INSTRUÇÃO NORMATIVA

Nº 11/2023

SEROPÉDICA/RJ, 22 de dezembro de 2023.

Institui o Programa de Governança em Privacidade e Proteção dos Dados Pessoais no âmbito do Instituto, em conformidade com o art. 50, § 2º da Lei Geral de Proteção de Dados Pessoais - LGPD.

A DIRETORIA-EXECUTIVA do SEROPREVI, usando das atribuições que lhe são conferidas por lei, e

CONSIDERANDO o disposto no inciso LXXIX, do art. 5º, da Constituição da República Federativa do Brasil de 1988, incluído pela Emenda Constitucional nº 115, de 10 de janeiro de 2022, o qual estabelece que é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais;

CONSIDERANDO o disposto na Lei Federal nº 13.709 de 2018, Lei Geral de Proteção de Dados Pessoais - LGPD;

CONSIDERANDO a deliberação do Conselho de Administração na 54ª Reunião Ordinária.

R E S O L V E:

Art. 1º Instituir o Programa de Governança em Privacidade e Proteção dos Dados Pessoais que será implementado pelos agentes de tratamento de dados pessoais no âmbito do Instituto, em conformidade com o art. 50, § 2º da Lei Geral de Proteção de Dados Pessoais - LGPD.

Parágrafo único. A elaboração do Programa é atribuição do Gabinete do Diretor-Presidente, devendo obedecer os dispostos na LGPD e as diretrizes da Autoridade Nacional de Proteção de Dados - ANPD, além dos demais regramentos sobre o tema.

Art. 2º Para fins desta Resolução considera-se:

I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

II - 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;

III - titular dos dados: pessoa natural a quem se referem os dados pessoais que são objetos de tratamento;

IV - agentes de tratamento: o controlador e o operador. Os indivíduos subordinados ou vinculados, como os funcionários, os servidores públicos ou as equipes de trabalho de um órgão ou de uma entidade, que atuam sob o poder diretivo do agente de tratamento não são considerados como controladores ou operadores;

V - controlador: o Instituto, a quem compete as principais decisões relativas aos elementos essenciais para o cumprimento da finalidade do tratamento de dados pessoais, bem como a definição da natureza dos dados pessoais tratados e a duração do tratamento;

VI - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais para a finalidade e instruções previamente estabelecidas pelo controlador. Em sendo pessoa jurídica, os empregados, administradores, sócios, servidores e outras pessoas naturais que a integram e cujos atos expressam a atuação desta, não são considerados como operadores.

VII - suboperador: é o contratado pelo operador, após a autorização formal do controlador, para auxiliar no tratamento de dados pessoais em nome do controlador, podendo ser equiparado ao operador perante a LGPD em relação às atividades que foi contratado para executar, no que se refere às responsabilidades.

VIII - encarregado de proteção de dados pessoais: pessoa indicada, mediante ato formal, pelo controlador e pelo operador, cuja identidade e informações de contato estarão divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador e do operador, sendo responsável por atuar como canal de comunicação entre o controlador, o operador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados - ANPD;

IX - tratamento de dados pessoais: 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 - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada, não sendo a única nem a principal base legal possível para viabilizar o tratamento de dados pessoais;

XI - incidente de segurança com dados pessoais: qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais;

XII - Autoridade Nacional de Proteção de Dados - ANPD: órgão da Administração Pública Federal, cujos papéis e competências estão definidos na LGPD, entre eles: elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação.

Art. 3º O Programa de Governança em Privacidade e Proteção dos Dados Pessoais será coordenado pelo Encarregado de Proteção de Dados Pessoais, que será apoiado por todos os setores do Instituto, tendo livre acesso a todos eles.

Art. 4º O Programa de Governança em Privacidade e Proteção dos Dados Pessoais deverá conter os elementos constantes do art. 50, §2º da LGPD, sendo composto, no mínimo, dos seguintes instrumentos:

I - Termo de Uso;

II - Termo de Consentimento;

III - Inventário de Dados Pessoais;

IV - Orientações do Controlador para o Operador;

V - Plano de Análise de Riscos;

V - Plano de Adequação;

VI - Aviso de Privacidade e Política de Privacidade;

VIII - Política de Cookies;

IX - Plano de Resposta aos Incidentes de Proteção de Dados Pessoais;

X - Relatório de Incidente de Proteção de Dados Pessoais;

XI - Política de Controle de Acessos;

XII - Relatório de Impacto de Proteção de Dados de Pessoais (RIPD);

XIII - Proposta de Cronograma de Identificação e de Mapeamento dos Instrumentos Jurídicos para fins de adequação às leis de proteção de dados pessoais dos órgãos e das entidades; e

XIV - Cronograma de Implementação do Programa.

§1º Para iniciar a implementação do Programa, o Encarregado de Proteção de Dados Pessoais deverá elaborar e publicar, o cronograma previsto no inciso XIV.

§2º Após a elaboração dos instrumentos constantes do caput do art. 4º, estes deverão ser submetidos a apreciação da Diretoria-Executiva e do Conselho de Administração.

Art. 5º As orientações e elementos mínimos para elaborar os instrumentos do Programa encontram- se no Anexo Único desta Instrução Normativa, cujo prazo para elaboração e implementação é de 90 dias após a publicação desta Instrução Normativa.

Art. 6º Os instrumentos relativos ao Programa deverão ser revistos e atualizados anualmente.

Art. 7º Esta Instrução Normativa entrará em vigor na data de sua publicação, revogando-se as disposições em contrário.

ANEXO ÚNICO

A) TERMO DE USO

1. O Termo de Uso é o documento que estabelece as regras e as condições de uso em que ocorrem os tratamentos de dados do Instituto, devendo permitir a publicização das atividades, e suas finalidades específicas, realizadas quando houver tratamento de dados pessoais, especialmente (mas não limitado a) para a execução de políticas públicas, em cumprimento ao art. 23, inciso I, da LGPD.

2. O agente de tratamento de dados pessoais deve se pautar pela obrigação de transparência com o titular de dados, devendo o Termo de Uso informar como as atividades de tratamento de dados atendem às obrigações constantes na LGPD, principalmente aos direitos do titular constantes do art. 9º e do art. 18.

3. O Termo de Uso deve conter, no mínimo, os seguintes elementos:

I - Identificar quais os tratamentos de dados pessoais são realizados pelo controlador, e suas bases legais;

II - Na hipótese de a base legal ser execução de políticas públicas pelo controlador, deve ser destacado o regramento legal em que consta a política pública e a finalidade específica do uso dos dados pessoais, destacando-se a real necessidade de utilização daquele dado para a política pública executada;

III - Identificar eventuais contratos, convênios e termos de cooperação que servem de subsídio para a execução descentralizada da política pública;

IV - Identificar as atribuições do Instituto que justificam a execução daquela finalidade pública;

V - Identificar quais compartilhamentos de dados pessoais são realizados, com quais instituições e quais os regramentos (leis, decretos, portarias, resoluções, convênios, Acordos) que fundamentam tal compartilhamento;

VI - Informar a dispensa do consentimento, na hipótese de tratamento de dados pessoais sensíveis, conforme art. 11, II, b, da LGPD;

VII - Informar o ciclo de vida dos dados;

VIII - Informar os direitos do titular dos dados pessoais;

IX - Informar responsabilidades do usuário e da Administração Pública;

X - Outros requisitos que possam auxiliar no cumprimento das disposições da LGPD, principalmente a garantia dos direitos do titular de dados.

4. O Termo de Uso estará disponível publicamente no sítio eletrônico, atualizando com a periodicidade mínima prevista no art. 6º desta Instrução Normativa.

B) TERMO DE CONSENTIMENTO

1. O Termo de Consentimento é o documento pelo qual o titular dos dados formaliza o consentimento fornecido ao controlador ou operador quando a base legal de tratamento for aquela constante do art. 7º, I, da LGPD.

2. O consentimento é a manifestação livre, informada, inequívoca e, para o caso do tratamento na hipótese do art. 11, I, da LGPD, de forma específica e destacada, pela qual o titular concorda com o tratamento dos seus dados pessoais para uma finalidade determinada.

3. O Termo de Consentimento deve ser redigido de maneira clara, objetiva e, sempre que possível, baseado em linguagem simples, de modo a facilitar a compreensão do titular dos dados.

C) INVENTÁRIO DE DADOS PESSOAIS

1. O Inventário de Dados Pessoais é o documento que consiste no registro interno das operações de tratamento dos dados pessoais realizados pelo Instituto, em cumprimento ao art. 37 da LGPD.

2. O Inventário de Dados Pessoais deve conter, no mínimo, os seguintes elementos:

I - A identificação do processo de negócio/serviço;

II - Os ativos que serão utilizados para fazer o tratamento de dados;

III - Finalidade do tratamento (o que o Instituto faz com o dado pessoal);

IV - Atores envolvidos;

V - Dados pessoais e dados pessoais sensíveis utilizados;

VI - Categoria dos titulares dos dados pessoais;

VII - Origem dos dados;

VIII - Localização e forma de armazenamento;

IX - Base legal de tratamento (art. 7º, 11 e 14 da LGPD);

X - Previsão legal;

XI - Ciclo de vida dos dados pessoais;

XII - Compartilhamentos com terceiros;

XIII - Transferência internacional de dados (art. 33 LGPD); e]

XIV - Medidas de segurança da informação atualmente adotadas.

3. O inventário de dados pessoais deve incluir todas as operações de tratamento de dados pessoais, incluindo dados em meio físico e digital, devendo novos sistemas ou aplicações ou banco de dados já terem suas informações inseridas e atualizadas no inventário.

4. O inventário de dados pessoais deve ser tratado como um diagnóstico do estado da arte de como o tratamento de dados é realizado pelo Instituto, devendo ser o mais completo e detalhado possível, atualizado com periodicidade anual e servir como subsídio para a elaboração do Plano de Análise de Riscos, entre outros instrumentos do Programa.

D) ORIENTAÇÕES DO CONTROLADOR PARA O OPERADOR

1. As Orientações do Controlador para o Operador devem estar contidas em um documento que estabelece as regras para a execução do tratamento de dados pessoais pelos Operadores, em cumprimento ao art. 39, da LGPD.

2. Os contratos, convênios, acordos de cooperação técnica, termos de parceria e demais instrumentos jurídicos congêneres devem prever como um dos seus anexos o documento que contém as orientações específicas para tratamento de dados pessoais fornecidas pelo controlador ao operador.

3. Caso os contratos, convênios, acordos de cooperação técnica, termos de parceria e demais instrumentos jurídicos congêneres não possuam cláusula específica e destacada acerca do tratamento de dados pessoais, devem ser aditados para conter tais cláusulas e para conter as Orientações do Controlador para o Operador.

4. As Orientações do Controlador para o Operador devem conter, no mínimo, os elementos decisórios principais, entre os quais destacam-se a finalidade do tratamento, estipulando os objetivos que justificam a realização do tratamento, a natureza dos dados pessoais tratados, a duração do tratamento, incluindo o estabelecimento de prazo para a eliminação dos dados, entre outros elementos que podem ser considerados essenciais a depender do contexto e das peculiaridades do caso concreto.

E) PLANO DE ANÁLISE DE RISCOS

1. O Plano de Análise de Riscos é o documento que sistematiza a identificação dos riscos incidentes no tratamento de dados pessoais que podem vir a gerar risco às liberdades civis e aos direitos dos titulares de dados, de forma a subsidiar a elaboração do RIPD, em cumprimento ao artigos 5º, XVII, e 38, parágrafo único, da LGPD.

2. O Plano de Análise de Riscos deve conter, no mínimo, os seguintes elementos:

I - Descrição do risco;

II - Fundamentação do risco;

III - Classificação do risco;

IV - Ações para mitigação do risco;

V - Definição do risco residual esperado após a realização das ações de mitigação dos riscos;

VI - Etapa de monitoramento do risco residual; e

VII - Procedimento de comunicação de quaisquer alterações incidentes sobre o(s) risco(s) e/ou os controles instituídos.

3. O Plano de Análise de Riscos deve incluir todas as operações de tratamento de dados pessoais, incluindo dados em meio físico e digital, devendo os novos sistemas ou aplicações ou banco de dados já terem suas informações inseridas e atualizadas no Plano.

4. O Plano de Análise de Riscos deve ser tratado como um diagnóstico do estado da arte de como o tratamento de dados é realizado pelo Instituto, devendo ser o mais completo e detalhado possível, devendo ser atualizado anualmente.

5. O Plano de Análise de Riscos contemplará apenas os riscos ao cumprimento das legislações e melhores práticas de proteção de dados pessoais, não sendo considerados todos os possíveis riscos de segurança da informação incidentes, que serão objeto de regulamentação específica.

F) PLANO DE ADEQUAÇÃO

1. O Plano de Adequação é o documento que contém as diretrizes gerais para uma boa governança e alinhamento às práticas da LGPD, estabelecendo as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais, em cumprimento ao artigo 50 da LGPD.

2. O Plano de Adequação deve conter, no mínimo, os seguintes elementos:

I - Identificar quais as tecnologias, processos e mudanças organizacionais que precisam ser implementadas para garantir o atendimento aos direitos dos titulares de dados pessoais e aos princípios constantes na LGPD;

II - Descrever de que modo serão implementadas as ações de mitigação dos riscos identificados no Plano de Análise de Riscos;

III - Apontar de que forma as medidas de segurança da informação apontadas no Inventário de Dados Pessoais precisam ser aperfeiçoadas e atualizadas para que sejam adotados os controles de segurança adequados para o tratamento dos dados;

IV - Elaborar um cronograma de implementação das medidas identificadas como necessárias à adequação;

V - Adequar os processos de trabalho, serviços e políticas públicas seguindo boas práticas de minimização de dados pessoais, privacidade por padrão e privacidade desde a concepção (privacy by design);

VI - Oferecer elementos para suportar a elaboração do Relatório de Impacto a Proteção de Dados Pessoais (RIPD);

VII - Estabelecer processo de comunicação com a ANPD e com o titular de dados na hipótese de ocorrência de incidentes de proteção de dados pessoais ou vazamento de dados pessoais;

VIII - Indicar de que modo será dada publicidade das informações relativas ao tratamento de dados em veículos de fácil acesso, preferencialmente nos sítios eletrônicos dos órgãos e das entidades;

IX - Indicar de que modo serão atendidas as exigências que vierem a ser estabelecidas pela ANPD, nos termos do art. 23, § 1º, e do art. 27, parágrafo único da LGPD; e

X - Desenvolver plano de capacitação sobre privacidade e proteção de dados pessoais para os servidores do Instituto.

3. O Instituto deverá tornar o seu Plano de Adequação acessível a todos os servidores, conselheiros e membros de colegiados, devendo ser feitos esforços no sentido de capacitar e sensibilizar para a necessidade de realizar as adequações necessárias.

4. O Plano de Adequação deverá ser atualizado anualmente.

G) POLÍTICA DE PRIVACIDADE E AVISO DE PRIVACIDADE

1. A Política de Privacidade é o documento interno pelo qual o controlador informa aos seus agentes públicos a forma como realiza os tratamentos de dados pessoais de um dado serviço ou aplicação ou banco de dados, sendo um documento para uso interno do órgão ou entidade.

2. Aviso de Privacidade é o documento externo pelo qual o controlador transparece ao usuário do serviço ou da aplicação ou do banco de dados a forma como realiza os tratamentos de dados pessoais, e como o Poder Público fornecerá privacidade ao usuário, em cumprimento ao art, 23, I, da LGPD, explicitando, ainda, de que modo são garantidos os direitos do titular constantes do art. 9º e 18.

3. O Aviso de Privacidade deve conter, no mínimo, os seguintes elementos:

I - Identificação dos Controladores;

II - Identificação dos Operadores (se cabível);

III - Identificação do Encarregado;

IV - Identificação de quais dados são tratados;

V - Identificação de como os dados são coletados;

VI - Quais os tratamentos realizados e para qual finalidade;

VII - Quais compartilhamentos de dados pessoais são realizados, com quem e em razão de qual finalidade; e

VIII - Tratamento posterior dos dados para outras finalidades.

4. A Política de Privacidade deve conter, no mínimo, os seguintes elementos:

I - Identificação dos Controladores;

II - Identificação dos Operadores;

III - Identificação dos Encarregados;

IV - Identificação de quais dados são tratados;

V - Identificação de como os dados são coletados;

VI - Quais os tratamentos realizados e para qual finalidade;

VII - Quais compartilhamentos de dados pessoais são realizados, com quem e em razão de qual finalidade;

VIII - Regras de segurança da informação dos dados pessoais;

IX - Tratamento posterior dos dados para outras finalidades; e

X - Transferência internacional de dados.

5. O Aviso de Privacidade estará disponível publicamente no sítio eletrônico, atualizando anualmente, sendo desnecessária a publicação da Política de Privacidade.

H) POLÍTICA DE COOKIES

1. A Política de Cookies é o documento informativo pelo qual o usuário deverá ser informado sobre quais dados são coletados e armazenados ao navegar por uma das páginas de titularidade do Instituto, e para qual funcionalidade, além de quais medidas de segurança são implementadas em seu uso.

2. A Política de Cookies deve conter, no mínimo, os seguintes elementos:

I - Quais cookies são utilizados (cookies proprietários e de terceiros);

II - Quais os dados são coletados pelos cookies;

III - Qual a finalidade do uso de cookies;

IV - Como o usuário pode obter mais informações sobre os cookies de terceiros utilizados no serviço.

3. Além da elaboração da Política de Cookies, deve ser disponibilizado no site um banner ou aviso para dar ciência ao usuário, com o mapeamento e discriminação dos cookies, permitindo que o usuário possa fazer escolhas e possa definir, sistemicamente, o que acontece quando se recusa um ou outro grupo.

4. O banner ou aviso para dar ciência ao usuário deve ser redigido em português.

5. A Política de Cookies estará disponível publicamente nos sítios eletrônicos.

I) PLANO DE RESPOSTA AOS INCIDENTES DE PROTEÇÃO DE DADOS PESSOAIS

1. O Plano de Resposta aos Incidentes de Proteção de Dados Pessoais é o documento que estabelece quais protocolos deverão ser seguidos em caso de ocorrência de incidentes, em atendimento ao art. 50, § 2º, II, g, da LGPD.

2. O Plano de Resposta deverá estabelecer quais as medidas de resposta para a hipótese de ocorrência dos riscos contidos no Plano de Análise de Riscos, estabelecendo medidas de curto, médio e longo prazos, recursos disponibilizados para a resposta, atores responsáveis e de que modo serão remediados os danos causados pelos incidentes.

3. Todos os servidores, estagiários, conselheiros e membros de colegiados do Instituto que realizam tratamento de dados pessoais devem tomar ciência das medidas contidas no Plano de Resposta.

J) RELATÓRIO DE INCIDENTE DE PROTEÇÃO DE DADOS PESSOAIS

1. O Relatório de Incidentes de Proteção de Dados Pessoais é o documento que informa detalhadamente sobre o incidente que ocorreu, e de que modo a comunicação deverá ser feita, em atendimento ao art. 50, § 2º , II, g, da LGPD.

2. O Relatório de Incidentes deverá comunicar detalhadamente o incidente, que deverá ser feita em prazo razoável, conforme definido pela ANPD, e deverá mencionar, no mínimo

I - a descrição da natureza dos dados pessoais afetados;

II - as informações sobre os titulares envolvidos;

III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

IV - os riscos relacionados ao incidente;

V - os motivos da demora, no caso de a comunicação não ter sido imediata; e

VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

3. O Encarregado deve elaborar o Relatório, que deve ser validado pelo Diretor-Presidente previamente ao envio à ANPD.

4. O Relatório em sua versão final deve ser tornado público, devendo ser excluídas as informações sobre os titulares envolvidos.

K) POLÍTICA DE CONTROLE DE ACESSOS

1. A Política de Controle de Acesso tem como objetivo, habilitar o acesso de serviços e de sistemas de responsabilidade do Instituto, apenas ao usuário devidamente autorizado.

2. A Política de Controle de acesso deverá, no mínimo:

I - definir claramente as responsabilidades/papéis dos intervenientes desse processo;

II - atender ao princípio do menor privilégio; e

III - possuir perfis de acesso bem definidos e regras claras para habilitação, suspensão e revogação de direitos de acesso e que trate:

a) o controle de acesso aos registros de eventos (logs);
b) o controle de acesso às configurações dos sistemas (perfis administrativos);
c) o controle de acesso às cópias de segurança;
d) o controle de acesso às informações sensíveis e situações que requeiram a propriedade do não- repúdio e o acesso via certificado digital; e
e) os processos formais para a solicitação de acesso aos perfis dos sistemas, permitindo verificar, inclusive, os autorizadores que concederam as permissões ao usuário.

3. O Instituto deve realizar periodicamente a revisão dos direitos de acesso e da sua Política de Controle de Acesso.

4. Todos os servidores, estagiários, conselheiros e membros de colegiados do Instituto que realizam tratamento de dados pessoais devem tomar ciência das medidas contidas na Política de Controle de Acesso.

L) RELATÓRIO DE IMPACTO DE PROTEÇÃO DE DADOS PESSOAIS (RIPD)

1. O Relatório de Impacto à Proteção de Dados Pessoais (RIPD) é o documento que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco, em atendimento ao art. 5º, inciso XVII, da LGPD.

2. O RIPD deverá conter elementos e informações de todos os instrumentos constantes desta Instrução Normativa, além de informações adicionais que o encarregado de dados julgar pertinentes.

3. A ANPD poderá solicitar aos agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público.

4. A elaboração do Relatório de Impacto à Proteção de Dados Pessoais deverá seguir as orientações e metodologia divulgadas pela ANPD.

M) PROPOSTA DE CRONOGRAMA DE IDENTIFICAÇÃO E MAPEAMENTO DOS INSTRUMENTOS JURÍDICOS PARA FINS DE ADEQUAÇÃO AS LEIS DE PROTEÇÃO DE DADOS PESSOAIS DO INSTITUTO

1. O controlador deverá identificar os seus contratos, convênios, Termos de Cooperação, Acordos de Resultados, editais de licitação e demais documentos jurídicos congêneres em que se realize o tratamento ou o compartilhamento de dados pessoais e que possam precisar de futuras modificações para serem adequados à LGPD.

2. O Encarregado deverá elaborar um cronograma para identificar e mapear os instrumentos jurídicos para fins de adequação às leis de proteção de dados pessoais.

N) CRONOGRAMA DE IMPLEMENTAÇÃO DO PROGRAMA

1. O Instituto elaborará um cronograma de implementação dos instrumentos do Programa, que demonstrará o comprometimento do agente de tratamento de dados em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais, conforme art. 50, §2º, inciso I, alínea "a".

2. O cronograma de implementação deverá conter as etapas de elaboração dos instrumentos, informando, sempre que possível, prazos e responsáveis, cabendo revisão dos prazos, desde que justificada.

3. O cronograma de implementação deve ser tornado público no site do Instituto.

Assinaturas do Documento

Documento Assinado Eletronicamente por **ROSELI RODRIGUES DE NOVAES DA SILVA - DIRETORA ADMINISTRATIVA E FINANCEIRA** , **CPF:** 037.62*.**7-*1 em **27/12/2023 08:54:19**, Cód. Autenticidade da Assinatura: **0894.7V54.019E.2253.3300**, Com fundamento na Lei Nº 14.063, de 23 de Setembro de 2020.

Documento Assinado Eletronicamente por **ALUIZIO MACENA DA COSTA - DIRETOR PREVIDENCIÁRIO** , **CPF:** 556.05*.**7-*4 em **22/12/2023 15:36:39**, Cód. Autenticidade da Assinatura: **1537.3Z36.639Z.4242.0340**, Com fundamento na Lei Nº 14.063, de 23 de Setembro de 2020.

Documento Assinado Eletronicamente por **HUGO LOPES DE OLIVEIRA - DIRETOR-PRESIDENTE**, **CPF:** 142.75*.**7-*0 em **22/12/2023 12:30:52**, Cód. Autenticidade da Assinatura: **1248.3X30.452A.355Z.6868**, Com fundamento na Lei Nº 14.063, de 23 de Setembro de 2020.

Informações do Documento

ID do Documento: **25A.AE4** - Tipo de Documento: **INSTRUÇÃO NORMATIVA - Nº 11/2023**.

Elaborado por **HUGO LOPES DE OLIVEIRA**, **CPF:** 142.75*.**7-*0 , em **22/12/2023 12:30:52**, contendo 4.088 palavras.

Código de Autenticidade deste Documento: 12E1.7W30.752U.U216.0700

A autenticidade do documento pode ser conferida no site: **https://zeropapel.seroprevi.rj.gov.br/verdocumento**

Art. 4º A Prova de Vida será realizada no mês de aniversário do aposentado ou pensionista, preferencialmente através do aplicativo Gov.br disponibilizado pelo Governo Federal.
Art. 5º Quem não conseguir ou não desejar realizar a Prova de Vida pelo aplicativo Gov.br deverá obrigatoriamente comparecer ao Instituto no mês do seu aniversário, das 09h às 16h, no dia e horário de sua escolha.
Art. 6º E obrigatória a apresentação de documento original com foto para os que optarem pela Prova de Vida presencial conforme art. 5º.
Art. 7º Os pensionistas menores de dezoito anos que realizarem a Prova de Vida presencial deverão obrigatoriamente se fazer presentes junto aos seus responsáveis.
Art. 8º E expressamente vedada a realização de Prova de Vida através de procuração.
Art. 9º Aos aposentados e pensionistas que possuem incapacidade de locomoção é assegurado o direito de realização da Prova de Vida através da visita em sua residência de equipe de servidores do Instituto.
Parágrafo único - Nos casos de incapacidade de locomoção, o aposentado, pensionista ou seu Procurador deverá entrar em contato com o Instituto para agendamento da visita da equipe de servidores.
Art. 10 A não realização da Prova de Vida no mês de aniversário implicará na suspensão do pagamento do benefício de aposentadoria ou pensão no dia 10 do mês subsequente ao do aniversário, até que haja a regularização da situação.
Parágrafo único - Após regularizada a situação, o pagamento será liberado em até dois dias úteis.
Art. 11 Esta Instrução Normativa entrará em vigor na data de sua publicação, revogando-se as disposições em contrário, em especial a Instrução Normativa nº 02 de 2022.

HUGO LOPES DE OLIVEIRA
ROSELI RODRIGUES DE NOVAES DA SILVA
ALUIZIO MACENA DA COSTA

INSTRUÇAO NORMATIVA Nº 11 DE 22 DE DEZEMBRO DE 2023

Institui o Programa de Governança em Privacidade e Proteção dos Dados Pessoais no âmbito do Instituto, em conformidade com o art. 50, § 2º da Lei Geral de Proteção de Dados Pessoais - LGPD.

A DIRETORIA-EXECUTIVA do SEROPREVI, usando das atribuições que lhe são conferidas por lei, e

CONSIDERANDO o disposto no inciso LXXIX, do art. 5º, da Constituição da República Federativa do Brasil de 1988, incluído pela Emenda Constitucional nº 115, de 10 de janeiro de 2022, o qual estabelece que é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais;

CONSIDERANDO o disposto na Lei Federal nº 13.709 de 2018, Lei Geral de Proteção de Dados Pessoais - LGPD;

CONSIDERANDO a deliberação do Conselho de Administração na 54ª Reunião Ordinária.

R E S O L V E:

Art. 1º Instituir o Programa de Governança em Privacidade e Proteção dos Dados Pessoais que será implementado pelos agentes de tratamento de dados pessoais no âmbito do Instituto, em conformidade com o art. 50, § 2º da Lei Geral de Proteção de Dados Pessoais - LGPD.

Parágrafo único. A elaboração do Programa é atribuição do Gabinete do Diretor-Presidente, devendo obedecer os dispostos na LGPD e as diretrizes da Autoridade Nacional de Proteção de Dados - ANPD, além dos demais regramentos sobre o tema.

Art. 2º Para fins desta Resolução considera-se:

I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

II - 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;

III - titular dos dados: pessoa natural a quem se referem os dados pessoais que são objetos de tratamento;

IV - agentes de tratamento: o controlador e o operador. Os indivíduos subordinados ou vinculados, como os funcionários, os servidores públicos ou as equipes de trabalho de um órgão ou de uma entidade, que atuam sob o poder diretivo do agente de tratamento não são considerados como controladores ou operadores;

V - controlador: o Instituto, a quem compete as principais decisões relativas aos elementos essenciais para o cumprimento da finalidade do tratamento de dados pessoais, bem como a definição da natureza dos dados pessoais tratados e a duração do tratamento;

VI - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais para a finalidade e instruções previamente estabelecidas pelo controlador. Em sendo pessoa jurídica, os empregados, administradores, sócios, servidores e outras pessoas naturais que a integram e cujos atos expressam a atuação desta, não são considerados como operadores.

VII - suboperador: é o contratado pelo operador, após a autorização formal do controlador, para auxiliar no tratamento de dados pessoais em nome do controlador, podendo ser equiparado ao operador perante a LGPD em relação às atividades que foi contratado para executar, no que se refere às responsabilidades.

VIII - encarregado de proteção de dados pessoais: pessoa indicada, mediante ato formal, pelo controlador e pelo operador, cuja identidade e informações de contato estarão divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador e do operador, sendo responsável por atuar como canal de comunicação entre o controlador, o operador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados - ANPD;

IX - tratamento de dados pessoais: 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 - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada, não sendo a única nem a principal base legal possível para viabilizar o tratamento de dados pessoais;

XI - incidente de segurança com dados pessoais: qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais;

XII - Autoridade Nacional de Proteção de Dados - ANPD: órgão da Administração Pública Federal, cujos papéis e competências estão definidos na LGPD, entre eles: elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação.

Art. 3º O Programa de Governança em Privacidade e Proteção dos Dados Pessoais será coordenado pelo Encarregado de Proteção de Dados Pessoais, que será apoiado por todos os setores do Instituto, tendo livre acesso a todos eles.

Art. 4º O Programa de Governança em Privacidade e Proteção dos Dados Pessoais deverá conter os elementos constantes do art. 50, §2º da LGPD, sendo composto, no mínimo, dos seguintes instrumentos:

I - Termo de Uso;

II - Termo de Consentimento;

III - Inventário de Dados Pessoais;

IV - Orientações do Controlador para o Operador;

V - Plano de Análise de Riscos;

V - Plano de Adequação;

VI - Aviso de Privacidade e Política de Privacidade;

VIII - Política de Cookies;

IX - Plano de Resposta aos Incidentes de Proteção de Dados Pessoais;

X - Relatório de Incidente de Proteção de Dados Pessoais;

XI - Política de Controle de Acessos;

XII - Relatório de Impacto de Proteção de Dados de Pessoais (RIPD);

XIII - Proposta de Cronograma de Identificação e de Mapeamento dos Instrumentos Jurídicos para fins de adequação às leis de proteção de dados pessoais dos órgãos e das entidades; e

XIV - Cronograma de Implementação do Programa.

§1° Para iniciar a implementação do Programa, o Encarregado de Proteção de Dados Pessoais deverá elaborar e publicar, o cronograma previsto no inciso XIV.

§2° Após a elaboração dos instrumentos constantes do caput do art. 4°, estes deverão ser submetidos a apreciação da Diretoria-Executiva e do Conselho de Administração.

Art. 5° As orientações e elementos mínimos para elaborar os instrumentos do Programa encontram- se no Anexo Unico desta Instrução Normativa, cujo prazo para elaboração e implementação é de 90 dias após a publicação desta Instrução Normativa.

Art. 6° Os instrumentos relativos ao Programa deverão ser revistos e atualizados anualmente.

Art. 7° Esta Instrução Normativa entrará em vigor na data de sua publicação, revogando-se as disposições em contrário.

ANEXO UNICO

A) TERMO DE USO

1. O Termo de Uso é o documento que estabelece as regras e as condições de uso em que ocorrem os tratamentos de dados do Instituto, devendo permitir a publicização das atividades, e suas finalidades específicas, realizadas quando houver tratamento de dados pessoais, especialmente (mas não limitado a) para a execução de políticas públicas, em cumprimento ao art. 23, inciso I, da LGPD.

2. O agente de tratamento de dados pessoais deve se pautar pela obrigação de transparência com o titular de dados, devendo o Termo de Uso informar como as atividades de tratamento de dados atendem às obrigações constantes na LGPD, principalmente aos direitos do titular constantes do art. 9° e do art. 18.

3. O Termo de Uso deve conter, no mínimo, os seguintes elementos:

I - Identificar quais os tratamentos de dados pessoais são realizados pelo controlador, e suas bases legais;

II - Na hipótese de a base legal ser execução de políticas públicas pelo controlador, deve ser destacado o regramento legal em que consta a política pública e a finalidade específica do uso dos dados pessoais, destacando-se a real necessidade de utilização daquele dado para a política pública executada;

III - Identificar eventuais contratos, convênios e termos de cooperação que servem de subsídio para a execução descentralizada da política pública;

IV - Identificar as atribuições do Instituto que justificam a execução daquela finalidade pública;

V - Identificar quais compartilhamentos de dados pessoais são realizados, com quais instituições e quais os regramentos (leis, decretos, portarias, resoluções, convênios, Acordos) que fundamentam tal compartilhamento;

2. O Inventário de Dados Pessoais deve conter, no mínimo, os seguintes elementos:

I - A identificação do processo de negócio/serviço;

II - Os ativos que serão utilizados para fazer o tratamento de dados;

III - Finalidade do tratamento (o que o Instituto faz com o dado pessoal);

IV - Atores envolvidos;

V - Dados pessoais e dados pessoais sensíveis utilizados;

VI - Categoria dos titulares dos dados pessoais;

VII - Origem dos dados;

VIII - Localização e forma de armazenamento;

IX - Base legal de tratamento (art. 7°, 11 e 14 da LGPD);

X - Previsão legal;

XI - Ciclo de vida dos dados pessoais;

XII - Compartilhamentos com terceiros;

XIII - Transferência internacional de dados (art. 33 LGPD); e]

XIV - Medidas de segurança da informação atualmente adotadas.

3. O inventário de dados pessoais deve incluir todas as operações de tratamento de dados pessoais, incluindo dados em meio físico e digital, devendo novos sistemas ou aplicações ou banco de dados já terem suas informações inseridas e atualizadas no inventário.

4. O inventário de dados pessoais deve ser tratado como um diagnóstico do estado da arte de como o tratamento de dados é realizado pelo Instituto, devendo ser o mais completo e detalhado possível, atualizado com periodicidade anual e servir como subsídio para a elaboração do Plano de Análise de Riscos, entre outros instrumentos do Programa.

D) ORIENTAÇOES DO CONTROLADOR PARA O OPERADOR

1. As Orientações do Controlador para o Operador devem estar contidas em um documento que estabelece as regras para a execução do tratamento de dados pessoais pelos Operadores, em cumprimento ao art. 39, da LGPD.

2. Os contratos, convênios, acordos de cooperação técnica, termos de parceria e demais instrumentos jurídicos congêneres devem prever como um dos seus anexos o documento que contém as orientações específicas para tratamento de dados pessoais fornecidas pelo controlador ao operador.

3. Caso os contratos, convênios, acordos de cooperação técnica, termos de parceria e demais instrumentos jurídicos congêneres não possuam cláusula específica e destacada acerca do tratamento de dados pessoais, devem ser aditados para conter tais cláusulas e para conter as Orientações do Controlador para o Operador.

4. As Orientações do Controlador para o Operador devem conter, no mínimo, os elementos decisórios principais, entre os quais destacam-se a finalidade do tratamento, estipulando os objetivos que justificam a realização do tratamento, a natureza dos dados pessoais tratados, a duração do tratamento, incluindo o estabelecimento de prazo para a eliminação dos dados, entre outros elementos que podem ser considerados essenciais a depender do contexto e das peculiaridades do caso concreto.

E) PLANO DE ANALISE DE RISCOS

1. O Plano de Análise de Riscos é o documento que sistematiza a identificação dos riscos incidentes no tratamento de dados pessoais que podem vir a gerar risco às liberdades civis e aos direitos dos titulares de dados, de forma a subsidiar a elaboração do RIPD, em cumprimento ao artigos 5°, XVII, e 38, parágrafo único, da LGPD.

2. O Plano de Análise de Riscos deve conter, no mínimo, os seguintes elementos:

I - Descrição do risco;

II - Fundamentação do risco;

III - Classificação do risco;

IV - Ações para mitigação do risco;

V - Definição do risco residual esperado após a realização das ações de mitigação dos riscos;

VI - Etapa de monitoramento do risco residual; e

VII - Procedimento de comunicação de quaisquer alterações incidentes sobre o(s) risco(s) e/ou os controles instituídos.

3. O Plano de Análise de Riscos deve incluir todas as operações de tratamento de dados pessoais, incluindo dados em meio físico e digital, devendo os novos sistemas ou aplicações ou banco de dados já terem suas informações inseridas e atualizadas no Plano.

4. O Plano de Análise de Riscos deve ser tratado como um diagnóstico do estado da arte de como o tratamento de dados é realizado pelo Instituto, devendo ser o mais completo e detalhado possível, devendo ser atualizado anualmente.

5. O Plano de Análise de Riscos contemplará apenas os riscos ao cumprimento das legislações e melhores práticas de proteção de dados pessoais, não sendo considerados todos os possíveis riscos de segurança da informação incidentes, que serão objeto de regulamentação específica.

F) PLANO DE ADEQUAÇAO

1. O Plano de Adequação é o documento que contém as diretrizes gerais para uma boa governança e alinhamento às práticas da LGPD, estabelecendo as condições de

organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais, em cumprimento ao artigo 50 da LGPD.

2. O Plano de Adequação deve conter, no mínimo, os seguintes elementos:

I - Identificar quais as tecnologias, processos e mudanças organizacionais que precisam ser implementadas para garantir o atendimento aos direitos dos titulares de dados pessoais e aos princípios constantes na LGPD;

II - Descrever de que modo serão implementadas as ações de mitigação dos riscos identificados no Plano de Análise de Riscos;

III - Apontar de que forma as medidas de segurança da informação apontadas no Inventário de Dados Pessoais precisam ser aperfeiçoadas e atualizadas para que sejam adotados os controles de segurança adequados para o tratamento dos dados;

IV - Elaborar um cronograma de implementação das medidas identificadas como necessárias à adequação;

V - Adequar os processos de trabalho, serviços e políticas públicas seguindo boas práticas de minimização de dados pessoais, privacidade por padrão e privacidade desde a concepção (privacy by design);

VI - Oferecer elementos para suportar a elaboração do Relatório de Impacto a Proteção de Dados Pessoais (RIPD);

VII - Estabelecer processo de comunicação com a ANPD e com o titular de dados na hipótese de ocorrência de incidentes de proteção de dados pessoais ou vazamento de dados pessoais;

VIII - Indicar de que modo será dada publicidade das informações relativas ao tratamento de dados em veículos de fácil acesso, preferencialmente nos sítios eletrônicos dos órgãos e das entidades;

IX - Indicar de que modo serão atendidas as exigências que vierem a ser estabelecidas pela ANPD, nos termos do art. 23, § 1º, e do art. 27, parágrafo único da LGPD; e

X - Desenvolver plano de capacitação sobre privacidade e proteção de dados pessoais para os servidores do Instituto.

3. O Instituto deverá tornar o seu Plano de Adequação acessível a todos os servidores, conselheiros e membros de colegiados, devendo ser feitos esforços no sentido de capacitar e sensibilizar para a necessidade de realizar as adequações necessárias.

4. O Plano de Adequação deverá ser atualizado anualmente.

G) POLITICA DE PRIVACIDADE E AVISO DE PRIVACIDADE

1. A Política de Privacidade é o documento interno pelo qual o controlador informa aos seus agentes públicos a forma como realiza os tratamentos de dados pessoais de um dado serviço ou aplicação ou banco de dados, sendo um documento para uso interno do órgão ou entidade.

2. Aviso de Privacidade é o documento externo pelo qual o controlador transparece ao usuário do serviço ou da aplicação ou do banco de dados a forma como realiza os tratamentos de dados pessoais, e como o Poder Público fornecerá privacidade ao usuário, em cumprimento ao art, 23, I, da LGPD, explicitando, ainda, de que modo são garantidos os direitos do titular constantes do art. 9º e 18.

3. O Aviso de Privacidade deve conter, no mínimo, os seguintes elementos:

I - Identificação dos Controladores;

II - Identificação dos Operadores (se cabível);

III - Identificação do Encarregado;

IV - Identificação de quais dados são tratados;

V - Identificação de como os dados são coletados;

VI - Quais os tratamentos realizados e para qual finalidade;

VII - Quais compartilhamentos de dados pessoais são realizados, com quem e em razão de qual finalidade; e

VIII - Tratamento posterior dos dados para outras finalidades.

4. A Política de Privacidade deve conter, no mínimo, os seguintes elementos:

I - Identificação dos Controladores;

II - Identificação dos Operadores;

III - Identificação dos Encarregados;

IV - Identificação de quais dados são tratados;

V - Identificação de como os dados são coletados;

VI - Quais os tratamentos realizados e para qual finalidade;

VII - Quais compartilhamentos de dados pessoais são realizados, com quem e em razão de qual finalidade;

VIII - Regras de segurança da informação dos dados pessoais;

IX - Tratamento posterior dos dados para outras finalidades; e

X - Transferência internacional de dados.

5. O Aviso de Privacidade estará disponível publicamente no sítio eletrônico, atualizando anualmente, sendo desnecessária a publicação da Política de Privacidade.

H) POLITICA DE COOKIES

1. A Política de Cookies é o documento informativo pelo qual o usuário deverá ser informado sobre quais dados são coletados e armazenados ao navegar por uma das páginas de titularidade do Instituto, e para qual funcionalidade, além de quais medidas de segurança são implementadas em seu uso.

2. A Política de Cookies deve conter, no mínimo, os seguintes elementos:

I - Quais cookies são utilizados (cookies proprietários e de terceiros);

II - Quais os dados são coletados pelos cookies;

III - Qual a finalidade do uso de cookies;

IV - Como o usuário pode obter mais informações sobre os cookies de terceiros utilizados no serviço.

3. Além da elaboração da Política de Cookies, deve ser disponibilizado no site um banner ou aviso para dar ciência ao usuário, com o mapeamento e discriminação dos cookies, permitindo que o usuário possa fazer escolhas e possa definir, sistemicamente, o que acontece quando se recusa um ou outro grupo.

4. O banner ou aviso para dar ciência ao usuário deve ser redigido em português.

5. A Política de Cookies estará disponível publicamente nos sítios eletrônicos.

I) PLANO DE RESPOSTA AOS INCIDENTES DE PROTEÇAO DE DADOS PESSOAIS

1. O Plano de Resposta aos Incidentes de Proteção de Dados Pessoais é o documento que estabelece quais protocolos deverão ser seguidos em caso de ocorrência de incidentes, em atendimento ao art. 50, § 2º, II, g, da LGPD.

2. O Plano de Resposta deverá estabelecer quais as medidas de resposta para a hipótese de ocorrência dos riscos contidos no Plano de Análise de Riscos, estabelecendo medidas de curto, médio e longo prazos, recursos disponibilizados para a resposta, atores responsáveis e de que modo serão remediados os danos causados pelos incidentes.

3. Todos os servidores, estagiários, conselheiros e membros de colegiados do Instituto que realizam tratamento de dados pessoais devem tomar ciência das medidas contidas no Plano de Resposta.

J) RELATORIO DE INCIDENTE DE PROTEÇAO DE DADOS PESSOAIS

1. O Relatório de Incidentes de Proteção de Dados Pessoais é o documento que informa detalhadamente sobre o incidente que ocorreu, e de que modo a comunicação deverá ser feita, em atendimento ao art. 50, § 2º , II, g, da LGPD.

2. O Relatório de Incidentes deverá comunicar detalhadamente o incidente, que deverá ser feita em prazo razoável, conforme definido pela ANPD, e deverá mencionar, no mínimo

I - a descrição da natureza dos dados pessoais afetados;

II - as informações sobre os titulares envolvidos;

III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

IV - os riscos relacionados ao incidente;

V - os motivos da demora, no caso de a comunicação não ter sido imediata; e

VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

3. O Encarregado deve elaborar o Relatório, que deve ser validado pelo Diretor-Presidente previamente ao envio à ANPD.

4. O Relatório em sua versão final deve ser tornado público, devendo ser excluídas as informações sobre os titulares envolvidos.

K) POLITICA DE CONTROLE DE ACESSOS

1. A Política de Controle de Acesso tem como objetivo, habilitar o acesso de serviços e de sistemas de responsabilidade do Instituto, apenas ao usuário devidamente autorizado.

2. A Política de Controle de acesso deverá, no mínimo:

I - definir claramente as responsabilidades/papéis dos intervenientes desse processo;

II - atender ao princípio do menor privilégio; e

III - possuir perfis de acesso bem definidos e regras claras para habilitação, suspensão e revogação de direitos de acesso e que trate:

a) o controle de acesso aos registros de eventos (logs);
b) o controle de acesso às configurações dos sistemas (perfis administrativos);
c) o controle de acesso às cópias de segurança;
d) o controle de acesso às informações sensíveis e situações que requeiram a propriedade do não- repúdio e o acesso via certificado digital; e
e) os processos formais para a solicitação de acesso aos perfis dos sistemas, permitindo verificar, inclusive, os autorizadores que concederam as permissões ao usuário.

3. O Instituto deve realizar periodicamente a revisão dos direitos de acesso e da sua Política de Controle de Acesso.

4. Todos os servidores, estagiários, conselheiros e membros de colegiados do Instituto que realizam tratamento de dados pessoais devem tomar ciência das medidas contidas na Política de Controle de Acesso.

L) RELATORIO DE IMPACTO DE PROTEÇAO DE DADOS PESSOAIS (RIPD)

1. O Relatório de Impacto à Proteção de Dados Pessoais (RIPD) é o documento que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco, em atendimento ao art. 5º, inciso XVII, da LGPD.

2. O RIPD deverá conter elementos e informações de todos os instrumentos constantes desta Instrução Normativa, além de informações adicionais que o encarregado de dados julgar pertinentes.

3. A ANPD poderá solicitar aos agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público.

4. A elaboração do Relatório de Impacto à Proteção de Dados Pessoais deverá seguir as orientações e metodologia divulgadas pela ANPD.

M) PROPOSTA DE CRONOGRAMA DE IDENTIFICAÇAO E MAPEAMENTO DOS INSTRUMENTOS JURIDICOS PARA FINS DE ADEQUAÇAO AS LEIS DE PROTEÇAO DE DADOS PESSOAIS DO INSTITUTO

1. O controlador deverá identificar os seus contratos, convênios, Termos de Cooperação, Acordos de Resultados, editais de licitação e demais documentos jurídicos congêneres em que se realize o tratamento ou o compartilhamento de dados pessoais e que possam precisar de futuras modificações para serem adequados à LGPD.

2. O Encarregado deverá elaborar um cronograma para identificar e mapear os instrumentos jurídicos para fins de adequação às leis de proteção de dados pessoais.

N) CRONOGRAMA DE IMPLEMENTAÇAO DO PROGRAMA

1. O Instituto elaborará um cronograma de implementação dos instrumentos do Programa, que demonstrará o comprometimento do agente de tratamento de dados em adotar

processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais, conforme art. 50, §2º, inciso I, alínea "a".

2. O cronograma de implementação deverá conter as etapas de elaboração dos instrumentos, informando, sempre que possível, prazos e responsáveis, cabendo revisão dos prazos, desde que justificada.

3. O cronograma de implementação deve ser tornado público no site do Instituto.

HUGO LOPES DE OLIVEIRA
ROSELI RODRIGUES DE NOVAES DA SILVA
ALUIZIO MACENA DA COSTA

ATOS DO CONSELHO DE ADMINISTRAÇAO

ERRATA REFERENTE A ATA DA 54ª REUNIAO ORDINARIA DO CONSELHO DE ADMINISTRAÇAO

Onde se lê: "Aos trinta dias do mês de novembro do ano de dois mil e vinte e três, às onze horas e nove minutos, estiveram presentes em Reunião Ordinária Virtual os conselheiros Hugo Lopes de Oliveira (Presidente), Andréa Sani Braga da Silva (Vice-Presidente), Irenilva Silva de Souza Cardoso, Edison Rosa Alves Junior, Tiago Peixoto da Silva para tratarem da seguinte pauta..."

Leia-se: " Aos vinte dias do mês de dezembro do ano de dois mil e vinte e três, às onze horas e nove minutos, estiveram presentes em Reunião Ordinária Virtual os conselheiros Hugo Lopes de Oliveira (Presidente), Andréa Sani Braga da Silva (Vice-Presidente), Irenilva Silva de Souza Cardoso, Edison Rosa Alves Junior, Tiago Peixoto da Silva para tratarem da seguinte pauta..."

HUGO LOPES DE OLIVEIRA
ANDREA SANI BRAGA DA SILVA
IRENILVA SILVA DE SOUZA CARDOSO
EDISON ROSA ALVES JUNIOR
TIAGO PEIXOTO DA SILVA
Larissa Ribeiro Moreira Oliveira