade no caso de danos patrimoniais, morais, individuais ou coletivos derivados de violações à legislação de proteção de dados pessoais é solidária, e todos os agentes da cadeia envolvendo o tratamento de dados pessoais podem ser responsabilizados pelos eventuais danos causados.

I - Nesse sentido, a possibilidade de o IPSM ser responsabilizado pelas ações de terceiros, implica na necessidade de empregar os melhores esforços para verificar, avaliar e garantir que tais terceiros cumpram com as legislações de proteção de dados aplicáveis.

II - Dessa forma, todos os contratos com terceiros contém cláusulas referentes à proteção de dados pessoais, estabelecendo deveres e obrigações envolvendo a temática, e atestando o compromisso dos terceiros com as legislações de proteção de dados pessoais aplicáveis. Destaca-se, ainda, que esses contratos serão revisados e submetidos à aprovação da Procuradoria Jurídica do IPSM, conforme arcabouço normativo vigente.

III - Ao assinar o Contrato, os terceiros aceitam o Termo de Aceitação desta Política, da Política de Segurança da Informação e do Plano de Resposta a Incidentes de Segurança, submetendo as atividades contratadas no âmbito da relação com o IPSM bem como essas normativas.

Art. 16º O usuário externo se responsabiliza pela precisão e veracidade dos dados informados e reconhece que a inconsistência destes, poderá implicar a impossibilidade de se utilizar o sistema ou serviço solicitado.

I - Durante a utilização do serviço, a fim de resguardar e de proteger os direitos de terceiros, o usuário se compromete a fornecer somente seus dados pessoais, e não os de terceiros e mantê-los permanentemente atualizados.

II - O *login* e senha só poderão ser utilizados pelo usuário cadastrado. Ele se compromete em manter o sigilo da senha, que é pessoal e intransferível, não sendo possível, em qualquer hipótese, a alegação de uso indevido, após o ato de compartilhamento.

III - O usuário do serviço é responsável pela atualização das suas informações pessoais e consequências, na omissão ou erros nas informações pessoais cadastradas.

IV - O Usuário é responsável pela reparação de todos e quaisquer danos, diretos ou indiretos (inclusive decorrentes de violação de quaisquer direitos de outros usuários, de terceiros, inclusive direitos de propriedade intelectual, de sigilo e de personalidade), que sejam causados à Administração Pública, a qualquer outro Usuário, ou, ainda, a qualquer terceiro, inclusive em virtude do descumprimento do disposto nesta Política ou de qualquer ato praticado a partir de seu acesso ao serviço ou plataforma do IPSM ou terceiro ligado ao IPSM (Contratado ou Órgão em que o IPSM matem Controladoria Conjunta).

IV - O IPSM não poderá ser responsabilizado pelos seguintes fatos:

a) Equipamento infectado ou invadido por atacantes;

b) Equipamento avariado no momento do consumo de serviços;

c) Proteção do computador;

d) Proteção das informações baseadas nos computadores dos usuários;

e) Abuso de uso dos computadores dos usuários;

f) Monitoração clandestina do computador dos usuários;

g) Vulnerabilidades ou instabilidades existentes nos sistemas dos usuários;

h) Perímetro inseguro.

§1º Em nenhuma hipótese, o IPSM será responsabilizado pela instalação no equipamento do Usuário ou de terceiros, de códigos maliciosos (vírus, trojans, malware, worm, bot, backdoor, spyware, rootkit, ou de quaisquer outros que venham a ser criados), em decorrência da navegação na Internet pelo Usuário.

V - De modo a informar as regras previstas e responsabilidades, os usuários de serviços do IPSM serão informados em seus sistemas de informação por meio de Termos de Uso em sistemas. política de privacidade em sites, assinatura de termo de confidencialidade ou instrumento legal que informe seus direitos e deveres legais.

Art. 17º O IPSM por meio de seu programa de Implantação da Lei Geral de Proteção de Dados no âmbito do IPSM visa garantir o compromisso do IPSM em zelar pelo tratamento adequado de dados pessoais para fins legítimos que possam ser objeto de suas atividades e reforça o seu compromisso com boas práticas de privacidade e proteção de dados com as seguintes ações:

a) Produção e disseminação de informações, independente do formato, que descrevam as responsabilidades individuais dos destinatários desta Política, no âmbito da privacidade e proteção de dados pessoais;

b) Fornecimento de treinamentos, orientações e aconselhamentos para os empregados do IPSM e terceiros, incluindo, mas não se limitando a cursos online, workshops, reuniões internas, conversas regulares, palestras, dentre outras iniciativas; comungando conteúdos disponibilizados no formato digital e presencial.

c) Incorporação de preocupações e cuidados no tratamento de dados pessoais em todas as etapas de suas

atividades, incluindo, mas não se limitando a rotinas administrativas, atividades de pesquisa, prestação de serviços, atividades de cunho acadêmico, dentre outras.

d) Identificação e aprofundamento da avaliação dos riscos que podem comprometer o alcance dos objetivos do IPSM na área de privacidade e proteção de dados pessoais; definir, criar e implementar planos de ação e políticas para mitigar os riscos identificados; além de manter uma avaliação contínua dos cenários com vistas a avaliar se as medidas implementadas não requerem novas diretrizes e atitudes.

Art. 18º O IPSM, designara Encarregado de Dados , em conformidade com a Lei 13.709/2018, auxiliado pela sua equipe técnica e terá as seguintes responsabilidades:

a) Conduzir o Programa de Conformidade da LGPD no IPSM, zelando pela sua fiscalização;

b) Monitorar o cumprimento das legislações de proteção de dados pessoais aplicáveis, de acordo com as políticas do IPSM;

c) Orientar os destinatários desta Política quanto ao regime de privacidade e proteção de dados pessoais do IPSM;

d) Assegurar que as regras e orientações relativas à proteção de dados sejam informadas e incorporadas nas rotinas e práticas do IPSM;

e) Organizar treinamentos sobre proteção de dados pessoais no IPSM;

f) Prestar esclarecimentos, oferecer informações e apresentar relatórios sobre as operações de tratamento de dados pessoais e seus impactos para as autoridades públicas competentes (Ex:Ministério Público, Autoridade Nacional de Proteção de Dados Pessoais, etc.);

g) Responder às solicitações e reclamações de titulares de dados pessoais cujos dados tenham sido objeto de tratamento por uma unidade do IPSM.

h) Auxiliar em auditorias ou qualquer outra medida de avaliação e monitoramento envolvendo proteção de dados;

i) Elaborar os relatórios de impacto à privacidade e proteção de dados, pareceres e revisão de documentos no que se refere à proteção de dados.

Art. 19º Compete ao IPSM as decisões referentes ao tratamento de dados pessoais realizado, que conforme Lei Geral de Proteção de Dados define como controlador, em seu artigo 5º, competindo as decisões referentes ao tratamento de dados pessoais por sua Diretoria.

Art. 20º Em atendimento à Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2019), foi indicado o Encarregado de Dados para desempenhar o papel de encarregado e atuar como canal de comunicação entre o IPSM, que deverá ser publicado no site do IPSM, sendo seu e-mail institucional lgpd@ipsm.gov.br.

Art. 21º Para o recebimento de demandas dos titulares de dados pessoais, para exercício dos direitos previstos pela Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), será utilizado o Para o Fale Conosco da LGPD, instituído pela Secretaria de Planejamento e Gestão., visando maior confiabilidade pelo uso da Plataforma gov.br que utiliza o login único gov.br, para a abertura de solicitações, considerando o grau de confiança, na confirmação da identidade do titular, pois é necessário a validação dos dados do usuário, a partir das bases oficias de governo.

I - Ficará o Encarregado de Dados, responsável pelo acompanhamento, avaliação das demandas recebidas das solicitações dos titulares de dados , por meio deste sistema citado, de acordo com os termos legais.

II - O prazo a ser considerado para respostas das demandas será de até 20 (vinte) dias, podendo ser prorrogado por mais 10 (dez) dias mediante justificativa expressa a ser cientificado o requerente, conforme estabelece o art. 23 § 3º da Lei nº 13.709/2018 e art. 11 § 1º e 2º da Lei 12.527/2011.

III - A LGPD elenca as demandas que o titular tem direito de peticionar ao controlador (art. 18 da Lei nº

13.709/2018). Essas demandas estão classificadas pela categoria, no sistema Fale Conosco.

IV - O link de acesso é o https://cidadao.mg.gov.br/#/egov/servicos/requisicoes-lgpd

§1º Para outras requisições demandadas de órgãos Controladores, Auditorias e da Autoridade Nacional de Proteção de Dados – ANPD, deverão ser realizadas para o e-mail do Encarregado de Dados: lgpd@ipsm.gov.br

Art. 22º As normas de segurança da informação e prevenção contra incidentes de dados pessoais estão contidas na Política de Segurança da Informação do IPSM e nas normativas internas e documentos correlatos ao tema.

I - A Política de Segurança da Informação visa empregar medidas técnicas e organizacionais adequadas no trato com dados pessoais, e envidar esforços para proteção dos dados pessoais dos titulares de dados pessoais contra acessos não autorizados, perda, destruição, compartilhamento não autorizado, entre outras hipóteses.

II - O IPSM, por meio da Assessoria de Tecnologia da Informação e suas regulamentações de segurança da informação devem prezar pelo pilar da segurança da informação, ou seja a Integridade, Confidencialidade e Disponibilidade, aplicando os melhores métodos na Segurança da Informação e protegendo os dados de todos que compartilham.

Art. 23º Os destinatários desta Política se comprometem a participar dos treinamentos, *workshops*, encontros e capacitações propostos pelo IPSM para a ampliação da cultura de proteção de dados pessoais no Instituto.

I - Os empregados do IPSM cujas funções exigem o tratamento regular de dados pessoais ou os responsáveis pela implementação desta Política se comprometem a participar de treinamentos adicionais para ajudá-los a entender seus deveres e como cumpri-los.

II - O Encarregado de Dados, de modo a fomentar a Política de Segurança de Dados, poderá indicar a todos colaboradores por meio da Gerência de Recursos Humanos, cursos gratuitos ou pagos.

Art. 24º Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela Autoridade Nacional de Proteção de Dados, nos limites do Art. 52 da Lei nº 13.709/2018.

I - Toda Sanção será apreciada e realizada pela Autoridade Nacional de Proteção de Dados – ANPD.

II - O IPSM notificará a ANPD sobre possíveis irregularidades e vazamentos, ficando a ANPD, por meio de regulamento próprio, a aplicação sobre sanções administrativas a infrações a Lei, sendo esta responsável pelo cálculo do valor-base das sanções de multa e eventuais bloqueio de dados.

Art. 25º O IPSM realizará monitoramento, do uso de dados, por meio do Encarregado de Dados e seus colaboradores e assim, mantendo seu compromisso em zelar pelo tratamento adequado de dados pessoais para fins legítimos, que possam ser objeto de suas atividades e reforça o seu compromisso com boas práticas de privacidade e proteção de dados, comprometendo-se a se manter seu Programa de Conformidade da LGPD atualizado com as normas e recomendações emitidas pela ANPD ou outras autoridades competentes.

II - Esta política pode ser alterada conforme orientações do Comitê Estadual de Proteção de Dados Pessoais - CEPD, no âmbito do Estado de Minas Gerais, instituído pelo Decreto nº 48 237, de 22 de julho de 2021, com objetivo orientar os órgãos e entidades quanto à proteção de dados pessoais, no âmbito do Governo Estadual, pela criação de normatizações futuras pela Autoridade Nacional de Proteção de Dados - ANPD e por força de alteração das legislações vigentes.

É compromisso do IPSM revisitar a presente Política periodicamente pelo Grupo de Estudos da Lei Geral de Proteção de Dados - GT-LGPD/IPSM e, a seu critério, promover modificações que atualizem suas disposições de modo a reforçar o compromisso permanente do Instituto com a privacidade e a proteção de

dados pessoais, sendo comunicadas todas as alterações realizadas oportunamente pelos canais oficiais do Instituto.

Art. 26º - A Portaria é aprovada pela Diretoria do IPSM.

Art. 27º Esta Portaria entra em vigor na data de sua publicação.

Belo Horizonte, 11 de agosto de 2023.

Fabiano Villas Boas, Cel. PM QOR

Diretor-Geral do IPSM

Documento assinado eletronicamente por **Fabiano Villas Boas**, **Diretor(a) Geral**, em 11/08/2023, às 15:12, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017.

A autenticidade deste documento pode ser conferida no site http://sei.mg.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **71016627** e o código CRC **AA0AE0FB**.

Referência: Processo nº 2120.01.0008778/2020-50 SEI nº 71016627

MINAS GERAIS

WWW.JORNALMINASGERAIS.MG.GOV.BR ANO 131 – Nº 162 – 91 PÁGINAS BELO HORIZONTE, QUINTA-FEIRA, 17 DE AGOSTO DE 2023

Instituto de Previdência dos Servidores Militares - IPSM

Cel PM QOR Fabiano Villas Boas

PORTARIA DG Nº 1121/2023

Institui a Política de Privacidade e Proteção de Dados Pessoais , no âmbito do Instituto de Previdência dos Servidores Militares - IPSM.

O Diretor-Geral do Instituto de Previdência dos Servidores Militares do Estado de Minas Gerais (IPSM), no uso das atribuições que lhe confere art. 7º, inciso I, do Decreto 48.064, de 16 de outubro de 2020,

RESOLVE:

Art. 1º Instituir a Política de Privacidade e Proteção de Dados Pessoais no âmbito do IPSM, conforme normas nesta Portaria.

Art. 2º O INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES MILITARES DO ESTADO DE MINAS GERAIS – IPSM, tem como missão, garantir o benefício previdenciário e promover a atenção à saúde por meio de ações administrativas, em prol da segurança e qualidade de vida da Família Militar Mineira. Tem como visão, ser reconhecido como Entidade de excelência na gestão do Regime Próprio de Previdência dos militares do Estado e na promoção da assistência à saúde. Tem como valores a solidariedade, legalidade, ética, transparência, pontualidade, efetividade e impessoalidade.

Art. 3º Na aplicação da Lei Geral de Proteção de Dados, serão observados os princípios da legalidade, da impessoalidade, da moralidade, da publicidade, da eficiência, da supremacia do interesse público, da igualdade, do planejamento, da transparência, da eficácia, da motivação, da vinculação da lei especifica, do tratamento objetivo, da segurança jurídica, da razoabilidade, da proporcionalidade, da celeridade, da finalidade, da adequação, da necessidade, do livre acesso, da qualidade dos dados, da transparecia, da segurança, da prevenção, da não discriminação, da prestação de contas (Accountability).

I - A base legal para uso dos Dados Pessoais pelo IPSM se da com as Leis, Decretos e normas a seguir: Lei nº 12.527, de 18 de novembro de 2011, Lei nº 12.965, de 23 de abril de 2014, Lei nº 13.460, de 26 de junho de 2017, Lei nº 13.709, de 14 de agosto de 2018, Lei Federal nº 14.063, de 23 de setembro de 2020, Lei Federal nº 14.129, de 29 de março de 2021, Lei Estadual nº 24.030, de 29 de dezembro de 2021, Decreto Estadual nº 45.241, de 10 de dezembro de 2009, Decreto Estadual nº 45.969, de 24 de maio de 2012, Decreto Estadual nº 46.226, de 24 de abril de 2013, Decreto Estadual nº 46.765, de 26 de maio de 2015, Decreto Estadual nº 47.441, de 03 de julho de 2018, Decreto Estadual nº 47.974, de 05 de junho de 2020, Decreto nº 48 237, de 22 de julho de 2021, - Decreto Estadual nº 48.383, de 18 de Março de 2022, Resolução Seplag nº. 071, de 28 de novembro de 2003, Resolução Seplag 64, de 24 de novembro de 2008, Resolução Seplag n° 72, de 21 de setembro de 2009, Resolução nº 48, de 1° de julho de 2011, Resolução nº. 100, de 23 de dezembro de 2009, Resolução Seplag nº 017, de 11 de maio de 2010, Resolução Seplag nº 38, de 12 de julho de 2010, - Resolução Seplag nº 29, de 05 de julho de 2016, Resolução Seplag nº 63, de 14 de setembro de 2011 e a Resolução Seplag nº 084, DE 11 de novembro de 2022 e legislações da Tecnologia da Informação vigente, do Estado de Minas Gerais.

§1º Além das bases citadas, todo processo do IPSM pode ter sua legislação própria, sendo esta da área previdenciária, de saúde ou de atividade meio administrativa, como as áreas de contabilidade, recurso humanos, licitação, patrimônio entre outras.

Art 4º A presente Portaria contendo a Política de Privacidade e Proteção de Dados Pessoais, ou simplesmente "política", tem como objetivo fornecer orientações sobre como gerenciar as diversas atividades e operações de tratamento de dados pessoais existentes no IPSM. Este documento faz parte do programa de Implantação da Lei Geral de Proteção de Dados (Lei nº 13.709/2018 – "LGPD") e outras leis setoriais sobre o tema, no âmbito do IPSM, pelo Grupo de Estudos da Lei Geral de Proteção de Dados Pessoais - GT-LGPD/IPSM, da Tecnologia da Informação e subsidiarias aos processos desempenhados pelo IPSM.

I - O IPSM, consciente da importância e da necessidade de adequar as suas operações de tratamento de dados pessoais a uma nova e ampla regulação sobre o tema, no caso, a LGPD, aprovada em agosto de 2018, deu início, em julho de 2019, ao seu processo de conformidade à nova Lei.

II - Nota-se que a LGPD é uma lei transversal, que perpassa diferentes agentes econômicos no Brasil, do setor público e privado; e oferece as regras e condições para que os dados pessoais possam ser utilizado.

III - Na condução das atividades previstas em Leis e Estatutos, o IPSM realiza diversas operações de tratamento de dados pessoais, buscando o melhor interesse dos titulares dos dados e respeitando os seus direitos. Podendo ser caracterizado como Controlador de Dados Pessoais, Operador de Dados Pessoais, Controlador e Operador de Dados Pessoais ou ainda Controladoria Compartilhada de Dados Pessoais, de acordo com as definições da LGPD, reforçando em todas as posições que ocupar, o seu compromisso com o cumprimento das regras de privacidade e proteção de dados pessoais aplicáveis.

IV - Essas atividades abrangem uma série de particularidades nos tratamentos de dados pessoais realizados em sua estrutura, a exemplo o atendimento des obrigações legais específicas das legislações Previdenciárias e de Saúde de seus Beneficiários, de seus Colaboradores (Servidores, Estagiários, Funcionários Terceirizados), Fornecedores, Órgãos Parceiros e outros Órgãos reguladores, às quais muitas vezes, possuem sinergia com o campo da proteção de dados, como a necessidade de guarda permanente.

V - O processo de compliance regulatório, que culminará no Programa de Conformidade da LGPD, envolve um trabalho de interpretação da Lei para definições das obrigações legais, diagnóstico dos fatos pertinentes e relevantes para a sua aplicação e levantamento de fluxos e processos, que contribuem ou não para que os fatos estejam de acordo com o documento legal.

VI - Esta Política se insere em um conjunto amplo de elementos que integram o Sistema de Controles Internos e de Conformidade IPSM cuja coordenação fica a cargo do Grupo de Estudos da Lei Geral de Proteção de Dados - GT-LGPD/IPSM e deve ser lida e interpretada a partir do conjunto de documentos e normativos que compõem a estrutura de governança da informação no Instituto.

VII - O IPSM compreende que, em seus processos onde existe tratamento de dados pessoais, essas informações passam por diferentes meios de suporte, armazenamento e comunicação, sendo estes vulneráveis a fatores externos e internos que podem comprometer a proteção de dados pessoais e afetar negativamente a privacidade dos seus titulares, conforme descriminado nesta Política de Privacidade e Proteção de Dados Pessoais.

Art 5º Para os fins desta Portaria, considera-se:

a) Agentes de tratamento: o controlador e o operador. Responsabilização (do inglês accountability), remete à obrigação de membros de um órgão administrativo ou representativo de prestar contas a instâncias controladoras ou a sociedade de seus atos realizados. Também conhecida como prestação de contas, significa que quem desempenha funções de importância na sociedade deve responder pelas suas ações tanto para órgãos controladores quando solicitado e para sociedade de forma ativa.

b) Agente público: todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da Administração Pública, direta e indireta.

c) Agentes de Estado: inclui órgãos e entidades da Administração pública, além dos seus agentes públicos. causa potencial de um incidente, que pode vir a prejudicar o IPSM; utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

d) ATI – Assessoria de Tecnologia da Informação do IPSM;

e) Ativo de informação: Patrimônio intangível do IPSM, constituído por suas informações de qualquer natureza, incluindo de caráter estratégico, técnico, administrativo, financeiro, mercadológico, de recursos humanos, legal natureza, bem como quaisquer informações criadas ou adquiridas por meio de parceria, aquisição, licenciamento, compra ou confiadas ao IPSM, por parceiros, beneficiários, empregados e terceiros, em formato escrito, verbal, físico ou digitalizado, armazenada, trafegada ou transitando pela infraestrutura computacional do IPSM ou por infraestrutura externa contratada pela organização, além dos documentos em suporte físico, ou mídias eletrônicas transitadas dentro e fora de sua estrutura física.

f) Autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

g) Autoridade Nacional de Proteção de Dados – ANPD: Autoridade Nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional. software ou sistema de computador é geralmente uma porta de acesso não documentada que permite ao administrador entrar no sistema, solucionar problemas ou fazer manutenção. Quando for acessado por hackers e agências de inteligência para obter acesso ilícito, seja escravizar o computador ou espionagem. Por isso, a expressão assume diversos significados.

h) Banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico. suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados. são aplicações autônomas que rodam na Internet enquanto desempenham algum tipo de tarefa pré-determinada. Eles podem ser úteis e inofensivos para os usuários em geral, mas também podem ser usados de forma abusiva por criminosos.

i) Códigos maliciosos: é qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores.

j) Comitê Estadual de Proteção de Dados Pessoais do Estado de Minas Gerais - CEPED: Comitê instituído pelo Decreto nº 48 237, de 22 de julho de 2021, criado no ambito de Minas Gerais, com objetivo orientar os órgãos e entidades quanto à proteção de dados pessoais e responsável pela criação de normatizações;

k) Controladoria Conjunta: quando dois ou mais responsáveis pelo tratamento determinem conjuntamente as finalidades e os meios desse tratamento, ambos são responsáveis conjuntos pelo tratamento. Estes determinam, por acordo entre si e de modo transparente, as respectivas responsabilidades pelo cumprimento do presente regulamento, nomeadamente no que diz respeito ao exercício dos direitos do titular dos dados e aos respectivos deveres de fornecer as informações referidas, a menos e na medida em que as suas responsabilidades respectivas sejam determinadas pelo direito da União ou do Estado-Membro a que se estejam sujeitos. O acordo pode designar um ponto de contato para os titulares dos dados. medida de segurança adotada pelo IPSM para o tratamento de um risco específico.

l) Dado pessoal: informação relacionada a pessoa natural identificada ou identificável.

m) Dado pessoal sensível: dado pessoal sobre 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, quando vinculado a uma pessoa natural.

n) 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. propriedade dos ativos da informação do IPSM, de serem acessíveis e utilizáveis sob demanda, por partes autorizadas. exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.

o) Encarregado de Dados: 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).

- Grupo de Estudos da Lei Geral de Proteção de Dados Pessoais do IPSM.:

p) Incidente de Segurança: Um evento ou conjunto de eventos indesejados de segurança da informação que tem possibilidade significativa de afetar as operações ou ameaçar as informações e dados do IPSM.: propriedade dos ativos da informação do IPSM, de serem exatos e completos.

q) 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. Instituto de Previdência dos Servidores Militares de Minas Gerais

r) Login: termo em inglês logging in, que significa se conectar. Trata-se de um conjunto de credenciais que identificam usuários em um site, rede social, e-mail etc. Através desse mecanismo, os usuários podem não apenas acessar suas contas com maior segurança como também fazer alterações nelas. termo abreviado para "software malicioso" (malicious software). Esse software foi criado especificamente para obter acesso ou danificar um computador, sem o conhecimento do seu proprietário. Existem vários tipos de malware, incluindo spyware, keyloggers, vírus verdadeiros, worms ou qualquer outro tipo de código malicioso que se infiltra em um computador. pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

s) Perimetro Seguro: linha de divisão imaginária que separa a sua rede de dados da organização e seus dispositivos de outras redes e da internet. Fazer segurança de perímetro significa controlar tudo que tenta ultrapassar esta barreira. Por exemplo, se uma pessoa que não faz parte da empresa tentar acessar a sua rede, a segurança de perímetro vai impedir que ela tenha sucesso. Efeito da incerteza sobre os objetivos de segurança da informação do IPSM. software, na maioria das vezes malicioso, criado para esconder ou camuflar a existência de certos processos ou programas de métodos normais de detecção e permitir acesso exclusivo a um computador e suas informações.

t) Segurança da informação: A preservação das propriedades de confidencialidade, integridade e disponibilidade das informações do IPSM.

u) Senha: palavra-passe, PIN (personal identification number ou número de identificação pessoa), ou password (senha em inglês), é uma palavra ou código secreto previamente convencionado entre as partes como forma de reconhecimento. Em sistemas de computação, senhas são amplamente utilizadas para autenticar usuários e conceder-lhes privilégios — para agir como administradores de um sistema, por exemplo ou permitir-lhes o acesso a informações personalizadas armazenadas no sistema.

v) Sítios e aplicativos: sítios e aplicativos por meio dos quais o usuário acessa os serviços e conteúdos disponibilizados. tipo de malware – arquivo malicioso – que fica oculto no sistema enquanto registra informações e rastreia atividades online, nos computadores ou dispositivos móveis. O spyware pode monitorar, copiar e fazer registros que são enviados ao criminoso sobre o que se digita, carrega, baixa e armazena nos dispositivos. Algumas modalidades podem ativar câmeras e microfones para assistir e ouvir o alvo sem ser detectado. pessoa ou entidade que não participa diretamente em um contrato, em um ato jurídico ou em um negócio, ou que, para além das partes envolvidas, pode ter interesse num processo jurídico. pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

w) 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.

x) Trojan: também conhecido como cavalo de Troia (em inglês Trojan horse), é um malware que executa ações em um computador criando uma porta para uma possível invasão sem a autorização do usuário. Trata-se de um programa que tem um pacote de vírus e na maioria das vezes é utilizado para se conseguir informações de outros computadores ou executar operações indevidas em diversos dispositivos. Essas instruções são pré-programadas pelos criminosos e depois enviadas como vírus para as vítimas.

y) Uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados. ou "Usuário", quando individualmente considerado, todas as pessoas naturais que utilizarem qualquer serviço do IPSM.

z) Usuário da informação: Empregados com vínculo empregatício de qualquer área do IPSM ou terceiros alocados na prestação de serviços o IPSM, indiferente do regime jurídico a que estejam submetidos, assim como outros indivíduos ou organizações devidamente autorizados a utilizar manipular qualquer ativo de informação do IPSM para o desempenho de suas atividades profissionais;

aa) Violação de dados pessoais: é uma violação de segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso não autorizado a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento;

bb) Virus: Vírus atua se inserindo ou se anexando a um programa ou documento legítimo, que tenha suporte para macros, a fim de executar o seu código. Durante esse processo, um vírus pode potencialmente causar efeitos inesperados ou prejudiciais, como danificar o software do sistema, corrompendo ou destruindo os dados. Causa potencial de um incidente de segurança da informação, que pode vir a prejudicar as operações ou ameaçar as informações do IPSM.

cc) Transferência Internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro.

dd) Trojan: Tipo de malware mais perigoso que um vírus comum, pois sua propagação é rápida e ocorre sem controle da vítima. Assim que ele contamina um computador, o programa malicioso cria cópias de si mesmo em diferentes locais do sistema e se espalha para outras máquinas, seja por meio de Internet, mensagens, conexões locais, dispositivos USB ou arquivos. O objetivo do golpe, em geral, é roubar dados do usuário ou de empresas.

Art. 6º Esta Política se aplica - se:

a) aos Servidores, Estagiários e Funcionários Terceirizados do IPSM;

b) fornecedores que prestam serviços para o IPSM;

c) credenciados que prestam serviços de assistência à saúde aos Beneficiários do IPSM;

d) a todos os terceiros, sejam eles pessoas físicas ou jurídicas que atuam para ou em nome do IPSM em operações que envolvam tratamento de dados pessoais que sejam realizadas no escopo das atividades conduzidas pelo IPSM;

e) aos agentes de tratamento de dados pessoais externos ao IPSM que de qualquer forma, se relacionem com o Instituto;aos titulares de dados pessoais, cujos dados são tratados pelo IPSM (Beneficiários, Militares, Pensionistas, Servidores, Estagiários, Funcionários Terceirizados do IPSM entre outros);

§ 1º A adesão ao programa de conformidade do IPSM às leis de proteção de dados pessoais e aos diplomas normativos dele decorrentes, Programa de Conformidade da LGPD, incluindo a presente Política, é obrigatória a todos os destinatários acima indicados na medida em que se relacionam com o IPSM. Todas as operações que envolvam tratamento de dados pessoais que sejam realizadas no escopo das atividades conduzidas pelo IPSM estão sujeitas a tais normativas.

§ 2º A presente Política estabelece as diretrizes do IPSM para resguardo e uso de dados pessoais que venham a ser tratados em suas atividades, tendo como referência a Lei Geral de Proteção de Dados Pessoais, entre outras normas nacionais e internacionais relativas à privacidade e proteção de dados pessoais.

Art, 7º Esta Política estabelece diretrizes e regras para garantir que seus destinatários entendam e cumpram as legislações que versam sobre proteção de dados pessoais em todas as interações com atuais e futuros titulares de dados pessoais, terceiros e agentes de tratamento, externos ao IPSM no âmbito de suas atividades.

I - Para além dos conceitos definidos pelas normas que versam sobre privacidade e proteção de dados pessoais, as informações abarcadas pela presente Política incluem todos os dados detidos, usados ou transmitidos pelo ou em nome do IPSM, em qualquer tipo de mídia. Isso inclui dados pessoais registrados em papel, mantidos em sistemas de computador ou por meio de internet ou dispositivos portáteis, bem como dados pessoais transmitidos oralmente.

II - Esta política tem por propósito estabelecer diretrizes de Proteção de Dados que permitam o IPSM realizar o tratamento de dados pessoais, em conformidade com a legislação brasileira:

a) Orientar quanto à adoção de controles técnicos e administrativos para atendimento dos requisitos para Proteção de Dados Pessoais, conforme a legislação vigente;

b) Resguardar os titulares dos dados pessoais que são tratados pelo IPSM, garantindo direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural;

c) Prevenir possíveis causas de violações de dados pessoais e incidentes de segurança da informação relacionados ao tratamento de dados pessoais;

d) Minimizar os riscos, mantendo a credibilidade e confiança dos Beneficiários, Parceiros e Colaboradores, ou de qualquer outro impacto negativo do IPSM, como resultado de violações de dados.

II - O Escopo do uso de Dados no IPSM se aplica:

a) A operação de tratamento seja realizada em território nacional brasileiro;

b) Tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional;

c) Os dados pessoais, objeto do tratamento, tenham sido coletados no território nacional;

d) Nos objetivos finalísticos do IPSM;

e) Na execução da atividade meio, para obtenção de melhores resultados nos objetivos do IPSM.

Art. 8º São objetivos da Política de Privacidade e Proteção de Dados Pessoais IPSM:

a) Estabelecer as diretrizes e responsabilidades do IPSM, que assegurem e reforcem o compromisso do Instituto com o cumprimento das legislações de proteção de dados pessoais aplicáveis;

b) Descrever as regras a serem seguidas na condução das atividades e operações de tratamento de dados pessoais realizadas pelo IPSM e pelos destinatários desta Política, no âmbito das atividades do IPSM, que garantam a sua conformidade com as legislações de proteção de dados pessoais aplicáveis e, em especial, com a LGPD.

I - A presente Política deve ser lida em conjunto com as obrigações previstas nos documentos abaixo relacionados, que versam sobre informações em geral, e a complementam, quando aplicável:

a) Contratos e documentos congêneres do IPSM e outros documentos comparáveis, que dispõem sobre obrigações de confidencialidade em relação às informações mantidas pelo Instituto;

b) Políticas e normas de procedimentos de segurança da informação, bem como termos e condições de uso, que tratem sobre confidencialidade, integridade e disponibilidade das informações do IPSM;

c) Todas as normas internas e legislações pertinentes a tecnologia da informação e a respeito da proteção de dados pessoais que vierem a ser elaboradas e atualizadas, de tempos em tempos.

Art. 9º O IPSM cumprirá com os seguintes princípios de proteção de dados pessoais quando do tratamento de dados pessoais:

a) Finalidade:realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

b) Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

c) Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

d) Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

e) Qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

f) Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

g) Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

h) Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

i) Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

J) Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

I Esta Política de Privacidade poderá ser atualizada em decorrência de eventual atualização normativa, razão pela qual o usuário deverá consultar o site do IPSM sempre que possível.

Art. 10 º Todas as operações de tratamento de dados pessoais no âmbito das atividades conduzidas pelo IPSM terão uma base legal que legitime a sua realização, com estipulação da finalidade e designação dos responsáveis pelo tratamento.

I - O IPSM assume, como compromisso institucional, a avaliação periódica das finalidades de suas operações de tratamento, considerando o contexto em que estas operações se inserem, os riscos e benefícios que podem ser gerados ao titular de dados pessoais e o legítimo interesse do Instituto.

II - A realização de operações de tratamento de dados pessoais pelo IPSM poderá ser realizada:

a) Pela Administração Pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres;

b) Mediante o fornecimento de consentimento pelo titular de dados pessoais;

c) Para o cumprimento de obrigação legal ou regulatória;

d) Quando necessário, para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular de dados pessoais;

e) Para a proteção da vida ou da incolumidade física do titular de dados pessoais ou de terceiro;

f) Para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

g) Quando necessário para atender aos interesses legítimos do IPSM ou de terceiros.

III - O IPSM não realiza Transferência Internacional de dados. Caso seja necessário a qualquer tempo, será realizado a atualização desta Política de Privacidade de Dados e normatizado com base na Lei Geral de Proteção de Dados.

Art. 11º O IPSM reconhece que o tratamento de dados pessoais sensíveis representa riscos mais altos ao titular de dados pessoais e por esta razão, o Instituto assume o compromisso de resguardo e cuidados especiais frente ao tratamento de dados pessoais sensíveis:

I - Este compromisso incorpora os dados pessoais sensíveis enumerados no art. 5º, inciso II da LGPD, bem, para os fins desta Política e da Implantação da Lei Geral de Proteção de Dados no IPSM, serão tratados de forma devida.

II - Os dados pessoais de crianças e adolescentes serão tratados com o mesmo nível de cuidado exigido e oferecido aos dados pessoais sensíveis, mas também estarão sujeitos às disposições próprias estabelecidas no Capítulo II, Seção III, da LGPD, e outras normas específicas aplicáveis.

III - A realização de operações de tratamento de dados pessoais sensíveis pelo IPSM somente poderá ser realizada:

a) Quando o titular de dados pessoais ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

b) Sem fornecimento de consentimento do titular de dados pessoais, nos casos em que o tratamento for indispensável, conforme legislação pertinente e normas do IPSM;

c) Pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres;

d) O cumprimento de obrigação legal ou regulatória pelo IPSM;

e) O exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral;

f) Proteção da vida ou da incolumidade física do titular de dados pessoais ou de terceiros;

g) Tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.

Art. 12 - O objetivo da Política de Proteção de Dados no IPSM é garantir a gestão sistemática e efetiva de todos os aspectos relacionados à proteção de dados pessoais e dos direitos dos seus titulares, provendo suporte as operações críticas e minimizando riscos identificados e seus eventuais impactos a organização.

I - A Diretoria Geral , a Assessoria da Tecnologia da Informação e o Grupo de Estudos de Proteção de Dados - GT-LGPD/IPSM, estão comprometidos com uma gestão efetiva da Proteção de Dados Pessoais, e desta forma, adotam todas medidas cabíveis para garantir que esta política seja adequadamente comunicada, entendida e seguida em todos os níveis da organização. Revisões periódicas serão realizadas para garantir sua contínua pertinência e adequação as necessidades do o IPSM.

II - É política de uso de dados por parte do IPSM:

a) Garantir ao titular o tratamento de seus dados pessoais, excetuando-se casos onde a lei aplicável permitir especificamente o processamento de dados pessoais;

b) Garantir que o objetivo do tratamento de dados pessoais esteja em conformidade com a legislação vigente e de acordo com uma base legal permitida;Comunicar, de forma clara e adequadamente adaptada às circunstâncias, o tratamento de dados pessoais ao titular, conforme os dados são coletados ou usados pela primeira vez, em conformidade com o Relatório de Impacto de Dados Pesoais - RIPD;

c) Sempre que necessário, fornecer ao titular explicações suficientes sobre o tratamento de seus dados pessoais, conforme previsto na legislação vigente e base legal de uso;

d) Limitar a coleta de dados pessoais estritamente ao que é permitido de acordo com a legislação vigente, e os objetivos especificados, minimizando, onde possível, a coleta dos referidos dados pessoais;Limitar o uso, retenção, divulgação e transferência de dados pessoais ao necessário para cumprir com objetivos do IPSM, conforme legislação vigente;

e) Reter dados pessoais apenas, conforme tabela de temporalidade de processos do IPSM, para cumprir os propósitos de sua atividade fim;Garantir a precisão e qualidade dos dados pessoais tratados;Fornecer aos titulares dos dados pessoais tratados, informações claras e facilmente acessíveis sobre as políticas, termos de uso, procedimentos e práticas com relação ao tratamento de dados pessoais realizado pela organização;Notificar titulares, quando necessário, quando ocorrerem alterações significativas no tratamento dos seus dados pessoais, desde que dados são gerenciados e de responsabilidade do IPSM;

f) Garantir que titulares tenham a possibilidade de acessar e revisar seus dados pessoais, desde que sua identidade seja autenticada com um nível apropriado de garantia (senhas ou similar), e que não exista nenhuma restrição legal a esse acesso ou a revisão dos dados pessoais, desde que dados são gerenciados e de responsabilidade do IPSM;Garantir prestação de contas durante todo o tratamento de dados pessoais, incluindo quando dados pessoais forem compartilhados com terceiros;

g) Tratar integralmente violações de dados, garantindo que sejam adequadamente registradas, classificadas, investigadas, corrigidas e documentadas e reportadas a ANPD para demais providências;

h) Garantir que, na ocorrência de uma violação de dados, todas as partes interessadas serão notificadas, conforme requisitos e prazos previstos na Lei de Proteção de Dados e conforme determinado pela ANPD;

i) Documentar e comunicar, conforme apropriado, todas as políticas, procedimentos e práticas relacionadas à privacidade e proteção de dados.Garantir a existência de um responsável (DPO) por documentar, implementar e comunicar políticas, procedimentos e práticas relacionadas à privacidade e proteção de dados;

j) Adotar controles de segurança da informação, tanto técnicos quanto administrativos, suficientes para garantir níveis de proteção adequados para Dados Pessoais;

k) Disponibilizar políticas, normas e procedimentos para proteção de dados pessoais a todas as partes interessadas e autorizadas, tais como: Servidores, Colaboradores, Terceiros Contratados, Empregados, Credenciados e outros que compartilhem dados com o IPSM;

l) Garantir a educação e conscientização de Servidores, Colaboradores, Terceiros Contratados, Empregados, Credenciados e outros que compartilhem dados com o IPSM, sobre as práticas de proteção de dados pessoais adotadas pelo IPSM;

m) Melhorar continuamente a Gestão de Proteção de Dados Pessoais através da definição e revisão sistemática de objetivos de privacidade e proteção de dados pessoais em todos os níveis do IPSM;

n) Garantir a não discriminação no tratamento de dados pessoais, impossibilitando que estes sejam usados para fins discriminatórios, ilícitos ou abusivos;Garantir a conformidade integral com leis e regulamentações de proteção de Dados Pessoais.

Art. 13º É direito dos titulares de dados pessoais, quais sejam:
a) Direito de confirmação e acesso (Art. 18, I e II): é o direito do usuário de obter do serviço a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento e, se for esse o caso, o direito de acessar os seus dados pessoais.
b) Direito de retificação (Art. 18, III): é o direito de solicitar a correção de dados incompletos, inexatos ou desatualizados.
c) Direito à limitação do tratamento dos dados (Art. 18, IV): é o direito do usuário de limitar o tratamento de seus dados pessoais, podendo exigir a eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei Geral de Proteção de Dados, desde que a lei não exigir o fornecimento do dado ou para atividades meios e fins.
d) Direito de oposição (Art. 18, § 2º): é o direito do usuário de, a qualquer momento, se opor ao tratamento de dados por motivos relacionados com a sua situação particular, com fundamento em uma das hipóteses de dispensa de consentimento ou em caso de descumprimento ao disposto na Lei Geral de Proteção de Dados, desde que a oposição não impeça o mesmo de obter serviços do IPSM ou seja imposto ao IPSM por força de lei.
e) Direito de não ser submetido a decisões automatizadas (Art. 20, LGPD): o titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade, desde que a desde que a decisão não impeça o mesmo de obter serviços do IPSM ou seja imposto ao IPSM por força de lei.
f) Direito do acesso à informação (Lei 12.527 - Lei de Acesso à Informação): é dever do Estado garantir o direito de acesso à informação, que será franqueada, mediante procedimentos objetivos e ágeis, de forma transparente, clara e em linguagem de fácil compreensão.
g) Direito do respeito à intimidade (Constituição Federal, Art. 5º, X) - O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.
h) Direito de portabilidade dos dados (Art. 18, V): é o direito do usuário de realizar a portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial e compatibilidade de portabilidade da Administração Publica, uma vez que, haverá impossibilidades de portabilidades entre a Administração Privada e Pública, devido a peculiaridades de tecnologia de cada organização.
I - O IPSM reitera o seu compromisso com os direitos dos titulares de dados pessoais à transparência e à informação adequada, destacando o fornecimento de:
a) Informação das entidades públicas e privadas com as quais o IPSM realizou uso compartilhado de dados;
b) Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa limitação de uso dos direitos ao exercício e quando em norma especifica impedir tal execução;
c) Informação sobre a possibilidade de não exclusão de dados e sobre as consequências, tendo em vista a limitação da temporalidade do processo e de legislação especifica, que impede sua exclusão devido as Auditorias Internas e Externas.
Art. 14º Os deveres de cuidado, atenção e uso adequado de dados pessoais se estendem a todos os destinatários desta Política no desenvolvimento de seus trabalhos e atividades no IPSM, comprometendo-se a auxiliar o Instituto a cumprir suas obrigações na implementação de sua estratégia de privacidade e proteção de dados pessoais.
I - Incumbe aos titulares de dados pessoais comunicar ao IPSM sobre quaisquer modificações em seus dados pessoais na sua relação com o Instituto (ex: mudança de endereço), notificando- a preferencialmente na seguinte ordem:
a) Por meio da plataforma disponibilizada pelo IPSM com a qual o titular se relaciona;
b) Por e-mail endereçado ao responsável da Unidade responsável do IPSM com o qual o titular se relaciona;
c) Por e-mail endereçado diretamente ao IPSM, quando necessário; e
d) Por meio físico (ex: carta) endereçado diretamente ao IPSM, quando necessário.
II - O compartilhamento de dados pessoais de titulares de dados pessoais entre as Unidades do IPSM por empregados terceirizados do IPSM é permitido, desde que respeitada a sua finalidade e base legal, observado o princípio da necessidade, ficando o tratamento de dados pessoais sempre adstrito ao desenvolvimento de atividades autorizadas pelo Instituto e estabelecido no Contrato de trabalho.
III - São deveres dos Servidores, Estagiários do IPSM, Agentes de Tratamento de dados pessoais e terceiros (fornecedores e credenciados):
a) Não disponibilizar nem garantir acesso aos dados pessoais mantidos pelo IPSM para quaisquer pessoas não autorizadas ou competentes de acordo com as normas do Instituto.
b) Obter a autorização necessária para o tratamento de dados e ter os documentos necessários que demonstrem a designação de sua competência para a realização da operação de tratamento de dados lícita, nos termos do arcabouço normativo do IPSM que será elaborado.
c) Atender aos ditames da Lei nº 13.709/2018 (LGPD), observando o cumprimento das cláusulas contratuais firmadas (fornecedores e credenciados), assegurando que os empregados e outros profissionais sob sua direção e/ou controle respeitem o uso dos dados somente para as finalidades previstas em contrato, bem como adotar medidas de segurança administrativas, tecnológicas, técnicas e operacionais necessárias a resguardar os dados pessoais que lhe serão confiados, além de evitar o repasse de senhas e logins, e comunicar de imediato, a ocorrência de transferência, remanejamento ou demissão de funcionário, para que seja providenciada a revogação de todos os privilégios de acesso aos sistemas, informações e recursos do órgão contratante.
d) Cumprir as normas, recomendações, orientações de segurança da informação e prevenção de incidentes de segurança da informação publicadas pelo Instituto (Ex: Política de Segurança da Informação, Plano de Resposta a Incidentes de Segurança da Informação, orientações de gestão de senhas, dentre outras).
IV - É responsabilidade da Assessoria de Tecnologia da Informação - ATI:
a) Garantir que políticas, normas e procedimentos de Segurança da Informação sejam ajustados de forma a atender os requisitos da Política Geral de Proteção de Dados Pessoais;
b) Adotar medidas de segurança, tanto técnicas quanto administrativas, aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, conforme padrões mínimos recomendados pela autoridade nacional deproteção de dados pessoais.
c) Realizar o tratamento de incidentes de segurança da informação que envolvam o tratamento de dados pessoais, garantindo sua detecção, contenção, eliminação e recuperação dentro de um prazo razoável.
IV - É responsabilidade dos Usuários da Informação do IPSM:
a) Ler, compreender e cumprir integralmente os termos da Política Geral de Proteção de Dados Pessoais, bem como as demais normas e procedimentos de proteção de dados pessoais aplicáveis;
b) Encaminhar quaisquer dúvidas e/ou pedidos de esclarecimento sobre a Política Geral de Proteção de Dados Pessoais, suas normas e procedimentos ao Encarregado pelo Tratamento de Dados Pessoais ou, quando pertinente, ao Grupo de Estudos da Lei Geral de Proteção de Dados Pessoais- GT-LGPD/IPSM;
c) Comunicar ao Encarregado pelo Tratamento de Dados Pessoais qualquer evento que viole esta Política ou coloque/possa vir a colocar em risco Dados Pessoais tratados pelo IPSM;
d) Ter a ciência e o aceite integral das disposições da Política Geral de Proteção de Dados Pessoais, bem como as demais normas e procedimentos de segurança, assumindo responsabilidade pelo seu cumprimento;
e) Responder pela inobservância da Política Geral de Proteção de Dados Pessoais, normas e procedimentos relacionados ao tratamento de Dados Pessoais;
f) Apoiar o Encarregado pelo tratamento de dados pessoais na comunicação à autoridade nacional e ao titular dos dados pessoais em casos de ocorrência de incidente de segurança que possam acarretar risco ou dano relevante aos titulares.
V - É dever de todos os destinatários desta política:
a) Contatar o Encarregado do IPSM, quando da suspeita ou da ocorrência efetiva das seguintes ações:
b) Não realizar operação de tratamento de dados pessoais, sem base legal que a justifique;
c) Não realizar tratamento de dados pessoais sem a autorização por parte do IPSM no escopo das atividades que desenvolve;
d) Não realizar operação de tratamento de dados pessoais, desconformidade com a Política de Segurança da Informação do IPSM;
e) Realizar eliminação ou destruição não autorizada pelo IPSM de dados pessoais de plataformas digitais ou acervos físicos em todas as instalações do Instituto ou por ele utilizadas;
f) Realizar qualquer violação desta Política ou de qualquer um dos princípios de proteção de dados dispostos neste documento e na Lei Geral de Proteção de Dados.
Art.15º A LGPD estabelece que a responsabilidade no caso de danos patrimoniais, morais, individuais ou coletivos derivados de violações à legislação de proteção de dados pessoais é solidária, e todos os agentes da cadeia envolvendo o tratamento de dados pessoais podem ser responsabilizados pelos eventuais danos causados.
I - Nesse sentido, a possibilidade de o IPSM ser responsabilizado pelas ações de terceiros, implica na necessidade de empregar os melhores esforços para verificar, avaliar e garantir que tais terceiros cumpram com as legislações de proteção de dados aplicáveis.
II - Dessa forma, todos os contratos com terceiros contém cláusulas referentes à proteção de dados pessoais, estabelecendo deveres e obrigações envolvendo a temática, e atestando o compromisso dos terceiros com as legislações de proteção de dados pessoais aplicáveis. Destaca-se, ainda, que esses contratos serão revisados e submetidos à aprovação da Procuradoria Jurídica do IPSM, conforme arcabouço normativo vigente.
III - Ao assinar o Contrato, os terceiros aceitam o Termo de Aceitação desta Política, da Política de Segurança da Informação e do Plano de Resposta a Incidentes de Segurança, submetendo as atividades contratadas no âmbito da relação com o IPSM bem como essas normativas.
Art. 16º O usuário externo se responsabiliza pela precisão e veracidade dos dados informados e reconhece que a inconsistência destes, poderá implicar a impossibilidade de se utilizar o sistema ou serviço solicitado.
I - Durante a utilização do serviço, a fim de resguardar e de proteger os direitos de terceiros, o usuário se compromete a fornecer somente seus dados pessoais, e não os de terceiros e mantê-los permanentemente atualizados.
II - O login e senha só poderão ser utilizados pelo usuário cadastrado. Ele se compromete em manter o sigilo da senha, que é pessoal e intransferível, não sendo possível, em qualquer hipótese, a alegação de uso indevido, após o ato de compartilhamento.
III - O usuário do serviço é responsável pela atualização das suas informações pessoais e consequências, na omissão ou erros nas informações pessoais cadastradas.
IV - O Usuário é responsável pela reparação de todos e quaisquer danos, diretos ou indiretos (inclusive decorrentes de violação de quaisquer direitos de outros usuários, de terceiros, inclusive direitos de propriedade intelectual, de sigilo e de personalidade), que sejam causados à Administração Pública, a qualquer outro Usuário, ou, ainda, a qualquer terceiro, inclusive em virtude do descumprimento do disposto nesta Política ou de qualquer ato praticado a partir de seu acesso ao serviço ou plataforma do IPSM ou terceiro ligado ao IPSM (Contratado ou Órgão em que o IPSM matem Controladoria Conjunta).
IV - O IPSM não poderá ser responsabilizado pelos seguintes fatos:
a) Equipamento infectado ou invadido por atacantes;
b) Equipamento avariado no momento do consumo de serviços;
c) Proteção do computador;
d) Proteção das informações baseadas nos computadores dos usuários;
e) Abuso de uso dos computadores dos usuários;
f) Monitoração clandestina do computador dos usuários;
g) Vulnerabilidades ou instabilidades existentes nos sistemas dos usuários;
h) Perímetro inseguro.
§1º Em nenhuma hipótese, o IPSM será responsabilizado pela instalação no equipamento do Usuário ou de terceiros, de códigos maliciosos (vírus, trojans, malware, worm, bot, backdoor, spyware, rootkit, ou de quaisquer outros que venham a ser criados), em decorrência da navegação na Internet pelo Usuário.
V - De modo a informar as regras previstas e responsabilidades, os usuários de serviços do IPSM serão informados em seus sistemas de informação por meio de Termos de Uso em sistemas. política de privacidade em sites, assinatura de termo de confidencialidade ou instrumento legal que informe seus direitos e deveres legais.
Art. 17º O IPSM por meio de seu programa de Implantação da Lei Geral de Proteção de Dados no âmbito do IPSM visa garantir o compromisso do IPSM em zelar pelo tratamento adequado de dados pessoais para fins legítimos que possam ser objeto de suas atividades e reforça o seu compromisso com boas práticas de privacidade e proteção de dados com as seguintes ações:
a) Produção e disseminação de informações, independente do formato, que descrevam as responsabilidades individuais dos destinatários desta Política, no âmbito da privacidade e proteção de dados pessoais;
b) Fornecimento de treinamentos, orientações e aconselhamentos para os empregados do IPSM e terceiros, incluindo, mas não se limitando a cursos online, workshops, reuniões internas, conversas regulares, palestras, dentre outras iniciativas; comungando conteúdos disponibilizados no formato digital e presencial.
c) Incorporação de preocupações e cuidados no tratamento de dados pessoais em todas as etapas de suas atividades, incluindo, mas não se limitando a rotinas administrativas, atividades de pesquisa, prestação de serviços, atividades de cunho acadêmico, dentre outras.
d) Identificação e aprofundamento da avaliação dos riscos que podem comprometer o alcance dos objetivos do IPSM na área de privacidade e proteção de dados pessoais; definir, criar e implementar planos de ação e políticas para mitigar os riscos identificados; além de manter uma avaliação contínua dos cenários com vistas a avaliar se as medidas implementadas não requerem novas diretrizes e atitudes.
Art. 18º O IPSM, designara Encarregado de Dados , em conformidade com a Lei 13.709/2018, auxiliado pela sua equipe técnica e terá as seguintes responsabilidades:
a) Conduzir o Programa de Conformidade da LGPD no IPSM, zelando pela sua fiscalização;
b) Monitorar o cumprimento das legislações de proteção de dados pessoais aplicáveis, de acordo com as políticas do IPSM;
c) Orientar os destinatários desta Política quanto ao regime de privacidade e proteção de dados pessoais do IPSM;
d) Assegurar que as regras e orientações relativas à proteção de dados sejam informadas e incorporadas nas rotinas e práticas do IPSM;
e) Organizar treinamentos sobre proteção de dados pessoais no IPSM;
f) Prestar esclarecimentos, oferecer informações e apresentar relatórios sobre as operações de tratamento de dados pessoais e seus impactos para as autoridades públicas competentes (Ex:Ministério Público, Autoridade Nacional de Proteção de Dados Pessoais, etc.);
g) Responder às solicitações e reclamações de titulares de dados pessoais cujos dados tenham sido objeto de tratamento por uma unidade do IPSM.
h) Auxiliar em auditorias ou qualquer outra medida de avaliação e monitoramento envolvendo proteção de dados;
i) Elaborar os relatórios de impacto à privacidade e proteção de dados, pareceres e revisão de documentos no que se refere à proteção de dados.
Art. 19º Compete ao IPSM as decisões referentes ao tratamento de dados pessoais realizado, que conforme Lei Geral de Proteção de Dados define como controlador, em seu artigo 5º, competindo as decisões referentes ao tratamento de dados pessoais por sua Diretoria.
Art. 20º Em atendimento à Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2019), foi indicado o Encarregado de Dados para desempenhar o papel de encarregado e atuar como canal de comunicação entre o IPSM, que deverá ser publicado no site do IPSM, sendo seu e-mail institucional lgpd@ipsm.gov.br.
Art. 21º Para o recebimento de demandas dos titulares de dados pessoais, para exercício dos direitos previstos pela Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), será utilizado o Para o Fale Conosco da LGPD, instituído pela Secretaria de Planejamento e Gestão., visando maior confiabilidade pelo uso da Plataforma gov. br que utiliza o login único gov.br, para a abertura de solicitações, considerando o grau de confiança, na confirmação da identidade do titular, pois é necessário a validação dos dados do usuário, a partir das bases oficias de governo.
I - Ficará o Encarregado de Dados, responsável pelo acompanhamento, avaliação das demandas recebidas das solicitações dos titulares de dados , por meio deste sistema citado, de acordo com os termos legais.
II - O prazo a ser considerado para respostas das demandas será de até 20 (vinte) dias, podendo ser prorrogado por mais 10 (dez) dias mediante justificativa expressa a ser cientificado o requerente, conforme estabelece o art. 23 § 3º da Lei nº 13.709/2018 e art. 11 § 1º e 2º da Lei 12.527/2011.
III - A LGPD elenca as demandas que o titular tem direito de peticionar ao controlador (art. 18 da Lei nº 13.709/2018). Essas demandas estão classificadas pela categoria, no sistema Fale Conosco. IV - O link de acesso é o https://cidadao.mg.gov.br/#/egov/servicos/requisicoes-lgpd
§1º Para outras requisições demandadas de órgãos Controladores, Auditorias e da Autoridade Nacional de Proteção de Dados – ANPD, deverão ser realizadas para o e-mail do Encarregado de Dados: lgpd@ ipsm.gov.br
Art. 22º As normas de segurança da informação e prevenção contra incidentes de dados pessoais estão contidas na Política de Segurança da Informação do IPSM e nas normativas internas e documentos correlatos ao tema.
I - A Política de Segurança da Informação visa empregar medidas técnicas e organizacionais adequadas no trato com dados pessoais, e envidar esforços para proteção dos dados pessoais dos titulares de dados pessoais contra acessos não autorizados, perda, destruição, compartilhamento não autorizado, entre outras hipóteses.
II - O IPSM, por meio da Assessoria de Tecnologia da Informação e suas regulamentações de segurança da informação devem prezar pelo pilar da segurança da informação, ou seja a Integridade, Confidencialidade e Disponibilidade, aplicando os melhores métodos na Segurança da Informação e protegendo os dados de todos que compartilham.
Art. 23º Os destinatários desta Política se comprometem a participar dos treinamentos, workshops, encontros e capacitações propostos pelo IPSM para a ampliação da cultura de proteção de dados pessoais no Instituto.
I - Os empregados do IPSM cujas funções exigem o tratamento regular de dados pessoais ou os responsáveis pela implementação desta Política se comprometem a participar de treinamentos adicionais para ajudá-los a entender seus deveres e como cumpri-los.
II - O Encarregado de Dados, de modo a fomentar a Política de Segurança de Dados, poderá indicar a todos colaboradores por meio da Gerência de Recursos Humanos, cursos gratuitos ou pagos.
Art. 24º Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela Autoridade Nacional de Proteção de Dados, nos limites do Art. 52 da Lei nº 13.709/2018.
I - Toda Sanção será apreciada e realizada pela Autoridade Nacional de Proteção de Dados – ANPD.
II - O IPSM notificará a ANPD sobre possíveis irregularidades e vazamentos, ficando a ANPD, por meio de regulamento próprio, a aplicação sobre sanções administrativas a infrações a Lei, sendo esta responsável pelo cálculo do valor-base das sanções de multa e eventuais bloqueio de dados.
Art. 25º O IPSM realizará monitoramento, do uso de dados, por meio do Encarregado de Dados e seus colaboradores e assim, mantendo seu compromisso em zelar pelo tratamento adequado de dados pessoais para fins legítimos, que possam ser objeto de suas atividades e reforça o seu compromisso com boas práticas de privacidade e proteção de dados, comprometendo-se a se manter seu Programa de Conformidade da LGPD atualizado com as normas e recomendações emitidas pela ANPD ou outras autoridades competentes.
II - Esta política pode ser alterada conforme orientações do Comitê Estadual de Proteção de Dados Pessoais - CEPD, no âmbito do Estado de Minas Gerais, instituído pelo Decreto nº 48 237, de 22 de julho de 2021, com objetivo orientar os órgãos e entidades quanto à proteção de dados pessoais, no âmbito do Governo Estadual, pela criação de normatizações futuras pela Autoridade Nacional de Proteção de Dados - ANPD e por força de alteração das legislações vigentes.
É compromisso do IPSM revisitar a presente Política periodicamente pelo Grupo de Estudos da Lei Geral de Proteção de Dados - GT-LGPD/ IPSM e, a seu critério, promover modificações que atualizem suas disposições de modo a reforçar o compromisso permanente do Instituto com a privacidade e a proteção de dados pessoais, sendo comunicadas todas as alterações realizadas oportunamente pelos canais oficiais do Instituto.
Art. 26º - A Portaria é aprovada pela Diretoria do IPSM.
Art. 27º Esta Portaria entra em vigor na data de sua publicação.

Belo Horizonte, 11 de agosto de 2023.
(a) Fabiano Villas Boas, Cel. PM QOR
Diretor-Geral do IPSM

16 1830