Secretaria de Assistência Social, Combate à Fome e Políticas sobre Drogas

GOVERNO DE PERNAMBUCO
ESTADO DE MUDANÇA

BOLETIM INTERNO Nº 069/2024
Publicado em 25 de Julho de 2024

PRIMEIRA PARTE
Assuntos de Gabinete e Disciplinares

Sem alterações.

SEGUNDA PARTE
Assuntos de Conselhos, Comissões, Comitês e Colegiados

Sem alterações

TERCEIRA PARTE
Assuntos de Licitações, Contratos, Parcerias e Emendas

Sem alterações.

QUARTA PARTE
Assuntos de Pessoal

DESPACHOS DA GERÊNCIA GERAL DE GESTÃO DE PESSOAS

1. DEFIRO O GOZO DE LICENÇA PRÊMIO, em 15 de julho de 2024:

1.1 PROC. 1300000035.002932/2024-35 – LEON JOSÉ FERREIRA, mat. 167722-5, DIAS:60 - A PARTIR DE 08/07/2024 – DECÊNIO 4º.

2. DEFIRO O GOZO DE LICENÇA PRÊMIO, em 25 de julho de 2024:

2.1 PROC. 1300000035.002911/2024-10 – JOSÉ GONÇALVES DE LIMA, mat. 170.112-6, DIAS:30 - A PARTIR DE 03/07/2024 – DECÊNIO 3º.

3. DEFIRO A CONCESSÃO DE LICENÇA PRÊMIO, em 25/07/2024:

3.1 PROC. 1300000035.000547/2024-53 – SEVERINO RONALDO GOMES DE MENEZES, mat.171.401-5, A PARTIR DE 26/08/2022 – 3º DECÊNIO.

CIRILO JOSÉ CABRAL DE HOLANDA CAVALCANTE

Gerente Geral de Gestão de Pessoas

QUINTA PARTE
Assuntos Gerais e de Administração

PORTARIA SAS nº 107, de 25 de julho de 2024.

O SECRETÁRIO DE ASSISTÊNCIA SOCIAL, COMBATE À FOME E POLÍTICAS SOBRE DROGAS, no uso das atribuições conferidas pela Lei nº 18.139, de 18/01/23, atendendo o Decreto Estadual nº 49.265, de 6/08/20, RESOLVE:

Art. 1º Aprovar e instituir a Política de Proteção de Dados Pessoais Local (PPDPL), com o objetivo de estabelecer os princípios, diretrizes e responsabilidades mínimas a serem observados e seguidos para a proteção dos dados pessoais aos planos estratégicos, programas, projetos e processos da SAS, disposta no anexo I;

Art. 2º Aprovar e instituir a Política de Resposta ao Titular de Dados Pessoais (PRTDP), com o objetivo de instruir os agentes púbicos da Secretaria e orientar o titular de dados pessoais no exercício de seus direitos, disposta no anexo II; e

Art. 3º Aprovar e instituir o Plano de Gestão de Incidentes com Dados Pessoais (PGIDP), com objetivo de tratar os incidentes de segurança com dados pessoais ocorridos no âmbito da Secretaria de Assistência Social, Combate à Fome e Políticas sobre Drogas, disposto no anexo III.

CARLOS EDUARDO BRAGA FARIAS

ANEXO I

POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS LOCAL - PPDPL DA SECRETARIA DE ASSISTÊNCIA SOCIAL, COMBATE À FOME E POLÍTICAS SOBRE DROGAS DO ESTADO DE PERNAMBUCO

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 1º A Política de Proteção de Dados Pessoais Local - PPDPL - SAS tem por finalidade estabelecer os princípios, diretrizes e responsabilidades mínimas a serem observados e seguidos para a proteção dos dados pessoais aos planos estratégicos, programas, projetos e processos da Secretaria de Assistência Social, Combate à Fome e Políticas sobre Drogas do Estado de Pernambuco - SAS. Parágrafo único. A Política de Proteção de Dados Pessoais Local – PPDPL – SAS será também composta pelo Plano de Implementação de Controle.

Art. 2º A PPDPL - SAS e suas eventuais normas complementares, metodologias, manuais e procedimentos aplicam-se a todos os setores da SAS, abrangendo os servidores, prestadores de serviço, colaboradores, estagiários, consultores externos e quem, de alguma forma, desempenhe atividades de tratamento de dados pessoais, em nome da Secretaria.

CAPÍTULO II
DOS PRINCÍPIOS E OBJETIVOS

Art. 3º As atividades de proteção de dados pessoais no âmbito da SAS, bem como seus instrumentos resultantes, devem se guiar pelos seguintes princípios, além dos previstos no Decreto nº 49.265, de 6 de agosto de 2020:

I - aderência à integridade e aos valores éticos no tratamento de dados pessoais;

II - adequado suporte de tecnologia da informação para apoiar os processos de adaptação dos tratamentos de dados pessoais;

III - disseminação de informações necessárias ao fortalecimento da cultura do tratamento de dados pessoais em respeitos à Lei Federal nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais - LGPD;

IV - realização de avaliações periódicas internas para verificar a eficácia da proteção de dados pessoais, comunicando o resultado aos responsáveis pela adoção de ações corretivas;
V - estruturação do conhecimento e das atividades em metodologias, normas, manuais e procedimentos; e

VI - aderência dos métodos e modelos de tratamento de dados às exigências regulatórias da LGPD.

Art. 4º A PPDPL-SAS tem por objetivos:

I - proporcionar a adequação das atividades desenvolvidas pela SAS à Lei Geral de Proteção de Dados - LGPD e regulamentos emitidos pela Autoridade Nacional de Proteção de Dados Pessoais - ANPD, em consonância com atingimento dos objetivos estratégicos;

II - produzir informações íntegras, confiáveis e completas das demandas dos titulares dos dados;

III - salvaguardar o direito à proteção dos dados pessoais dos titulares;

IV - possibilitar a adequada apuração dos responsáveis, em todos os níveis, que tenham acesso inadequado aos dados pessoais, em especial, aqueles considerados sensíveis, considerando o disposto na Lei nº 6.123, de 20 de julho de 1968 (Estatuto do Servidor Público Estadual);

V- reduzir os riscos relacionados a incidentes envolvendo dados pessoais, com a implantação de medidas de controle de segurança da informação; e

VI - orientar e servir de diretriz para os agentes de tratamento.

CAPÍTULO III
DAS DIRETRIZES

Art. 5º São diretrizes da PPDPL-SAS:

I - a gestão da integridade com a promoção da cultura ética, focada na preservação da privacidade;

II - o fortalecimento da integridade institucional, a partir do diagnóstico de vulnerabilidades na segurança da informação;

III - a capacitação adequada do Encarregado pelo Tratamento de Dados Pessoais e sua equipe de apoio e dos agentes de tratamento;

IV - o fortalecimento dos mecanismos de comunicação de possíveis incidentes deve ser pautado por: tempestividade, implementação de melhorias de segurança e obtenção de informações sobre as origens da vulnerabilidade;

V - a disponibilização de informações ao titular primada pela atuação transparente e garantia da disponibilização do dado de forma clara, precisa e adequada, conforme legislação vigente; e

VI - a gestão de riscos será sistematizada e suportada pelas premissas de metodologias técnicas.

Parágrafo único. O modelo de gestão de gerenciamento de riscos deve seguir o método de priorização de processos, considerando sua relevância e impacto na estratégia da Secretaria.

CAPÍTULO IV
DOS INSTRUMENTOS

Art. 6º São instrumentos da PPDPL-SAS:

I - a metodologia: o modelo de gestão de riscos deve ser estruturado com base nas orientações da Secretaria da Controladoria-Geral do Estado;

II - a capacitação continuada: o Plano Anual de Capacitação, incluindo o eixo temático de Segurança da Informação e Proteção de Dados Pessoais;

III – a normatização: legislação, manuais e procedimentos formalmente definidos, em especial, no âmbito da SAS; e

IV - a solução tecnológica: o processo de gestão de riscos deve ser apoiado por adequado suporte de tecnologia da informação.

CAPÍTULO V
DAS INSTÂNCIAS DE SUPERVISÃO, DA COMPOSIÇÃO E DAS ATRIBUIÇÕES E RESPONSABILIDADES

Seção I
Da Controladora, do Encarregado e dos Operadores

Art. 7º A Secretaria de Assistência Social, Combate à Fome e Políticas sobre Drogas do Estado de Pernambuco é a Controladora dos dados pessoais por ela tratados, nos termos das suas competências legal e institucional.

Art. 8º O Secretário de Assistência Social, Combate à Fome e Políticas sobre Drogas do Estado de Pernambuco, enquanto representante legal, tem responsabilidade pela definição final da gestão dos riscos e controles internos quanto à adequação à LGPD na SAS, nos termos do art. 12 do Decreto nº 49.265, de 2020.

Art. 9º O Encarregado pelo Tratamento de Dados Pessoais, autoridade indicada pelo Secretário de Assistência Social, Combate à Fome e Políticas sobre Drogas do Estado de Pernambuco para fins da LGPD, terá responsabilidade pelo gerenciamento do projeto de implantação e dos riscos e controles internos quanto à adequação à LGPD na Secretaria, conforme art. 13 do Decreto nº 49.265, de 2020.

Parágrafo único. O Encarregado pelo Tratamento de Dados Pessoais da SAS será assessorado pelo Comitê de Proteção de Dados Pessoais - CPD, instituído por portaria do Secretário de Assistência Social, Combate à Fome e Políticas sobre Drogas do Estado de Pernambuco.

Art. 10. Os provedores de serviços de Tecnologia da Informação e Comunicação - TIC e demais prestadores de serviços à SAS que tratem dado pessoal em nome desta serão considerados operadores e deverão aderir a esta Política, além de cumprir os deveres legais, contratuais e de parceria respectivos, dentre os quais se incluirão, mas não se limitarão aos seguintes:

I - assinar contrato ou termo de compromisso com cláusulas específicas sobre proteção de dados pessoais requeridas pela SAS;

II - apresentar evidências e garantias suficientes de que aplica adequado conjunto de medidas técnicas e administrativas de segurança, no âmbito da tecnologia, para a proteção dos dados pessoais, segundo a legislação, os instrumentos contratuais e de compromissos;

III - manter os registros de tratamento de dados pessoais que realizar, assim como aqueles compartilhados, com condições de rastreabilidade e de prova eletrônica a qualquer tempo;

IV - seguir fielmente as diretrizes e instruções transmitidas pela SAS;

V - permitir acesso a dados pessoais somente para o pessoal autorizado que tenha estrita necessidade e que tenha assumido compromisso formal de preservar a confidencialidade e segurança de tais dados, devendo tal compromisso estar disponível em caráter permanente para exibição à SAS, mediante solicitação;

VI - permitir a realização de auditorias da SAS e disponibilizar toda a informação necessária para demonstrar o cumprimento das obrigações estabelecidas;

VII - auxiliar, sempre que necessário, no atendimento pela SAS de obrigações perante titulares de dados pessoais, autoridades competentes ou quaisquer outros legítimos interessados;

VIII - comunicar formalmente e de imediato à SAS a ocorrência de qualquer risco, ameaça ou incidente de segurança que possa acarretar comprometimento ou dano potencial ou efetivo a titular de dados pessoais, evitando atrasos por conta de verificações ou inspeções;

IX - descartar de forma irrecuperável, ou devolver para a SAS, todos os dados pessoais e as cópias existentes, após a satisfação da finalidade respectiva ou o encerramento do tratamento por decurso de prazo ou por extinção de vínculo legal ou contratual.

Seção II
Do apoio institucional

Art. 11. O Comitê de Proteção de Dados Pessoais será designado por meio de portaria do Secretário de Assistência Social, Combate à Fome e Políticas sobre Drogas do Estado de Pernambuco.

Art. 12. Os Gestores de Processos correspondem a todo e qualquer responsável pela unidade de execução de um determinado processo de trabalho, inclusive sobre a gestão de riscos.

Seção III
Das Atribuições e Responsabilidades

Art. 13. Compete ao Secretário de Assistência Social, Combate à Fome e Políticas sobre Drogas do Estado de Pernambuco, enquanto representante legal:

I - aprovar práticas e princípios de conduta e padrões de tratamento de dados pessoais;

II - aprovar as alterações da PPDPL-SAS;

III – aprovar o Plano de Implementação de Controles Internos;

IV - aprovar a estrutura, extensão e conteúdo do inventário de dados pessoais;

V - acompanhar os ajustes contratuais e de termos de compromisso decorrentes da implementação da PPDPL-SAS;

VI – tomar ciência do diagnóstico preliminar de controles internos;

VII - tomar conhecimento do andamento e resultados da avaliação de controles internos;

VIII - tomar ciência do monitoramento do PPDPL-SAS;

IX - aprovar e promover o Plano de Gestão de Incidentes com Dados Pessoais;

X - aprovar o Relatório de Impacto de Proteção aos Dados Pessoais, na forma da lei, com o apoio técnico das áreas jurídica e tecnológica da entidade;

XI - Designar o Encarregado pelo Tratamento de Dados Pessoais; e

XII - Designar o Comitê de Proteção de Dados Pessoais.

Art. 14. Compete ao Encarregado pelo Tratamento de Dados Pessoais:

I - propor práticas e princípios de conduta e padrões de tratamento de dados pessoais;

II - propor alterações da PPDPL-SAS;

III - consolidar propostas de ações, avaliar e elaborar o Plano de Implementação de Controles Internos;

IV - elaborar a estrutura, extensão e conteúdo do inventário de dados pessoais;

V - realizar, em conjunto com a Gerência Geral de Tecnologia e Informações Estratégicas, a Superintendência de Controle Interno e o Gestor de Processo, o diagnóstico preliminar e o inventário de dados pessoais;

VI - promover a aderência às regulamentações, leis, códigos, normas e padrões na condução da PPDPL-SAS;

VII - recomendar ajustes contratuais e de termos de compromisso decorrentes da implementação da PPDPL-SAS;

VIII - definir o diagnóstico preliminar de controles internos;

IX - instituir e acompanhar a avaliação de controles internos;

X - monitorar o PPDPL-SAS;

XI - elaborar o Plano de Gestão de Incidentes com Dados Pessoais;

XII - subsidiar a elaboração do Relatório de Impacto de Proteção aos Dados Pessoais, na forma da lei, com o apoio técnico das áreas jurídica e tecnológica do órgão;

XIII - cumprir os objetivos e metas previstas na Política de Proteção de Dados Pessoais Local;

XIV - receber reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências, em articulação com a Ouvidoria;

XV- receber comunicações da Autoridade Nacional de Proteção de Dados Pessoais - ANPD e adotar providências;

XVI - orientar os funcionários e os operadores no cumprimento das práticas necessárias à proteção de dados pessoais;

XVII - quando provocado, entregar o Relatório de Impacto de Proteção aos Dados Pessoais, na forma da lei, com o apoio técnico das áreas jurídica e tecnológica da entidade;

XVIII - atender às normas complementares da Autoridade Nacional de Proteção de Dados Pessoais; e

XIX - informar à Autoridade Nacional de Proteção de Dados Pessoais e aos titulares dos dados pessoais eventuais incidentes de privacidade de dados pessoais, dentro da execução de um Plano de Gestão de Incidentes com Dados Pessoais.

Art. 15. Compete à Gerência Geral de Assuntos Jurídicos:

I - auxiliar o Encarregado pelo Tratamento de Dados Pessoais, gestores de processos e aos operadores na resolução de controvérsias jurídicas relacionadas à aplicação da LGPD e dos normativos dela decorrentes;

II - emitir manifestações quanto aos aspectos jurídico-formais dos ajustes contratuais e de termos de compromisso decorrentes da implementação da PPDPL-SAS; e

III- apoiar a elaboração de normativos e instrumentos internos, em especial Termos de Uso e Termos de Consentimento, quanto à proteção de dados pessoais.

Parágrafo Único. O exercício das competências elencadas no caput deste dispositivo dar-se-ão à luz dos procedimentos estabelecidos no Decreto nº 52.359, de 02 de março de 2022, considerando a exclusividade da Procuradoria Geral do Estado na representação judicial e consultoria jurídica dos órgãos, autarquias e fundações públicas do Poder Executivo.

Art. 16. Compete à Gerência Geral de Tecnologia e Informações Estratégicas:

I – prestar orientação técnica ao Encarregado pelo Tratamento de Dados Pessoais e aos operadores sobre questionamentos e boas práticas em segurança da informação, no âmbito da tecnologia;

II - apoiar, no âmbito da tecnologia, as ações de capacitação nas áreas de Segurança da Informação e Proteção de Dados Pessoais;

III- apoiar o Encarregado pelo Tratamento de Dados Pessoais, a Superintendência de Controle Interno e os Gestores de Processos, na elaboração do diagnóstico preliminar e do inventário de dados pessoais;

IV - apoiar o Encarregado pelo Tratamento de Dados Pessoais, a Superintendência de Controle Interno e o Gestor de Processo, na avaliação de controles internos dos processos priorizados;

V - apoiar, com propostas técnicas de segurança da informação, no âmbito da tecnologia, a elaboração do Plano de Gestão de Incidentes com Dados Pessoais;

VI - apoiar a elaboração do Relatório de Impacto de Proteção aos Dados Pessoais;

VII - extrair estrutura e conteúdo de dados pessoais em sistemas informatizados para elaboração do inventário de dados pessoais;

VIII - extrair conteúdo de dados pessoais em sistemas informatizados para atendimentos das demandas dos titulares, quando não houver meio seguro de extração direta pelo Gestor de Processo correspondente ou pessoa de sua estrutura organizacional;

IX - apoiar, com propostas técnicas de segurança da informação, no âmbito da tecnologia, a elaboração instrumentos; e

X - apoiar a elaboração do Plano de Implementação de Controles Internos.

Art. 17. Compete à Superintendência de Controle Interno:

I - propor melhorias metodológicas no gerenciamento dos riscos associados à proteção de dados pessoais;

II - realizar, em conjunto com o Encarregado pelo Tratamento de Dados Pessoais, a Gerência Geral de Tecnologia e Informações Estratégicas e os Gestores de Processos, o diagnóstico preliminar e o inventário de dados pessoais;

III - realizar, em conjunto com o Encarregado pelo Tratamento de Dados Pessoais, a unidade de tecnologia da informação e os Gestores de Processos, a avaliação de controles internos dos processos priorizados;

IV - apoiar a elaboração do Relatório de Impacto de Proteção aos Dados Pessoais; e

V - apoiar a elaboração do Plano de Implementação de Controles Internos.

Art. 18. Compete à Ouvidoria:

I - apoiar no recebimento de manifestações e comunicações dos titulares de dados pessoais;

II - realizar a interlocução do titular de dados pessoais com o Encarregado pelo Tratamento de Dados Pessoais;

III - mapear as principais possíveis demandas dos titulares de dados pessoais, considerando o inventário de dados pessoais;

IV - apoiar o Encarregado pelo Tratamento de Dados Pessoais na propositura de ações que facilitem o atendimento às demandas dos titulares de dados pessoais; e

V - apoiar a transparência dos tratamentos de dados pessoais sob a responsabilidade da SAS.

Art. 19. Compete à Superintendência de Comunicação:

I - apoiar a promoção da disseminação da cultura de proteção de dados pessoais;

II – divulgar a oferta de capacitações dos agentes públicos no exercício do cargo, função e emprego no conteúdo de proteção de dados pessoais; e

III - praticar outros atos de natureza técnica e administrativa necessários ao exercício de suas responsabilidades.

Art. 20. Compete aos Gestores de Processos:

I - realizar, em conjunto com o Encarregado pelo Tratamento de Dados Pessoais, a Superintendência de Controle Interno e a Gerencia Geral de Tecnologia e Informações Estratégicas, a elaboração do diagnóstico preliminar e o inventário de dados pessoais;

II - realizar, em conjunto com o Encarregado pelo Tratamento de Dados Pessoais, a Superintendência de Controle Interno e a Gerencia Geral de Tecnologia e Informações Estratégicas, a avaliação de controles internos dos processos priorizados;

III - elaborar propostas de ação ao Plano de Implementação de Controles dos processos sob sua responsabilidade;

IV - cumprir os objetivos e as prioridades estabelecidas pelo Plano de Implementação de Controles;

V - gerenciar as ações do Plano de Implementação de Controles e avaliar os seus resultados dos processos sob sua responsabilidade;

VI - disponibilizar o conteúdo de dados pessoais para elaboração do inventário de dados pessoais;

VII - disponibilizar conteúdo de dados pessoais para atendimentos das demandas dos titulares;

VIII - cumprir com as recomendações e observar as orientações emitidas pelo Secretário de Assistência Social, Combate à Fome e Políticas sobre Drogas do Estado de Pernambuco e pelo Encarregado pelo Tratamento de Dados Pessoais; e

IX - adotar princípios de conduta e padrões de comportamento no âmbito da sua estrutura organizacional.

Art. 21. Compete ao Comitê de Proteção de Dados Pessoais:

I - acompanhar as ações para implementação da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados) no âmbito desta Secretaria, zelando pela observância das recomendações definidas no Decreto Estadual nº 49.265, de 2020 (Política Estadual de Proteção de Dados Pessoais – PEPDP);

II - coordenar ações, referente a elaboração do inventário e implementação de melhorias nos processos organizacionais, nas áreas de negócio responsáveis pelos mapeamentos dos tratamentos de dados;
III - assessorar o controlador de dados, quando solicitado, na formulação de princípios e diretrizes para a gestão de dados pessoais e na sua regulamentação;

IV - acompanhar o programa de conscientização sobre a LGPD no âmbito da SAS; e

V - auxiliar o Encarregado pelo Tratamento de Dados Pessoais, fornecendo-lhe subsídios e propostas para o desempenho de sua missão.

CAPÍTULO VI
DO TRATAMENTO DE DADOS PESSOAIS

Art. 22. O tratamento de dados pessoais pela SAS será realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar suas competências legais e de cumprir as atribuições legais do serviço público.

Parágrafo único. O Regulamento da SAS e demais normas de organização definem as funções e atividades que constituem as finalidades e balizadores do tratamento de dados pessoais para fins desta Política.

Art. 23. Em atendimento a suas competências legais, a SAS poderá, no estrito limite de suas atividades, tratar dados pessoais com dispensa de obtenção de consentimento pelos respectivos titulares.

Parágrafo único. Eventuais atividades que transcendam o escopo da função institucional estarão sujeitas à obtenção de consentimento dos titulares dos dados pessoais a serem objeto de tratamento.

Art. 24. A SAS manterá contratos com terceiros para o fornecimento de produtos ou a prestação de serviços necessários a suas operações, os quais poderão, conforme o caso, importar em disciplina própria de proteção de dados pessoais, a qual deverá estar disponível e ser consultada pelos interessados.

Art. 25. Os dados pessoais tratados pela SAS deverão ser:

I - protegidos por procedimentos internos para registrar autorizações e utilizações;

II - mantidos disponíveis, exatos, adequados, pertinentes e atualizados, sendo retificado ou eliminado o dado pessoal mediante informação ou constatação de impropriedade ou face a solicitação de remoção, devendo a neutralização ou descarte do dado observar as condições e períodos da tabela de temporalidade de retenção de dados;

III - compartilhados somente para o exercício das funções institucionais, para atendimento de políticas públicas aplicáveis ou com órgãos de pesquisa, anonimizados sempre que possível; e

IV - revistos em periodicidade mínima bianual, sendo de imediato eliminados aqueles que já não forem necessários, por terem cumprido sua finalidade ou por ter se encerrado o seu prazo de retenção.

Art. 26. A responsabilidade da SAS pelo tratamento de dados pessoais estará circunscrita ao dever de se ater ao exercício de sua competência legal e institucional e de empregar boas práticas de governança e de segurança.

Art. 27. Os casos omissos ou excepcionalidades serão deliberados pelo Secretário de Assistência Social, Combate à Fome e Políticas sobre Drogas do Estado de Pernambuco, consultado o Comitê de Proteção de Dados Pessoais e o Encarregado pelo Tratamento de Dados Pessoais.

ANEXO II

POLÍTICA DE RESPOSTA AO TITULAR DE DADOS PESSOAIS - PRTDP DA SECRETARIA DE ASSISTÊNCIA SOCIAL, COMBATE À FOME E POLÍTICAS SOBRE DROGAS DO ESTADO DE PERNAMBUCO

CAPÍTULO I
DA FINALIDADE E ABRANGÊNCIA

Art. 1º A Política de Resposta ao Titular de Dados Pessoais – PRTDP – SAS tem como objetivo tecer instruções para os agentes púbicos da Secretaria e orientar o titular de dados pessoais no exercício de seus direitos, especialmente no que diz respeito às solicitações sobre dados pessoais à Secretaria de Assistência Social, Combate à Fome e Políticas sobre Drogas.

Art. 2º Essa Política possui abrangência a todo aquele indivíduo submetido à Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709, de 14 de agosto de 2018, independentemente de possuir seu dado tratado pela Secretaria.

Art. 3º Esta Política tem efeitos nos casos em que a atuação da Secretaria se demonstra como Controladora de dados pessoais, de modo que todos os direitos previstos e elencados serão analisados, ainda que ilegítimos ou despropositados, para, a partir disso, atendidos caso ocorra previsão em lei.

Parágrafo único. Nas situações em que se evidenciar a atuação da Secretaria como Operador, deverá haver o direcionamento dos melhores esforços para levar ao conhecimento do Controlador a solicitação efetuada, como sinal de boas práticas.

CAPÍTULO II
DA FORMA DE CONTATO

Art. 4º A comunicação entre o titular de dados pessoais e a Secretaria será realizado pela Ouvidoria, através dos canais de comunicação disponibilizados em site oficial da Secretaria.

Art. 5º A Secretaria empreenderá todos os esforços para atender tais pedidos no menor espaço de tempo possível, respeitando os prazos sugeridos para cada tipo de solicitação.

CAPÍTULO III
DAS SOLICITAÇÕES

Seção I
Disposições gerais sobre as solicitações

Art. 6º Toda pessoa natural poderá entrar em contato com a Secretaria para apresentar solicitações pertinentes aos seus próprios dados pessoais.

Art. 7º As solicitações que podem ser realizadas por pessoas naturais compreendem, mas não se limitam a:

I - Solicitação de confirmação da existência de tratamento;

II - Solicitação de acesso aos dados;

III - Solicitação de correção de dados incompletos, inexatos ou desatualizados;

IV - Solicitação de bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a lei;

V - Solicitação de eliminação dos dados pessoais tratados com o consentimento do titular e revogação do consentimento;

VI - Solicitação de portabilidade dos dados pessoais; e

VII - Solicitação de informação das entidades públicas e privadas com as quais a Secretaria realizou uso compartilhado de dados e solicitações diversas.

Art. 8º A Secretaria preserva o direito de não atender solicitações que se mostrem infundadas, excessivas, ilegais, envolveria um esforço desproporcional para atendimento, implique em divulgação e exposição de segredos comercial e industrial da SAS ou quando houver qualquer risco de violação de dados pessoais.

Parágrafo único. Nas situações previstas no caput deste artigo, a Secretaria apresentará sua justificativa fundamentada diante da impossibilidade de atendimento.

Art. 9º Em solicitações realizadas por terceiros devem-se apresentar instrumento de procuração por meio de instrumento público, registrado em Cartório de Notas, com a finalidade específica da solicitação apresentada.

Parágrafo único. Se não houver evidências de que terceiros estejam autorizados a agir em nome do titular, a Secretaria não atenderá a solicitação.

Art. 10. É assegurada a gratuidade das solicitações realizadas por pessoa natural, nos termos do artigo 6º.

Parágrafo único. A Secretaria não custeará nem reembolsará as despesas em cartório, necessárias para a solicitações realizadas por terceiros, previsto no artigo 9º dessa Política.

Art. 11. Durante o processo de resposta ao titular de dados pessoais, a Secretaria deve realizar a validação do titular do dado pessoal, como medida de mitigação de riscos.

Art. 12. Para efeitos da contagem de qualquer prazo em dias indicados nessa Política, computar-se-ão somente os dias úteis vigentes na cidade do Recife, que serão contados excluindo o dia do começo e incluindo o dia do vencimento.

Art. 13. O registro de solicitações será armazenado pelo período de cinco anos, com os dados pessoais do solicitante anonimizados em até três dias úteis após a data de envio da resposta, de maneira que seja impossível a identificação do titular.

Parágrafo único. Novas solicitações de um mesmo titular, após a anonimização dos dados, deverão passar por uma nova etapa de autenticação, visto que não serão armazenados dados pessoais de solicitantes após a resposta.

Seção II
Solicitação de confirmação da existência do tratamento

Art. 14. Mediante a solicitação de confirmação da existência de tratamento, a Secretaria responderá se realiza ou não realiza o tratamento de dados pessoais do solicitante.

Parágrafo único. Em resposta de inexistência de dados armazenados pela Secretaria, é possível que ocorra a eliminação ou anonimização dos dados pessoais, de maneira que seja impossível identificar o titular do dado, não sendo este mais considerado um dado pessoal.

Art. 15. O prazo para a resposta de solicitações de confirmação da existência do tratamento é de cinco dias úteis.

Seção III
Solicitação de acesso aos dados

Art. 16. Mediante solicitação de acesso aos dados pessoais, a Secretaria exibirá todos os dados pessoais que são tratados, do titular solicitante.

Parágrafo único. Caso não seja identificado o tratamento dos dados pessoais solicitados, a Secretaria retornará com a informação negativa, de acordo com os artigos 14 e 15 desta Política.

Art. 17. O prazo para a resposta de solicitação de acesso aos dados pessoais é de dez dias úteis.

Seção IV
Solicitação de correção de dados incompletos, inexatos ou desatualizados

Art. 18. Após acesso aos seus dados pessoais, conforme solicitação disposta nos artigos 16 e 17 desta Política, o titular solicitante poderá realizar a solicitação de correção de dados incompletos, inexatos ou desatualizados.

Parágrafo único. Não serão atendidas as solicitações de complementações de tipos de dados além daqueles que a Secretaria considera necessários para a finalidade do tratamento.

Art. 19. Caso a Secretaria tenha alguma dúvida diante da solicitação de alteração de dados, pode solicitar o envio digitalizado do documento que contenha o dado a ser alterado, como forma de validação da informação, preservando assim a qualidade dos dados pessoais.

Art. 20. O prazo para a resposta de solicitação de correção de dados incompletos, inexatos ou desatualizados é de dez dias úteis.

Seção V
Solicitação de bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a Lei

Art. 21. O titular pode realizar a solicitação de bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a Lei, mediante as seguintes condições:

I – o tipo de dado pessoal não é necessário ou condiz para com a finalidade do tratamento;

II – o tratamento do dado pessoal não é realizado de acordo com alguma hipótese legal prevista na LGPD; ou

III – o dado pessoal é tratado em desconformidade com a LGPD.

Art. 22. O prazo para a resposta de solicitação de bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a Lei é de dez dias úteis.

Seção VI
Solicitação de eliminação dos dados pessoais tratados com o consentimento do titular e revogação do consentimento

Art. 23. O titular solicitante tem o direito de requerer a eliminação ou exclusão de seus dados pessoais, quando tratados sob o seu consentimento.

Parágrafo único. Este não é um direito absoluto, pois pode haver razões legais ou legítimas para reter os dados pessoais.

Art. 24. O titular solicitante tem o direito de revogar o consentimento para o tratamento de seus dados nos casos em que o referido tratamento for baseado no consentimento.

Parágrafo único. A retirada do consentimento não afeta a legalidade do tratamento baseado no consentimento antes da respectiva retirada.

Art. 25. O prazo para a resposta de solicitação de eliminação dos dados pessoais tratados com o consentimento do titular é de dez dias úteis.

Art. 26. O prazo para a resposta de solicitação da revogação do consentimento do titular é de cinco dias úteis.

Seção VII
Solicitação de portabilidade dos dados pessoais

Art. 27. O titular solicitante tem o direito de solicitar a portabilidade dos dados a outro fornecedor de serviço ou produto, da iniciativa pública ou privada.

Art. 28. Os dados pessoais devem ser transferidos em formato estruturado, em formato legível por máquina, sempre que tal seja tecnicamente possível.

Parágrafo único. Não é obrigação da Secretaria adotar ou manter sistemas de tratamento que sejam tecnicamente compatíveis com o outro fornecedor.

Art. 29. A Secretaria não poderá ser responsabilizada por eventual violação desse arquivo e dados armazenados após sair da esfera de controle.

Art. 30. O prazo para a resposta de solicitação de portabilidade dos dados pessoais é de vinte dias úteis.

Seção VIII
Solicitação de informação das entidades públicas e privadas com as quais a Secretaria realizou uso compartilhado de dados

Art. 31. A pessoa natural poderá solicitar informações das entidades públicas e privadas com as quais a Secretaria realizou uso compartilhado de dados, sendo por nós respondido quais dados pessoais realizou-se o uso compartilhado e com quais entidades.

Art. 32. O prazo para a resposta de Solicitação de informação das entidades públicas e privadas com as quais a Secretaria realizou uso compartilhado de dados é de vinte dias úteis.

Seção IX
Solicitações diversas

Art. 33. A pessoa natural poderá realizar solicitações não previstas nesta Política, a qual será respondida caso não exista nenhuma vedação que fundamente a justa recusa pela Secretaria.

Art. 34. Considerando a impossibilidade de previsão do teor da solicitação, o prazo para a resposta pela Secretaria é de, no máximo, a depender da solicitação, de trinta dias úteis.

CAPÍTULO IV
DA CONTIUIDADE

Art. 35. Esta Política deve ser revisada com periodicidade anual ou conforme o entendimento e decisão do Comitê de Proteção de Dados Pessoais – CPD – SAS.

Art. 36. Esta Política poderá ser atualizada conforme alterações legislativas ou procedimentais da Secretaria com relação ao tratamento de dados pessoais.

ANEXO III

PLANO DE GESTÃO DE INCIDENTES COM DADOS PESSOAIS - PGIDP
Secretaria de Assistência Social, Combate à Fome e Políticas sobre Drogas do Estado de Pernambuco - SAS/PE

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

EQUIPE TÉCNICA DE ELABORAÇÃO

Encarregado pelo Tratamento de Dados Pessoais
Luan Moura Paes Barreto

Comitê de Proteção de Dados Pessoais
Sandra Carla Leal Santos
Bruna van der Linden Barbosa
Márcio Alexandre Marques Silva
Semíramis da Rocha Vieira Chaves de Oliveira
Ricardo Pereira da Silva
Thais Estevam Fernandes de Castro
Maria Clara da Conceição Silva

Superintendência de Controle Interno
Miriam Araújo Teixeira

SUMÁRIO

1. INTRODUÇÃO

Este Plano de Tratamento de Incidentes com Dados Pessoais tem por finalidade apresentar orientações, com o intuito de auxiliar os agentes públicos da SAS responsáveis por realizarem a gestão de respostas à incidentes de segurança com dados pessoais no âmbito institucional. Trazendo uma visão macro sobre resposta a esses incidentes, para fomentar a adequação à Lei Geral de Proteção de Dados Pessoais.
O plano dispõe de medidas que devem ser adotadas no caso de uma emergência ou evento de risco que possa ocasionar danos aos ativos tecnológicos da SAS, viabilizando, inclusive, a comunicação apropriada e tempestiva à ANPD, quando for o caso.
Este plano será publicado nos seguintes endereços eletrônicos https://www.sas.pe.gov.br/lgpd/ e https://www.sas.pe.gov.br/lei-de-acesso-a-informacao/ onde deverá ser mantido atualizado frequentemente, de acordo com as novas diretrizes determinadas pelas autoridades em privacidade e segurança da informação ou segundo eventuais alterações que ocorram nos normativos vigentes relacionados à privacidade e segurança da informação e outras referências utilizadas neste documento.

2. OBJETIVOS

2.1 OBJETIVO GERAL

Orientar os responsáveis por realizarem a gestão de respostas à incidentes de segurança com dados pessoais da SAS em como responder às emergências com incidentes de segurança da informação, de forma documentada, formalizada, rápida e confiável, ao passo em que resguarde as evidências que possam ajudar a prevenir novos incidentes e a atender às exigências legais de comunicação e transparência.

2.2 OBJETIVOS ESPECÍFICOS

Determina-se como objetivos específicos deste plano:

- Conferir clareza sobre o fluxo de procedimentos adequados e responsáveis no caso de incidentes;
- Preservar a reputação e imagem da SAS;
- Assegurar respostas rápidas, efetivas e coordenadas;
- Quantificar e monitorar desempenho; e
- Evoluir continuamente com as lições aprendidas.

3. DEFINIÇÕES GERAIS

Para auxílio na leitura deste plano, serão adotadas as seguintes definições:

Agente de tratamento: aqueles que podem ter alguma ação no tratamento de um incidente que coloque em risco a segurança dos dados pessoais.

Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais.

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

Encarregado pelo Tratamento de Dados Pessoais: é a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Autoridade Nacional de Proteção de Dados (ANPD): entidade responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional, conforme as atribuições descritas no art. 55-J da LGPD e no Decreto nº 10.474 de 26 de agosto de 2020.

Dado pessoal: é toda informação relacionada à pessoa natural identificada ou identificável.

Inventário de Dados Pessoais (IDP): representa um artefato primordial para documentar o tratamento de dados pessoais realizados pela instituição.

Incidente: evento, ação ou omissão que tenha permitido ou possa vir a permitir acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou, ainda, apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação.

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 em 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.

Incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.

Medidas de segurança: medidas técnicas e/ou administrativas adotadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

Lei Geral de Proteção de Dados Pessoais (LGPD): Lei no 13.709, de 14 de agosto de 2018, cujo objetivo é proteger os direitos fundamentais de privacidade e de liberdade de cada indivíduo.

Relatório final: documento que contém todas as evidências e ações realizadas para tratamento do incidente e que deve ser emitido ao final das tratativas.

Relatório de Impacto a Proteção de Dados (RIPD): documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que tem o potencial de gerar riscos às liberdades civis e aos direitos fundamentais dos titulares, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

4. INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS

Em caso de incidente que coloque em risco a segurança de dados pessoais devem ser realizados alguns procedimentos específicos que são listados abaixo:

4.1. AVALIAR INTERNAMENTE O INCIDENTE

Avaliar internamente o incidente para obter informações iniciais sobre o impacto do ocorrido, tais como:

- Origem;
- Categoria;
- Quantidade de titulares e de dados pessoais afetados;
- Categoria e quantidade de dados afetados;
- Consequências do incidente para os titulares e para a entidade;
- Criticidade; e
- Probabilidade.

Além disso, é necessário preservar todas as evidências do incidente.

4.2. COMUNICAR AO ENCARREGADO

Comunicar ao encarregado da entidade a existência do incidente, caso envolva dados pessoais.

4.3. REGISTRAR INCIDENTE DE SEGURANÇA

É necessário o registro de informações sobre o incidente de segurança, sendo estas mantidas por um prazo de, no mínimo, cinco anos.
Conforme o art. 10 da Resolução CD/ANPD Nº 15/2024, o controlador é responsável por manter o registro do incidente de segurança, mesmo que não tenha sido comunicado à ANPD e aos titulares. Tal registro deverá conter minimamente os seguintes itens:

I. A data de conhecimento do incidente;
II. A descrição geral das circunstâncias em que o incidente ocorreu;
III. A natureza e a categoria de dados afetados;
IV. O número de titulares afetados;
V. A avaliação do risco e os possíveis danos aos titulares;
VI. As medidas de correção e mitigação dos efeitos do incidente, quando aplicável;
VII. A forma e o conteúdo da comunicação, se o incidente tiver sido comunicado à ANPD e aos titulares; e
VIII. Os motivos da ausência de comunicação, quando for o caso.

4.4. CONSULTAR O SETOR DE TECNOLOGIA DA INFORMAÇÃO DA SECRETARIA

Consultar o setor de tecnologia da informação em caso de incidentes na rede computacional. Após análise preliminar do incidente, o setor deve dar ciência aos gestores dos processos afetados, informando, por exemplo, registros de acesso e análise do fluxo de dados, identificando uma possível continuidade do ataque.

4.5. COMUNICAR A TODOS OS ENVOLVIDOS

O Controlador deve comunicar a existência do incidente a todos os envolvidos, conforme o caso e termos previstos na LGPD.

4.6. COMUNICAR À ANPD

Comunicar à ANPD e ao titular de dados pessoais (conforme art. 48 da LGPD) a existência do incidente e encaminhar o relatório inicial.

4.7. EMITIR O RELATÓRIO FINAL

Emitir o relatório final contendo os tipos de dados e a quantidade de titulares afetados. Deve também acompanhar um relatório técnico de tratamento que permita avaliar a extensão e adequação de medidas para incidentes futuros.

5. RESPOSTAS AOS INCIDENTES DE SEGURANÇA

A SAS deverá dar respostas aos seus incidentes conforme as orientações das fases descritas abaixo, utilizando o fluxo detalhado e o checklist disponíveis no final deste documento.

5.1. PREPARAÇÃO/NOTIFICAÇÃO

Fase de importante estabelecimento da capacidade de resposta à incidentes, como também a evitá-los e garantir que sistemas, redes e aplicativos sejam suficientemente seguros. Nesta fase, o Encarregado pelo Tratamento de Dados Pessoais, o Setor de Tecnologia da Informação e a Equipe Técnica de Segurança da Informação estarão preparados para responder e dar os encaminhamentos para juntos atuarem na resposta aos incidentes.

5.2. ANÁLISE/AVALIAÇÃO

Os incidentes podem ser detectados por vários meios ou recebidos nos canais de comunicação da SAS. Assim que o órgão for notificado deverá ser iniciada uma avaliação mais detalhada do incidente pelo Encarregado e a Equipe Técnica de Segurança da Informação, que farão a classificação e definirão a sua criticidade.

5.2.1. Avaliação do incidente

Quando a Secretaria tem conhecimento do incidente de segurança, deve ser realizada uma avaliação interna para que sejam obtidas informações como:

a) qual vulnerabilidade: foi explorada no evento, abrangendo situações como: acesso indevido aos dados pessoais; roubo de dados; ataques cibernéticos; erros de programação de aplicativos e sistemas internos;

engenharia social; descartes indevidos; repasse de dados pessoais; roubo, venda e utilização de dados tutelados pela entidade; comprometimento de senhas de acesso; e outras.

b) fonte dos dados pessoais: meio pelo qual foram obtidos os dados pessoais, tais como preenchimento de formulário eletrônico ou não eletrônico por parte do titular, API, uso compartilhado de dados, XML e cookies.

c) categoria de dados pessoais: sensíveis e de crianças e adolescentes.

d) extensão do vazamento: quantificar os titulares e os dados pessoais que tiveram a sua segurança violada neste evento.

e) avaliação do impacto ao titular: avaliar quais são os impactos que o incidente pode gerar aos titulares.

f) avaliação do impacto no serviço: avaliar os impactos que o incidente pode gerar a entidade como perda de confiabilidade do cidadão, ações judiciais, danos à imagem da instituição em âmbito nacional e internacional, prejuízo à entidade em contratos com fornecedores e clientes, e impacto total ou parcial nas atividades desenvolvidas pela entidade.

Figura 1: Atividades de avaliação interna do incidente com dados pessoais

Fonte: Guia de Resposta a Incidentes de Segurança Ministério da Gestão e da Inovação em Serviços Públicos

5.3. CONTENÇÃO, ERRADICAÇÃO E RECUPERAÇÃO

O Gestor do Processo e o responsável pelo sistema impactados, quando for o caso, devem ser acionados para se manifestarem sobre os procedimentos de resposta, contenção e erradicação.
O objetivo das medidas de contenção e erradicação é limitar o dano e isolar os sistemas afetados para evitar mais danos. Nessa fase, conforme a necessidade e a autorização obtida, poderá ser realizado o desligamento dos sistemas inteiros ou de funcionalidades específicas e colocados avisos de indisponibilidade para manutenção. Todos os cuidados devem ser adotados para não impactar evidências que poderiam ser usadas para identificar autoria, origem e método usado para quebrar a segurança.

5.4. ATIVIDADES PÓS-INCIDENTE

Na fase de atividades pós-incidente, serão implementadas algumas atividades em busca da melhoria contínua de seus processos de resposta a incidentes, além de definir procedimentos para retenção de evidências e uso dos dados coletados em incidentes.

6. COMUNICAÇÃO À ANPD E TITULAR DE DADOS PESSOAIS

6.1. À ANPD

A ANPD estipula o prazo de 3 (três) dias úteis para comunicação de incidente de segurança à proteção de dados que será contado a partir do conhecimento pelo controlador de que o incidente afetou os dados pessoais por ele tratado. O incidente deve ser comunicado pelo Controlador, por meio do encarregado (acompanhado de documento comprobatório de vínculo contratual, empregatício ou funcional), ou por meio de representante constituído respeitando o prazo estabelecido. O art. 48 da LGPD e o art. 5º da Resolução CD/ANPD Nº 15/2024 determinam que o controlador tem o dever de comunicar à ANPD e ao titular dos dados pessoais a ocorrência de incidente de segurança que tenha potencial de risco ou dano relevante que possam afetar consideravelmente seus interesses e direitos fundamentais e, cumulativamente, envolver, pelo menos, um dos seguintes critérios:

a) dados pessoais sensíveis;
b) dados de crianças, de adolescentes ou de idosos;
c) dados financeiros;
d) dados de autenticação em sistemas;
e) por sigilo legal, judicial ou profissional; ou
f) dados em larga escala.

A Autoridade Nacional de Proteção de Dados disponibiliza, em seu sítio eletrônico, uma página com as orientações para a comunicação de incidentes de segurança. A página pode ser acessada no site da ANPD através do seguinte link: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca.

6.2. AO TITULAR DE DADOS PESSOAIS

Cabe ao controlador comunicar ao titular dos dados pessoais a ocorrência de incidente de segurança que tenha potencial de lhe gerar riscos ou danos relevantes. Tal comunicação deve ser realizada de maneira transparente, podendo ser realizada por meios diversos, incluindo mensagens diretas (e-mails, SMS), banners, notificações em sites, comunicações postais e anúncios.
A comunicação do incidente aos titulares deve ser feita em linguagem clara e simplificada e mencionar, no que couber, os elementos previstos no §1º do Art. 48 da LGPD, e do Art. 9º da Resolução CD/ANPD Nº 15/2024, tais como:

• A descrição geral do incidente e a data da ocorrência;
• A natureza dos dados pessoais afetados e os riscos relacionados ao incidente com a identificação dos possíveis impactos aos titulares;
• As medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
• O motivo da demora, no caso de a comunicação não ter sido feita no prazo determinado;
• As medidas tomadas e recomendadas para reverter ou mitigar os efeitos do incidente;
• A data do conhecimento do incidente de segurança;
• O contato do encarregado ou o ponto de contato para que os titulares obtenham informações a respeito do incidente; e
• Outras informações que possam auxiliar os titulares a prevenirem possíveis danos.

Se, pela natureza do incidente, não for possível identificar individualmente os titulares afetados, o controlador deverá comunicar a ocorrência do incidente pelos meios de divulgação disponíveis, tais como seu sítio eletrônico, aplicativos, suas mídias sociais e canais de atendimento ao titular, de modo que a comunicação permita o conhecimento amplo, com direta e fácil visualização, pelo período mínimo de 3 (três) meses, conforme a Resolução CD/ANPD Nº 15/2024. Além disso, o controlador deve incluir no processo de comunicação de incidente uma declaração de que a comunicação aos titulares foi realizada, indicando os meios de comunicação ou divulgação utilizados.

7. RELATÓRIO FINAL DO INCIDENTE

Após a coleta de todas as informações e evidências, o Encarregado com o apoio da Equipe Técnica de Segurança da Informação, irá concluir o Relatório Final do Incidente. O Relatório final será realizado com base em todas as evidências coletadas desde a identificação do incidente até o final das apurações. Nesse documento constará, além de todas as informações sobre o incidente, todas as propostas de melhorias e/ou aquisições sugeridas para redução dos riscos de novas ocorrências. O relatório, além de ter uma função de comprovação das medidas tomadas pela SAS frente às autoridades, é importante para que todos os envolvidos e demais servidores possam aprender com o ocorrido, podendo compreender suas causas, bem como avaliar em que sentido seu Plano de Respostas a Incidentes e seus procedimentos foram efetivos ou não, analisando a atuação dos responsáveis.
O relatório final do incidente será assinado pelo Encarregado e deve ficar disponível para consulta em caso de atualização do relatório de impacto à proteção de dados (RIPD). Esse relatório poderá, ainda, ser apresentado a autoridades policiais, órgãos reguladores ou demais envolvidos.

8. EXTINGUIR O PROCESSO DE COMUNICAÇÃO DO INCIDENTE

O processo de comunicação de incidente será considerado extinto nas seguintes hipóteses:

• Caso não sejam identificadas evidências suficientes da ocorrência do incidente;
• Caso a ANPD considere que o incidente não possui potencial para acarretar risco ou dano relevante aos titulares;
• Caso o incidente não envolva dados pessoais;

• Caso tenham sido tomadas todas as medidas adicionais para mitigação ou reversão dos efeitos gerados; ou
• Realização da comunicação aos titulares e adoção das providências pertinentes pelo controlador, em conformidade com a LGPD e as determinações da ANPD;

ATENÇÃO

Mesmo com a declaração da extinção do processo de comunicação de incidente de segurança, a ANPD poderá determinar a adoção de medidas de segurança diretamente relacionadas ao incidente com intuito de salvaguardar os direitos dos titulares (Resolução CD/ANPD Nº 15, Artigo 23 Parágrafo Único).

9. ANEXOS

Todos os anexos referentes a este plano podem ser acessados em:
https://drive.expresso.pe.gov.br/s/irow43Vg3f801dK.

CARLOS EDUARDO BRAGA FARIAS

Secretário de Assistência Social, Combate à Fome e Políticas sobre Drogas

25 de Julho de 2024.

CARLOS EDUARDO BRAGA FARIAS

Secretário de Assistência Social, Combate à Fome e Políticas sobre Drogas - SAS

Secretaria de Assistência Social, Combate à Fome e Políticas sobre Drogas.