POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - PSI

Novembro - 2025

Sumário

1 - APRESENTAÇÃO

O **Instituto de Gestão Previdenciária e Proteção Social do Estado do Pará - IGEPPS**, no seu papel da gestão dos benefícios previdenciários do Regime de Previdência Estadual e dos Fundos Financeiro de Previdência do Estado do Pará e Previdenciário do Estado do Pará (Finanprev e Funprev), conforme dispõe o art. 60-A, da Lei Complementar nº 39/2002, entende a importância de ter uma Política de Segurança da Informação e Proteção de Dados Pessoais que trate de forma adequada o cenário de Transformação Digital atual como essencial para o alcance da sua missão e objetivos estratégicos. Assim, O IGEPPS por meio desta política, declara formalmente seu compromisso com a Segurança da Informação e Proteção de Dados Pessoais.

Esta Política observa e operacionaliza, no que couber, os requisitos de segurança e boas práticas previstos nos artigos 46 a 50 da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD).

A Política de Segurança da Informação – PSI, do IGEPPS é o documento que orienta e define os princípios, as diretrizes, normas e procedimentos corporativos para garantir a proteção, confidencialidade, integridade e disponibilidade das informações, dos serviços e dos sistemas de TIC da organização. A Segurança da Informação e Proteção de Dados Pessoais é vital para a qualidade dos serviços e o sucesso do Instituto, bem como, para a confiança do público em geral, fornecedores e prestadores de serviços.

O presente documento alinha-se institucionalmente à Lei Geral de Proteção de Dados (LGPD), estando também subordinado e integrado às recomendações Procuradoria jurídica - PROJUR do IGEPPS, apresentando-se às diversas áreas estratégicas como apoio e cooperação para o bom desempenho do Instituto. Além disso, está baseada nas recomendações propostas pelas normas ABNT NBR ISO/IEC 27001:2013 e 27002:2013.

Devemos lembrar também que a LGPD inaugura uma nova cultura de privacidade e proteção de dados no país, o que demanda a conscientização de toda a sociedade acerca da importância dos dados pessoais e os seus reflexos em direitos fundamentais.

2 – JUSTIFICATIVA

Atualmente, a Tecnologia da Informação e Comunicação – TIC é elemento-chave para qualquer negócio. Independentemente do porte ou da área de atuação das empresas, os grandes destaques do mercado operam seus principais sistemas em computadores e com grande dependência da conectividade. Esse é um dos motivos que justificam a necessidade de uma Política de Segurança da Informação e Proteção de Dados nas empresas.

Isto se deve ao fato que nas últimas décadas, houve um significativo aumento da quantidade de informações sensíveis circulando de um ponto a outro tanto dentro da organização como dela para o mundo todo, via Internet. A proliferação dos dispositivos móveis e dos serviços de *cloud computing* (computação em nuvem) também vêm impulsionando este cenário.

Desta forma, para conseguir atender seus objetivos estratégicos e prestar um serviço de qualidade à população é questão de primeira necessidade ter políticas que, documentadas, detalhem procedimentos e diretrizes para eliminar a subjetividade ao lidar com informações sensíveis. Assim, o IGEPPS pode melhor gerenciar os riscos por meio de controles bem definidos, que ainda fornecem referências para auditorias e ações corretivas, agregando mais valor ao negócio da empresa.

Concluindo, uma Política de Segurança da Informação é fundamental para o IGEPPS, de forma a proteger seus ativos, garantir a confidencialidade dos dados, mitigar riscos, cumprir regulamentações e manter a confiança dos usuários internos e externos, cidadãos e órgãos conveniados. Ela serve como um guia abrangente para promover a segurança em todas as operações do Instituto.

3 – OBJETIVO

O objetivo desta política é estabelecer princípios, diretrizes e responsabilidades para a Gestão da Segurança da Informação e Proteção de Dados Pessoais no IGEPPS, visando preservar os ativos de TIC de ameaças internas e externas, garantindo a confidencialidade, integridade e disponibilidade das informações, minimizando os riscos por meio da implementação de controles apropriados e buscando a conformidade com leis, normas e padrões vigentes. Esta Política observa os arts. 46 a 50 da Lei nº 13.709/2018 (LGPD), assegurando medidas de segurança,

prevenção, responsabilização e prestação de contas no tratamento de dados pessoais.

As seguintes normas complementares operacionalizam os princípios, diretrizes e controles estabelecidos nesta Política de Segurança da Informação:

I – Normas para Gestão de Riscos de Segurança da Informação;

II – Normas para Gestão de Incidentes de Segurança Cibernética;

III – Normas para Educação e Cultura em Segurança Cibernética;

IV – Normas de Gestão de Acessos para Usuários;

V – Normas para Gestão de Vulnerabilidades;

VI – Normas de Segurança para Teletrabalho;

VII – Normas para Uso de Dispositivos Móveis;

VIII – Normas para Backup e Restauração de Dados.

A aplicação e o cumprimento destas normas são de responsabilidade do Comitê de Segurança da Informação – CSI, instituído pela portaria n° 572 de 06 de agosto de 2025 *que é o órgão colegiado,* e das unidades organizacionais conforme escopo e competências definidas em cada instrumento normativo.

4 - TERMOS E DEFINIÇÕES

Para fins dessa política, entende-se por:

4.1 - Agente de tratamento: o controlador e o operador;

4.2 - Ameaça: qualquer causa potencial de um incidente indesejado que possa resultar em impacto nos objetivos do negócio;

4.3 - Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

4.4 - Ativo: qualquer coisa que represente valor para a instituição;

4.5 - Ativo de TIC: conjunto de conhecimentos e dados que tem valor para uma instituição, e seus meios de armazenamento, transmissão e processamento, equipamentos necessários a isso, sistemas utilizados para tal e locais onde se encontram esses meios e equipamentos, e recursos humanos que a eles têm acesso;

4.6 - Ativo de TIC patrimonial: subconjunto de ativos de TIC, compreendendo os meios de transmissão, armazenamento e processamento de dados,

equipamentos necessários a isso, sistemas utilizados para tal e locais onde se encontram tais meios e equipamentos;

4.7 - Autoridade Nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional;

4.8 - Backup: cópia de dados em meio separado do original, de forma a protegê-los de qualquer eventualidade;

4.9 - Banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

4.10 - Bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

4.11 - Colaborador: empregado, comissionado, terceirizado, estagiário ou jovem aprendiz da IGEPPS;

4.12 - Computação em nuvem: modelo computacional que permite acesso por demanda, independentemente da localização geográfica, a um conjunto de recursos computacionais configuráveis, que possam ser rapidamente provisionados e liberados com o mínimo de esforço de gerenciamento ou interação com o provedor de serviços;

4.13 - Confidencialidade: garantia de que a informação é acessível somente por pessoas devidamente autorizadas a ter acesso à mesma;

4.14 - Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

4.15 - Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. O controlador é o agente responsável por tomar as principais decisões referentes ao tratamento de dados pessoais e por definir a finalidade deste tratamento. Entre essas decisões, incluem-se as instruções fornecidas a operadores contratados para a realização de um determinado tratamento de dados pessoais;

4.16 - Comitê de Segurança da Informação - CSI;

4.17 - Criticidade: importância da informação para a continuidade das operações da instituição;

4.18 - Custodiante: pessoa ou instituição com atribuição fornecida pelo proprietário do ativo de TIC de guardá-lo e protegê-lo adequadamente;

4.19 - Dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

4.20 - Dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

4.21 - Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

4.22 - Dados não aplicáveis à LGPD: informações onde os dados são anônimos, ou que tiverem sido anonimizados, não sendo a pessoa natural assim identificada ou identificável, ou em casos em que tais dados não forem sequer relacionados à pessoa natural;

4.23 - Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário;

4.24 - Dispositivos móveis: equipamentos portáteis dotados de capacidade computacional ou de armazenamento, entre os quais se incluem, não se limitando a estes: *notebooks, netbooks, smartphones, tablets, pendrives, USB drives, HDS* externos e cartões de memória;

4.25 - Eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

4.26 - Encarregado: 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);

4.27 - Fornecedor: pessoa física ou jurídica que mantém contrato de prestação de serviços ou fornecimento de equipamentos, materiais e seus representantes ou empregados;

4.28 - Incidente: evento não planejado relativo à TIC que pode acarretar prejuízos à empresa ou mesmo violar as regras de segurança da informação;

4.29 - Informação: conjunto organizado de dados, que constitui uma mensagem;

4.30 - Integridade: salvaguarda da exatidão completa da informação e dos métodos de processamento;

4.31 - LGPD: Lei Geral de Proteção de Dados Pessoais, lei nº 13.853, de 2019;

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

4.33 - Órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no país, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico;

4.35 - PoSIC: Política de Segurança da Informação e Comunicação dos Ambientes de TIC, do Governo do Estado do Pará, instituída pelo Decreto Estadual Nº 1.762, de 28 de dezembro de 2017.

4.36 - Proprietário de ativo de TIC: responsável primário pelo ativo de TIC;

4.37 - **RIPD:** Relatório de Impacto à Proteção de Dados Pessoais, documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

4.38 - ROPA: Registro de Operações de Tratamento de Dados Pessoais, documento exigido ao controlador e ao operador, disposto no artigo 37 da LGPD;

4.39 - Segurança física: proteção dos ativos físicos de uma empresa contra furto, roubo, dano ou acesso não autorizado;

4.40 - Segurança lógica: proteção de dados e sistemas contra ameaças internas e externas;

4.41- Suboperador: pessoa natural ou jurídica, de direito público ou privado, contratada pelo operador para auxiliá-lo a realizar o tratamento de dados pessoais em nome do controlador;

4.42 - Termo de uso e privacidade: comunicação enviada ao titular dos dados ou usuário de serviço com a finalidade de esclarecer a política de tratamento de dados, explicitando os dados coletados e a forma de sua utilização, em observância às disposições da LGPD;

4.43 - Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

4.44 - Transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

4.45 - Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

4.46 - Uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

4.47 - Usuário: pessoa que acessa ou utiliza de forma legítima e autorizada um serviço ou informação.

5 - ABRANGÊNCIA

5.1 - Abrangência Geral

As ações referentes à Segurança da Informação e Proteção aos Dados Pessoais abrangem todos os ativos de TIC gerenciados pelo IGEPPS, independentemente da titularidade de propriedade ou localização geográfica, bem como os processos de todas as unidades organizacionais, extensivas, no que couber, aos serviços e produtos oferecidos aos clientes, devendo ser seguidas, dentro de suas responsabilidades, por todos os colaboradores e fornecedores.

Esta Política aplica-se também ao tratamento de dados pessoais, observando os arts. 46 a 50 da Lei nº 13.709/2018 (LGPD), que estabelecem medidas de segurança, prevenção, responsabilização e auditoria relativos ao tratamento de dados pessoais.

5.2 - Abrangência específica à proteção de dados pessoais

As ações específicas ao tratamento de dados pessoais abrangem os seguintes tipos de dados:

5.2.1 - Dados dos servidores efetivos, temporários, comissionados e Estagiários do IGEPPS, para fins de gerenciamento de recursos humanos, incluindo contratação, remuneração, gestão de benefícios, gestão de

desempenho, disciplina e rescisão, bem como para fins de contatos de emergência.

5.2.2 - Dados de titulares cujos dados são controlados pelos clientes internos e externos do IGEPPS, para fins de atendimento às especificações dos serviços contratados, enquanto operador, de acordo com as especificações exigidas pelo cliente para o tratamento de dados em observância à LGPD.

5.2.3 - Dados de usuários dos sítios e aplicativos móveis do IGEPPS, para fins de habilitar as principais funções, garantir a segurança, melhorar a funcionalidade, aprimorar e personalizar a experiência de navegação e analisar o tráfego e uso do sítio ou aplicativo.

5.2.4 - Dados dos representantes de clientes e fornecedores do IGEPPS, para fins de relacionamentos de negócio.

5.2.5 - Dados de visitantes e público em geral, para fins de segurança durante o acesso às dependências físicas do IGEPPS.

5.2.6 - Dados de todos os colaboradores do IGEPPS, para fins de operacionalização de seus processos.

5.2.7 - Dados de pessoas naturais em situações diversas, não previstas expressamente nessa política, mas de acordo com a LGPD.

6 - RESPONSABILIDADES

As responsabilidades relativas às ações de Segurança da Informação e Proteção aos Dados Pessoais são as seguintes:

6.1 - Comitê de Segurança da Informação - CSI

6.1.1 - Atuar no planejamento e coordenação da segurança da informação e proteção de dados pessoais, discutindo e organizando as ações inerentes ao tema.

6.1.2 - Ajustar e propor melhorias à PSI

6.1.3 - Estabelecer as responsabilidades complementares e adjacentes à PSI.

6.1.4 - Acompanhar, monitorar e avaliar a execução da PSI.

6.1.5 - Formular, revisar e estabelecer normas, procedimentos, planos, processos e demais ações, de acordo com os princípios e as diretrizes estabelecidas na PSI.

6.1.6 - Orientar e estimular a governança e adoção de boas práticas quanto aos aspectos relacionados à Segurança da Informação e Proteção aos Dados Pessoais.

6.1.7 - Gerenciar os riscos da Segurança da Informação e Proteção aos Dados Pessoais.

6.1.8 - Cumprir outras responsabilidades estabelecidas em ato próprio de criação ou alteração do CSI.

6.2 Encarregado

6.2.1 - Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências.

6.2.2 - Receber comunicações da Autoridade Nacional (ANPD) e adotar providências.

6.2.3 - Orientar os funcionários e os contratados do IGEPPS a respeito das práticas a serem tomadas em relação à proteção de dados pessoais.

6.2.4 - Executar as demais atribuições determinadas pela Presidência do IGEPPS ou estabelecidas em normas complementares.

6.3 Presidência

6.3.1 - Estimular a adoção de práticas de Segurança da Informação e Proteção de Dados Pessoais, inclusive disponibilizando os recursos necessários para tanto.

6.3.2 - Nomear o encarregado, dando-lhe recursos e condições necessárias para o desempenho de suas atividades.

6.3.3 - Garantir a disseminação e o cumprimento dessa política, inclusive disponibilizando recursos necessários para tanto.

6.3.4 - Comunicar à Autoridade Nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

6.3.5 - Criar o Comitê de Segurança da Informação – CSI.

6.4 - Todas as unidades organizacionais

6.4.1 - Adotar as normas e procedimentos relativos à Segurança da Informação e Proteção aos Dados Pessoais, associados a ativos de TIC e processos de cada área de atuação.

6.4.2 - Participar da análise de riscos de ativos de TIC e processos, dentro de sua área de atuação.

6.4.3 - Colaborar na elaboração de normas e procedimentos relativos à Segurança da Informação e Proteção aos Dados Pessoais.

6.4.4 - Cumprir as responsabilidades específicas estabelecidas pelo CSI.

6.5 Colaboradores e fornecedores

6.5.1 - Realizar a proteção e salvaguarda dos ativos de TIC, de que sejam usuários ou que tenham acesso, independente das medidas de segurança implementadas.

6.5.2 - Registrar e informar incidentes relativos à Segurança da Informação e Proteção aos Dados Pessoais, de modo que possam ser avaliados e tratados, conforme Norma II – Normas para Gestão de Incidentes de Segurança Cibernética.

6.5.3 - Manter o sigilo dos dados manipulados, quando necessário, inclusive quanto a dados pessoais tratados no IGEPPS.

6.5.4 - Especificamente para os fornecedores e no papel de suboperador, realizar o tratamento de dados seguindo as instruções fornecidas pelo IGEPPS e pelo controlador.

6.6 Proprietário de ativo de TIC

6.6.1 - Classificar os ativos de TIC de acordo com seu grau de criticidade e sigilo.

6.6.2 - Autorizar o acesso ao ativo de TIC, de acordo com as normas de controle de acesso.

6.6.3 - Definir o custodiante, se necessário.

6.7 Custodiante de Ativo de TIC

6.7.1 - Realizar controles de segurança com base no valor do ativo que o proprietário determinar.

6.8 - Gestor de Acessos e Privilégios

6.8.1 - A concessão, revisão e revogação de acessos aos ativos de TIC serão formalizadas e registradas, garantindo a aplicação do princípio do menor privilégio, a **Segregação de Funções (SoD - Segregation of Duties)** para

evitar conflitos de interesse, e a realização de revisões periódicas de perfis e direitos de acesso.

6.8.2 - Revisar e validar periodicamente as concessões de acesso, garantindo que permissões correspondam às necessidades funcionais atuais dos usuários.

6.8.3 - Revogar acessos imediatamente quando usuários mudarem de função, saírem da organização ou não mais necessitarem de privilégios.

6.8.4 - Manter registro de todas as concessões, modificações e revogações de acesso, com rastreabilidade de aprovação.

6.8.5 - Comunicar ao CSI violações ou tentativas de acesso não autorizado para investigação e tratamento conforme Norma II – Gestão de Incidentes de Segurança Cibernética

6.9 - Da gestão de segurança na relação com terceiros

6.9.1. A segurança da informação e a proteção de dados devem ser parte integrante da relação com fornecedores e terceiros.

6.9.2. Instrumentos contratuais e Acordos de Processamento de Dados (DPA) devem estabelecer, no mínimo, as seguintes obrigações para o terceiro:

a) Dever de confidencialidade sobre as informações acessadas;

b) Obrigação de notificar o IGEPPS sobre qualquer incidente de segurança da informação ou violação de dados pessoais em prazo predefinido;

c) Garantia de direito de auditoria ou apresentação de relatórios de asseguramento para verificar a conformidade dos controles de segurança;

d) Definição de regras claras para a retenção e o descarte seguro das informações ao término da relação contratual, em alinhamento com a LGPD e a Tabela de Temporalidade.

7 - PRINCÍPIOS

7.1 - Princípios Gerais

Os princípios orientadores das ações de Segurança da Informação e Proteção de Dados Pessoais do IGEPPS estão alinhados com aqueles descritos na PoSIC estadual, sendo os seguintes:

7.1.1 - Alinhamento estratégico: O IGEPPS deverá alinhar a segurança da informação com sua missão institucional e o seu planejamento estratégico, de forma a construir as ações de acordo com os objetivos e metas da instituição.

7.1.2 - Diversidade organizacional: As ações relativas à segurança da informação devem levar em consideração a diversidade das suas atividades, respeitando sua natureza e finalidade.

7.1.3 - Garantia da Segurança das Informações: Deve-se sempre buscar a implantação de ações que busquem garantir os princípios da segurança da informação: a confidencialidade, a integridade e a disponibilidade das informações.

7.1.4 - Propriedade da informação: Toda informação produzida no IGEPPS é de sua propriedade e não de seus colaboradores ou fornecedores, exceto os casos onde a Instituição atua como custodiante da informação, devendo seu uso ser destinado, exclusivamente, a atender aos interesses da Instituição.

7.1.5 - Alinhamento com os aspectos legais (Conformidade): Devem ser cumpridas as normas legais e regulamentares de abrangência estadual e federal, as políticas e as diretrizes estabelecidas para o negócio e para as atividades do Estado, bem como se deve evitar, detectar e tratar qualquer desvio ou inconformidade que possa ocorrer.

7.2 - Princípios específicos à proteção de dados pessoais

Os princípios específicos, orientadores das ações de proteção de dados pessoais no IGEPPS estão alinhados à LGPD, sendo os seguintes:

7.2.1 - A proteção aos dados pessoais tem como fundamentos:

7.2.1.1 - O respeito à privacidade;

7.2.1.2 - A autodeterminação informativa;

7.2.1.3 – A liberdade de expressão, de informação, de comunicação e de opinião;

7.2.1.4 - A inviolabilidade da intimidade, da honra e da imagem;

7.2.1.5 - O desenvolvimento econômico e tecnológico, bem como a inovação;

7.2.1.6 - A livre iniciativa, a livre concorrência e a defesa do consumidor; e

7.2.1.7 - Os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

7.2.2 - São princípios da proteção de dados pessoais:

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

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

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

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

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

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

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

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

7.2.2.9 - Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

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

7.3 - Do ciclo de vida e descarte da informação

7.3.1. O tratamento da informação e dos dados pessoais deve abranger todo o seu ciclo de vida, desde a coleta ou produção até o seu descarte definitivo.

7.3.2. Os prazos de retenção das informações e os critérios para seu descarte seguro deverão seguir o disposto na Tabela de Temporalidade de Documentos do órgão e nas demais legislações aplicáveis, em estrita observância ao princípio da necessidade da LGPD. O descarte deve garantir a eliminação segura e irrecuperável da informação.

8 - DIRETRIZES

8.1 - Diretrizes Gerais

O IGEPPS deverá cumprir as seguintes diretrizes relativas à segurança da informação, de forma geral:

8.1.1 - Planejamento Estratégico: Incluir no planejamento estratégico do IGEPPS diretrizes e metas relacionadas à Segurança da Informação e Proteção de Dados Pessoais, para fortalecer o alinhamento entre a TIC e os planejamentos da instituição e do Governo do Estado, com o objetivo de promover e motivar a criação de uma cultura de Segurança da Informação e Proteção de Dados Pessoais, conforme disposto na PoSIC do Pará.

8.1.2 - Padrões a serem adotados: Fundamentar a elaboração de normas e procedimentos da segurança da informação e proteção de dados pessoais de acordo com as normas técnicas ABNT NBR ISO/IEC 27001 e 27002.

8.1.3 - Gerenciamento de Riscos, conforme Norma I – Normas para Gestão de Riscos de Segurança da Informação.: ativar a gestão de riscos para os ativos de TIC (processos, produtos e serviços desenvolvidos, adquiridos, implementados ou disponibilizados) no IGEPPS.

8.1.4 - Seleção de mecanismos de segurança: selecionar os mecanismos de segurança considerando-se os fatores de riscos, tecnologias e custos.

8.1.5 - Comunicação, conscientização e capacitação:

8.1.5.1 - Implementar um sistema de conscientização sobre Segurança da Informação e Proteção de Dados Pessoais de forma que todos sejam informados sobre as obrigações legais e potenciais riscos a que estão expostos os ativos de TIC, proporcionando assim, maior cooperação para o cumprimento das orientações;

8.1.5.2 - Informar e capacitar regularmente todos os colaboradores sobre as normas e procedimentos da segurança da informação, de acordo com suas funções, inclusive publicando-os na intranet corporativa, garantindo assim maior efetividade e eficácia das ações.

8.1.6 - Linhas de defesa: implementar o modelo de três linhas de defesa como base para as ações de segurança da informação e proteção de dados pessoais;

8.1.6.1 - Primeira linha: todos os colaboradores e fornecedores;

8.1.6.2 - Segunda linha: governança;

8.1.6.3 - Terceira linha: auditoria.

8.1.7 - **Monitoramento e Auditoria:** seguir a legislação ao efetuar o monitoramento e auditoria relativa à segurança da informação e tratamento de dados pessoais.

8.1.8 - **Conformidade com a política estadual:** Efetuar a verificação de conformidade com a PoSIC do Pará, sempre que necessário, sendo documentada em relatório de avaliação de conformidade, o qual será encaminhado ao Comitê de Segurança da Informação - CSI

8.1.9 - **Limite e compartilhamento de responsabilidades:** definir e acordar junto a clientes e fornecedores os limites e compartilhamentos de responsabilidades nas ações de segurança da informação e proteção de dados pessoais, considerando inclusive a interdependência das operações efetuadas por estas, como, por exemplo, entre o transporte de dados, serviços de disponibilização de infraestrutura de processamento e armazenamento de dados, e a implementação e operacionalização de sistemas aplicativos.

8.1.10 - **Segurança e privacidade "by design":** adotar ações de segurança da informação e proteção de dados pessoais em todas as etapas dos projetos

e processos, desde sua concepção inicial, permeando o ciclo de vida dos serviços da organização, com o objetivo de agregar e garantir integridade e privacidade aos seus projetos, processos e produtos finais.

8.1.11 - Produtos e serviços: Cada produto ou serviço deve ser disponibilizado aos clientes com um mínimo de controle de segurança, analisado e projetado caso a caso, considerando-se os requisitos de segurança e proteção de dados pessoais do cliente e a conveniência do próprio IGEPPS, em relação aos riscos legais ou de imagem e enquanto agente de modernização do governo do estado, sem descartar a possibilidade de customização específica a determinado cliente ou projeto.

8.1.12 - "Cybersecurity Framework" (NIST): Estabelecer estratégia de segurança baseada no paradigma NIST (Identify, Protect, Detect, Respond, Recover), alinhado com LGPD. Todas as diretrizes operacionais (8.2–8.6) devem ser implementadas conforme este framework.

8.1.13 – Controles e Normas: Implementar controles de segurança para riscos gerais (comuns a todos os ativos) e riscos específicos (determinados ativos de TIC), através de normas e procedimentos operacionais detalhados em: - 8.2: Proteção de Dados Pessoais (LGPD) - 8.3: Gestão de Vulnerabilidades (Norma V) - 8.4: Gestão de Incidentes (Norma II) - 8.5: Educação e Capacitação (Norma III) - 8.6: Segurança no Teletrabalho (Norma VI) - 8.7: Segurança em Dispositivos Móveis (Norma VII) - 8.8: Gestão de Backup e Restauração (Norma VIII)

8.1.14 - A verificação da conformidade com esta Política e suas normas será realizada por meio de avaliações contínuas e/ou auditorias periódicas, cujos resultados serão tratados como entradas para o processo de gestão de riscos.

8.1.15 - As não conformidades identificadas deverão ser registradas e tratadas como riscos, gerando um Plano de Ação Corretiva com responsáveis e prazos definidos. A eficácia das ações implementadas será monitorada pelo Comitê de Segurança da Informação - CSI.

8.1.16 - Qualquer exceção à aplicação de um controle de segurança previsto nesta Política ou em suas normas deverá ser formalizada através de um **Termo de Aceite de Risco**, aprovado pela alçada competente. O termo deve justificar a necessidade da exceção, avaliar os riscos residuais, definir controles compensatórios e estabelecer um prazo de validade para reavaliação.

8.2 - Diretrizes Específicas à Proteção de Dados Pessoais

O IGEPPS deverá cumprir as seguintes diretrizes específicas à proteção de dados pessoais:

8.2.1 - Hipóteses de tratamento: seguir as hipóteses de tratamento de dados pessoais e dados pessoais sensíveis previstas na LGPD, em especial nos artigos 7º e 11.

8.2.2 - Finalidade e hipóteses legais: identificar, especificar e documentar as finalidades, hipóteses de tratamento e bases legais que fundamentam as atividades de tratamento de dados pessoais e dados pessoais sensíveis.

8.2.3 - Minimização: limitar a quantidade de dados pessoais tratados ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

8.2.4 - Anonimização dos dados: anonimizar, sempre que possível, os dados pessoais utilizados para fins de estudos por órgão de pesquisa.

8.2.5 - Direitos dos titulares: atender, a pedido do titular, em relação aos seus dados tratados pelo IGEPPS, a qualquer momento e mediante requisição:

8.2.5.1 - A confirmação da existência de tratamento.

8.2.5.2 - O acesso aos dados.

8.2.5.3 - A correção de dados incompletos, inexatos ou desatualizados.

8.2.5.4 - A anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD.

8.2.6 - Compartilhamento, transferência e divulgação: seguir estritamente a legislação ao efetuar o compartilhamento, a transferência ou a divulgação de dados pessoais.

8.2.7 - Operação e suboperação: Efetuar as seguintes ações, enquanto operador:

8.2.7.1 - Seguir as instruções de tratamento de dados determinadas pelo controlador;

8.2.7.2 - Solicitar ao controlador as instruções de tratamento de dados, com as respectivas hipóteses legais de tratamento;

8.2.7.3 - Obter autorização do controlador, através de contratos, convênios ou assemelhados, para obter auxílio nas operações de

tratamento de dados a eventuais suboperadores, explicitando a cadeia de responsáveis pelo tratamento dos dados;

8.2.7.4 - Garantir que toda a cadeia de suboperadores tratem os dados seguindo as instruções fornecidas pelo controlador.

8.2.8 - Transparência: dar publicidade, enquanto controladora, sobre a finalidade e a forma como os dados pessoais serão tratados, através da elaboração e divulgação de termo de uso e privacidade.

8.2.9 - Transferência Internacional: praticar a transferência internacional de dados, quando necessário, nos termos das leis vigentes.

8.2.10 - Instrução a operadores: instruir os operadores, por meio de instrumentos adequados, quanto ao tratamento dos dados por ela controlados.

8.2.11 - Comercialização: não comercializar, na qualidade de operadora, os dados que

8.3 – Gestão de vulnerabilidades

8.3.1 - Identificar, avaliar, priorizar e mitigar vulnerabilidades em ativos de TIC; operacionalizar controles de detecção e remediação, conforme Norma V – Normas para Gestão de Vulnerabilidades em Ativos de TIC.

8.3.2 - CSI coordena programa; Unidades de TI realizam scans, avaliações e testes de penetração; Proprietários de ativos aprovam remediação; Fornecedores informam vulnerabilidades identificadas.

8.3.3 - Realizar avaliações de vulnerabilidades periodicamente (trimestral/semestral); manter registro de vulnerabilidades identificadas, priorização e status de remediação; comunicar críticas ao CSI e proprietários para ação imediata.

8.3.4 - Operacionalizar: scanning automatizado; testes de penetração; análise de código; avaliação de configurações; priorização por severidade; plano de remediação com SLA.

8.4 — Gestão de Incidentes

8.4.1 - Os incidentes de segurança da informação deverão ser registrados, classificados por gravidade, e tratados de forma a conter a ameaça. O processo deve prever um plano de comunicação proporcional ao impacto e a elaboração de um relatório de lições aprendidas para mitigar futuras ocorrências. Quando envolverem dados pessoais, o processo observará os prazos e critérios de

comunicação à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares afetados.

8.4.2 - CSI coordena resposta; Unidades de TI executam análise e remediação; Proprietários de ativos são notificados; colaboradores reportam incidentes.

8.4.3 - Manter plano de resposta a incidentes com papéis definidos, cronograma de ação e comunicação. Documentar lições aprendidas.

8.5 – Diretrizes de educação, conscientização e capacitação

8.5.1 - Objetivos: Disseminar cultura de Segurança da Informação e proteção de dados pessoais; assegurar compreensão de responsabilidades; promover conscientização contínua; capacitar com competências técnicas e comportamentais; atender requisitos da LGPD, conforme Norma III – Normas para Educação e Cultura em Segurança Cibernética.

8.5.2 - Responsabilidades: CSI coordena e aprova programas; Unidades de TI/RH implementam treinamentos; Gestores garantem participação; colaboradores participam regularmente.

8.5.3 - Implementação: A estratégia será executada por meio de um Programa de Educação e Conscientização Continuada, estruturado da seguinte forma:

a) Treinamento obrigatório de integração (onboarding) para todos os novos colaboradores e terceiros antes da concessão de acessos críticos;

b) Reciclagem anual obrigatória para todo o público-alvo, com avaliação de conhecimento para aferir a absorção do conteúdo;

c) Ações de conscientização recorrentes (ex: campanhas de phishing simulado, comunicados, pílulas de conhecimento) para reforçar a cultura de segurança;

d) O registro de participação, os resultados das avaliações e os indicadores de efetividade (KPIs) servirão como evidências formais de conformidade para fins de auditoria e para a demonstração de accountability perante a ANPD.

8.5.4 - Temas essenciais: Princípios de SI (CIA); LGPD e direitos de titulares; políticas e procedimentos; gestão de senhas; identificação de ameaças; manejo seguro de dados; uso seguro de dispositivos; resposta a incidentes.

8.5.5 - Abrangência: Colaboradores (efetivos, comissionados, temporários); fornece-dores e terceiros; novos colaboradores; colaboradores em mudança de função ou acesso a sistemas críticos.

8.6 – Segurança no Teletrabalho

8.6.1 - Estabelecer diretrizes e controles para segurança da informação em ambientes de trabalho remoto, garantindo confidencialidade, integridade e disponibilidade de dados, conforme Norma VI – Normas para Segurança no Teletrabalho e Ambientes Remotos.

8.6.2 - Responsabilidades: CSI aprova política de teletrabalho; Unidades de TI fornecem VPN, criptografia e antimalware; Gestores monitoram conformidade; Colaboradores implementam medidas de segurança física e lógica.

8.6.3 - Controles de acesso: Exigir autenticação multifator (MFA) para acessar sistemas; usar VPN criptografada; bloquear acesso não autorizado.

8.6.4 - Segurança física: Garantir ambiente seguro e privado (webcam coberta, sem acesso de terceiros); manter documentos físicos protegidos; bloquear dispositivos quando ausente.

8.6.5 - Segurança lógica: Manter software atualizado; usar antimalware; não conectar redes públicas (WiFi aberto); desabilitar bluetooth quando não necessário; sincronizar dados com backup seguro.

8.6.6 - Comunicação: Usar apenas canais corporativos (e-mail, chat corporativo); não usar WhatsApp pessoal ou redes sociais para dados confidenciais.

8.6.7 - Incidentes: Reportar imediatamente tentativas de acesso não autorizado, roubo ou perda de dispositivos ao CSI.

8.7 – Segurança em dispositivos móveis

8.7.1 - Estabelecer controles de segurança para dispositivos móveis (notebooks, smartphones, tablets, pendrives, USB drives, HDS externos, cartões de memória) que acessem, armazenem ou processem dados da organização, conforme Norma VII – Normas para Segurança em Dispositivos Móveis e Portáteis.

8.7.2 - Responsabilidades: CSI aprova política de dispositivos móveis; Unidades de TI implementam controles de MDM (Mobile Device Management); Proprietários de ativos definem requisitos; Usuários seguem práticas seguras.

8.7.3 - Controles obrigatórios: Autenticação multifator (MFA); criptografia de dados em repouso e em trânsito; bloqueio remoto e limpeza de dados; atualização automática de software; desabilitar câmeras/Bluetooth desnecessários; antimalware instalado.

8.7.4 - Uso pessoal: Proibir armazenamento de dados sensíveis em dispositivos pessoais; se BYOD permitido, implementar containerização de dados corporativos; segregar dados pessoais de corporativos.

8.7.5 - Perda ou roubo: Reportar imediatamente ao CSI; bloquear e limpar remotamente dispositivos perdidos; investigar possível exfiltração de dados; documentar incidente.

8.7.6 - Terceirizados e fornecedores: Exigir conformidade com política de dispositivos móveis via contrato; auditar regularmente.

8.8 – Gestão de backup e restauração

8.8.1 - Implementar estratégia abrangente de backup e restauração para garantir continuidade das operações e recuperação de dados em caso de falha, desastre ou incidente, conforme Norma VIII – Normas para Backup, Arquivamento e Restauração de Dados.

8.8.2 - Responsabilidades: CSI coordena estratégia; Unidades de TI implementam backups; Proprietários de ativos validam criticidade; Custodiantes monitoram integridade.

8.8.3 - Política de backup - A estratégia de backup e recuperação será formalizada em norma complementar, definindo os Objetivos de Tempo de Recuperação (RTO) e Objetivos de Ponto de Recuperação (RPO) para sistemas e ativos críticos. A arquitetura de cópias de segurança deverá seguir a regra 3-2-1: no mínimo três cópias dos dados, em duas mídias (ou tecnologias) diferentes, com pelo menos uma cópia mantida off-site (em local geograficamente distinto) ou offline. A eficácia do processo será validada por meio de testes periódicos de restauração, cujos resultados devem ser registrados e analisados.

8.8.4 - Armazenamento: Manter backups offline ou geograficamente distribuídos; criptografar todos os backups; testar restauração regularmente (trimestral); documentar procedimentos.

8.8.5 - Testes de recuperação: Executar simulados de desastre semestralmente; validar tempo de restauração; documentar lições aprendidas; atualizar plano de continuidade conforme necessário.

8.8.6 - Retenção: Definir períodos de retenção conforme legislação (LGPD, normas fiscais); descartar backups obsoletos de forma segura; manter cadeia de custódia de mídia.

8.9 - Classificação da Informação

8.9.1 - Os ativos de informação devem ser classificados com base em sua criticidade e sensibilidade, conforme o seguinte esquema de quatro níveis:

a) **Público:** Informação de divulgação livre.
b) **Uso Interno:** Acesso restrito a colaboradores e parceiros contratuais.
c) **Confidencial:** Dados sensíveis, com acesso seletivo e controlado.
d) **Restrito:** Informação crítica e altamente sensível, com acesso estritamente controlado e limitado.

8.9.2 A classificação será definida pelo proprietário do ativo, com os critérios e procedimentos detalhados conforme disposto nas Normas para Gestão de Riscos de Segurança da Informação, orientando o manejo, o acesso e a proteção dos ativos, a fim de garantir a aplicação de controles de segurança proporcionais aos riscos.

8.10 - Temporalidade e Descarte de Informação

8.10.1 - A temporalidade para guarda e descarte seguro de todos os ativos de informação deve ser mantida em sistema específico, alinhada aos requisitos legais, regulatórios e do negócio detalhada conforme disposto nas Normas para Gestão de Riscos de Segurança da Informação.

8.10.2 - O descarte deve ser realizado de forma segura e irreversível, de modo proporcional à classificação da informação, ao final de seu ciclo de vida útil.

8.11 - Auditoria e Monitoramento de Acesso

8.11.1 O acesso aos ativos de informação deve ser registrado e monitorado periodicamente, com ênfase nos ativos classificados como Confidenciais e Restritos conforme as Normas de Gestão de Acessos para Usuários.

8.11.2 Auditorias regulares devem ser conduzidas para verificar a conformidade dos acessos com as políticas de segurança e para detectar atividades incomuns ou não autorizadas conforme disposto nas Normas para Gestão de Incidentes de Segurança Cibernética.

ASSINATURAS

Número do Protocolo: 2026/2174887

Anexo/Sequencial: 2

Este documento foi assinado eletronicamente na forma do Art. 6º do Decreto Estadual Nº 2.176, de 12/09/

Assinatura(s) do Documento:

Assinado eletronicamente por: CESAR AUGUSTO CAVALCANTE VALENTE,
CPF: ***.488.702-**
Em: 04/02/2026 15:01:41
Aut. Assinatura: af89dcbf887bdc9d3bc7592cea28177ef8c766e5777b9a61a044a335a060a718

Identificador de autenticação: 954417c9-58a7-4a3e-a51f-be0f8bce796a
Confira a autenticidade deste documento em
https://www.sistemas.pa.gov.br/validacao-protocolo