MANUAL DE NORMAS E PROCEDIMENTOS DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

Recife, 26 de novembro de 2025

Sumário

1. Sobre o Manual

O Manual de Normas e Procedimentos de Proteção de Dados Pessoais (LGPD) da Sociedade Pernambucana de Combate ao Câncer - SPCC é um documento de orientação que formula regras de boas práticas e de governança que estabelecem as condições de organização e funcionamento, bem como outros procedimentos relacionados com o tratamento de dados pessoais em compliance com a **Lei Geral de Proteção de Dados - LGPD, Lei 13.709 / 2018.**

Além de adotar um conjunto padronizado e sistematizado de informações claras para o tratamento de dados pessoais, demonstra o comprometimento da SPCC em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais.

1.1. Diretrizes deste manual

I. Aplicável a todo o conjunto de dados pessoais que estejam sob controle da SPCC, independentemente do modo como se realizou sua coleta, armazenamento, compartilhamento, eliminação ou processamento;

II. Esteja adaptado à estrutura, escala e ao volume das operações, bem como à sensibilidade dos dados tratados;

III. Referenciar as políticas com base em processo de avaliação sistemática de impactos e riscos à privacidade;

IV. Estabelecer relação de confiança com o titular dos dados, por meio de atuação transparente e que assegure mecanismos de participação do titular;

V. Estar integrado a estrutura geral de governança da SPCC, estabelecendo e aplicando mecanismos de supervisão internos e externos;

VI. Ser atualizado periodicamente, no mínimo a cada 12 meses, com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas de suas operações.

2. Sobre a Lei Geral de Proteção de Dados (LGPD)

A Lei Geral de Proteção de Dados (LGPD) estabelece normas sobre o tratamento de dados pessoais, abrangendo tanto os meios digitais quanto outros formatos. O objetivo dessa legislação é proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade das pessoas naturais. Dessa forma, ela garante que a coleta, armazenamento e utilização de dados sejam realizados de maneira ética e transparente.

Os fundamentos da LGPD refletem os valores essenciais para a proteção de dados pessoais. Entre eles, destacam-se o respeito à privacidade, à autodeterminação informativa, a liberdade de expressão, comunicação e opinião, bem como a inviolabilidade da intimidade, honra e imagem.

O alcance da LGPD é amplo e se aplica a todas as operações de tratamento de dados pessoais realizadas por pessoas físicas ou jurídicas, independentemente do meio utilizado ou do local onde os dados estejam armazenados.

2.1. Definições

As definições dos termos utilizados neste manual seguem as descritas na **LGPD no seu Art. 5,** abaixo algumas delas:

- **Dado pessoal:** Qualquer informação que permita identificar uma pessoa ou esteja relacionada a ela.
- **Dado pessoal sensível:** Informações que revelem origem racial ou étnica, religião, opinião política, filiação a organizações, dados sobre saúde, vida sexual, características genéticas ou biométricas, desde que estejam vinculadas a uma pessoa.
- **Titular:** A pessoa a quem os dados pessoais se referem.
- **Controlador:** Quem decide como e por que os dados pessoais serão tratados, podendo ser uma pessoa física ou jurídica, pública ou privada.

- **Operador:** Quem realiza o tratamento dos dados pessoais sob as instruções do controlador, podendo também ser pessoa física ou jurídica, pública ou privada.
- **Agência Nacional de Proteção de Dados (ANPD):** Órgão público responsável por fiscalizar e garantir que a LGPD seja cumprida em todo o Brasil.
- **Encarregado:** Pessoa indicada pelo controlador para ser o canal de comunicação com a ANPD e os titulares dos dados.
- **Agentes de tratamento:** O controlador e o operador, responsáveis pelo uso dos dados pessoais.
- **Tratamento:** Qualquer operação feita com dados pessoais, como coleta, armazenamento, compartilhamento, processamento ou exclusão.
- **Consentimento:** Acordo livre e claro do titular, autorizando o uso de seus dados para um propósito específico.
- **Bloqueio:** Suspensão temporária do uso dos dados pessoais, mas mantendo-os armazenados.
- **Eliminação:** Exclusão definitiva dos dados armazenados.
- Uso compartilhado de dados: Quando dados pessoais são usados por diferentes órgãos ou empresas, de forma autorizada, para cumprir suas funções legais.
- **Dado anonimizado:** Dados tratados para que não seja possível identificar a pessoa a quem pertencem.

2.2. Princípios para as atividades de tratamento de dados pessoais

Os princípios orientam como os dados devem ser tratados conforme a LGPD na SPCC.

- **Finalidade:** Os dados pessoais só podem ser utilizados quando forem realmente necessários e para motivos claros, justificados, específicos e informados ao titular.

- **Adequação:** O uso dos dados deve estar alinhado com a finalidade inicialmente comunicada ao titular dos dados.

- **Necessidade:** Apenas os dados essenciais para atingir o objetivo proposto devem ser coletados e tratados, evitando excessos.

- **Livre acesso:** O titular tem direito de consultar suas informações de forma simples, gratuita e acessível, seja fisicamente ou digitalmente, sempre que solicitar.

- **Qualidade dos dados:** Os dados pessoais devem ser armazenados com precisão e clareza, garantindo que permaneçam atualizados.

- **Transparência:** Os titulares devem saber como seus dados serão tratados, por quanto tempo serão armazenados e com quem poderão ser compartilhados. Todas as informações devem ser claras e fáceis de acessar.

- **Segurança:** Medidas técnicas e administrativas devem ser adotadas para proteger os dados contra acessos não autorizados, perdas, alterações, destruição ou vazamentos.

- **Prevenção:** Devem ser implementadas ações para evitar riscos e danos no tratamento de dados, como medidas de segurança, organização de processos e conscientização dos colaboradores.

- **Não discriminação:** Os dados pessoais não podem ser utilizados para práticas discriminatórias, abusivas ou ilegais.

- **Responsabilização e prestação de contas:** A SPCC deve demonstrar que cumpre todas as normas e que adota medidas eficazes para garantir a proteção das informações.

2.3. Dos requisitos para tratamento de dados pessoais

O tratamento de dados pessoais só pode ser realizado em situações específicas, com as devidas bases legais e seguindo os princípios da LGPD, garantindo a proteção dos direitos dos titulares.

2.3.1. Do consentimento do titular dos dados

A coleta do consentimento é a principal base legal para todo tratamento de dados pessoais sensíveis, conforme o **art. 11, I da LGPD.** A lei é clara ao afirmar que o consentimento é necessário, salvo nas hipóteses expressamente previstas no inciso II do mesmo artigo.

Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

I- Quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades determinadas;

II- Sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a) Cumprimento de obrigação legal ou regulatória pelo controlador;

b) Tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

c) Realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

d) Exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da **Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);**

e) Proteção da vida ou da incolumidade física do titular ou de terceiros;

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

g) Garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso

de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

h) No que se refere à dispensa do consentimento, é importante destacar que as exceções previstas nas alíneas “e” e “f” do inciso II do art. 11 da LGPD aplicam-se apenas a situações de risco ou perigo iminente à vida ou à incolumidade física do titular, como casos de urgência médica. Portanto, essas exceções não justificam o tratamento rotineiro de dados pessoais sensíveis e não exime a obrigação de obter o consentimento do paciente;

i) O consentimento do titular deve ser formalizado por escrito ou de forma que comprove sua manifestação de vontade;

j) Quando feito por escrito, o consentimento deve constar de cláusula destacada no termo devendo haver a entrega e leitura pelo titular dos dados do Termo de Consentimento antes de assinar ou marcar o consentimento;

k) Quando realizado por meios eletrônicos, seja por assinatura digitalizada (ex. tablet em que o paciente assina) ou pela confirmação em formulário eletrônico rastreável, o sistema que registrou o consentimento deverá estar apto para tal, como registro de hora, local, log de auditoria e controles de acesso (rastreável), carimbo de tempo;

l) A SPCC é responsável por provar que o consentimento foi obtido de acordo com a Lei;

m) É proibido realizar o tratamento de dados com vícios no consentimento, que deve ser específico e relacionado a finalidades determinadas. Autorizações genéricas são nulas;

n) Dados tornados manifestamente públicos pelo titular não exigem consentimento, mas os direitos do titular e os princípios da lei devem ser respeitados;

o) O compartilhamento de dados pessoais é dispensado de consentimento quando houver outra base legal prevista na LGPD.

p) O titular tem o direito de revogar o consentimento a qualquer momento por meio de procedimento gratuito e fácil via central de privacidade disponibilizado no site www.hcp.org.br, Tratamentos realizados enquanto o consentimento estava vigente permanecem válidos, a menos que haja solicitação de eliminação dos dados. Alterações em informações relevantes

devem ser comunicadas ao titular, que pode revogar seu consentimento caso discorde.

2.3.2. Cumprimento de obrigação legal ou regulatória

A SPCC pode realizar o tratamento de dados pessoais sem necessidade de consentimento quando este for estritamente necessário para cumprir obrigações legais, regulatórias ou para a execução de políticas públicas previstas em leis, regulamentos ou contratos. É crucial que essa base legal seja aplicada apenas quando a obrigação de cumprir a lei ou o regulamento recair diretamente sobre a própria instituição, conforme estabelecido no **Art. 7º da LGPD.**

Em todos os casos, os titulares dos dados devem ser claramente informados sobre o tratamento de seus dados, incluindo a base legal específica que o justifica. Em caso de dúvidas sobre a aplicação desta base legal, o colaborador deverá entrar em contato com o Encarregado de Proteção de Dados (DPO) através do e-mail dpo@hcp.org.br ou com o Departamento Jurídico pelo e-mail juridico@hcp.org.br.

2.3.3. Realização de estudos e pesquisas

A atividade científica, desenvolvida pela SPCC, apoia-se amplamente na coleta, análise e tratamento de dados pessoais e sensíveis.

a) O tratamento de dados pessoais para fins de pesquisa é permitido, desde que observadas as exigências legais e éticas aplicáveis. Sempre que possível, é recomendável que os dados sejam anonimizados, de forma a proteger a identidade dos titulares e reduzir riscos à privacidade;

b) A LGPD prevê bases legais específicas para o uso de dados em pesquisas científicas. A justificativa legal adequada varia conforme a natureza e a origem da pesquisa:

- Pesquisas conduzidas diretamente por órgãos de pesquisa da própria SPCC podem se apoiar nos artigos 7º, 11º e 13º da LGPD. Nesses casos, o tratamento de dados pessoais, inclusive sensíveis, pode ocorrer sem

consentimento, desde que respeitados os princípios da Lei, em especial os da finalidade, necessidade, minimização e transparência.

- Pesquisas de interesse exclusivamente individual ou acadêmico de um médico ou colaborador, mesmo que vinculadas à SPCC, não se enquadram no **art. 13º da LGPD.** Para esses casos, é obrigatório obter consentimento livre, informado e inequívoco do titular, especialmente para o tratamento de dados sensíveis. Além disso, é essencial que os dados compartilhados passem por processo de anonimização.

a) De forma prática, se alguém solicitar o acesso a informações de caráter pessoal que estejam sob a guarda da administração pública, e essa informação for considerada essencial para o interesse público ou para preservar direitos fundamentais, o órgão público deve comunicar ao titular dos dados e informá-lo de que ele pode se opor ao compartilhamento da informação. O titular tem o prazo de 20 dias para apresentar sua oposição formal;

b) É terminantemente proibida a divulgação de resultados ou trechos de estudos que possam revelar a identidade dos titulares dos dados. Os responsáveis pelo estudo devem garantir a guarda segura das informações e são vedadas quaisquer transferências de dados pessoais a terceiros, salvo quando previstas em lei ou com base em consentimento específico.

2.3.4. Execução de contratos

O tratamento pode ocorrer quando necessário para executar contratos ou etapas preliminares relacionadas a contratos em que o titular dos dados esteja envolvido, a pedido do próprio titular, devendo todos os contratos serem analisados pelo departamento jurídico da SPCC para validar as cláusulas de privacidade de dados.

2.3.5. Exercício regular dos direitos em processos judiciais

a) O inciso **VI do art. 7º da LGPD** autoriza o tratamento de dados pessoais sem a necessidade de consentimento do titular quando a finalidade for subsidiar o exercício regular de direitos em processos judiciais, administrativos ou arbitrais, sejam eles em andamento ou ainda por serem iniciados;

b) A SPCC, no papel de controlador, tem respaldo legal para produzir provas, mesmo que isso envolva dados pessoais da outra parte ou de terceiros, sem a necessidade de consentimento. No entanto, esse tratamento deve sempre observar os princípios da LGPD, especialmente os da finalidade, necessidade, adequação e transparência, conforme previsto no **art. 6º da Lei;**

2.3.6. Interesses Legítimos

a) O legítimo interesse é a hipótese legal prevista no art. 7º, IX da Lei Geral de Proteção de Dados Pessoais, que autoriza o tratamento de dados pessoais (não sensíveis), quando necessário para atender aos interesses legítimos do controlador ou de terceiros, desde que tais interesses e finalidades não violem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais;

b) A ANPD orienta que o tratamento de dados com respaldo no legítimo interesse deve ser precedido de um teste de balanceamento que considere, de um lado, os interesses do controlador e de outro, os direitos e liberdades fundamentais dos titulares;

c) A realização do teste de balanceamento deverá estar alinhado com o disponibilizado pela ANPD no seu Guia Orientativo Hipóteses Legais de Tratamento de Dados Pessoais Legítimo Interesse (link disponível na seção de referências);

d) A SPCC não deve realizar o tratamento com base na hipótese legal do legítimo interesse caso o teste de balanceamento conclua pela prevalência dos direitos e liberdades fundamentais e legítimas expectativas dos titulares;

2.3.7. Proteção da vida ou da integridade física do titular ou de terceiros

Para a proteção da vida ou da integridade física do titular ou de terceiros o tratamento de dados pessoais é permitido exclusivamente em procedimentos de saúde realizados por profissionais de saúde ou autoridades sanitárias.

2.3.8. Tutela da saúde

A base legal da tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária, prevista no **art. 11, II, "f", da LGPD,** permite o tratamento tanto de dados sensíveis quanto de dados não sensíveis, desde que esse tratamento tenha como finalidade a proteção da saúde do titular ou de terceiros;

- A tutela da saúde só se aplica legitimamente quando:

a) O tratamento for necessário para atividades-fim da assistência em saúde (ex.: diagnóstico, atendimento, tratamento, cuidados médicos);

b) For realizado por profissionais de saúde legalmente habilitados e vinculados ao dever de sigilo;

c) O objetivo for efetivamente a proteção da saúde do titular ou de terceiros.

Esta hipótese não deve ser utilizada em todas as etapas e operações da unidade de saúde. É importante distinguir as atividades assistenciais das demais operações internas ou administrativas (como faturamento, auditoria, marketing, gestão de contratos etc.).

2.3.9. Tratamento de Dados pela Administração Pública

Ainda que a SPCC seja uma entidade de direito privado, ela atua como extensão operacional da Administração Pública, executando uma política pública de

saúde (SUS), por delegação do Estado ou Município. Portanto, ao realizar o tratamento de dados de pacientes para cumprir exigências legais, contratuais ou regulatórias previstas em seu vínculo com o ente público, está legitimada a utilizar essa base legal, desde que respeite os princípios da LGPD, especialmente os da finalidade, necessidade, transparência e segurança.

2.3.10. Execução de Políticas Públicas

a) A base legal da execução de políticas públicas permite o tratamento de dados pessoais sem consentimento, quando o tratamento é respaldado por contratos, convênios ou instrumentos similares com a Administração Pública (Secretarias de Saúde), como é o caso da SPCC, atuando em nome do poder público no contexto do Sistema Único de Saúde (SUS).

2.3.11. Quadro Comparativo (Exemplos Práticos)

Base Legal (LGPD)	Descrição	Quando se aplica	Exemplos Práticos
Execução de Políticas Públicas *(Art. 7º, III)*	Permite o tratamento para execução de políticas públicas previstas em lei, regulamento ou contrato com o poder público.	Quando atuar sob contrato de gestão, convênio ou instrumento similar, com ente público. No contexto SPCC, executando atividades do SUS.	Coleta de dados para atendimento em hospitais públicos; envio de relatórios de produção à Secretaria de Saúde.
Cumprimento de Obrigação Legal ou Regulamentar *(Art. 7º, II)*	Permite o tratamento necessário para cumprir exigências legais ou regulatórias.	Em processos exigidos por normas da saúde, vigilância sanitária, ANS, Ministério da Saúde, etc.	Envio de dados ao e-SUS, CNES, notificações compulsórias, auditorias de órgãos reguladores.

Tutela da Saúde *(Art. 11, II, "f")*	Permite o tratamento de dados sensíveis para proteção da saúde, quando feito por profissionais de saúde ou por seus responsáveis.	Quando o tratamento está diretamente relacionado ao atendimento assistencial e realizado por profissionais de saúde.	Diagnóstico médico, tratamento, internações, prescrição de medicamentos, atendimento de urgência.
Proteção da Vida ou da Incolumidade Física *(Art. 7º, VII)*	Permite o tratamento de dados necessário para proteger a vida ou integridade física do titular ou de terceiros.	Em emergências, risco de vida ou saúde pública. Pode ser usado mesmo sem consentimento.	Atendimento de urgência; acesso a dados em situações críticas (acidentes, surtos, pandemias).
Execução de Contrato *(Art. 7º, V)*	Permite o tratamento necessário para executar ou preparar contrato com o titular dos dados.	Em relações contratuais com colaboradores, fornecedores ou prestadores de serviço.	Processos seletivos, contratos de trabalho, gestão de folha de pagamento, prestação de contas com convênios.
Consentimento do Titular *(Art. 7º, I)*	Exige que o titular autorize de forma livre, informada e específica o uso dos seus dados.	Quando não há outra base legal aplicável e o tratamento é opcional ou envolve finalidades secundárias.	Uso de imagem em campanhas institucionais, pesquisas acadêmicas por terceiros, ações de comunicação e marketing.
Exercício Regular de Direitos *(Art. 7º, VI)*	Permite o uso de dados para defesa em processos judiciais, administrativos ou arbitrais.	Quando precisar usar dados como prova ou para defender-se formalmente.	Defesa em ações judiciais, processos trabalhistas, sindicâncias, auditorias ou processos ético-profissionais.

2.4. Tratamento de Dados de Crianças e Adolescentes

O tratamento de dados de crianças e adolescentes é pautado pelo interesse público e pela proteção integral desse grupo vulnerável, conforme estabelecido no Estatuto da Criança e do Adolescente **(Lei nº 8.069/1990 e Lei 15.211/2025).**

- As principais bases legais aplicáveis são:

  - Execução de Políticas Públicas **(Art. 7º, III e Art. 11, II, "b", LGPD)**
  - Tutela da Saúde **(Art. 11, II, "f", LGPD)**
  - Proteção da Vida ou da Incolumidade Física **(Art. 7º, VII, LGPD)**

Essas bases legais asseguram que o tratamento de dados sensíveis de menores ocorra com a finalidade de garantir o direito constitucional à saúde, dentro das rotinas assistenciais, preventivas, diagnósticas, terapêuticas ou de acompanhamento médico promovidas pela SPCC e suas unidades sob gestão;

Nos casos em que o tratamento de dados não estiver vinculado diretamente à execução das políticas públicas de saúde será exigido o consentimento específico, destacado e com linguagem acessível, fornecido pelos pais ou responsáveis legais, conforme dispõe o **Art. 14 da LGPD;**

Esse consentimento deve ser obtido de forma clara, transparente, documentada e adequado à faixa etária, garantindo que os representantes legais compreendam a finalidade do uso dos dados, e que a criança ou adolescente, sempre que possível, também tenha conhecimento adequado à sua faixa etária;

O tratamento de dados pessoais de menores de idade deve seguir os princípios da LGPD, com atenção especial a finalidade, necessidade, segurança e transparência.

A SPCC deve implementar procedimentos internos rigorosos com o objetivo de minimizar a exposição de dados pessoais sensíveis de crianças e adolescentes. Entre as medidas recomendadas, destacam-se:

- Controle de acesso às informações, permitindo o acesso apenas a profissionais diretamente envolvidos no atendimento ou tratamento do menor;
- Segmentação de perfis de usuários, com níveis de permissão compatíveis com as atribuições funcionais de cada colaborador;

- Capacitação contínua das equipes, visando garantir a confidencialidade, a integridade e a correta utilização das informações sensíveis;
- Realização das coletas de dados sempre que possível na presença dos pais ou responsáveis legais, assegurando maior transparência e respeito à autonomia familiar.

Quando necessário, o compartilhamento de dados com órgãos como o Ministério da Saúde, Secretarias Estaduais e Municipais de Saúde, vigilância epidemiológica ou sistemas oficiais poderá ocorrer sem necessidade de consentimento, desde que estritamente para fins de cumprimento de políticas públicas de saúde, obrigações legais ou para a proteção da vida e da saúde do paciente;

2.5. Sanções

A LGPD é aplicável a todas às pessoas jurídicas de direito público ou privado que realizam o tratamento de dados pessoais no território nacional, incluindo instituições privadas, sem fins lucrativos, filantrópicas e 100% SUS.

Ainda que a SPCC exerça relevante papel na assistência oncológica, da saúde da mulher, de unidade de emergência 24 horas e atendimentos especializados de forma pública e gratuita, e seja conveniada à Secretaria Estadual ou Municipal de Saúde de Pernambuco, isso não a isenta da possibilidade de aplicação das sanções previstas na LGPD, caso se constate o descumprimento das normas de proteção de dados pessoais;

A ANPD poderá aplicar as seguintes sanções, previstas no Art. 52, conforme resolução CD/ANPD Nº 4, de 24 de fevereiro de 2023:

- Advertência, com indicação de prazo para adoção de medidas corretivas;
- Multa simples, de até 2% do faturamento da instituição no Brasil, no seu último exercício, limitada a R$ 50 milhões por infração;
- Multa diária, respeitado o limite total de R$ 50 milhões;
- Publicização da infração, após sua apuração e confirmação com objetivo de reforçar o princípio da transparência da LGPD, estimular a

- responsabilidade institucional, permitir que os titulares afetados tomem medidas de proteção;
- Bloqueio dos dados pessoais a que se refere a infração até sua regularização;
- Eliminação dos dados pessoais relacionados à infração;
- Suspensão parcial do funcionamento do banco de dados a que se refere a infração por até seis meses, prorrogável por igual período;
- Suspensão do exercício da atividade de tratamento de dados pessoais a que se refere a infração por até seis meses, prorrogável por igual período;
- Proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

3. Responsabilidades

As responsabilidades são distribuídas entre os envolvidos: Controlador, Operador, encarregado pelo tratamento de dados e demais setores, as quais relacionamos a seguir:

3.1. Geral

Cada colaborador, independentemente de seu cargo ou setor, é fundamental na proteção de dados e na conformidade com a LGPD. A responsabilidade não se limita a departamentos específicos.

- **Leitura e Compreensão:** é responsabilidade de cada colaborador ler, compreender e seguir todas as políticas e procedimentos internos relacionados à LGPD e à segurança da informação da SPCC;
- **Adesão às Regras:** aplicar as regras na prática diária, desde o manuseio de prontuários, acesso a sistemas e envio de e-mails até o descarte de informações;

- **Necessidade de Saber:** acessar, coletar ou compartilhar dados pessoais apenas se for estritamente necessário para a execução de suas tarefas e com a devida base legal. Se não é da sua atribuição, não acessar;

- **Evitar impressões desnecessárias de documentos com dados pessoais:** quando for preciso imprimir, garantir que sejam descaracterizados e descartados corretamente após o uso;

- **Bloquear o computador ao se ausentar da estação de trabalho:** evitar deixar documentos com dados pessoais expostos ou em locais de fácil acesso;

- **Engajamento:** participar ativamente de todos os treinamentos e ações de conscientização sobre LGPD promovidos pela SPCC. O conhecimento é a principal ferramenta de prevenção;

- **Cultura de Privacidade:** contribuir para a construção de uma cultura organizacional que valoriza a privacidade e a proteção de dados como um pilar fundamental da excelência hospitalar;

- **Compartilhamento de Dados:** dados pessoais só podem ser compartilhados com terceiros mediante termo de consentimento expresso do titular, salvo exceções legais (como obrigação legal, cumprimento de política pública ou para proteção da vida/incolumidade física do titular). O compartilhamento deve ser justificado pela finalidade do tratamento e limitado aos dados estritamente necessários.

- **Confidencialidade:**

  I. Sempre que dados forem compartilhados com parceiros ou fornecedores, devem ser estabelecidos acordos de confidencialidade e termos de tratamento de dados, garantindo que eles também sigam as normas da LGPD;

  II. Manter a confidencialidade de todas as informações de pacientes, colaboradores e terceiros às quais tiver acesso;

III. Nunca discutir informações confidenciais em locais públicos e/ou com pessoas não autorizadas.

- **Descaracterização e Descarte Seguro:** Documentos físicos ou eletrônicos que contenham dados pessoais devem ser descaracterizados e descartados de forma segura (se físico, triturado ou incinerado; se eletrônico, deve ser excluído de forma permanente, impossibilitando a recuperação) após o atendimento da finalidade de uso do dado ou a expiração do prazo legal de guarda;

- **Política de Segurança da Informação:** É obrigatório seguir rigorosamente a Política de Segurança da Informação da unidade;

- **Senhas:** Crie e utilize senhas fortes e únicas para todos os seus sistemas e computadores, e garanta que elas sejam absolutamente intransferíveis. Isso significa que sua senha é exclusivamente sua; ela não pode, sob hipótese alguma, ser passada ou cedida a qualquer outra pessoa. Você é o único responsável por manter sua senha em segredo e por todas as ações realizadas com ela. Essa responsabilidade individual é crucial para assegurar a proteção de todos os sistemas e dados;

- **Acesso e Permissões**: O acesso a sistemas e dados deve ser concedido apenas a usuários autorizados e conforme a necessidade de suas funções (princípio do mínimo privilégio);

- **Spam / Phishing:** Não clicar em links ou abrir anexos de remetentes desconhecidos e/ou suspeitos. Estar atento a tentativas de phishing (e-mails ou mensagens falsas), malware e outras ameaças cibernéticas. Em caso de dúvida, entrar em contato com a equipe de TI;

- **Criptografia Obrigatória**: Todas as mídias removíveis (pendrives, HDs externos, smartphones etc.) utilizadas para armazenar ou transportar dados pessoais devem ser obrigatoriamente criptografadas;

- **Uso Restrito:** O uso de mídias removíveis deve ser restrito aos casos estritamente necessários e sempre autorizado pela equipe de Tecnologia da Informação (TI) conforme Política de Segurança da Informação;

- **Softwares Mensageria:** Não tratar dados pessoais em softwares de mensageria como o WhatsApp, similares ou outras plataformas de comunicação não corporativas;

- **E-mail Corporativo:** Caso seja imprescindível e haja base legal para o tratamento de dados pessoais por e-mail, utilizar exclusivamente o e-mail corporativo. Atentar aos endereços dos destinatários e dos copiados para certificar-se de que somente quem necessita do dado para uma finalidade específica irá receber;

- **Atenção ao Conteúdo:** Evitar compartilhar informações sensíveis por e-mail sem as devidas precauções (ex: criptografia, senha para acesso ao anexo, links compartilhados somente nominalmente a quem tem o direito de acesso);

- **Google Drive e similares:** É proibido o uso de ferramenta não corporativa e sem a devida licença de uso, para tratamento de dados pessoais;

- **Ferramentas e Sistemas corporativos:** O tratamento de dados pessoais deve ser realizado exclusivamente nos sistemas oficiais da SPCC. Utilizar apenas os sistemas, e-mails corporativos e dispositivos autorizados pelas unidades da SPCC para o tratamento de dados pessoais;

- **Dispositivos Particulares:** Não tratar dados pessoais em dispositivos móveis particulares (pessoais), como celulares, tablets ou notebooks;

- **Dispositivos Corporativos:** Se o uso de dispositivo móvel corporativo for necessário para o tratamento de dados, ele deve seguir a Políticas de Segurança da Informação da unidade;

- **Política de Privacidade de Dados:** Todos os colaboradores, terceiros, prestadores de serviços ou que de alguma forma faça parte das atividades da SPCC devem conhecer e seguir rigorosamente a Política de Privacidade de Dados e este manual;

- **Avaliação de Impacto:** Acionar a equipe de privacidade para avaliação de impacto no tratamento de dados pessoais sempre que for implementar ou alterar um processo ou sistema computacional que envolva o tratamento de dados pessoais, bem como em qualquer compartilhamento de dados com terceiros;

- **Comunicação de Incidentes:** Comunicar imediatamente à equipe de privacidade (ou ao seu superior direto, que deve acionar a equipe de privacidade) qualquer suspeita ou ocorrência de incidente envolvendo dados pessoais, como vazamento, acesso não autorizado, perda de documentos, etc. A agilidade no reporte é crucial para mitigar danos. A comunicação pode ser realizada diretamente na central de privacidade no site do HCP (https://www.hcp.org.br/privacidade-e-seguranca) ou pelo dpo@hcp.org.br;

- **Atualização do Inventário de Dados:** Acionar a equipe de privacidade quando ocorrer qualquer mudança de processo que possa afetar o fluxo de dados pessoais, para que o inventário de dados se mantenha atualizado;

- **Não prints ou Compartilhamento de Telas:** Não tirar nem compartilhar prints (capturas de tela) de sistemas que contenham dados pessoais. Nunca tirar fotos, fazer "prints" de telas ou compartilhar imagens de prontuários, sistemas ou qualquer documento que contenha dados pessoais;

- **Imagens de Pessoas:** Não coletar, armazenar ou compartilhar imagens de pessoas sem o consentimento expresso do titular da imagem ou devidamente enquadrado em uma base legal;

- **Planos de Ação:** Os responsáveis por cada setor devem reportar à equipe de privacidade com regularidade (não maior que 30 dias) sobre as ações e

medidas adotadas em relação ao plano de ação de conformidade com a LGPD e quaisquer desafios identificados;

- **Minimização de Dados:** Não tratar dados pessoais além do estritamente necessário para atender a finalidade pretendida. O princípio da minimização de dados é fundamental;

- **Período de Retenção:** Os dados devem ser armazenados apenas pelo período necessário para cumprir sua finalidade ou conforme exigido por lei;

- **Classificação de Dados:** Classificar os dados conforme sua natureza (pessoais e sensíveis) e relevância, identificando aqueles que requerem maior proteção;

- **Classificação da Informação:** Classificar as informações conforme sua confidencialidade (confidencial, restrito e público) e relevância, identificando aqueles que requerem maior proteção;

- **Dúvidas sobre como tratar um dado, com quem compartilhar ou se uma situação é um incidente:** Sempre procurar o DPO ou a equipe de privacidade de dados (dpo@hcp.org.br / (81) 3217-8340 / 989495260) antes de agir.

3.2. Controlador

Cabe ao controlador a decisão sobre como os dados deverão ser tratados; fazendo e mantendo registro das operações e ainda promovendo reparos sobre o tratamento de dados considerados irregulares. Compromete-se a:

a) Envolver prontamente o DPO em todos os assuntos relacionados à proteção de dados pessoais;

b) Verificar se o DPO executa suas tarefas de forma autônoma e independente;

c) Abster-se de atribuir tarefas ao DPO que possam levar a, ou resultar em um conflito de interesses;

d) Decidir sem demora acerca da tomada de medidas de adequação, mitigação de danos e endereçamento de riscos, violações, incidentes e outras questões relacionados à segurança da informação, privacidade e proteção de dados levadas à alta-diretoria pelo DPO;

e) Aprovar comunicações e respostas às autoridades e ao público em geral;

f) Manter os dados de contato do DPO disponíveis ao público.

3.3. Operador

a) Executar a decisão do controlador e orientações do Encarregado pelo Tratamento de Dados Pessoais;

b) Manter registro das operações e se dispor a executar os reparos se houver inconformidade com a legislação ou com a Política de Privacidade de Dados Pessoais;

c) Deverá seguir todas as regras contidas neste Manual de Normas.

3.4. DPO

a) Realizar suas atividades em conformidade com o **art. 41 da Lei Geral de Proteção de Dados Pessoais e resolução CD/ANPD Nº 18, de 16 de julho de 2024;**

b) Informar e aconselhar o Controlador e seus colaboradores que realizam operações de tratamento de dados sobre suas obrigações nos termos da Lei Geral de Proteção de Dados Pessoais (LGPD) e de qualquer lei aplicável à proteção de dados;

c) Monitorar a conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD) e quaisquer outras disposições aplicáveis à proteção de dados;

d) Monitorar as estratégias do Controlador para a proteção de dados pessoais, incluindo a alocação de responsabilidades, conscientização e treinamento do pessoal envolvido nas operações de tratamento de dados e verificações relacionadas;

e) Cooperar com a ANPD;

f) Atuar como ponto de contato da ANPD em questões relacionadas com o tratamento de dados pessoais, incluindo consultas prévias sobre a avaliação de impacto à proteção de dados nos termos da Lei Geral de Proteção de Dados Pessoais (LGPD), quando apropriado, assessorando em todas as outras questões;

g) Atuar como ponto de contato para o exercício dos direitos dos titulares de dados nos termos da LGPD e processar suas consultas relacionadas às atividades de tratamento de dados;

h) Monitorar e dar suporte na gestão de inventários, matrizes de riscos e planos de ações que envolvam tratamento de dados pessoais;

i) Monitorar, revisar e apoiar para manter atualizada a Política de Segurança da Informação, Política de Backup, Política de Continuidade de Negócios, Política de Recuperação de Desastres;

j) Construir, revisar e manter atualizada as políticas que tratam dados pessoais: Privacidade de Dados, Política para Gestão dos Termos de Consentimento e Termos de Uso.

k) Construir, revisar e manter atualizados o Plano de Comunicação de Incidentes envolvendo dados pessoais;

l) Monitorar, revisar e apoiar para manter atualizada a Política de Classificação das Informações, Política de Descaracterização, Descarte e Sanitização de Dados;

m) Apoiar para manter atualizada as adequações contratuais com operadores, termos de acordos de confidencialidade e sigilo com fornecedores, clientes e empregados;

n) Construir, revisar e manter atualizado o Relatório de Impacto à Privacidade de Dados (RIPD) e Avaliações de Impacto (DPIA);

o) Criar, monitorar e revisar processo para garantir os direitos dos titulares;

p) Criar, monitorar e revisar canal de comunicação do titular dos dados pessoais com a instituição;

q) Criar, monitorar e revisar o processo de gerenciamento de violações e notificações necessárias;

r) Criar, monitorar e revisar o plano de gestão de crise em caso de incidente/ violação de dados;

s) Instituir e operacionalizar o Comitê de Segurança de Dados.

t) Realizar relatórios periódicos para a alta gestão sobre o nível de adequação à LGPD.

3.5. Tecnologia da Informação (TI)

➢ **O papel da TI em relação à LGPD é:**

a) Garantir a implementação e gestão de criptografia em dados em trânsito e em repouso;

b) Manter sistemas de controle de acesso baseado em função, garantindo que apenas usuários autorizados tenham acesso aos dados estritamente necessários para suas funções;

c) Implementar e gerenciar firewalls, sistemas de detecção e prevenção de intrusão (IDS/IPS), e outras ferramentas para proteger a rede hospitalar contra acessos não autorizados e ataques cibernéticos.

d) Implementar e gerenciar ferramentas de monitoramento de logs e auditoria para rastrear o acesso e as atividades nos sistemas que tratam dados pessoais, permitindo a detecção de atividades suspeitas e a responsabilização em caso de incidentes;

e) Realizar varreduras regulares de vulnerabilidade e garantir a aplicação de patches e atualizações de segurança nos sistemas;

f) Desenvolver, implementar e testar planos de backup, continuidade de negócios e recuperação de desastres.

g) Apoiar o mapeamento completo dos dados pessoais que são coletados, onde são armazenados, como são processados, com quem são compartilhados e por quanto tempo são retidos.

h) Assegurar que novos sistemas e aplicações sejam desenvolvidos ou contratados com a privacidade e a segurança como premissa desde o início (privacy by design e security by design) e passem por testes rigorosos de segurança e conformidade com a LGPD;

i) Garantir que todos os sistemas e aplicações, antes de entrarem em produção, passem por testes de segurança da informação;

j) Implementar métodos seguros para a sanitização dos dados contidos nos meios digitais, garantindo que as informações não possam ser recuperadas, quando da realização do descarte ou fim da vida útil do equipamento;

k) Avaliar e garantir que os fornecedores de tecnologia e serviços que têm acesso a dados pessoais estejam em conformidade com a LGPD, através

de cláusulas contratuais específicas e auditorias, e com padrões de segurança da informação de mercado;

l) Fornecer e gerenciar as ferramentas e processos para anonimização e pseudonimização de dados quando necessário;

m) Desenvolver e manter, em conjunto com o DPO, um plano de resposta a incidentes de segurança da informação, definindo os passos a serem seguidos em caso de vazamento ou acesso indevido a dados pessoais;

n) Atuar para conter e erradicar incidentes de segurança, minimizando o impacto e a extensão da violação de dados;

o) Realizar análises forenses para determinar a causa, o escopo e o impacto de um incidente, auxiliando na comunicação às autoridades e aos titulares dos dados;

p) Trabalhar em estreita colaboração com o DPO para investigar e reportar incidentes, garantindo que as obrigações legais sejam cumpridas.

q) Colaborar na criação e aplicação de treinamentos contínuos para todos os colaboradores sobre as melhores práticas de segurança da informação.

3.6. Recursos Humanos (RH)

A atuação proativa e diligente do RH é crucial para mitigar riscos, garantir a privacidade e a segurança das informações dos profissionais da SPCC e, consequentemente, fortalecer a confiança e a reputação da instituição.

- **Suas responsabilidades abrangem:**

a) Obter o consentimento explícito do titular para o tratamento de dados pessoais quando esta for a base legal adequada;

b) Informar de forma clara e objetiva aos titulares dos dados quais dados serão coletados, a finalidade do tratamento, como serão utilizados, com quem serão compartilhados e por quanto tempo serão armazenados;

c) Estabelecer um processo claro e eficiente para atender às solicitações dos titulares de dados sobre seus direitos, em conjunto com DPO;

d) Treinar, em conjunto com o DPO, regularmente toda a equipe de RH sobre as disposições da LGPD, as políticas e procedimentos internos de proteção de dados e as melhores práticas de segurança da informação no manuseio de dados pessoais;

e) Apoiar a promoção de uma cultura de privacidade e segurança da informação em toda a Instituição;

f) Promover auditorias internas para verificar a conformidade dos processos, políticas e termos de consentimento dá área e identificar pontos de melhoria em conjunto com o DPO.

3.7. Jurídico

O Setor Jurídico desempenha uma função consultiva, estratégica e de mitigação de riscos para a conformidade com a Lei Geral de Proteção de Dados (LGPD).

- **O papel do setor jurídico em relação à LGPD é:**

a) Fornecer pareceres jurídicos sobre a aplicação da LGPD em casos específicos;

b) Monitorar as atualizações da LGPD, regulamentações da ANPD e decisões judiciais que possam impactar o tratamento de dados na SPCC;

c) Revisar e incluir cláusulas de proteção de dados em todos os contratos com fornecedores, parceiros e prestadores de serviços que tenham acesso ou tratem dados pessoais em nome da SPCC;

d) Apoiar na construção e revisão das políticas de privacidade de dados;

e) Apoiar na construção e revisão dos termos de consentimento para tratamento de dados, assegurando que sejam específicos, livres, informados e inequívocos;

f) Apoiar na construção e revisar termos de uso para aplicativos ou plataformas digitais utilizadas pela SPCC que envolvam dados pessoais.;

g) Apoiar a avaliação de riscos legais associados ao tratamento de dados, auxiliando na identificação de vulnerabilidades e na proposição de medidas mitigadoras;

h) Participar da elaboração e revisão das avaliações de impacto, garantindo que as avaliações considerem os aspectos legais e os riscos à privacidade e aos direitos dos titulares;

i) Atuar na resposta a incidentes de segurança da informação que envolvam dados pessoais, auxiliando na análise da conformidade legal da resposta, na comunicação à ANPD e aos titulares, e na mitigação de possíveis sanções;

j) Orientar sobre a forma correta de responder a reclamações de titulares de dados e ofícios da ANPD ou de outras autoridades;

k) Oferecer suporte e orientação jurídica a todos os setores da SPCC sobre suas responsabilidades e obrigações quanto à LGPD;

l) Colaborar na elaboração e condução de treinamentos sobre LGPD para os colaboradores, com foco nos aspectos jurídicos e nas implicações de não conformidade;

m) Prestar assessoria jurídica ao Encarregado de Dados (DPO) da SPCC, auxiliando-o na interpretação da lei, na elaboração de relatórios e na comunicação com a ANPD e os titulares;

n) Representar a SPCC em processos administrativos ou judiciais relacionados à proteção de dados pessoais, incluindo autuações da ANPD, ações de titulares ou disputas com terceiros;

o) Atuar em negociações que envolvam o tratamento ou compartilhamento de dados pessoais, protegendo os interesses da SPCC.

3.8. Qualidade

O Departamento de Qualidade desempenha o papel de integrador e proporciona melhoria contínua crucial para a conformidade com a LGPD. Sua atuação se baseia na garantia de que os processos relacionados ao tratamento de dados pessoais não apenas sigam as normas, mas sejam otimizados, documentados e constantemente aprimorados para assegurar a segurança e a privacidade.

➢ **O papel do Departamento da Qualidade em relação à LGPD é:**

- Colaborar ativamente no mapeamento de todos os processos internos assistenciais da unidade que envolvem tratamento de dados pessoais, identificando os fluxos, as etapas e os responsáveis em cada fase.
- Ao desenvolver e padronizar os procedimentos operacionais padrão (POPs) das áreas assistenciais, garantir que as diretrizes da LGPD sejam incorporadas às rotinas diárias;
- Assegurar o controle de versão de todos os documentos e registros relacionados à LGPD, garantindo que apenas as versões aprovadas e atualizadas estejam em uso;

- Nas verificações internas periódicas realizadas nos diversos setores assistenciais da SPCC observar a aderência aos POPs, incluindo aspectos ligados à LGPD, com apoio do DPO;
- Atuar em conjunto com o DPO para gerenciar as não conformidades identificadas relacionadas à LGPD, investigando as causas-raiz e propondo ações corretivas e preventivas;
- Analisar incidentes ou não conformidades para evitar sua recorrência e aprimorar continuamente o sistema de gestão da privacidade;
- Colaborar na elaboração e execução de programas de treinamento e conscientização contínuos sobre LGPD e as responsabilidades de cada colaborador;
- Colaborar com a comunicação interna para disseminação da cultura de proteção de dados;
- Incentivar e implementar práticas que garantam a qualidade, exatidão e atualização dos dados pessoais, um princípio fundamental da LGPD.

3.9. Líderes

As lideranças (Diretoria, Superintendências, Líderes e Coordenações) são essenciais para a conformidade contínua com a LGPD. Cabe às lideranças:

I. Demonstrar compromisso com a proteção e privacidade de dados;

II. Comunicar a importância da LGPD de forma clara e contínua para suas equipes, explicando a necessidade da proteção de dados e os benefícios para o paciente, para as unidades de saúde e para cada colaborador;

III. Integrar a proteção de dados nas estratégias e planos de suas respectivas áreas, priorizando projetos e iniciativas que melhorem a segurança e a privacidade;

IV. Apoiar a aquisição e implementação de ferramentas e tecnologias que fortaleçam a segurança dos dados;

V. Assegurar que as políticas e procedimentos de proteção de dados sejam compreendidos e aplicados por todos os membros de suas equipes;

VI. Monitorar ativamente se suas equipes estão seguindo as diretrizes, realizando verificações periódicas e atuando sobre desvios;

VII. Garantir que todos os colaboradores sob sua liderança participem dos treinamentos de LGPD e segurança da informação, e que o conhecimento adquirido seja aplicado na prática;

VIII. Auxiliar na identificação de riscos relacionados ao tratamento de dados pessoais em seus respectivos processos e áreas de atuação

IX. Desenvolver e acompanhar planos de ação para mitigar riscos e corrigir não conformidades;

X. Reforçar a importância do reporte imediato de incidentes de segurança da informação ou suspeitas de violação de dados à equipe de privacidade.

XI. Tomar decisões rápidas e assertivas em caso de incidentes, seguindo o plano de resposta e as orientações do DPO;

XII. Promover a colaboração entre as diferentes áreas do hospital para resolver questões complexas de proteção de dados;

XIII. Incentivar e acolher o feedback das equipes para a melhoria contínua dos processos de tratamento de dados;

XIV. Participar da revisão periódica das políticas e procedimentos de LGPD, garantindo que estejam sempre atualizados e eficazes.

4. Dos direitos dos titulares

A previsão sobre o direito do titular encontra-se no artigo 18º da Lei Geral de Proteção de Dados. Para estar em conformidade com o atendimento aos direitos dos titulares, a SPCC deverá:

a) Fornecer aos titulares de dados pessoais, de forma clara e facilmente acessível, informações que identifiquem o controlador e descrevem o tratamento de seus dados pessoais;

b) Implementar políticas, procedimentos e/ou mecanismos para os titulares de dados pessoais acessarem, corrigirem e/ou excluírem os seus dados pessoais;

c) Informar aos terceiros com quem os dados pessoais foram compartilhados sobre qualquer modificação, cancelamento ou desaprovação pertinente aos dados pessoais compartilhados, e implementar políticas e procedimentos apropriados e/ou mecanismos para fazê-lo;

d) Ser capaz de fornecer uma cópia dos dados pessoais que são tratados, quando requerido pelo titular de dados pessoais;

e) Definir e documentar políticas e procedimentos para tratamento e respostas a solicitações legítimas dos titulares de dados pessoais;

f) Garantir que os pacientes e colaboradores tenham o direito de questionar decisões tomadas exclusivamente por sistemas de computador. Deve ter um processo claro para entender como essas decisões automáticas os afetam e assegurar que os direitos do titular dos dados sejam sempre respeitados.

Para exercer seus direitos, conhecer as políticas e práticas, o titular de dados poderá realizar pelo portal de privacidade de dados da SPCC disponibilizado no site https://www.hcp.org.br/privacidade.

5. Medidas de Privacidade e Segurança

5.1. Administrativas

As medidas administrativas para proteção de dados pessoais são desenvolvidas pela administração da instituição, por orientação da própria Lei e do controlador, com o intuito de desenvolver mecanismos de proteção dos dados, sejam eles no ambiente digital ou no ambiente físico. Não bastando o uso de dispositivos de segurança no ambiente digital, é necessário que a instituição desenvolva técnicas administrativas que possam garantir a proteção desses dados.

- **Abaixo algumas medidas administrativas:**

5.2. Política de Segurança da Informação - PSI

É a Política desenvolvida pela instituição para as orientações internas que dizem respeito à segurança e proteção de dados para organizar, orientar e conduzir a melhor forma de interagir com a informação, a segurança e a proteção dos dados num conjunto de sistemas, redes e programas existentes no ambiente digital.

A política pode ser consultada na Intranet de cada unidade.

5.2.1. Política de Privacidade

A Política de Privacidade é o documento institucional que estabelece como a SPCC manterá os dados dos titulares em privacidade e segurança, detalhando as regras de uso, guarda, manutenção, eliminação e compartilhamento de dados pessoais, visando assegurar a conformidade legal e o direito fundamental à privacidade dos titulares, conforme previsto na legislação vigente.

A política pode ser consultada no portal (site) de cada unidade.

5.2.2. Cláusulas contratuais

É obrigatório que todos os contratos que envolvam o tratamento de dados pessoais contenham cláusulas específicas sobre a LGPD. Essas cláusulas devem estabelecer a finalidade, os princípios e a responsabilidade de cada parte no tratamento dos dados, garantindo a conformidade legal. Tais disposições são essenciais para assegurar a confidencialidade, a proteção dos dados (incluindo o trânsito, arquivamento e eliminação) e para definir as condutas a serem seguidas, mitigando riscos e estabelecendo responsabilidades claras entre a SPCC e seus parceiros.

5.3.Técnicas

As medidas técnicas de Privacidade estão relacionadas às ações de tecnologia que visam proteger os dados e garantir a privacidade através do controle de acesso, da criptografia, da auditoria, do uso de softwares e ferramentas de segurança da informação e da anonimização dos dados.

6. Tratamento de dados sensíveis

O Tratamento de Dados Pessoais sensíveis está previsto no art.11º da Lei Geral de Proteção de Dados, e estão diretamente ligados a algo discriminatório na informação de: origem racial e formação étnica, convicções religiosas, opiniões políticas, filiação a Sindicatos, dados referentes à saúde, à vida sexual, dados genéticos ou biométricos, sendo esses dados que irão seguir a justificativa de tratamento nas hipóteses legais de consentimento explícito.

7. Tratamento de dados pessoais de crianças e adolescentes

O acesso aos dados de crianças e adolescentes são específicos e seu consentimento é obrigatório pelos pais ou responsáveis e de acordo com o interesse. É necessário que haja uma conscientização do não compartilhamento dos dados e que não haja o repasse sem a autorização formal dos responsáveis.

8. Compartilhamento de dados pessoais

a) É proibido o compartilhamento de dados pessoais sem o consentimento específico do titular, exceto nas hipóteses legais.

b) Deve ocorrer, quando autorizado ou previsto em lei, exclusivamente por meios e canais seguros e criptografados.

c) Identificar e documentar as bases relevantes para a transferência de dados pessoais;

d) Especificar e documentar os países e as organizações internacionais para os quais os dados pessoais possam possivelmente ser transferidos;

e) Registrar a transferência de dados pessoais para/ou de terceiros e assegurar a cooperação com essas partes para apoiar futuras solicitações relativas às obrigações para os titulares de dados pessoais;

f) Registrar a divulgação de dados pessoais para terceiros, incluindo quais dados pessoais foram divulgados, para quem e quando;

9. Programa de Governança em Privacidade de Dados

O Programa de Governança em Privacidade da instituição é fundamentado em um conjunto abrangente de normas e leis, incluindo a LGPD, o Código de Defesa do

Consumidor, o Marco Civil da Internet, a Lei de Acesso à Informação e regulamentações setoriais específicas (ANVISA, CFM, ANS, sindicatos), além das normas técnicas ISO/IEC aplicáveis (Série 27000, 27701, 19134, 29151 etc.). A implementação e a conformidade do programa são estruturadas em seis etapas principais: (I) Planejamento, (II) Treinamento e Conscientização, (III) Inventário de Dados Pessoais, (IV) Matriz de Risco, (V) Plano de Ação e (VI) Governança.

9.1.Planejamento

Etapa desenvolvida pelo DPO onde serão definidos de forma detalhada os passos que servirão de guia aos envolvidos no projeto de adequação a LGPD (Nomeação do DPO, Formação do Comitê de Proteção e Privacidade de Dados, identificação setores, líderes e operadores, estratégia de comunicação, cronograma do projeto), viabilizando que os objetivos sejam alcançados sem desvios significativos quanto ao tempo, custos, escopo, recursos e formas de comunicação.

9.2.Treinamento e Conscientização

Serão realizadas palestras e workshops, on line ou presencialmente, capacitando quanto aos principais conceitos fundamentais da LGPD, riscos e impactos no tratamento de dados pessoais, medidas de proteção e contextos práticos do uso de dados pessoais na rotina da unidade e o modo de protegê-los, garantindo a privacidade dos titulares.

9.3.Inventário de Dados Pessoais – IDP

O IDP é o mapa dos processos existentes em cada setor com o objetivo de identificar como e quais dados pessoais e sensíveis são coletados, armazenados (estruturados e não estruturados), compartilhados, processados, eliminados, quais os operadores envolvidos, quais as hipóteses de tratamento, previsão legal, as medidas de segurança, as finalidades, tempo de retenção, frequência de tratamento, contratos envolvidos, benefícios esperados para o titular, benefícios esperados para a instituição, uso de termos de consentimento, sistemas computacionais, transferência internacional de dados e abrangência do tratamento.

9.4.Matriz de Risco

A matriz de risco norteia a análise dos processos sugestivos de risco, vulnerabilidade de vazamento de dados ou políticas de adequação que se enquadrem num modo novo de coleta, guarda, processamento, compartilhamento ou eliminação.

A Matriz de Risco é elaborada, pela equipe de privacidade, com base no IDP e auxilia a priorizar e gerenciar os riscos associados ao tratamento de dados pessoais. Ao cruzar a probabilidade de ocorrência de um incidente com seu potencial impacto sobre os titulares de dados e o negócio, a matriz permite identificar as prioridades para mitigação.

Ao término da construção da matriz deve ser realizada devolutiva para o gestor da área analisada.

9.5.Plano de Ação

A equipe de Privacidade de Dados deverá elaborar o plano de ação como resultado da análise feita na matriz de risco e apresentá-lo ao gestor da área.

O plano de ação conterá as medidas sugeridas para os riscos identificados com as suas devidas priorizações. Cada ação sugerida estará referenciada a uma ou mais medidas de segurança da informação e uma ou mais medida para gestão da privacidade dos dados, com seu respectivo prazo para realização.

O objetivo será tratar o risco dentro da seguinte medida de mitigação:

- Eliminação: Remover completamente a fonte de risco;
- Redução: Diminuir a probabilidade ou o impacto do risco;
- Transferência: Transferir o risco para terceiros;
- Aceitação: Aceitar o risco, sabendo dos seus potenciais impactos.

9.6.Plano de comunicação de incidentes envolvendo dados pessoais

O Plano estabelece as medidas a serem adotadas em caso de um incidente que possa causar danos à instituição e/ou aos titulares dos dados. Garantindo,

inclusive, a comunicação apropriada e tempestiva à ANPD e aos titulares dos dados, quando aplicável.

O Plano de Comunicação está disponível na Intranet na área da LGPD.

10. Comitê de Proteção de Dados e Privacidade.

Comitê instituído pela Portaria nº 007, de 19 de setembro de 2024, com a finalidade de garantir o cumprimento da Lei Geral de Proteção de Dados, através do presidente do comitê, o DPO (Encarregado de Dados), e os demais membros das Superintendências e representantes das áreas de TI, Jurídico, RH/DP e Qualidade.

O Comitê reunir-se-á com periodicidade mínima trimestral, de forma ordinária, para definição de atividades, acompanhamento e evolução dos atos realizados, e extraordinariamente, a qualquer tempo mediante convocação prévia por qualquer dos membros, quando a situação assim o exigir, inclusive na identificação de possível incidente de segurança envolvendo dados pessoais.

A Portaria completa está disponível na Intranet na área da LGPD.

11. Privacidade e Segurança desde o início do processo

Para prevenir problemas de privacidade, garantindo que a proteção de dados seja parte integrante de todas as nossas atividades, cada processo ou rotina de tratamento de dados somente deverá iniciar com as devidas medidas de privacidade e segurança de dados.

Ao criar ou ajustar um processo, sistema ou serviço, a proteção de dados deve ser aplicada desde a fase de planejamento, e não como algo a ser adicionado depois. Por padrão, as configurações de privacidade e segurança devem ser sempre as mais protetivas possíveis para o titular dos dados e a SPCC.

12. Avaliação de Impacto à Proteção de Dados (DPIA)

O DPIA é uma ferramenta para identificar e mitigar riscos à privacidade antes que um novo processo, sistema ou tecnologia seja implementado ou quando houver uma alteração significativa em um já existente que envolva dados pessoais.

É um processo proativo para:

- Identificar e analisar os riscos que o tratamento de dados pessoais pode gerar para os direitos e liberdades dos titulares;
- Definir e implementar medidas eficazes para mitigar ou eliminar esses riscos;
- Demonstrar a conformidade da SPCC com a LGPD e o compromisso com a proteção de dados.

13. Relatório interno de comunicação de incidente com dados pessoais

O Relatório Interno de Comunicação de Incidente de Segurança com Dados Pessoais é uma documentação interna do incidente, das medidas tomadas e da análise de risco, e tem como propósito o cumprimento do princípio de responsabilização e prestação de contas (art. 6º, X – LGPD): 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.

Este relatório é construído pelo DPO em conjunto com as áreas ou titulares envolvidos no incidente.

Após a conclusão da apuração, é apresentado para assinatura e ciência à Superintendência Geral de Controladoria, Superintendência da área, Gerente da área envolvida e DPO.

O relatório deverá conter no mínimo: Dados do controlador, identificação (DPO), identificação e descrição do Incidente, data da ocorrência, data do conhecimento, data da comunicação à ANPD, data comunicação aos titulares, categoria dos titulares de dados afetados, metodologia utilizada, lista de pessoas envolvidas e consultadas,

dados violados, avaliação do risco, natureza do incidente, impacto potencial (Operacional, financeiro, reputacional, legal/regulatório), probabilidade de materialização, gravidade, impacto, risco geral, indicação de políticas supostamente violadas, controles internos falhos, medidas adotadas ou a serem adotadas para corrigir ou mitigar as causas do incidente.

14. Relatório de Impacto à Proteção de Dados Pessoais - RIPD

O RIPD visa descrever os 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 (Art. 5º, XVII da Lei 13.709/2018 - LGPD).

Este relatório é construído pelo DPO em conjunto com as áreas da SPCC. Após a conclusão do relatório, é apresentado para assinatura e ciência à Superintendência Geral de Controladoria, Superintendência Geral e DPO.

Sua construção deverá seguir o padrão e orientação, conforme ANPD.

15. Referências

Guia Orientativo Legítimo Interesse. ANPD. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/copy_of_guia_legitimo_interesse.pdf. Acesso em 04/12/2025.

Guia de Boas Práticas para Implementação na Administração Pública Federal. Gov.br. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/guias/guia_lgpd.pdf. Acesso em 04/12/2025.

Programa de Privacidade e Segurança da Informação (PPSI). Governo Digital. Privacidade e Segurança. Gov.br. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca. Acesso em 04/12/2025

Manual de Proteção de Dados Pessoais. Controladoria Geral do Estado de Pernambuco. Disponível em https://www.scge.pe.gov.br/lgpd-rede-de-encarregados/. Acesso em 04/12/2025.

Manual LGPD. Instituto de Registro de Títulos e Documentos e de Pessoas Jurídicas do Brasil. Disponível em: https://irtdpjbrasil.org.br/files/orientacoes-tecnicas/MANUAL-DA-LGPD-2-2.pdf. Acesso em 04/12/2025.

Manual Encarregados Governo do Estado de Goiás. Controladoria Geral do Estado. Disponível em: https://lgpd.go.gov.br/wp-content/uploads/sites/7/2023/04/Manual-dos-encarregados-pelo-tratamento-de-dados-pessoais.pdf. Acesso em: 04/12/2025

CNS – CONSELHO NACIONAL DE SAÚDE; Código de Boas Práticas: Proteção de Dados para Prestadores Privados de Saúde. Disponível em: https://cnsaude.org.br/wp-content/uploads/2021/03/Boas-Praticas-Protecao-Dados-Prestadores-Privados-CNSaude_ED_2021.pdf, 2021. Acesso em: 04/12/2025.

Hospital de Câncer de Pernambuco PORTARIA Nº 007 de 19 de setembro de 2024 - Comitê de Proteção de Dados e Privacidade – CPDP.

DECRETO Nº 49.265, DE 6 DE AGOSTO DE 2020. Política Estadual de Proteção de Dados Pessoais do Poder Executivo Estadual. Disponível em: https://legis.alepe.pe.gov.br/texto.aspx?id=51399. Acesso em: 04/12/2025

RESOLUÇÃO CD/ANPD Nº 4/2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-regulamento-de-dosimetria/Resolucaon4CDANPD24.02.2023.pdf. Acesso em: 04/12/2025.

Medidas de Privacidade e Segurança – ANPD. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-guia-de-seguranca-para-agentes-de-tratamento-de-pequeno-porte. Acesso em 04/12/2025.

Direito dos Titulares. Disponível em: https://www.gov.br/mec/pt-br/acesso-a-informacao/lgpd/direitos-titulares-dados. Acesso em 04/12/2025.

ABNT NBR ISO/IEC 27701:2019: Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes. Rio de Janeiro, 2019

NBRISO/IEC29134 DE 06/2024. Tecnologia da informação — Técnicas de segurança — Orientações para avaliação de impacto de privacidade.

16. Controle de versões

A tabela abaixo relaciona os campos necessários para o controle das atualizações, revisões e aprovações do manual de processo, a serem preenchidos sempre que julgado necessário

CONTROLE DE REVISÕES E ALTERAÇÕES				
Revisão	**Data**	**Responsável**	**Tipo de alteração**	**Revisor Aprovador**
1	25/11/2025	João Carlos C. Job	Elaboração	Superintendentes
2	04/12/2025	Kauane Silva	Padronização	Renata Galindo

ELABORADOR	João Carlos C. Job *João Job*		
REVISÃO	Controladoria *Danielle Cavalcanti* *Viviane Farias*		
APROVADOR (SUPERINTENDÊNCIA)	Josenildo Sá	*Felipe Nunes Bonifácio* Felipe Bonifácio	*Genes Cavalcanti* Genes Cavalcanti
	Luiz Caetano Jansen Perei Luiz Caetano Jansen	*Cláudia Maria de Souza Ba* Cláudia Barbosa	*Sidney Batista Neves* Sidney Neves
TEMPO DE VIGÊNCIA: 24 MESES			

Manual LGPDv3.pdf

Documento número #5aa6efdf-0b78-40e4-b7ac-0e1acd939d9c

Hash do documento original (SHA256): 7e602aeaf946ead8907afcd658179cc6774e89cc47c3f2ddad1f2326909df908

Assinaturas

Felipe Nunes Bonifácio
[redacted]
Assinou em 12 dez 2025 às 10:40:58

Felipe Nunes Bonifácio

Danielle Cavalcanti
[redacted]
Assinou em 11 dez 2025 às 14:13:40

Danielle Cavalcanti

João Carlos Castro Job
[redacted]
Assinou em 11 dez 2025 às 09:02:21

João Carlos Castro Job

Viviane Farias
[redacted]
Assinou em 11 dez 2025 às 14:19:09

Viviane Farias

Luiz Caetano Jansen Pereira da Silva
[redacted]
Assinou em 11 dez 2025 às 21:53:46

Luiz Caetano Jansen Pereira da Silva

Genes Cavalcanti
[redacted]
Assinou em 15 dez 2025 às 17:22:24

Genes Cavalcanti

Sidney Batista Neves
[redacted]
Assinou em 16 dez 2025 às 13:50:44

Sidney Batista Neves

André Meira de Vasconcellos
[redacted]
Assinou em 29 dez 2025 às 09:22:23

Josenildo Martins Sá
[redacted]
Assinou em 22 dez 2025 às 08:28:49


Josenildo Martins Sá

Isabela Coutinho
[redacted]
Assinou em 05 jan 2026 às 15:43:14

Luciana Venâncio
[redacted]
Assinou em 07 jan 2026 às 09:39:48

Anna Buarque
[redacted]
Assinou em 08 jan 2026 às 16:22:48

Cláudia Maria de Souza Barbosa
[redacted]
Assinou em 09 jan 2026 às 12:37:31


Cláudia Maria de Souza Barbosa

Log

[redacted]