

PROGRAMA DE GOVERNANÇA E PRIVACIDADE

ELABORADO: ASCOI/CODISE
VERSÃO 1.0



SUMÁRIO

Composição.....	3
Histórico de Versão.....	4
Lista de Abreviaturas e Siglas	5
Contextualização.....	5
Abrangências e Exceções.....	6
Categorias.....	7
Princípios.....	7
Titular dos dados	8
Tratamento de dados.....	9
Adequação à Lei Geral de Proteção de Dados	9
Ciclo de vida do tratamento de dados pessoais.....	9
Campanha de conscientização e publicidade	9
Dos direitos dos titulares dos dados.....	9
Cookies.....	10
Firewall.....	10
Backup.....	11
Gestão de Vulnerabilidades.....	12
Decreto Estadual nº 41.006/2021.....	12

Composição

Diretor-Presidente da CODISE

José Matos Lima Filho

Encarregado Setorial

Zarath Machado da Rocha – Coord. de Proteção e Tratamento de Dados e Informações – COPTDI

Comitê Executivo

Andréa Freire Resende – Coodenadoria de Licitações e Contratos – COLIC

Aristides Ferreira da Silva Neto – Coordenadoria de Transparência e Controladoria – COTCON

Eliema Cardoso Pires da Rosa – Coordenadoria de Auditoria Interna – COAUDIN

Etel Soares Mendes – Assessoria de Controle Interno – ASCOI

Flávio César Carvalho Menezes – Chefe Assessoria Jurídica - ASSEJ

Francisco Manuel Navarro Caldas – Coordenadoria de Tecnologia da Informação – COTIN

Gildo de Souza Xavier Neto – Diretor da Diretoria Administrativa Financeira – DAF

Marcos Nazareno Pacheco Bastos – Assessoria de Planejamento e Coodenação – APLAC

Histórico de Versões

Data	Versão	Descrição	Autoria
05/07/2022	1.0	Primeira versão do Programa de Privacidade da CODISE	ASCOI

Lista de Abreviaturas e Siglas

ANPD	Autoridade Nacional de Proteção de Dados
ASCOI	Assessoria de Controle Interno
CEPDP	Comitê Executivo da Política de Proteção de Dados Pessoais
CGPEPDP	Conselho de Governança da Política Estadual de Proteção de Dados Pessoais
COTIN	Coordenadoria de Tecnologia da Informação
LAI	Lei de Acesso à Informação - Lei nº 12.527/2011
LC	Lei Complementar
LGPD	Lei Geral de Proteção de Dados Pessoais - Lei nº 13.709/2018
PGP	Programa de Governança em Privacidade
PSI	Política de Segurança da Informação
RIPD	Relatório de Impacto de Proteção de Dados Pessoais
TIC	Tecnologia da Informação e Comunicação

Contextualização

O Programa de Governança de Privacidade (PGP) da CODISE tem como objetivo garantir a proteção de dados e a privacidade em todas as etapas de desenvolvimento de seus processos de trabalho, internos e externos.

Os dados pessoais são o princípio de qualquer operação nas organizações públicas e privadas. Nessas informações residem a ‘alma dos negócios’, que se materializa no relacionamento da organização com o cliente ou com o cidadão.

Quanto a isso, com a vigência da Lei Federal nº 13.709/2018 – Lei Geral de Proteção de Dados (LGPD), todas as áreas da iniciativa pública e privada precisam redobrar sua atenção no tratamento desse material, inclusive sua disponibilização em sítios eletrônicos.

A LGPD garante, por um lado, mais segurança aos titulares dos dados pessoais, por outro, obriga as organizações, dentre elas a CODISE, a aplicarem essa legislação no seu dia a dia.

Some-se a isso que, no âmbito do Poder Executivo Estadual, foi publicado o Decreto Estadual nº 41.006/2021, que instituiu a Política Estadual de Proteção de Dados Pessoais e que servirá de baliza para que a CODISE implante adequadamente as ações de proteção e tratamento de dados pessoais.

Abrangências e Exceções

Todas as organizações com atuação no Brasil devem seguir a Lei Geral de Proteção de Dados, sendo que estão sujeitas às regras os negócios em que: (I) a operação de tratamento seja realizada no território nacional; (II) a atividade de tratamento vise a oferta ou o fornecimento de bens ou serviços, bem como o tratamento de dados pessoais de indivíduos localizados no Brasil; ou (III) os dados pessoais, objeto do tratamento, tenham sido coletados no território nacional.

Cabe resaltar que a LGPD não se aplica ao tratamento de dados pessoais: (I) realizado por pessoa natural para fins exclusivamente particulares e não econômicos; (II) para fins exclusivamente jornalísticos, artísticos e acadêmicos; (III) para fins exclusivo de segurança pública e de Estado, defesa nacional ou atividades de investigação e repressão de infrações penais; ou (IV) provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que essa nação proporcione grau de proteção de dados pessoais adequado ao previsto na LGPD.

Principais pontos da LGPD

Categorias

Os dados relativos às pessoas naturais (também denominadas pessoas físicas) podem ser divididos em três segmentos:

Dados pessoais: são relacionados à pessoa natural, sendo identificados ou identificáveis, como: nome, endereço, documentos (RG, CPF, título de eleitor), foto, localização, e-mail e características pessoais.

Dados pessoais sensíveis: são aqueles relacionados à origem racial ou étnica; à convicção religiosa; à opinião política; à filiação a sindicato ou organização de caráter religioso, filosófico ou político; à saúde ou à vida sexual e à genética ou biometria, quando vinculados a uma pessoa natural.

Dados anonimizados: são dados que não possibilitam a identificação de seu titular. Neste caso, a LGPD não é aplicada, salvo quando a reversão do processo seja possível, por meios técnicos razoáveis.

Sobre menores de idade, a Lei Geral de Proteção de Dados (LGPD) também protege crianças e adolescentes na internet. Desta forma, é imprescindível obter o consentimento de um dos responsáveis pelo menor de idade e solicitar apenas os dados pessoais estritamente necessários para a atividade em questão, sendo ainda vetado o repasse desses dados a terceiros. Sem o consentimento, pode-se coletar apenas os dados para contato urgente com os responsáveis, garantindo-se a proteção da criança e do adolescente.

Princípios

A LGPD estabelece os seguintes princípios a serem considerados, além da prática da boa-fé, para as atividades de tratamento de dados pessoais:

Finalidade: ações firmadas em propósitos legítimos, específicos, explícitos e informados ao titular dos dados.

Adequação: compatibilidade do tratamento com as finalidades informadas.

Necessidade: limitação do tratamento ao mínimo necessário para suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos.

Livre acesso: consulta facilitada e gratuita, pelos titulares, sobre a forma e a duração do tratamento, além da integralidade dos **dados** pessoais.

Qualidade dos dados: garantia de exatidão, clareza, relevância e atualização dos dados.

Transparência: informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial, caso existentes.

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

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

Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.

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

Titular dos dados

Conforme disposto na LGPD, o titular dos dados é a pessoa natural a quem se refere os dados pessoais, objeto de tratamento. Como o próprio nome da lei já evidencia, os dados relacionados à pessoa jurídica não estão no escopo desta nova legislação brasileira.

Para garantir os direitos fundamentais de liberdade, intimidade e privacidade das pessoas físicas, a Lei Geral de Proteção de Dados prevê um conjunto de direitos aos titulares dos dados pessoais tratados:

- Confirmação da existência de tratamento de dados.
- Acesso aos dados pessoais.
- Correção de dados incompletos, inexatos ou desatualizados.
- Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a lei.
- Direito à portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, desde que sejam observados os segredos comercial e industrial – caso existentes.
- Eliminação de dados pessoais tratados com o consentimento do titular, exceto para o cumprimento de obrigação legal ou regulatória pelo controlador; estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados; transferência a terceiro, desde que sejam respeitados os requisitos de tratamento desta lei; ou uso exclusivo do controlador, vedado o acesso por terceiro, desde que os dados sejam anonimizados.
- Informação sobre os dados compartilhados com outras organizações.
- Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa.
- Revogação do consentimento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, retificando os tratamentos realizados sob amparo do consentimento manifestado anteriormente.

Tratamento de dados

São consideradas atividades de tratamento de dados todas aquelas que utilizem um dado pessoal em sua operação, como as ações de coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Adequação à Lei Geral de Proteção de Dados

Para cumprir a missão de proteger os dados de pessoas físicas, a LGPD impõe que as Organizações públicas e privadas realizem o tratamento de dados pessoais dos cidadãos. Com isso, torna-se imprescindível adaptar processos e procedimentos para garantir segurança e evitar multas e penalidades dispostas pela lei.

Neste cenário, em todas as áreas da CODISE, principalmente, na Jurídico, de Recursos Humanos, de Contratos e de Tecnologia da Informação, são mapeados os dados pessoais, identificando-se a aplicação da LGPD.

Ciclo de vida do tratamento de dados pessoais

Estratégico para o tratamento correto dos dados pessoais, o acompanhamento do seu ciclo de vida é primordial para a adoção de medidas adequadas. Por isso, é preciso entender os dados pessoais que são gerenciados, bem como os processos, projetos, serviços e ativos.

O ciclo de vida do tratamento de dados pessoais envolve as seguintes etapas:

Coleta - Momento de obtenção, recepção ou produção de dados pessoais independentemente do meio utilizado.

Processamento - Operação onde ocorre a classificação, utilização, reprodução, processamento, avaliação ou controle da informação, extração e modificação de dados pessoais.

Retenção - Fase em que ocorre o armazenamento de dados pessoais pela Organização, seja de forma física ou digital.

Compartilhamento - Etapa que reúne a transmissão, distribuição, comunicação, transferência, difusão ou compartilhamento de dados pessoais.

Eliminação - Fase destinada à exclusão ou eliminação dos dados.

Campanha de conscientização e publicidade

A instituição de uma campanha de conscientização e publicidade é uma ação que visa principalmente a mudança cultural quanto ao tratamento de dados pessoais, uma vez que a LGPD é transdisciplinar e deve ser cumprida no decorrer de todo o ciclo de vida do tratamento de dados

peçoais.

No mais, na própria LGPD (art. 50, I, “a”) se verifica que o PGP deve adotar processos e políticas internas que assegurem o cumprimento de normas e boas práticas relativas à proteção de dados pessoais, o que poderá ser incentivado por meio da campanha de conscientização e publicidade.

Quanto a isso, a CODISE já elaborou folder, banner, cartilha, manual de conduta, além de disponibilizar página na web (<https://codise.se.gov.br/lgpd/>) e e-mail, afim de promover a conscientização dos funcionários e demais envolvidos, sobre a importância e responsabilidade de todos no processo de tratamento de dados em conformidade com a LGPD.

A campanha é contínua, informando sobre a aplicabilidade de normas correlatas à LGPD, políticas relacionadas, consequências em decorrência de suas violações, bem como sobre os canais para sanar dúvidas e receber reclamações e denúncias.

Dos direitos dos titulares dos dados

Os direitos dos titulares em relação aos seus dados pessoais:

- a. Receber informações claras e completas sobre o tratamento de seus dados pessoais;
- b. Solicitar o acesso a seus dados pessoais e/ou a confirmação da existência de tratamento de dados pessoais pela CODISE;
- c. Solicitar que seja retificado quaisquer dados pessoais imprecisos, incompletos e desatualizados;
- d. Discordar das atividades de tratamento em circunstâncias específicas, solicitando a anonimização ou eliminação de dados pessoais;
- e. Solicitar a portabilidade de seus dados pessoais;
- f. Revogar o consentimento a qualquer momento, quando a CODISE, excepcionalmente, tratar seus dados pessoais com base no consentimento;
- g. Peticionar perante a Autoridade Nacional de Proteção de Dados.

Cookies

Os cookies são pequenos arquivos armazenados no computador, smartphone ou outro dispositivo de internet quando o usuário visita um determinado site. Eles geralmente são definidos apenas em resposta às ações feitas, por exemplo, para definir as preferências do usuário. Em relação a isso, **o site da CODISE não utiliza ou armazena nenhum tipo de cookie.**

Firewall

É a primeira linha de defesa que um sistema ou rede tem contra ataques ou intrusos de origem externa. Esta barreira pode ser implementada de duas formas: hardware ou software.

A CODISE utiliza o Firewall da Empresa Sergipana de Tecnologia da Informação – EMGETIS, estabelecendo os filtros e padrões de segurança no acesso a internet.

Backup

A CODISE possui uma política de backup e recuperação de dados, garantindo que cópias de segurança estejam disponíveis sempre que preciso. O procedimento de recuperação é testado com regularidade, garantindo a disponibilidade das informações.

A execução do Backup dos sistemas da CODISE é dividido entre a EMGETIS e a CODISE. Os Backups da EMGETIS são executados em fita e disco, e na CODISE apenas em disco.

Gestão de Vulnerabilidades

A gestão de vulnerabilidades objetiva a realização de monitoramento e aplicação de resolução/mitigação de eventuais falhas existentes em sistemas inseridos no contexto da CODISE, prevenindo a exploração de tais vulnerabilidades, identificando e aplicando soluções pontuais.

A CODISE reforça as ações de gestão de vulnerabilidades, analisando-as periodicamente, registrando e notificando os envolvidos, evitando a destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito de dados.

Decreto Estadual nº 41.006/2021

O Decreto Estadual n.º 41.006, de 5 de outubro de 2021, institui a Política Estadual de Proteção de Dados Pessoais do Poder Executivo Estadual, cria o Conselho de Governança da Política Estadual de Proteção de Dados Pessoais – CGPEPDP, nos termos da Lei (Federal) nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais – LGPD, altera o inciso I do art. 2º, o “caput” do art. 7º e o “caput” do art. 9º, do Decreto Estadual nº 40.370, de 30 de abril de 2019, que regulamenta o funcionamento da Ouvidoria Geral do Estado - OGE, e dá providências correlatas.

O Conselho de Governança da Política Estadual de Proteção de Dados Pessoais – CGPEPDD é composto por representantes dos seguintes órgãos: Procuradoria-Geral do Estado – PGE, Secretaria de Estado da Administração – SEAD, Secretaria de Estado da Transparência e Controle – SETC, Secretaria de Estado da Fazenda – SEFAZ e Secretaria de Estado Geral de Governo – SEGG.

Além disso, para cumprir o Decreto, a CODISE designará um Comitê Executivo da Política Estadual de Proteção de Dados Pessoais-CEPDP e o Encarregado Setorial.

O Encarregado Setorial deve aceitar reclamações e comunicações dos titulares de dados pessoais, orientar os servidores, funcionários e os contratados a respeito das práticas a serem tomadas em relação à proteção de dados pessoais, coordenar o Comitê Executivo da Política de Proteção de Dados Pessoais – CEPDP e atender às normas complementares da Autoridade Nacional de Proteção de Dados – ANPD.

Os Comitês Executivos da Política Estadual de Proteção de Dados Pessoais – CEPDP serão formados por equipe multidisciplinar, com no máximo 09 (nove) membros, devendo participar, preferencialmente, servidores das áreas de: comunicação, controle interno, financeira, gestão de

contratos, gestão de pessoal, jurídica, planejamento e tecnologia da informação.

A gestão da Política Estadual de Proteção de Dados Pessoais ocorrerá de maneira descentralizada, por meio do Encarregado Setorial e do Comitê Executivo de Proteção de Dados Pessoais– CEPDP, todos sob a coordenação técnica do Encarregado Central, que será do quadro de pessoal da Secretaria de Estado da Transparência e Controle-SETC.

Para mais informações, acesse:

<https://codise.se.gov.br/lgpd/>

Produção: ASCOI