TCESE
TRIBUNAL DE CONTAS DO ESTADO DE SERGIPE

/ tcese

CARTILHA DA

LEI GERAL DE PROTEÇÃO DE DADOS NO TCE/SE

tce.se.gov.br

O QUE É LGPD?

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, é uma norma federal de abrangência nacional que estabelece os direitos dos (as) titulares de dados pessoais, como a liberdade, privacidade e livre formação da personalidade.

A Lei fala sobre como os dados pessoais, dispostos em meio físico ou digital devem ser tratados pelas pessoas físicas ou jurídicas de direito público ou privado, garantindo conhecimento, controle e transparência na coleta, processamento, uso e compartilhamento de informações pessoais.

Isso faz valer um dos fundamentos da Lei que é a autodeterminação informativa, ou seja, o poder que cada cidadão tem sobre seus próprios dados, tanto daqueles armazenadas em bancos de dados digitais quanto dos disponíveis em meios físicos.

A LGPD NO TCE

Diante da entrada em vigor da Lei, o TCE-SE assumiu um compromisso com a proteção de dados pessoais, buscando adequar-se à LGPD e implementar as melhores práticas na proteção de dados e segurança das informações.

Esta Cartilha visa demonstrar os principais aspectos e a importância da adequação à LGPD, tendo em vista que o TCE-SE realiza constantemente a coleta, o uso e o compartilhamento de dados pessoais no exercício de suas atribuições, sendo também modelo aos jurisdicionados.

CONCEITOS BÁSICOS

Titular: é a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento, sendo que, como a existência da pessoa natural termina com a morte, só é tido como titular a pessoa viva.

Dados pessoais: são todas e quaisquer informações que identificam ou possam identificar uma pessoa natural, como: nome, CPF, endereço, e-mail, identidade, idade, telefone, número de matrícula, entre outros.

Dados pessoais sensíveis: são dados pessoais que receberam um cuidado especial pela Lei por poderem causar alguma discriminação ao titular se tratados indevidamente. São eles: origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização religiosa ou política, dado referente à saúde ou à vida sexual: dado genético ou biométrico.

Dados anonimizados: são aqueles relativos a um titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento. O dado perde o caráter pessoal associado a um indivíduo, não sendo possível que se descubra quem era a pessoa titular do dado. Um exemplo de dados anonimizados são os dados estatísticos.

Tratamento: operação realizada com dados pessoais como coleta, acesso, armazenamento, eliminação e transferência, entre outros.

Controlador: pessoa natural ou jurídica, de direito público ou privado que decide como, quando e porque tratar os dados pessoais.

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

Encarregado: pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados.

Autoridade Nacional de Proteção de Dados (ANPD): é a agência reguladora vinculada ao Ministério da Justiça responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

Banco de Dados: é um conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

PRINCÍPIOS DA LGPD

Finalidade: Os dados pessoais devem ser tratados para propósitos específicos e legítimos, explicitamente informados ao titular.

Adequação: Deve haver compatibilidade do tratamento com as finalidades informadas ao titular no momento da coleta, em conformidade com o contexto da relação estabelecida entre as partes.

Necessidade: Os tratamentos de dados pessoais devem contemplar somente os dados mínimos necessários para atingir o propósito informado ao titular.

Transparência e livre acesso: Os titulares devem ser informados sobre como e quando seus dados são tratados, garantindo-lhes o direito de acessá-los.
Não discriminação: Os dados pessoais não podem ser utilizados para discriminar ou prejudicar seus titulares.

Segurança e prevenção: Devem ser adotadas medidas técnicas e organizacionais para proteger as informações pessoais contra acessos não autorizados, perda, destruição, tratamento inadequado, de modo a evitar danos aos titulares, incluindo ações proativas para identificar e mitigar riscos.

Quantidade dos dados: Assegura, aos titulares, o direito de manter seus dados corretos, precisos, relevantes e atualizados.

Responsabilização e Prestação de Contas: Os agentes de tratamento devem garantir e prestar contas sobre a observância e o cumprimento das normas da LGPD.

HIPÓTESES LEGAIS DO TRATAMENTO DE DADOS PESSOAIS

Para a LGPD, o tratamento de dados pessoais abrange as seguintes atividades: coleta, retenção, processamento, compartilhamento e eliminação.

A norma estabelece algumas hipóteses para a coleta, o uso ou o compartilhamento de dados pessoais, quais sejam:

Cumprimento de obrigação leal ou regulatória – Permissão para uso de dados para o cumprimento de uma obrigação legal ou regulatória, ou seja, informações essenciais para atender determinada Lei.

Execução de políticas públicas – Permite que o poder público utilize informações pessoais para cumprir políticas previstas em Lei.

Realização de estudos por órgão de pesquisa – A utilização de dados por órgão de pesquisa, a exemplo do IBGE, também é permitida por Lei. Essas informações devem ser anônimas sempre que possível.

Execução ou criação de contrato – Criação ou execução de contrato permite a utilização dos dados pessoais.

Exercício regular de direitos – Outra utilização dos dados acontece para exercício regular do direito. Isso significa que se determinada pessoa ou empresa necessita dessas informações para conseguir direitos em um processo administrativo, arbitral ou judicial, o tratamento está liberado.

Proteção da vida –A Lei também deixa claro que os dados pessoais devem ser utilizados para proteção da vida. Isso pode acontecer, por exemplo, em algum acidente no qual é preciso ter acesso aos documentos do acidentado para comunicar familiares e chamar o resgate. Portanto, sempre que os dados pessoais forem utilizados para garantir a integridade física ou até mesmo a vida de uma pessoa, a Lei dá garantia desse uso.

Tutela de saúde – Essa base tem relação com os profissionais da área de saúde. Esse grupo tem liberação legal para utilizar os dados pessoais que são necessários para desempenhar suas funções. Tal necessidade pode acontecer ao passar um resultado de determinado exame para o paciente ou para saber quais pessoas fazem parte de um grupo foco de vacinação, por exemplo.

Legitimo interesse – Essa é uma das bases mais abrangentes, pois indica que, se houver o interesse legítimo do controlador dos dados, é possível usar essas informações para determinadas finalidades. Assim, a legalidade deve ser analisada caso a caso. Apesar de ser uma Lei mais genérica, ela aumenta as responsabilidades de quem controla os dados. Desse modo, é bom ressaltar que tal Lei não é uma base legal para tratamento de dados pessoais sensíveis. Portanto, os órgãos reguladores podem pedir, a qualquer momento, que a empresa explique porque e como está utilizando determinados dados.

Tutela de saúde – Essa base tem relação com os profissionais da área de saúde. Esse grupo tem liberação legal para utilizar os dados pessoais que são necessários para desempenhar suas funções. Tal necessidade pode acontecer ao passar um resultado de determinado exame para o paciente ou para saber quais pessoas fazem parte de um grupo foco de vacinação, por exemplo.

O QUE É POLÍTICA DE SEGURANÇA DE INFORMAÇÃO (PSI)

A PSI define regras e responsabilidades para proteção de dados, minimizando riscos, violação ou perdas de dados. É o compromisso da instituição em proteger as informações de sua propriedade ou guarda preservando a integridade.

O Decreto nº 41.006/2021 instituiu a Política Estadual de Proteção de dados pessoas, na administração pública no Estado de Sergipe.

O QUE É UM INCIDENTE DE SEGURANÇA DA INFORMAÇÃO (ISI)

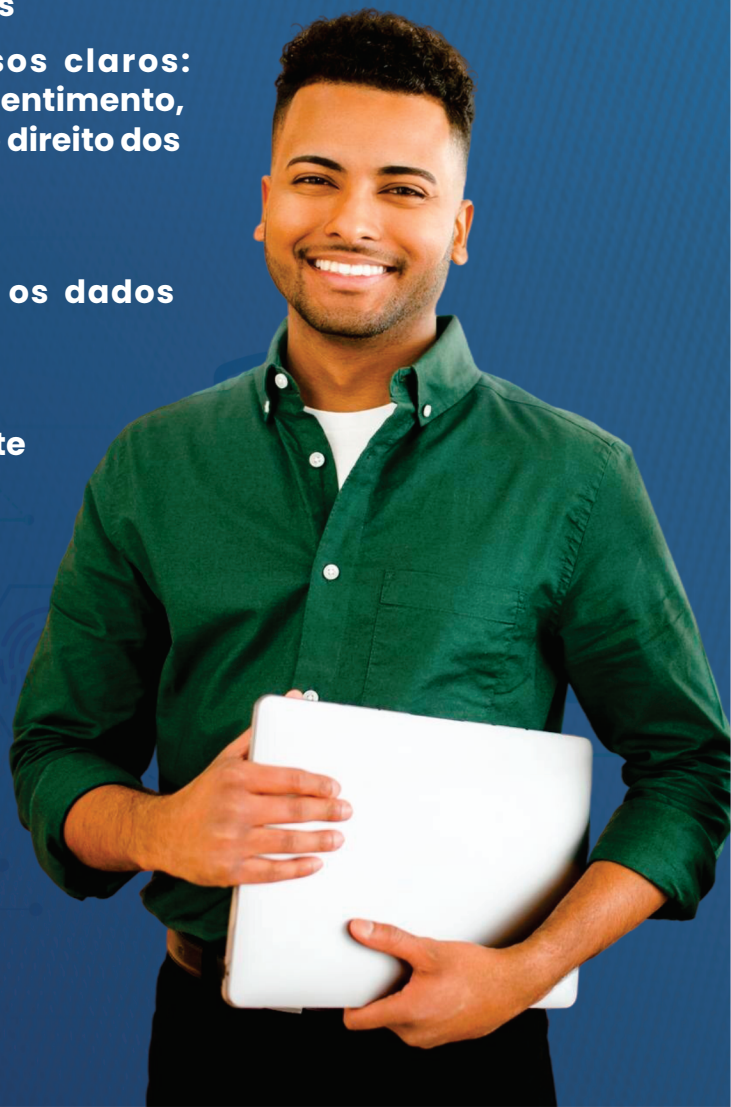
Um ISI é um evento, confirmado ou suspeito, que impacta a confidencialidade, integridade ou disponibilidade de informações ou sistemas. Pode ser um tratamento de dados inadequados ou ilícitos, violação intencional, um erro acidental, como também desrespeito à política de segurança que coloque em risco a segurança de dados e sistemas de uma organização.

LGPD E LEI DE ACESSO A INFORMAÇÃO (LAI)

A LGPD e a LAI são leis complementares que buscam garantir direitos fundamentais relacionados à informação em sentido amplo. Enquanto a LGPD foca na proteção dos dados pessoais e na privacidade dos indivíduos, a LAI visa promover a transparência e o acesso às informações públicas. Ambas são fundamentais e devem ser interpretadas de forma a harmonizar o direito de acesso à informação e à proteção de dados pessoais.

DICAS PARA SERVIDORES NO TRATAMENTO DE DADOS

1. Conheça a LGPD profundamente, familiarize-se com os artigos.
2. Mapeie e categorize os dados relativos ao seu setor de trabalho
3. Estabeleça bases legais para tratamento
4. Minimize e proteja os dados utilizados
5. Implemente políticas e processos claros: política de privacidade, gestão de consentimento, planos e respostas a incidentes, respeite o direito dos titulares dos dados.
6. Nomeie um encarregado de dados.
7. Monitore e audite regularmente os dados tratados.
8. Mantenha a transparência sempre
9. Atualize sua equipe continuadamente



TCESE
TRIBUNAL DE CONTAS DO ESTADO DE SERGIPE