Boletim de Serviço Eletrônico em 23/08/2023
DOU de 23/08/2023, seção 1, página 69/72

INSTITUTO NACIONAL DO SEGURO SOCIAL

RESOLUÇÃO CEGOV/INSS Nº 32, DE 15 DE AGOSTO DE 2023

Aprova o Programa de Governança em Privacidade.

O **COMITÊ ESTRATÉGICO DE GOVERNANÇA DO INSTITUTO NACIONAL DO SEGURO SOCIAL – CEGOV/INSS**, no uso das atribuições que lhe confere a Portaria nº 3.213/PRES/INSS, de 10 de dezembro de 2019, e considerando o contido no Processo Administrativo nº 35014.107438/2023-48,

RESOLVE:

Art. 1º Aprovar, nos termos do Anexo, o Programa de Governança em Privacidade, que tem por objetivo fortalecer a cultura de proteção e tratamento dos dados pessoais dos cidadãos, a fim de que as atribuições constitucionais determinadas ao INSS possam ser exercidas com excelência, atendendo aos preceitos da Lei Geral de Proteção de Dados, bem como aos demais instrumentos normativos vigentes.

Parágrafo único. O Programa de que trata o **caput** encontra-se em conformidade com as diretrizes estabelecidas pela Secretaria de Governo Digital, por meio dos Guias de Elaboração divulgados.

Art. 2º Esta Resolução entra em vigor em 1º de setembro de 2023.

ALESSANDRO ANTONIO STEFANUTTO
Presidente

ANDRÉ PAULO FÉLIX FIDELIS
Diretor de Benefícios e Relacionamento com o Cidadão

SANDRA CRISTINA CARDOSO DE SOUZA LUNA
Diretora de Gestão de Pessoas
Substituta

DÉBORA APARECIDA ANDRADE FLORIANO
Diretora de Orçamento, Finanças e Logística
Substituta

ANA CAROLINA TIETZ
Diretora de Governança, Planejamento e Inovação

AILTON NUNES DE MATOS JÚNIOR
Diretor de Tecnologia da Informação

Documento assinado eletronicamente por **SANDRA CRISTINA CARDOSO DE SOUZA LUNA**, **Diretor(a) de Gestão de Pessoas Substituto(a)**, em 15/08/2023, às 17:35, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 .

Documento assinado eletronicamente por **DEBORA APARECIDA ANDRADE FLORIANO**, **Diretor(a) de Orçamento, Finanças e Logística Substituto(a)**, em 15/08/2023, às 18:00, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **ALESSANDRO ANTONIO STEFANUTTO**, **Presidente**, em 15/08/2023, às 18:02, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 .

Documento assinado eletronicamente por **ANA CAROLINA TIETZ**, **Diretor(a) de Governança, Planejamento e Inovação**, em 15/08/2023, às 18:10, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 .

Documento assinado eletronicamente por **ANDRE PAULO FELIX FIDELIS**, **Diretor(a) de Benefícios e Relacionamento com o Cidadão**, em 15/08/2023, às 18:34, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 .

Documento assinado eletronicamente por **AILTON NUNES DE MATOS JUNIOR**, **Diretor(a) de Tecnologia da Informação**, em 15/08/2023, às 18:35, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 .

A autenticidade deste documento pode ser conferida no site https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **12733284** e o código CRC **122E3D32**.

ANEXO

RESOLUÇÃO CEGOV/INSS Nº 32, DE 15 DE AGOSTO DE 2023

PROGRAMA DE GOVERNANÇA EM PRIVACIDADE

1. INTRODUÇÃO

1.1 O Programa de Governança em Privacidade – PGP, elaborado pelo INSS, por intermédio da Diretoria de Governança, Planejamento e Inovação – DIGOV, tem fundamento na Lei nº 13.709, de 14 de agosto de 2018, (Lei Geral de Proteção de Dados Pessoais – LGPD) que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade, bem como o livre desenvolvimento da personalidade da pessoa natural.

1.2 O INSS se caracteriza como uma organização pública prestadora de serviços previdenciários para a sociedade brasileira, tendo como:

I - missão: a garantia da proteção social aos cidadãos, através do reconhecimento de direitos, cuja atuação encontra-se descrita no art. 201 da Constituição Federal, o qual preconiza que a organização do Regime Geral de Previdência Social tem caráter contributivo e filiação obrigatória; e

II - visão: ser reconhecido pela excelência no relacionamento do cidadão, o que implica, necessariamente, na proteção dos dados pessoais sob sua tutela, também com excelência.

1.3 Diante do enorme desafio, o INSS vem procurando preservar a integridade da qualidade do atendimento, buscando alternativas de melhoria contínua, com programas de modernização e excelência operacional, ressaltando a maximização e otimização de resultados e de ferramentas que fundamentem o processo de atendimento ideal aos anseios da sociedade em geral.

1.4 Além disso, assim como outros órgãos e entidades da Administração Pública, que coletam e tratam dados para o fornecimento de seus serviços, o INSS tem o dever legal de se adequar à LGPD, principalmente por ter a condição de controlador de dados referente às diversas bases de dados que estão diretamente ligadas às políticas públicas.

1.5 Assim, tendo em vista que os controladores, no âmbito de suas competências, são responsáveis pelo tratamento de dados pessoais e poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização e funcionamento, assim como demais procedimentos relacionados ao tratamento de dados pessoais, torna-se premente a necessidade de elaboração do PGP.

1.6 Por fim, é importante ressaltar que o PGP leva em consideração a estrutura organizacional do INSS e suas especificidades. Ademais, atua de forma complementar e adicional às ações já em andamento, e não visa substituir demais documentos e atos normativos que disponham sobre o tratamento de dados no âmbito do INSS.

1.7 Nesse contexto, o PGP poderá ser atualizado e ampliado sempre que necessário para manter alinhamento com a alta administração e com as diretrizes determinadas pela Autoridade Nacional de Proteção de Dados – ANPD.

2. OBJETIVO

2.1 O PGP tem como objetivo fortalecer a cultura de proteção e tratamento dos dados pessoais dos cidadãos, a fim de que possam ser exercidas com excelência as atribuições constitucionais determinadas ao INSS, atendendo aos preceitos da LGPD, bem como aos demais instrumentos normativos vigentes.

3. ETAPAS DE IMPLEMENTAÇÃO

3.1 Iniciação e Planejamento

3.1.1 O Encarregado

3.1.1.1 O encarregado é o responsável por atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD. Nesse sentido, em cumprimento ao art. 41 da LGPD, o INSS designou, por meio da Portaria PRES/INSS nº 30, de 15 de fevereiro de 2023, um servidor como Encarregado pelo Tratamento de Dados Pessoais do INSS, ao qual caberá as seguintes atribuições:

I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

II - receber comunicações da ANPD e adotar providências;

III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

3.1.1.2 Importa ressaltar que o apoio da alta administração é essencial para o sucesso do trabalho executado pelo encarregado, incluindo seu envolvimento nas decisões e recursos suficientes para pessoal, treinamento, entre outros.

3.1.2 Alinhamento de Expectativas com a Alta Administração

3.1.2.1 O INSS é a maior Autarquia da América Latina e, portanto, tem sob sua gestão os dados de beneficiários, segurados, dependentes, bem como de benefícios previdenciários e assistenciais, tendo assim relações com diversas entidades externas, além dos dados dos seus próprios colaboradores, o que faz com que o escopo do INSS seja bastante amplo e complexo no que diz respeito ao tratamento de dados pessoais sob seus cuidados.

3.1.2.2 Ainda no ano 2020 foram iniciadas as tratativas para desenvolver estudos, planejar e executar a implantação da LGPD, no âmbito do INSS.

3.1.2.3 Desde então, as decisões são submetidas ao Comitê Temático de Governança Digital – CTGD e ao CEGOV da alta gestão do INSS, nos quais todas as necessidades levantadas e ações a serem realizadas são propostas à presidência e diretores.

3.1.2.4 Ademais, considerando que a DIGOV, patrocinadora do PGP, é um órgão de assistência direta e imediata à Presidência, resta clarividente o cumprimento da etapa de alinhamento de expectativas com a alta administração.

3.1.2.5 Outrossim, o PGP é passível de revisão e atualização, conforme necessidades do INSS ou para manter alinhamento com as diretrizes da ANPD.

3.1.3 Medidas de Segurança

3.1.3.1 Ressalta-se que a segurança da informação no âmbito do INSS é constantemente revista e aprimorada com a adoção de novas medidas, tendo em vista o cenário de transformação digital por que passam todos os Órgãos da Administração Pública Federal direta, autárquica e fundacional, bem como a necessidade de atendimento ao disposto no **caput** do art. 46 da LGPD:

> "Art. 46. Os agentes de tratamento devem adotar medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito."

3.1.3.2 As ações de controle de segurança referentes à proteção de dados no INSS devem ser um conjunto amplo de medidas que tenha como objetivo minimizar os riscos presentes nos ativos de informação, tendo como norteadores normas de segurança internacionalmente aceitas, tais como as ISO 27001/27002 e a extensão ISO 27701:2019, que especifica os requisitos e fornece diretrizes para o estabelecimento, implementação, manutenção e melhoria contínua de um Sistema de Gestão de Privacidade da Informação (SGPI).

3.1.3.3 O Guia de Boas Práticas da LGPD, desenvolvido pelo Comitê Central de Governança de Dados instituído pelo Decreto nº 10.046, de 9 de outubro de 2019, com o objetivo de fornecer orientações de boas práticas aos órgãos e entidades da Administração Pública Federal direta, autárquica e fundacional para as operações de tratamento de dados pessoais, constitui também uma fonte de consulta para desenvolvimento de medidas de segurança da informação, no âmbito do INSS.

3.1.3.4 Dentre as medidas já adotadas pelo INSS, considera-se relevante a criação de um fluxo de atendimento aos incidentes cibernéticos de vazamento de dados de servidores, elaborado pela Diretoria de Tecnologia da Informação - DTI, em conjunto com a DIGOV, que prevê a forma de tratamento dos incidentes de vazamento de dados, com plano de resposta e medidas mitigadoras, buscando diminuir o impacto desses vazamentos, tanto no caso de eventuais aspectos financeiros, como de integridade e segurança dos sistemas corporativos, em atuação conjunta com a Empresa de Tecnologia e Informações da Previdência - Dataprev, bem como para proporcionar a consolidação das informações sobre os incidentes, necessária para estudos e propostas de Ações de Conformidade com viés de prevenção e correção.

3.1.4 Estrutura Organizacional para Governança e Gestão da Proteção de Dados Pessoais

3.1.4.1 O Anexo I do Decreto nº 10.995, de 14 de março de 2022, apresenta a Estrutura Regimental do INSS, a qual contém a DIGOV. Esta possui em sua estrutura a Coordenação de Proteção de Dados Pessoais - COPDP, vinculada à Coordenação-Geral de Conformidade - CGCONF, como setores responsáveis por orientar sobre temas afetos à LGPD.

3.1.4.2 As competências da COPDP constam no art. 33 do Anexo da Portaria PRES/INSS nº 1.532, de 8 de dezembro de 2022, que aprovou o Regimento Interno do INSS, quais sejam:

> Art. 33. À Coordenação de Proteção de Dados Pessoais compete:
>
> I - propor, implantar e avaliar a Política Institucional de Proteção de Dados Pessoais e da

Privacidade, nos termos da legislação vigente;

II - orientar a elaboração, aprovar os Relatórios de Impacto à Proteção de Dados Pessoais e monitorar a implantação das medidas mitigadoras propostas pelas áreas do Instituto;

III - receber:

a) reclamações e comunicações dos titulares dos dados pessoais e adotar providências; e

b) comunicações da Autoridade Nacional de Proteção de Dados - ANPD e articular a adoção das providências junto às áreas envolvidas;

IV - orientar as unidades e colaboradores a respeito de boas práticas de proteção de dados pessoais;

V - promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade;

VI - disponibilizar à ANPD, a qualquer momento, informe das operações de tratamento de dados pessoais, com a emissão de parecer técnico; e

VII - promover ações de cooperação com as entidades públicas ou privadas relacionadas à proteção de dados pessoais.

3.1.4.3 Para promover a gestão da Proteção de Dados Pessoais no âmbito do INSS, além da atuação da equipe de proteção de dados que é coordenada pela já citada COPDP e do encarregado de proteção de dados, para melhor integração com as áreas técnicas, é importante destacar o papel do Comitê Temático de Gestão da Informação - CTGI, que conta com a participação de servidores indicados por todas as Diretorias, além da Procuradoria Federal Especializada - PFE, Auditoria-Geral, Corregedoria-Geral, e Presidência, devendo o CTGI:

I - aprovar procedimentos e normas internas que orientem o compartilhamento de dados sob gestão do INSS com outras organizações da administração pública e da sociedade civil, bem como a categorização dos níveis de compartilhamento desses dados com outras entidades da administração pública federal direta, autárquica e fundacional, bem como de outras esferas;

II - propor o compartilhamento específico de dados sob gestão do INSS com essas mesmas entidades, além da necessidade de acompanhar as deliberações e orientações do Comitê Central de Governança de Dados; e

III - instituir procedimentos e normas internas para o levantamento das informações sujeitas à classificação de sigilo, a formalização dos termos de classificação e o tratamento das informações classificadas, a promoção do compartilhamento amplo de dados abertos, em transparência ativa, relativos aos benefícios concedidos e a outras bases de dados sob gestão do INSS sobre as quais não recaia vedação expressa de acesso, o fomento da transparência e o acesso à informação.

3.1.5 Inventário de Dados Pessoais

3.1.5.1 O Inventário de Dados Pessoais consiste em documentar o tratamento de dados pessoais realizado pela Instituição, consoante art. 37 da LGPD. Objetiva fazer um balanço do que o INSS faz com os dados pessoais disponíveis em seus sistemas, identificando os agentes de tratamento, quais dados pessoais são tratados, onde estão armazenados, quais operações são realizadas com eles e os demais atributos necessários a uma avaliação de risco e de conformidade com a legislação regulatória em vigor.

3.1.5.2 De uma forma geral, esse registro mantido pelo IDP é aplicável pelo INSS para as seguintes finalidades:

I - cumprimento de obrigação legal ou regulatória pelo controlador; e

II - execução de políticas públicas.

3.1.5.3 As formas de entrada em bancos de dados geridos pelo INSS são diversas, visto que este realiza a gestão de benefícios previdenciários e assistenciais, além do Seguro-Desemprego do Pescador Artesanal. Para a realização de políticas públicas, o INSS detém a gestão do Cadastro de Pessoas através do Cadastro Nacional de Informações Sociais – CNIS, que contém informações de diversas bases governamentais. Assim, os dados são coletados nos sistemas geridos pelo INSS, através de um cadastro do cidadão para filiação na condição de contribuinte obrigatório ou não, bem como quando da requisição de algum benefício ou serviço administrado pelo INSS.

3.1.5.4 A retenção/armazenamento ou eliminação é realizada conforme legislação vigente e não há descarte, seguindo obrigações legais do Controlador.

3.1.5.5 Convém destacar que o INSS tem adotado medidas para garantir a segurança de dados na análise de benefícios, seguindo as normas de privacidade dos dados pessoais e de segurança da informação, entre elas a Instrução Normativa PRES/INSS nº 128, de 28 de março de 2022, que prevê, no § 1º do art. 523 que os processos administrativos previdenciários, em virtude dos dados pessoais e sigilosos neles contidos, são de acesso restrito aos interessados e a quem os represente, salvo determinação judicial ou solicitação do Ministério Público, esta devidamente justificada, para fins de instrução de processo administrativo de sua competência.

3.1.5.6 Atualmente, possuímos 158 (cento e cinquenta e oito) sistemas catalogados no nível da Administração Central, alguns criados e mantidos pela operadora de dados (Dataprev), outros pela DTI, além daqueles regionais que não foram catalogados em sua completude. Não obstante, há sistemas operados por empresas privadas, como correio eletrônico, ferramenta de disponibilização e criação de painéis, armazenamento de dados em nuvens, dentre outros.

3.1.5.7 Quanto aos sistemas corporativos, utilizamos o catálogo de dados da operadora Dataprev, atualmente na versão 1.23.4 de 2 de fevereiro de 2023. Os sistemas operacionais internos são acompanhados pela DTI. Contudo, quanto aos sistemas manufaturados e operados regionalmente, objetivamos catalogá-los e acompanhá-los com apoio da DTI.

3.1.5.8 A elaboração e manutenção do Inventário de Dados Pessoais será executada em consonância com o material produzido pela Secretaria de Governo Digital – SGD que subsidiará sua construção, pelos responsáveis por cada sistema operacional, aos quais caberá informar sobre alterações implementadas nos processos organizacionais, cabendo ao Encarregado pelo Tratamento de Dados Pessoais o acompanhamento e gestão desse inventário, até que seja publicada a Política de Privacidade e Proteção de Dados em sua totalidade, ocasião em que esta atribuição poderá ser designada a outro responsável.

3.1.6 Levantamento de Contratos relacionados a Dados Pessoais

3.1.6.1 Os acordos, contratos e convênios no âmbito do INSS podem ser firmados de maneira centralizada pela Administração Central, os quais são monitorados cada qual pela sua área de atuação, como também descentralizados pelas Superintendências Regionais e Gerências-Executivas, necessitando, de forma geral, de levantamento e verificação quanto à adequação à LGPD.

3.1.6.2 Para que essa adequação ocorra de maneira concatenada e padronizada, já que a elaboração de acordos e convênios está distribuída em toda a estrutura, faz-se necessária a elaboração de um Guia de Adequação de Contratos e Convênios. O Guia estabelecerá parâmetros que venham a sanear a necessidade de adequação com cláusulas elaboradas para assegurar a proteção dos dados pessoais, tanto nos novos contratos como nas renovações dos vigentes. Integrarão o documento os modelos de acordos e convênios internacionais inspirados nos modelos de **Standard Contractual Clauses** (SCC) que a Comissão Europeia publicou, com base em **Data Processing Agreements** (DPAs), para que haja adequação aos padrões internacionais.

3.1.6.3 Cabe ainda mencionar a importância da elaboração de um Inventário de Contratos, Convênios e Ajustes que poderá ser assessorada pela Equipe de Tratamento de Dados Pessoais, com apoio do Encarregado de Dados e da Coordenação-Geral de Licitações e Contratos, da Divisão de Gerenciamento de Acordos de Cooperação e da Coordenação de Acordos Internacionais de Benefícios, cuja manutenção será de responsabilidade dos fiscais designados para cada instrumento, aos quais caberá manter atualizadas as informações pertinentes.

3.1.6.4 É essencial para a gestão e governança das atividades de tratamento de dados pessoais, especialmente no que diz respeito ao monitoramento e vigência de termos e legislação que disciplinam a questão, a estruturação de uma solução de informática para a devida gestão, acompanhamento e controle dos acordos, convênios e contratos, que deve ser construída considerando o número elevado desses instrumentos, a qual proporcionará um inventário centralizado, podendo-se catalogar facilmente todos os instrumentos de contrato, convênios ou ajustes diversos que contenham dados pessoais, contribuindo para possíveis e necessárias adequações contratuais, tanto nos contratos existentes, quanto nos futuros.

3.1.7 Plano de conscientização, treinamento e comunicação

3.1.7.1 Para que um Programa de Governança em Privacidade tenha êxito em sua implantação é essencial que toda a Instituição esteja bem alinhada. Uma boa maneira de disseminar conhecimento é a partir de programas de treinamento e conscientização do corpo funcional, sem olvidar que planos de comunicação devem ser continuamente desenvolvidos.

3.1.7.2 Campanhas de treinamento e comunicação devem informar leis e políticas aplicáveis, as consequências por violá-las e incentivar procedimentos de denúncia, com a divulgação dos canais para tal.

3.1.7.3 O plano de conscientização, treinamento e comunicação:

I - trará previsão de calendário periódico de cursos com certificação, versando sobre as temáticas tangentes aos direitos à privacidade e à proteção dos dados pessoais, tais como segurança da informação, direito à privacidade e gestão de risco; e

II - contemplará a consolidação de material, atualizado periodicamente, com instruções e normas de boas práticas envolvendo segurança da informação, disponibilizado a todos os colaboradores, além de medidas que visem a internalização da cultura de proteção de dados pessoais nas unidades do INSS.

3.1.8 Diagnóstico de Maturidade da Organização quanto à adequação à LGPD

3.1.8.1 Neste ponto, apresenta-se uma análise do atual estágio de adequação do INSS em relação à LGPD, realizada em conformidade com o Guia de Elaboração de Programa de Governança em Privacidade e por meio da utilização da ferramenta para análise de maturidade da SGD que foi disponibilizada no sítio eletrônico Pesquisa SISP GOV.

3.1.8.2 Cabe ressaltar que essa não é a primeira vez que o INSS realiza esse levantamento, já que, anteriormente, teve que avaliar o grau de maturidade em privacidade de dados pessoais, por conta do Acórdão 1384/2022 do Tribunal de Contas da União.

3.1.8.3 É oportuno identificar que a ferramenta de análise de maturidade da SGD é composta por um questionário de 33 (trinta e três) perguntas acerca dos expedientes adotados pela Administração em relação ao grau de desenvolvimento. Essas perguntas envolvem 7 (sete) áreas de atuação, que são: governança, conformidade legal e respeito aos princípios, transparência e direitos do titular, rastreabilidade, adequação de contratos e de relações com parceiros, segurança da informação, transparência e violação de dados.

3.1.8.4 Partindo de tais premissas, é conveniente a comparação da maturidade dos processos de gestão de informações pessoais em cada uma dessas áreas, possibilitando ao INSS uma clara compreensão dos pontos em que mais evoluiu e em quais se deve envidar mais esforços para o atingimento do grau de excelência e referência em gestão de dados pessoais

3.1.8.5 Governança:

3.1.8.5.1 As ações adotadas já tiveram repercussão com a ampliação do grau neste quesito. Para sua progressão, um plano de comunicação e capacitação institucional estruturada apresentam-se como instrumentos necessários para aumentar o grau de maturidade. Esse plano engloba as atividades promovidas visando a conscientização tanto do público interno quanto do público externo, principais interessados na proteção de seus dados pessoais.

3.1.8.6 Conformidade legal e respeito aos princípios:

3.1.8.6.1 Apresentou-se como um dos pontos com o maior índice de maturidade e do qual se busca o atingimento do nível de excelência, embora resta evidente o quão desafiador se mostra, dada a magnitude do banco de dados utilizado pelo INSS, que além de receber dados de outras bases também é fonte para diversas outras entidades. Assim, tendo este PGP como instrumento, o INSS pretende fazer com que toda a organização se adeque totalmente aos parâmetros de conformidade legal e respeito aos princípios contidos na LGPD.

3.1.8.7 Transparência e direitos do titular:

3.1.8.7.1 O principal canal de recepção dos serviços institucionais, “Meu INSS”, já possui Política de Privacidade de Dados, que embora necessite de revisão constante devido as especificidades do INSS, demonstra avanço considerável, devendo ser ampliada aos demais sistemas.

3.1.8.8 Rastreabilidade:

3.1.8.8.1 Quanto ao quesito da rastreabilidade, o INSS passou a adotar o **privacy by design** em todos os novos sistemas, sendo possível a identificação do responsável pela consulta aos dados pessoais e também sua alteração, por meio de consulta individual em cada sistema. Por outro lado, parte dos sistemas desenvolvidos anteriormente à vigência da LGPD possui uma maior limitação, sendo possível identificar a autoria somente nos casos de alteração dos dados.

3.1.8.8.2 Em relação aos sistemas que fazem parte do legado, objetiva-se a implementação de um único portal de acesso a todos os sistemas por meio da autenticação via Sistema de Gerenciamento de Identidade - Gerid, superando as limitações de rastreabilidade já mencionadas.

3.1.8.9 Adequação de contratos e de relações com parceiros

3.1.8.9.1 A Política de Privacidade de Dados está presente nos novos contratos, termos de parceria e acordos, pactuados a nível de Administração Central, padrão este que deverá ser seguido no caso das Superintendências Regionais e Gerências-Executivas.

3.1.8.9.2 Para os documentos do legado, será realizada a implementação e revisão de todos os contratos, termos de parceria e acordos que estão em fase de aditivação.

3.1.8.10 Segurança da informação

3.1.8.10.1 Considerada um dos pontos cruciais em matéria de proteção de dados, tem atenção especial do PGP que buscará implementar todas as ações necessárias para o seu aprimoramento, face ao crescente risco global.

3.1.8.10.2 Importante destacar a evolução obtida nesse ponto com relevantes ações institucionais, entre elas: a inclusão de cláusula contratual com a operadora Dataprev com aplicação da ISO 27701, a certificação digital e autenticação em duas etapas que reforça a privacidade e proteção de dados pessoais.

3.1.8.11 Violação de dados

3.1.8.11.1 Este tema pode ser analisado por duas vertentes: dados digitais e dados analógicos. No primeiro, já existem fluxos publicados de tratamento de incidentes que visam prevenir e tratar os possíveis incidentes de vazamento de dados. Quanto aos incidentes relativos aos vazamentos de dados analógicos, a Coordenação-Geral de Conformidade publicará um manual de procedimentos a serem utilizados pelo INSS em conformidade com a LGPD.

3.2 Construção e Execução

3.2.1 Políticas e práticas para proteção da privacidade do cidadão e Política de Segurança da Informação.

3.2.1.1 Dada a relevância do INSS para a sociedade brasileira, é de fundamental importância a construção de uma Política de Proteção da Privacidade que deve ser considerada por todos,

da alta administração ao nível operacional.

3.2.1.2 A Política de Privacidade aqui tratada consiste em um documento interno, que tem como objetivo trazer informações sobre o tratamento dos dados pessoais que sejam necessárias para o atendimento das metas institucionais, garantindo que o uso dos dados pessoais seja adequado às legislações específicas.

3.2.1.3 Na Política de Proteção de Dados Pessoais deve constar seu objetivo, deixando clara a razão de sua existência e quais as metas a serem alcançadas, delimitando seu escopo, apontando a área de atuação e os responsáveis pela coleta, retenção, processamento, compartilhamento e eliminação de dados pessoais, além de garantir uma estrutura para adequação às normas que regem a matéria, com previsão de eventuais sanções em caso de descumprimento.

3.2.1.4 No que se refere à Política de Segurança da Informação, considerando que o INSS tem como uma de suas missões institucionais o reconhecimento de direito aos cidadãos e que para isso possui um dos maiores bancos de dados pessoais da América Latina, a atualização das tecnologias disponíveis no mercado em termos de Segurança da Informação deve estar na pauta das tratativas do INSS junto à empresa de tecnologia que lhe presta serviços, no caso a Dataprev, de modo a garantir um sistema mais moderno e seguro de proteção dos dados pessoais.

3.2.1.5 Atualmente o INSS conta com algumas normas referentes à segurança da Informação, quais sejam:

I - as Portarias:

a) DTI/INSS:

1. nº 1. 22, de 13 de maio de 2022, que designa os membros da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR do INSS;

2. nº 88, de 27 de dezembro de 2022, que estabelece o Plano de Gestão de Incidentes Cibernéticos (PGIC) no âmbito do Instituto Nacional do Seguro Social – INSS; e

3. nº 89, de 28 de dezembro de 2022, que dispõe sobre a Metodologia para elaboração de Planos de Continuidade de Negócio - PCN de Tecnologia da Informação;

b) DIRBEN/INSS:

1. nº 991, de 28 de março de 2022, que aprova as Normas Procedimentais em Matéria de Benefícios; e

2. nº 1.100, de 18 de janeiro de 2023, que altera o Livro II das Normas Procedimentais em Matéria de Benefícios, que disciplina os procedimentos e rotinas de benefícios do Regime Geral de Previdência Social - RGPS no âmbito do INSS, aprovado pela Portaria DIRBEN/INSS nº 991, de 28 de março de 2022;

II - as Resoluções CEGOV/INSS:

a) nº 9, de 31 de agosto de 2020, que atualiza a Política de Segurança da Informação do Instituto Nacional do Seguro Social – POSIN-INSS; e

b) nº 28, de 28 de dezembro de 2022, que institui o Plano Diretor de Segurança da Informação - PDSI 2023-2025 do Instituto Nacional do Seguro Social.

3.2.1.6 Assim, torna-se imprescindível o constante aprimoramento das normas que compõem e fundamentam a estrutura da Política de Segurança da Informação do INSS, verificando se não há tratamento excessivo de dados, se os controles de segurança são suficientes para os dados tratados, bem como se é necessária a retenção de determinados dados tratados e a revisão de contratos.

3.2.1.7 Por fim, não se pode deixar de considerar que, em razão das funções institucionais do INSS, há rotineiramente a necessidade de relacionamento com outros órgãos da Administração Pública, ocorrendo o compartilhamento e a transferência de dados, devendo sempre ser levada em consideração essa característica no planejamento, construção, implementação e atualização de suas políticas.

3.2.2 Cultura de segurança e proteção de dados, e Privacidade desde a Concepção (PdC)

3.2.2.1 Para que alcancemos a institucionalização de uma cultura de proteção e privacidade de dados, devemos investir em capacitações e desenvolver campanhas de conscientização de forma contínua.

3.2.2.2 Todavia, devido às dimensões do INSS, métodos de treinamento e conscientização podem variar, incluindo cursos de capacitação presenciais ou a distância, reuniões de equipe, boletins informativos, e-mails, folhetos, **slogans** e informações no portal eletrônico.

3.2.2.3 Assim, enquanto conhecimentos gerais sobre a Política de Privacidade devem ser comunicados a todo corpo funcional e colaboradores, algumas funções podem necessitar de capacitações específicas e mais especializadas.

3.2.2.4 Nesse sentido, os cursos devem ser destinados a todos os colaboradores, com abordagem e metodologia que respeite as especificidades e características institucionais.

3.2.2.5 Assim sendo, as áreas da Autarquia devem ser capacitadas de maneira planejada e com objetivos específicos, a fim de haver maior aderência aos temas a elas direcionados.

3.2.2.6 Desse modo, a área de:

I - Gestão de Pessoas deve ser capacitada sobre procedimentos administrativos para tratar dados pessoais do corpo funcional durante todo o ciclo de vida dos dados;

II - Tecnologia da Informação deve ser preparada para a implementação de medidas

técnicas de segurança, visando a proteção dos dados pessoais tratados no âmbito institucional;

III - Ouvidoria deve receber destaque pois recebe solicitações e reclamações de titulares de dados, com respeito aos seus direitos e eventuais vazamentos; e

IV - Comunicação Social deve compreender muito bem o Programa de Governança em Privacidade para que atue como parceira e colaboradora na criação de campanhas de conscientização para todo o corpo funcional.

3.2.2.7 Quanto ao conceito de PdC, é importante ressaltar que a privacidade e a proteção de dados devem ser consideradas desde a concepção e perdurar por todo o ciclo de vida do projeto, sistema, serviço, produto ou processo, conforme o art. 46 da LGPD.

3.2.2.8 Por este motivo, os novos sistemas operacionais da principal operadora (Dataprev), conforme previsto em contrato, já adotam o **privacy by design**.

3.2.2.9 Destacamos alguns valores desse modelo a seguir:

I - a proatividade e não reatividade, ao se incluir a privacidade como parte dos requisitos de engenharia do sistema para evitar a ocorrência dos riscos de privacidade;

II - a incorporação de controles de privacidade, oferecendo o máximo grau de privacidade que serão auditados e avaliados continuamente, sendo parte integrante do sistema, sem diminuir a funcionalidade;

III - a visibilidade e transparência, a partir do uso de controles transparentes, permitindo que indivíduos exerçam seus direitos com confiança; e

IV - o respeito pela privacidade do usuário que deve ser alcançado por meio de medidas como padrões fortes de privacidade, avisos apropriados e interfaces amigáveis que forneçam autonomia ao titular dos dados.

Nota: **privacy by design**
A LGPD exige a implantação do **privacy by design**, que nada mais é do que a adoção de medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais, desde a fase de concepção do produto ou do serviço até a sua execução.

3.2.3 Relatório de Impacto à Proteção de Dados Pessoais (RIPD)

3.2.3.1 O RIPD é um instrumento fundamental para avaliação da conformidade do tratamento de dados pessoais em relação à LGPD. Um dos objetivos do RIPD é descrever os processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como de análise do controlador com relação às medidas, salvaguardas e mecanismos de mitigação de riscos adotados.

3.2.3.2 Devido à capilaridade das atividades do INSS, há uma grande quantidade de ferramentas utilizadas para o atingimento de sua finalidade institucional, tendo sido catalogados, até o momento, 158 (cento e cinquenta e oito) sistemas, alguns criados e mantidos pela operadora de dados

(Dataprev), outros pela DTI.

3.2.3.3 O INSS em parceria com a Dataprev elaborou e documentou os RIPDs de maior relevância e impacto nas operações com dados pessoais, o que não afasta a necessidade de manter processo contínuo de mapeamento e de elaboração de relatório de impacto de todos os sistemas e processos existentes, dando prioridade aos RIPDs das extrações que envolvam transferência de dados a outros órgãos.

3.2.4 Adequação das Cláusulas Contratuais

3.2.4.1 À luz da LGPD, é fundamental uma análise precisa da classificação de uma entidade como controladora ou operadora, para que se definam responsabilidades em contratos firmados entre agentes de tratamento e na adoção das medidas contratuais adequadas, a fim de mitigar riscos inerentes ao tratamento de dados pessoais.

3.2.4.2 Dessa forma, há necessidade de estruturação de cláusulas nos contratos, convênios e nos acordos, ou transferências de dados, para que cláusulas de proteção de dados estejam inclusas e claras, dentre as quais destacam-se:

I - a obrigação do tratamento dos dados nos acordos, contratos ou convênios que forem eventualmente coletados, conforme sua necessidade ou obrigatoriedade;

II - o respeito aos princípios da finalidade, adequação, necessidade, transparência, livre acesso, qualidade dos dados, segurança, prevenção, não discriminação e responsabilização;

III - a garantia da confidencialidade dos dados por meio de uma política interna de privacidade, a fim de respeitar, por si, seus funcionários e seus prepostos, que é o objetivo do PGP;

IV - o uso e arquivamento somente pelo tempo necessário para a execução dos serviços acordados, contratados ou conveniados. E, ao seu fim, a eliminação dos dados coletados, excetuando-se os que se enquadrarem no disposto no inciso I do art. 16 da LGPD; e

V - quando da transferência de dados, deve o contrato, acordo ou convênio deixar claro que, uma vez transferidos os dados, a responsabilidade por eles cabe ao receptor dos mesmos, sendo o responsável pelo tratamento dos dados autorizados àquele.

3.2.5 Termo de Uso e Política de Privacidade

3.2.5.1 As informações expostas no Termo de Uso e na Política de Privacidade devem sempre ser oferecidas com exatidão, clareza e relevância, além de serem periodicamente atualizados e prezar pela fidedignidade das informações. Além disso, sua disponibilização deve ser em local de fácil acesso para garantir que o usuário/titular tome conhecimento sobre o serviço e tratamento dos dados pessoais. Podem, ainda, constar de um único documento ou documentos separados.

3.2.5.2 Termo de Uso

3.2.5.2.1 O Termo de Uso informa as regras a que o usuário está sujeito ao utilizar o serviço, seja por meio de aplicações, como sítios, sistemas e aplicativos para dispositivos móveis. Já a Política de Privacidade deriva do princípio da transparência que é devida ao titular de dados pessoais, pelos agentes de tratamento, os quais devem informar como as atividades de tratamento de tais dados atendem àqueles princípios dispostos no art. 6º da LGPD.

3.2.5.2.2 Cabe ressaltar a importância da participação da PFE, que deve ser consultada ao longo das atividades de elaboração, de modo a confirmar se as cláusulas escritas no Termo de Uso estão de acordo com as legislações vigentes e se possuem validade jurídica.

3.2.5.2.3 Os requisitos básicos para a elaboração do Termo de Uso são:

I - aceitação, concordância ou ciência do Termo de Uso: este item deve informar ao usuário que a utilização do serviço está condicionada à aceitação, concordância ou ciência com os termos e condições estabelecidos pelo fornecedor do serviço;

II - definições do Termo de Uso: é de suma importância que o Termo de Uso seja compreensível para todos que utilizam o serviço, explicando-se os termos técnicos e legais, com linguagem simples e acessível, evitando o uso de siglas, jargões e estrangeirismos, e sejam padronizadas para toda a Administração Pública utilizando-se, por tal motivo e, preferencialmente, aquelas constantes do Glossário de Segurança da Informação do GSI (Portaria GSI/PR nº 93, de 18 de outubro de 2021) e legislações correlatas;

III - arcabouço legal: a legalidade como princípio constitucional é condição essencial de toda ação do Estado. Assim, o Termo de Uso deverá estar em conformidade com a legislação que respalda a atuação do INSS bem como com os instrumentos legais que têm relação direta com a utilização de sítios, sistemas ou aplicativos para dispositivos móveis desenvolvidos ou utilizados pelo INSS;

IV - descrição do serviço: as informações sobre o serviço oferecido devem ser fornecidas aos usuários de maneira clara, para evitar o mau uso do serviço e posteriores reclamações, descrevendo sua finalidade, forma de utilização, a previsão do tempo de espera, documentos necessários e os mecanismos de consulta ao andamento do serviço solicitado e de eventuais manifestações, além de informações sobre outros meios disponíveis quando o serviço estiver inoperante;

V - direitos do usuário do serviço: o Termo de Uso deverá deixar claro quais são os direitos do usuário de acordo com aqueles constantes na LGPD, na Lei nº 13.460, de 26 de junho de 2017, que dispõe sobre participação, proteção e defesa dos direitos do usuário dos serviços públicos da administração pública, e demais normas regulatórias;

VI - responsabilidades do usuário e da Administração Pública: assim como o usuário deve tomar ciência de seus direitos, também deverá ser informado sobre suas responsabilidades ao acessar os serviços disponibilizados pelo INSS, utilizando-os adequadamente e colaborando para a correta prestação do serviço, seja pelo zelo com suas credenciais de acesso, seja pela veracidade das informações e documentos apresentados, entre outros. Da mesma forma, também deverão ser delimitadas as responsabilidades, resguardando-se de quaisquer riscos e protegendo os direitos do INSS e dos usuários. Na especificação das responsabilidades do INSS é recomendado atentar para os normativos que norteiam a prestação dos serviços na Administração Pública, como por exemplo: a Lei nº 13.460, de 2017 (participação, proteção e defesa dos direitos do usuário dos serviços públicos), Decreto nº 9.094, de 17 de julho de 2017 (regulamenta dispositivos da Lei nº 13.460, de 2017) e Lei nº 14.129, de 29 de março de

2021 (Lei do Governo Digital), bem como todas as legislações inerentes ao uso correto dos dados pessoais;

VII - Política de Privacidade: faz parte do Termo de Uso, no qual deverá constar o caminho ou o **link** que leva até a Política de Privacidade do INSS para que o usuário possa acessar facilmente;

VIII - mudanças no Termo de Uso: havendo necessidade, o Termo de Uso poderá ser revisto e a atualização ocorrida deve ser acrescentada ao termo. Nesses casos, deve ser informada ao usuário a forma de comunicação das mudanças realizadas, o número da versão e a data da última atualização do documento;

IX - informações para contato: é importante que os canais de atendimento sejam divulgados pelo sítio do INSS, nas redes sociais, pelo aplicativo Meu INSS, pela Central 135, informando o horário de atendimento, para orientações e esclarecimentos acerca do serviço;

X - foro: eleição de foro diz respeito ao comprometimento das partes envolvidas na prestação do serviço – cidadão e administração pública – caso uma delas entenda que questões presentes no Termo de Uso do serviço tenham sido violadas. Por ser o INSS uma Autarquia Federal, sugere-se o texto exemplificativo constante no Guia de elaboração desenvolvido pela SGD:

> Este Termo será regido pela legislação brasileira. Qualquer reclamação ou controvérsia com base neste Termo será dirimida exclusivamente pela Justiça Federal, na seção judiciária do domicílio do usuário, por previsão do artigo 109, §§ 1º, 2º e 3º da Constituição Federal.

3.2.5.3 Política de Privacidade

3.2.5.3.1 Política de Privacidade: é um documento informativo pelo qual o prestador de serviço transparece ao usuário a forma como o serviço realiza o tratamento dos dados pessoais e como ele fornece privacidade ao usuário, cumprindo, fundamentalmente, o dever de transparência disposto como princípio na LGPD. Trata-se aqui de uma política de privacidade externa, que faz parte do Termo de Uso, também podendo ser chamada de "aviso de privacidade" que fornecerá às pessoas externas à organização um aviso sobre as práticas de privacidade adotadas, bem como outras informações relevantes. Os requisitos básicos para a elaboração da Política de Privacidade são:

I - definições da Política de Privacidade: assim como no Termo de Uso, a Política de Privacidade deve ser acessível e de fácil compreensão, contendo explicação de termos técnicos e legais para melhor entendimento de todos que fizerem uso dos serviços ofertados;

II - base legal para tratamento de dados pessoais: a hipótese de tratamento de dados pessoais autorizada pela LGPD, bem como sua previsão legal devem ser informadas ao titular dos dados. Assim, sendo uma Autarquia Federal, responsável por administrar diversos benefícios sociais e previdenciários, o tratamento dos dados pelo INSS encontra respaldo nos arts. 7º e 11 da LGPD, no que se refere ao tratamento de dados para cumprimento de obrigação legal ou regulatória pelo controlador e tratamento compartilhado de dados necessários à execução de políticas públicas previstas em leis ou regulamentos;

III - Controlador, Operador e Encarregado: o titular dos dados tem direito de acesso às informações de contato do controlador, que deverão ser disponibilizadas de forma clara, adequada e

ostensiva contendo a identificação, endereço e informações de contato do controlador, que nesse caso é o INSS. A LGPD também estabelece a necessidade de disponibilizar informações sobre as responsabilidades dos agentes que realizarão o tratamento dos dados do controlador, que nesse caso, é realizado pela Dataprev como operador. Da mesma forma, deve ser informado que os dados do encarregado constam no site do INSS e restar claro que dúvidas podem ser sanadas pelos canais devidos;

IV - direitos do titular dos dados pessoais: toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade. Assim, visando o princípio da transparência, numa Política de Privacidade devem ser informados os direitos de seus titulares, especialmente aqueles descritos nos artigos 9º e 18 da LGPD;

V - tratamento dos dados e sua finalidade: é realizado pelo INSS para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as suas atribuições do serviço público. Assim, deve restar claro na Política de Privacidade quais dados serão tratados e qual sua finalidade. Os principais tratamentos de dados realizados pelo INSS estão relacionados à atualização de dados cadastrais, atualização e informações relativas aos vínculos de trabalho, remunerações e contribuições e dados de dependentes. O tratamento das informações se destina, como regra, à análise, concessão e manutenção de benefícios. No entanto, outros dados poderão ser tratados e devem ser igualmente informados. Destaca-se nessa seção o atendimento aos princípios estabelecidos no art. 6º da LGPD, especialmente o princípio da necessidade, que estabelece a limitação do tratamento ao mínimo necessário para a realização das finalidades previstas, de forma proporcional e não excessiva;

VI - coleta dos dados: além de especificar quais dados são coletados, é importante esclarecer ao titular como os dados são obtidos. Os dados mais relevantes para o reconhecimento de direitos vêm do CNIS, do Cadastro Único (CadÚnico), do eSocial e do Sistema Nacional de Informações de Registro Civil, que são bases de dados onde estão armazenadas as informações trabalhistas dos cidadãos, registro de nascimento, casamento e óbito. Todavia, outras bases de dados, inclusive de outros órgãos, podem ser utilizadas. Pode, ainda, haver coleta de informações por meio de funcionalidades específicas do dispositivo do usuário como, por exemplo, pela câmera, para dados de biometria;

VII - compartilhamento de dados: para estar em conformidade com a LGPD, o serviço deverá informar ao titular do dado que utiliza o serviço sobre o uso compartilhado de dados pelo controlador e a finalidade de seu compartilhamento. Ao realizar o compartilhamento dos dados, deverá sempre ser observada a inclusão de cláusulas de preservação de sigilo das informações;

VIII - transferência internacional de dados: para os casos que envolvam transferência de dados entre países, deve-se deixar claro para o titular quais os dados serão transferidos internacionalmente, para qual finalidade, quais países estão envolvidos e qual o grau de proteção e privacidade fornecido por eles;

IX - segurança dos dados: é fundamental que sejam apresentadas ao titular dos dados as medidas de segurança que foram implementadas no serviço que trata seus dados pessoais, além de definir meios para que seja comunicado sobre a ocorrência de incidente de segurança que lhe possa acarretar risco ou dano relevante. Também é importante citar qual o canal de comunicação para que o titular reporte possíveis violações, falhas e vulnerabilidades do serviço, que esteja em consonância com o Plano de Gestão de Incidentes Cibernéticos ou outros planos que venham a ser elaborados;

X - cookies: a sua utilização deve considerar a hipótese legal que considere a prévia autorização do usuário ou qualquer outra hipótese que respalde a coleta desses dados, devendo estar claro

o aviso sobre sua utilização, consentimento e informar a respeito de quais dados pessoais são coletados, armazenados e para qual finalidade;

XI - tratamento posterior dos dados para outras finalidades: deve ser comunicado ao titular do dado, informando-o a respeito de quais dados poderão ser utilizados para tratamentos posteriores e qual a sua finalidade.; e

XII - mudanças na Política de Privacidade: a política poderá ser alterada a qualquer momento para atender à evolução do serviço oferecido ou à LGPD. Por isso, recomenda-se que seja informada ao usuário a forma de comunicação das mudanças realizadas, sua versão atual e a data da última atualização do documento. Deverão ainda ser mantidas informações das datas de vigor e teor das versões anteriores.

3.3 Monitoramento

3.3.1 O monitoramento objetiva verificar se as medidas implementadas estão de acordo com o instituído no PGP e as recomendações emitidas nos RIPDs, bem como se aquelas medidas foram suficientes para conformidade do tratamento de dados à LGPD e para solucionar a situação apontada nos relatórios como inadequada frente aos critérios adotados.

3.3.2 Indicadores de performance

3.3.2.1 Devem buscar identificar o grau de conformidade do INSS frente à LGPD. Destarte, deve dispor de ferramentas e métodos para aferição das medidas de proteção da privacidade já implementadas, a fim de verificar a evolução das unidades no processo de adequação dos serviços e sistemas, bem como se as medidas adotadas são suficientes e atendem aos requisitos de proteção dos dados.

3.3.2.2 A avaliação deve buscar identificar o grau de aderência e conformidade com a LGPD, podendo ser realizado anualmente, e abranger a avaliação dos índices de:

I - maturidade, a ser realizado através do Diagnóstico de Adequação à LGPD;

II - internalização institucional referente à LGPD, o qual poderá ser mensurado por meio de formulários elaborados e aplicados nas diversas etapas - implantação, pós campanha de comunicação, pós capacitação; e

III - adequação de acordos, contratos e convênios à LGPD.

3.3.3 Gestão de incidentes

3.3.3.1 Um incidente de segurança com dados pessoais é qualquer evento adverso confirmado, decorrente de ato intencional ou acidental, relacionado à violação na segurança de dados pessoais, que resulte em divulgação, alteração, destruição ou perda indevidas, bem como acessos não autorizados aos dados pessoais, ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, independentemente do meio em que estão armazenados, comprometendo a confidencialidade, integridade

ou disponibilidade de dados pessoais.

3.3.3.2 Para a eficiência da gestão de incidente é imprescindível a definição dos atores, papéis e responsabilidades, sejam individuais ou coletivos, além da elaboração e divulgação de fluxos com a descrição das atividades de tratamento de incidentes.

3.3.3.3 Em relação aos incidentes de segurança cibernéticos que dizem respeito ao possível vazamento de dados de servidores (de rede, nuvem ou outros), o INSS conta hoje com um fluxo de tratamento definidos pela DTI e DIGOV, que compreende as respostas e formas de tratamento a serem implementadas no caso de incidentes.

3.3.3.4 Dessa forma, o aprimoramento e as atualizações constantes nesse fluxo são medidas imprescindíveis para o fortalecimento da gestão de incidentes no âmbito do INSS, tendo em vista as evoluções tecnológicas e os graves danos à proteção de dados que os incidentes cibernéticos de vazamento de dados podem causar.

3.3.3.5 Assim, o mapeamento e acompanhamento dos incidentes, já previstos no fluxo de respostas aos incidentes cibernéticos, também devem ser constantemente aprimorados, procurando ferramentas cada vez mais eficientes. Estudos para propostas de ações na esfera de proteção têm potencial para fortalecer cada vez mais todo o sistema de gestão de incidentes.

3.3.3.6 A confecção de normas referentes a gestão de incidentes deve ser pautada na clareza das informações, definições objetivas das responsabilidades dos atores envolvidos, alinhamento técnico com a operadora, bem como a definição do escopo e objetivo da norma deve ser compreensível a todos.

3.3.3.7 Além dos incidentes de natureza cibernética, existem outros que também podem comprometer a privacidade no tratamento dos dados pessoais. O vazamento desses dados é um dos mais conhecidos incidentes de segurança e ocorre quando dados são indevidamente acessados, coletados e divulgados ou repassados a terceiros. O dano ao titular pode ser das mais diversas naturezas, como fraudes, tentativas de golpes, uso indevido dos dados, venda dos dados, etc.

3.3.3.8 Para os casos que representem incidentes de segurança, mas não necessariamente envolvam tecnologia da informação, deverá ser desenvolvido plano de resposta, definindo-se fluxos, papéis e responsabilidades, considerando também as orientações da ANPD e demais normativos de regência.

3.3.3.9 A gestão de incidentes de privacidade deve consistir, portanto, na recepção, tratamento e resposta a esses incidentes, buscando identificar sua causa raiz, documentar e avaliar os riscos que afetem as operações de tratamento de dados pessoais.

3.3.4 Análise e Reporte de Resultados

3.3.4.1 A análise e divulgação da evolução das ações e dos resultados obtidos são essenciais para o fortalecimento da cultura de privacidade dos dados e para demonstrar o valor do PGP. Nesse sentido, o INSS disponibilizará as referidas informações através do Portal do INSS, bem como as reportará para toda a alta administração.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL, Constituição da República Federativa do Brasil de 1988. Brasília, DF: 1988

BRASIL, Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais – LGPD. Brasília, DF: 2018

BRASIL, Decreto nº 10.046, de 9 de outubro de 2019. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Brasília, DF: 2019

BRASIL, Decreto nº 10.995, de 14 de março de 2022. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Instituto Nacional do Seguro Social - INSS e remaneja e transforma cargos em comissão e funções de confiança. Brasília, DF: 2022

INSS, Instituto Nacional do Seguro Social. Portaria PRES/INSS nº 30, de 15 de fevereiro de 2023. Designa o Encarregado de Dados no INSS

INSS, Instituto Nacional do Seguro Social. Portaria PRES/INSS nº 1.532, de 8 de dezembro de 2022. Aprova o Regimento Interno do INSS.

INSS, Instituto Nacional do Seguro Social. Portaria DTI/INSS Nº 88, de 27 de dezembro de 2022. Estabelece o Plano de Gestão de Incidentes Cibernéticos (PGIC) no âmbito do Instituto Nacional do Seguro Social;

INSS, Instituto Nacional do Seguro Social. Instrução Normativa PRES/INSS nº 128, de 28 de março de 2022. Disciplina as regras, procedimentos e rotinas necessárias à efetiva aplicação das normas de direito previdenciário.

CCGD, COMITÊ CENTRAL DE GOVERNANÇA DE DADOS. Guia de Boas Práticas LGPD.

SGD, SECRETARIA DE GOVERNO DIGITAL, Guia de Elaboração de Programa de Governança em Privacidade

SGD, SECRETARIA DE GOVERNO DIGITAL, Guia de elaboração de Termo de Uso e Política de Privacidade para serviços públicos

SGD, SECRETARIA DE GOVERNO DIGITAL, Guia de elaboração de inventário de dados pessoais

INSS, Lei Geral de Proteção de Dados Pessoais (LGPD), disponível em https://www.gov.br/inss/pt-br/acesso-a-informacao/lei-geral-de-protecao-de-dadospessoais, acessado em 05/04/2023.

INSS, A LGPD e o INSS, disponível em https://www.gov.br/inss/pt-br/centrais-deconteudo/publicacoes/apresentacoes/SaibaMaisLGPDINSS.pdf, acessado em 05/04/2023

INSS, Política de Privacidade do Meu INSS, disponível em https://www.gov.br/inss/ptbr/canais_atendimento/saiba-tudo-sobre-o-meu-inss/politica-de-privacidade-do-meu-inss, acessado em 05/04/2023

ANPD, Autoridade Nacional de Proteção de Dados. Comunicação de incidente de segurança, disponível em https://www.gov.br/anpd/ptbr/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis, acessado em 06/04/2023