Terracap
Agência de Desenvolvimento do Distrito Federal

Lei nº 13.709/2018
Decreto Distrital nº 42.036/2021
Resolução CD/ANPD nº 1/2021
Circular n.º 6/2021 – CGDF/OGDF
Decisão DIRET nº 234 de 04/05/2022
Decisão CONAD nº 009 de 20/06/2022

PLANO DE AÇÃO

PARA ADEQUAÇÃO DA TERRACAP À LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

SUMÁRIO

APRESENTAÇÃO

A utilização de dados pessoais pelas empresas públicas e privadas tem se tornado cada vez mais frequente, principalmente em decorrência da globalização da economia e do avanço tecnológico.

Nesse contexto, nos encontramos em um cenário de utilização de ferramentas virtuais em larga escala, as quais podem contribuir para a otimização de tempo e melhor uso de recursos, sem, contudo, descuidar das formalidades legais e dos direitos assegurados aos titulares de dados.

Diante desse cenário, com a entrada em vigor da Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n.º 13.709, de 14 de agosto de 2018, as empresas passaram a ter a necessidade de se adequarem. A referida Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, sendo que as normas gerais contidas na aludida Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios.

Logo, urge que os órgãos e entidades do Governo do Distrito Federal adotem providências para adequar-se a essa Lei. Nesse sentido, a direção da Terracap, por intermédio da Portaria nº 037/2021 - PRESI, criou o Grupo de Trabalho multissetorial(GT/LGPD) com o objetivo de iniciar os procedimentos para adequação da Terracap à LGPD.

Cabe destacar que a Terracap é considerada "Controlador", nos termos do art. 4º, do Decreto distrital nº 42.036, de 27 de abril de 2021.

Como um dos produtos desse esforço conjunto do GT/LGPD, surge o presente Plano de Ação para adequação da Agência de Desenvolvimento do Distrito Federal - Terracap, que foi submetido e aprovado pela Decisão DIRET nº 234/2022, propondo-se a atiar como instrumento orientador de conformidade da empresa à Lei Geral de Proteção de Dados Pessoais, juntamente com as diretrizes do Programa de Governança em Privacidade - PGP aprovado pelo CONAD pela Decisão nº 009/2022)

INTRODUÇÃO

A LGPD - Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) veio para dar mais privacidade, proteção e participação no tratamento de dados pessoais, garantindo aos titulares que seus dados sejam utilizados de forma transparente e segura. Ela foi publicada em agosto de 2018, entrando em vigor em setembro de 2020. As sanções administrativas impostas passaram a valer somente a partir de agosto de 2021. Em 2022 iniciou-se o ciclo de monitoramento da ANPD com as atividades a serem desenvolvidas como parte do processo de fiscalização, que compreende a orientação, prevenção e repressão.

Com o advento da LGPD, priorizar-se-á a mudança da forma como as empresas deverão cuidar dos dados pessoais coletados nas suas atividades, trazendo obrigações para si e direitos para o titular dos dados pessoais.

Em um contexto de um mundo globalizado onde frequentemente ocorrem vazamentos de dados de milhares de pessoas, a Terracap preocupa-se em proporcionar mais segurança, privacidade e proteção aos dados dos seus clientes, empregados e visitantes, buscando regulamentar internamente todo o tratamento de dados realizado e que, por isso, como parte de uma mudança de cultura de privacidade, esse assunto deve ser objeto de conhecimento amplo por todos.

Este Plano de Ação para adequação da Terracap à Lei Geral de Proteção de Dados Pessoais - LGPD, em consonância com a aludida Lei e as diretrizes do Programa de Governança em Privacidade - PGP, propõe ser um documento norteador da adequação da Lei no âmbito da Terracap, objetivando apontar os caminhos que deveremos trilhar para estarmos em conformidade com a nova legislação.

Tais orientações são fundamentais não só para garantir a correta aplicabilidade da lei, mas também para evitar a violação dos direitos do titular de dados em relação ao tratamento realizado pela Terracap.

Ao estruturar o planejamento desse trabalho, o GT/LGPD teve como parâmetro, além da própria LGPD, o Decreto distrital nº 42.036, de 27 de abril de 2021, o Manual da Lei Geral de Proteção de Dados (LGPD), da Subsecretaria de Inovação/Casa Civil do GDF, a Resolução CD/ANPD nº 1/2021, da Autoridade Nacional de Proteção de Dados, guias operacionais para adequação à LGPD da Secretaria de Governo Digital do Ministério da Economia (SGD-ME) e demais orientações da doutrina.

O referido Plano de Ação, assim como todas as ações de conformidade, será revisto e atualizado, sempre que necessário, para adequar-se às determinações da Terracap, da Autoridade Nacional de Proteção de Dados (ANPD) e dos órgãos de controle interno e externo, bem como para melhor esclarecer algum trecho específico, ou diante de eventuais atualizações legislativas ou de novos entendimentos sobre a matéria.

OBJETIVO GERAL

Nortear, em consonância com o Programa de Governança em Privacidade - PGP, a implementação de conformidade da Lei n.º 13.709/18 (Lei Geral de Proteção de Dados Pessoais – LGPD), no âmbito da Terracap.

OBJETIVOS ESPECÍFICOS

- Identificar as atividades prioritárias a serem desenvolvidas para o atendimento das disposições previstas na LGPD;
- Indicar as medidas necessárias para a adequação da Terracap à Lei Geral de Proteção de Dados Pessoais;
- Fixar parâmetros para assegurar a transparência, a segurança e o respeito aos direitos dos titulares de Dados Pessoais nos serviços prestados pela empresa;
- Fomentar a cultura de Privacidade e Proteção de Dados Pessoais junto aos empregados da Terracap; e
- Promover o engajamento interssetorial no atendimento aos marcos de conformidade atinentes à LGPD.

CONCEITOS

É imperioso neste momento destacar os principais conceitos trazidos pela Lei Geral de Proteção de Dados Pessoais, como: tratamento de dados, titular de dados, dado pessoal e dado pessoal sensível.

Tratamento de dados

É toda e qualquer operação realizada com dados pessoais, desde a coleta até o seu descarte. O art. 5º, inciso X, da Lei menciona expressamente outros exemplos: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Titular dos Dados

Toda pessoa física a quem um dado pessoal se referir.

Dado pessoal

Toda informação relacionada a uma pessoa física identificada ou identificável. Nessa categoria, podemos dizer que os dados pessoais podem ser diretos, como, por exemplo, RG, CPF, endereço, nascimento; ou indiretos, que são dados que possivelmente identifiquem pessoas, como, por exemplo, localização geográfica, perfil de consumo, comportamental, preferências, cookies, IP.

Dado pessoal sensível

É todo dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. Aos dados pessoais sensíveis a LGPD prevê tratamento restrito e especial.

PRINCÍPIOS

Os princípios dispostos na LGPD são a base para a adequação da nossa empresa. Ao atender aos princípios, nesse processo, garantiremos a observância às diretrizes aplicáveis às suas demais disposições. Nesse aspecto, além da boa-fé, vale lembrar outros dez princípios elencados no art. 6º da LGPD, os quais devem orientar o tratamento de dados pessoais:

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

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

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

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

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

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

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

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

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

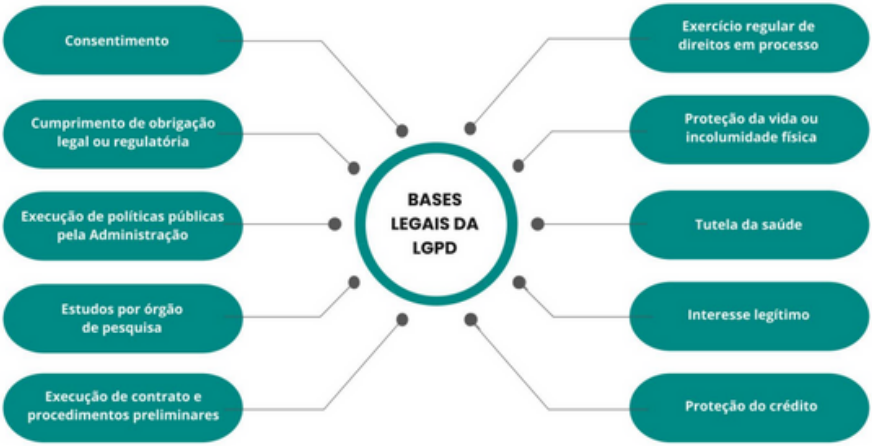
X - Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

HIPÓTESES DE TRATAMENTO DE DADOS PESSOAIS

A LGPD destaca que o tratamento de dados pessoais somente poderá ser realizado se estiver entre as dez hipóteses ou requisitos elencados no art. 7º da Lei, ou seja, a empresa só pode tratar dados pessoais se o tratamento estiver enquadrado em pelo menos um desses requisitos, que são chamados de bases legais. Seja qual for a base legal para o tratamento de dados, essa decisão deve ser registrada e documentada pelo Controlador e pelo Operador.

A regra geral é que as empresas só podem tratar dados pessoais se tiverem enquadradas em uma base legal, ou seja, com uma autorização que suporte esse tratamento. Para cada finalidade de tratamento é necessário indicar o requisito ou a hipótese legal adequada.

No artigo 7º da LGPD, encontramos as dez bases legais para atender esse requisito quando o tratamento realizado for de dados pessoais comuns.



HIPÓTESES DE TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS

A LGPD diferencia dado pessoal comum, do dado pessoal sensível, que é tratado com mais rigor pela lei e que, portanto, deve ser coletado e tratado de forma diferenciada.
O tratamento de dados pessoais sensíveis está disciplinado no artigo 11 da LGPD.

DIREITOS DOS TITULARES

Nos termos do art. 17 da Lei Geral de Proteção de Dados Pessoais, toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade.

A LGPD estabelece diversos direitos que o titular possui e pode exercer em relação aos agentes de tratamento a qualquer momento e mediante requerimento expresso que deverá ser atendido sem qualquer cobrança de custos para o titular.

Conforme o art. 18 da LGPD, ao titular estão garantidos os direitos de:

Direitos:

- Direito De Confirmação Do Tratamento
- Direito de Acesso
- Direito de Correção de Dados Incompletos, Inexatos ou Desatualizados
- Direito à Anonimização, Bloqueio ou Eliminação Dos Dados
- Direito à Portabilidade
- Direito à Eliminação dos Dados Tratados com Consentimento do Titular
- Direito à Informação do Compartilhamento dos Dados
- Direito à Possibilidade do Não Fornecimento do Consentimento
- Direito à Revogação Do Consentimento
- Direito de Petição
- Direito de Oposição

TRABALHOS JÁ REALIZADOS PELO GT/LGPD

1. A LGPD e demais Leis sobre proteção de dados

A proteção de dados pessoais configura-se da interpretação conjunta da Constituição Federal, do Código de Defesa do Consumidor (Lei nº 8.078/1990), da Lei de Acesso à Informação (Lei nº 12.527/2011), do Marco Civil da Internet (Lei nº 12.965/2014), da Lei do Cadastro Positivo (Lei nº 12.414/2011) e, agora, da LGPD – Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018).

Nesse sentido, o primeiro e mais evidente ponto de encontro entre essas leis é o direito à informação. Mesmo antes da LGPD, ao consumidor já era dado conhecer o que, afinal, era feito com seus dados, onde eram armazenados e com quem e para que finalidades eram compartilhados. A CF/88 estabeleceu, em seu art. 5º, a proteção ao direito da personalidade e, principalmente as garantias dadas pela liberdade de expressão e pelo direito à informação.

Nessa esteira, o Código de Defesa do Consumidor (CDC), visando proteger o consumidor da utilização abusiva de seus dados, marcou importante modernização do ordenamento civil brasileiro, suprindo muitas das lacunas deixadas pela ausência de um marco normativo específico sobre dados pessoais.

A Lei de Acesso à Informação – LAI (Lei nº 12.527/2011, no âmbito federal e a Lei 4.990/2012, no DF), que regulamentam o direito constitucional de acesso às informações públicas, também trouxeram importantes avanços no que tange à proteção de dados. A LAI ainda dispõe que o tratamento de informações pessoais deve ser feito de forma transparente, e qualquer transferência a terceiros apenas pode ser realizada caso estipulada por previsão legal ou com consentimento expresso do titular dos dados.

Posteriormente, veio o Marco Civil da Internet (Lei 12.965/14), que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil, sedo essencial para fornecer uma regulamentação básica às atividades online no Brasil.

A Lei do Cadastro Positivo veio estabelecer os requisitos para o tratamento de dados no âmbito da formação do histórico de crédito, prevê a inclusão automática de consumidores e amplia o acesso de instituições financeiras ao cadastro positivo de crédito.

Por seu turno, a LGPD – Lei Geral de Proteção de Dados Pessoais dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Assim, de forma harmoniosa, a LGPD também deverá ser interpretada e aplicada à luz dos princípios garantidos pela Constituição, tais como a dignidade da pessoa humana, a privacidade, o sigilo de dados e a proteção do consumidor, de maneira a dialogar com as demais fontes normativas do ordenamento jurídico brasileiro, principalmete as citadas acima, pois todas elas asseguram direitos relacionados à proteção de dados e à privacidade, no seu campo de aplicação.

TRABALHOS JÁ REALIZADOS PELO GT/LGPD

2. Mapeamento e tratamento dos dados pessoais no âmbito da Terracap

O mapeamento de dados, ou ainda, o data mapping ou inventário de dados, refere-se a um documento essencial quando estamos no processo de adequação às normas de proteção de dados.

O documento – ou planilha de mapeamento de dados - deve refletir o caminho percorrido pelo dado pessoal dentro da empresa, incluindo os processos e procedimentos pelos quais o dado transita. Ou seja, qual a origem, a hipótese ou base legal que respalda o tratamento deste dado pessoal, o nível de segurança da base de dados a qual o dado pertence, entre outras informações necessárias para a análise de risco e vulnerabilidades técnicas e jurídicas.

É o documento pelo qual a empresa terá o conhecimento de todos os dados pessoais tratados por ela por diversas unidades e o ciclo de vida desses dados, identificando tudo o que acontece com o dado, ou seja, a forma como são coletados, onde são armazenados, se são compartilhados, os sistemas e bancos de dados utilizados, o tempo de retenção e até a forma de descarte.

O GT/LGPD realizou entrevistas com os gestores das principais unidades de tratamento de dados identificadas na empresa e aplicação de questionário. De posse das informações coletadas, foi realizado diagnóstico preliminar do trabalho, todavia, ainda será necessário aprofundamento junto a todas as principais unidades da empresa.

Assim, foi possível realizar um diagnóstico sobre as principais unidades coletoras de dados pessoais(conforme abaixo), que deverão ser tratadas com prioridade, e os seus principais processos motivadores da coleta e tratamento de dados pessoais, sistemas e bancos de dados utilizados e que, em uma fase posterior, será necessário mapear individualmente por unidade e/ou processos, a fim de cumprir, desta forma, a exigência constante no art. 37 da LGPD, onde determina que o controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem.

GEATE **Atendimento ao Cliente**	**GECOP/NUCCA/CPLIC** **Gestão de Contratos e Licitações**
GEPES **Gestão de Pessoas**	**OUVID** **Ouvidoria**
GECOM/COPLI **Licitação Pública de Imóveis**	**GERAT/RECEPÇÃO** **Cadastro dos Visitantes**
GERAT/NUDOC **Gestã o de documentação e arquivo**	**GEVED/COVED** **Regularização de Imóveis - Venda Direta**
ASCOM **Comunicação**	**ASINF** **Segurança da Informação**

TRABALHOS JÁ REALIZADOS PELO GT/LGPD

3. Mapeamento dos riscos dos tratamentos de dados na Terracap (matriz de riscos)

Os riscos são todas aquelas operações ou atos praticados em nome da empresa, que de alguma forma violam ou possa ocasionar uma violação à LGPD. Em outras palavras, são pontos de atenção que podem gerar algum prejuízo para a empresa por estarem em desconformidade com a Lei.

O mapeamento dos riscos realizado serviu para verificar quais riscos a empresa corre em decorrência do tratamento de dados e quais as medidas deverão ser adotadas para eliminá-los. O mapeamento dos riscos realizado pelo GT/LGPD foi avaliado de acordo com a sua criticidade.

Assim, para cada risco identificado foi proposto um marco de conformidade ou uma ação para mitigar esses riscos. Ao final do mapeamento, foi elaborada a matriz preliminar de riscos onde estão relacionados os riscos identificados e que posteriormente foi submetida à análise da COINT/DIGER e aprovada da DIRET.

Para a identificação e análise preliminar de riscos relacionados à LGPD foi utilizada a Metodologia de Gestão de Riscos da Terracap, objetivando nortear o tratamento de dados pessoais em observância aos requisitos previstos pela Lei nº 13.709/2018. As etapas cumpridas para o mapeamento de riscos relativos à LGPD foram:

* **Identificação das causas de riscos**: causas de riscos relacionados à proteção e privacidade de dados pessoais, tendo como fonte as respostas do diagnóstico aplicado junto às áreas internas da Terracap e os roteiros para revisão do mapeamento de processos realizado sob o aspecto da LGPD.
* **Identificação de riscos:** a identificação de riscos foi baseada nas causas apontadas, apresentado os pontos de possível desconformidade com as consequências as quais a Terracap pode estar sujeita.
* **Análise de severidade:** realização da análise de probabilidade de ocorrência e impacto das consequências dos riscos identificados e classificação de acordo com a Metodologia de gestão de riscos utilizada pela Terracap.

Para a identificação dos riscos, o GT/LGPD realizou a análise de aderência das práticas da Terracap à LGPD, no que tange à coleta e tratamento de dados pessoais e, com o apoio da DIGER, listou os principais eventos de risco encontrados. Em seguida, foram feitas as avaliações de probabilidade e impacto de cada evento de risco levantado, com base na Política de Gestão de Riscos e na Gestão de Riscos aplicadas no âmbito da Terracap.
A partir daí esse trabalho será um importante instrumento para orientar as entregas a serem elaboradas junto às unidades, visando à mitigação dos riscos mapeados, que deverão ser detalhadas e implementadas pelos setores da Terracap responsáveis por cada temática envolvida, conforme este Plano de Ação para adequação da Terracap à Lei Geral de Proteção de Dados – LGPD.

TRABALHOS JÁ REALIZADOS PELO GT/LGPD

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

O Relatório de Impacto à Proteção de Dados Pessoais – RIPD é definido como a documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco (Art. 5º, XVII, da Lei 13.709/2018).

Poderá ser solicitado a qualquerm tempo pela Autoridade Nacional de Proteção de Dados (ANPD) ou quando houver infração da LGPD em decorrência do tratamento de dados pessoais por órgãos públicos, nos termos da combinação dos artigos 31 e 32 da referida Lei.

Para sua elaboração, foi utilizada a metodologia da Secretaria de Governo Digital do Ministério da Economia com as devidas adaptações à nossa realidade e demais orientações trazidas pelo manual de boas práticas, bem como pelo manual da LGPD, elaborado pela Subsecretaria de inovação do Distrito Federal, de acordo com as etapas abaixo:

Na primeira etapa, foi identificada a necessidade de elaboração do RIPD, nos termos dos Art. 5º, XVII; Art. 10º, II, §3º; Art. 32; Art. 38, pú, todos da Lei 13.709/2018 (LGPD).

Na segunda etapa, foram descritos os principais tipos de tratamento de dados realizados pela empresa, com detalhes sobre como as informações são utilizadas, incluindo o desenho do fluxo dos dados pessoais nos processos de negócio.

Na terceira etapa, foi realizada consulta por meio de questionários às principais unidades orgânicas da empresa responsáveis pelos processos de coleta de dados.

Na quarta etapa, foi avaliada a necessidade e proporcionalidade da coleta de dados, identificando quais as bases legais utilizadas para o tratamento de dados pessoais e a garantia da qualidade e limitação do tratamento ao mínimo necessário para a realização de suas finalidades, nos termos do art. 6º, III.

Na quinta etapa, foi tratada a identificação e avaliação dos riscos que geram impacto potencial sobre o titular dos dados pessoais, ocasionando uma avaliação do nível potencial de risco para cada evento.

Na sexta etapa, foram identificadas as medidas para tratar os riscos, nos termos do art. 5º, XVII da LGPD, que preconiza que o Relatório de Impacto deve descrever "medidas, salvaguardas e mecanismos de mitigação de risco", por meio de medidas de segurança, técnicas e administrativas, aptas a proteger os dados contra acessos não autorizados e de situações acidentais ou ilícitas de compartilhamento.

Por fim, a **sétima etapa** traz a formalização da aprovação do relatório com as assinaturas dos responsáveis pela direção da empresa.

TRABALHOS JÁ REALIZADOS PELO GT/LGPD

5. Programa de Governança em Privacidade de Dados

A LGPD preconiza que as atividades de tratamento de dados pessoais deverão observar as boas práticas e padrões de governança em Privacidade de dados e segurança da informação.

A criação de um programa de governança e boas práticas é um dos principais passos para a conformidade. É ele que dará um norte de como seguir com a adequação e manutenção das práticas de proteção de dados e facilitará a compreensão dos colaboradores.

Com a criação do programa, a Terracap poderá se planejar melhor e focar na implementação em cada um de seus setores da empresa, sabendo exatamente o que precisará ser modificado ou adaptado para cumprimento das exigências legais.

O Programa de Governança em Privacidade – PGP consiste na captura e consolidação dos requisitos de privacidade e segurança com o intuito de ditar e influenciar como os dados pessoais são manuseados no seu ciclo de vida como um todo.

As características mínimas estão no inciso I, § 2º, Art. 50 da LGPD:

1. Comprometimento do controlador em adotar processos e políticas internas que cumpram normas e boas práticas relativas à proteção de dados pessoais
2. Aplicável a todo o conjunto de dados pessoais sob seu controle, independentemente da forma coletada
3. Adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados
4. Estabelecimento de políticas e salvaguardas adequadas, baseadas em processo de avaliação sistemático de impactos e riscos à privacidade
5. Estabelecimento de relação de confiança com o titular, por meio de atuação transparente com mecanismos de participação do titular
6. Integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos
7. Com planos de resposta a incidentes e remediação
8. Constantemente atualizado com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas

MARCOS DE CONFORMIDADE COM A LGPD

(Plano de ação)

Após o diagnóstico realizado pelo GT/LGPD e posterior análise dos riscos pela COINT/DIGER, listamos abaixo as sugestões dos marcos de conformidade identificados, que deverão ser implementados após decisão da alta direção da empresa. O Plano de Ação elenca as atividades necessárias para que o órgão entre em conformidade com as exigências da LGPD. As ações apresentadas não encontram-se em ordem de prioridades, podendo ser executadas de acordo com as orientações do Comitê de Proteção e Privacidade de Dados Pessoais - CPRID, criado para o fim de monitorar o cumprimento dessas ações junto às unidades.

1. Política de retenção e descarte de dados pessoais

2. Política de privacidade (interna e externa)

3. Registro de atividades de tratamento de dados pessoais

4. Inventário de Dados Pessoais

5. Adequação de formulários de cadastro (físicos e digitais)

6. Inclusão de opção de opt-out em peças de publicidade enviadas aos clientes

7. Relatório de impacto à proteção de dados pessoais - RIPD

8. Implementação das Diretrizes de controle de acesso previstas na POSIC

9. Norma de procedimento de atendimento aos pedidos dos titulares

10. Norma sobre permissão de acesso aos processos administrativos

11. Monitoramento e controle das soluções de segurança da informação

12. Implementação de LOG'S de auditoria nas tabelas de dados críticos

13. termos de confidencialidade

14. Adequação dos contratos

15. Minutas padrão de contratos

16. Norma de anonimização de dados pessoais

17. Plano de respostas a incidentes de Segurança

18. Comitê de proteção e Privacidade de Dados - CPRID

19. Treinamentos internos sobre a LGPD

20. Comunicação interna para divulgação da LGPD

21. Nomeação de DPO (Encarregado setorial de dados)

22. Concepção de novos produtos (principio de privacy by design)

MARCOS DE CONFORMIDADE COM A LGPD

1. Política de retenção e descarte de dados pessoais

A Política de retenção e descarte de dados pessoais tem sua referência legal nos artigos 6º, II, III, IV; 9º, II; 15; 16; 37 e 40, da LGPD. Nela, deve constar a informação, dentre outros aspectos, sobre a forma de armazenamento e descarte dos dados após o alcance de sua finalidade, como o titular pode requerer a eliminação dos dados e qual a área responsável pelo descarte. A elaboração desse documento envolve conceitos de temporalidade e arquivísticos e deve ser publicado no Portal da empresa, de modo a cumprir o princípio da transparência e deve ser clara e conter procedimentos para assegurar que os dados serão eliminados na forma exigida pela LGPD.

Os principais pontos exigidos por essa política são:

- Indicar quais dados são cobertos pela política de retenção de dados;
- Definir os prazos para armazenamento dos dados;
- Detalhar os tipos de dados que precisam ser retidos por mais tempo que outros;
- Programar revisões regulares de dados armazenados para determinar se as informações ainda são necessárias;
- Certificar-se de que todos os funcionários estejam cientes dessa política;
- Garantir que seja explicado, no momento da coleta, por quanto tempo os dados ficarão retidos e da possibilidade de direito de revogação do consentimento;
- Garantir que os dados pessoais sensíveis sejam excluídos prontamente e não sejam armazenados por mais tempo do que o estritamente necessário;
- Cobrir os métodos que devem ser usados para excluir dados físicos e digitais;
- Documentar a política de retenção de dados. Pode ser necessário fornecer aos reguladores no caso de uma auditoria ou investigação de uma reclamação.

2. Política de privacidade (interna e externa)

A política de privacidade é um dos instrumentos de conformidade e faz parte da estrutura de documentos para a proteção de dados. Objetiva dar visibilidade ao tratamento de dados pessoais, atendendo aos princípios da Lei Geral de Proteção de Dados Pessoais (LGPD), visando também esclarecer quais informações são coletadas dos titulares e de que forma esses dados são utilizados. Dessa forma, a organização demonstra profissionalmente seu compromisso com a transparência no tratamento dos dados pessoais.

É importante destacar a diferença entre a política de privacidade interna e a externa. A política externa é um documento endereçado ao cliente externo e deve ser disponibilizado no Portal para fins de transparência. A política de privacidade interna é dirigida aos empregados e deve ser publicada na intranet da empresa. Nela, são estabelecidas as intenções e práticas no tratamento de dados pessoais.

A LGPD, em seu Art. 6, inciso VI, estabelece como um de seus princípios a transparência, que é a garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.

A Política de privacidade tem sua referência legal nos artigos 6º, VI; 9, I, II, III, IV, V, VI e VII, da LGPD.

Pontos que devem constar na Política de Privacidade de Dados Pessoais:

1. Identidade e detalhes de contato da organização, seu representante e seu encarregado (DPO);
2. Motivos pelos quais os dados pessoais dos titulares serão tratados;
3. Quais os dados que serão tratados;
4. Bases legais a serem utilizadas para o tratamento dos dados pessoais coletados;
5. Por quanto tempo os dados serão mantidos (prazos de retenção);
6. Informações acerca da transferência de dados para terceiros, incluindo o nome ou segmento dos terceiros e o motivo da transferência;
7. Informações acerca da transferência internacional de dados;
8. Informação sobre os direitos do titular dos dados (art. 18, LGPD);
9. Formas de contato para dúvidas relativas à Política de Privacidade;
10. Informações sobre os princípios da Lei, incidentes de segurança, etc.

3. Registro de atividades de tratamento de dados pessoais

O registro de atividades de tratamento de dados pessoais tem sua referência legal nos artigos 6º, II, III, IV; 9, II; 15; 16; 30; 37 e 40, da LGPD.
Manter esse registro atualizado também viabiliza a proteção dos dados pessoais, pois, para bem atender às exigências da LGPD é necessário que a empresa tenha pleno conhecimento do tratamento de dados que realiza.
Pelos termos do art. 37 da Lei Geral de Proteção de Dados/LGPD (lei 13.709/18) os agentes de tratamento de dados devem manter o registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.
Esse registro pode ser definido como a compilação estruturada dos tratamentos de dados pessoais realizados dentro da organização. Ou seja, é o documento que registra e organiza tais informações. A partir da vigência da LGPD, as organizações, privadas ou públicas, devem manter o registo de tratamento de dados pessoais, sob pena de serem responsabilizadas.
Portanto, muito mais do que o cumprimento de uma obrigação legal, o registro de operações irá ajudar na implementação dos controles necessários para atender aos princípios e demais obrigações impostas pela LGPD por proporcionar os seguintes benefícios:

- Identificação dos tipos de dados tratados pela organização;
- Conhecimento das bases legais que legitimam o tratamento dos dados pessoais;
- Facilita o atendimento das solicitações dos titulares, como a confirmação da existência do tratamento e o acesso aos dados;
- Saber onde os dados pessoais estão armazenados;
- Transparência sobre as medidas técnicas e administrativas adotadas para garantir a segurança e proteção dos dados pessoais.

O registro de operações de tratamento de dados pessoais pode ser realizado por meio do mapeamento dos dados pessoais a partir de entrevistas com os colaboradores da organização ou da descoberta de dados pessoais, pelo uso de soluções tecnológicas.

4. Inventário de Dados Pessoais

O Inventário de Dados Pessoais representa o documento primordial para registrar o tratamento de dados pessoais realizados pela empresa, em alinhamento ao previsto pelos 6, II, III, IV; 9, II; 15; 16 e, principalmente, o art. 37 da Lei Geral de Proteção de Dados Pessoais (LGPD).
Nesse sentido, o inventário consiste em uma excelente forma de fazer um balanço do que o órgão e entidade faz com os dados pessoais, identificando quais dados pessoais são tratados, onde estão e que operações são realizadas com eles.
De uma forma geral, esse registro mantido pelo inventário de dados envolve descrever informações em relação ao tratamento de dados pessoais realizado pelo órgão ou entidade como:

- atores envolvidos (agentes de tratamento e o encarregado);
- finalidade (o que a instituição faz com o dado pessoal);
- hipótese (arts. 7º e 11 da LGPD);
- previsão legal;
- dados pessoais tratados pela instituição;
- categoria dos titulares dos dados pessoais;
- tempo de retenção dos dados pessoais;
- instituições com as quais os dados pessoais são compartilhados;
- transferência internacional de dados (art. 33 LGPD); e
- medidas de segurança atualmente adotadas.

Vale destacar que o inventário de dados representa um documento importante de governança de dados pessoais e de subsídio para avaliação de impacto à proteção de dados pessoais, com vistas a verificar a conformidade da instituição no que se refere ao preconizado pela LGPD.

5. Adequação de formulários de cadastro (físicos e digitais)

O formulário (físico ou digital) é o meio pelo qual muitas empresas utilizam para coletar os dados de seus potenciais clientes. Com a LGPD, é preciso que essa coleta esteja de acordo com as exigências da Lei. Esse é um processo que, agora, é obrigatório. (Referência: Art. 6º V, 39, 42, 44 e 50).
O consentimento do titular não é obrigatório em todos os tratamentos de dados. Porém, nos formulários faz-se necessário um campo no qual a pessoa possa autorizar o uso de suas informações pessoais. O titular deve concordar em receber e-mails, e no campo deve ficar explícito que a inscrição pode ser cancelada a qualquer momento (opt-out). Em outros casos, caso a coleta dos dados não necessite do consentimento, por utilização de outra base legal, mesmo assim essa informação deve ser oferecida ao titular nos termos da LGPD, o que significa que a Terracap deve se adequar às normas estabelecidas e, por isso, necessita atualizar todos os seus formulários de cadastro que possibilitem a entrada de dados pessoais.

6. Inclusão de opção de opt-out em peças de publicidade enviadas aos clientes

O opt-out é a possibilidade de uma empresa oferecer o descadastramento no e-mail marketing, permitindo que seu público desautorize o envio de novos conteúdos e materiais a partir daquele momento, ou seja, é a possibilidade de os seus contatos se descadastrarem da sua lista de e-mails. Caso algum contato da sua base não tenha mais interesse em receber seus e-mails, ele poderá apenas solicitar que seja removido. Dessa forma, sua empresa precisa oferecer ferramentas para que ele faça o seu descadastro, caso queira.

Para melhor disciplinar esse trabalho, a empresa deverá elaborar um guia de orientação para que o setor de comunicação divulgue como deverá ser tratado o dado pessoal pela empresa. Além disso, deverá utilizar-se de boas práticas na utilização de OPT-OUT, como:

- Não envie e-mails para o contato que solicitou o opt-out;
- Deixe o link visível no Portal;
- Tenha listas separadas de usuários ativos de sua base com aqueles que optaram por não mais receber suas mensagens,
- Não compre base de e-mails,
- Mantenha sua base de dados revisada e atualizada;
- Informe ao titular o que a empresa faz com seus dados coletados, etc.

7. Relatório de impacto à proteção de dados pessoais - RIPD)

O Relatório de Impacto à Proteção de Dados Pessoais - RIPD é definido como a documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco (A principal referência legal está no Art. 5º, XVII, 10 §3º, 32 e 38 da Lei 13.709/2018).

Representa documento fundamental a fim de demonstrar que o controlador realizou uma avaliação dos riscos nas operações de tratamento de dados pessoais que são coletados, tratados, usados, compartilhados e quais medidas são adotadas para mitigação dos riscos que possam afetar as liberdades civis e direitos fundamentais dos titulares desses dados.

A Lei dispõe ainda que este relatório poderá ser solicitado pela Autoridade Nacional de Proteção de Dados (ANPD) quando houver infração da LGPD em decorrência dos dados pessoais por órgãos públicos, nos termos da combinação dos artigos 31 e 32 da referida Lei.

O artigo 38, da referida lei, aduz que a ANPD poderá determinar a qualquer momento ao controlador que elabore o RIPD, contendo, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a garantia da segurança das informações e a análise do controlador com relação as medidas, salvaguardas e mecanismos de mitigação de risco adotados.

Nesse sentido, torna-se necessário, tendo em conta a grande quantidade de dados pessoais coletados e tratados na empresa, que o RIPD seja elaborado e mantido atualizado periodicamente.

8. Implementação das Diretrizes de controle de acesso previstas na POSIC

A Política de Segurança da Informação na Terracap - POSIC, institucionalizado pela Norma de Segurança da Informação – TIS 03, estabelece critérios para operacionalizar a política de segurança da informação no âmbito da Terracap.
Nela, estão regulamentados os critérios de acesso aos sistemas corporativos e as regras de acesso a colaboradores externos à Terracap.
A Terracap possui um sistema de controles de acessos aos seus sistemas (GIA) com funcionalidades de concessão e revogação de acessos, e controle dos perfis dos sistemas. Todos os sistemas da Terracap estão interligados a esse sistema central, sendo ele o responsável pela gestão de acessos aos sistemas internos da Companhia.
A POSIC normatizou que cada gestor do sistema será o responsável pela gestão dos acessos aos respectivos sistemas, incluindo a concessão de novos acessos e a revogação de acessos de empregados. Atualmente, apesar da norma, a gestão de acessos ainda é feita totalmente pela ASINF.

9. Norma de procedimento de atendimento aos pedidos dos titulares.

Para garantir o exercício dos direitos dos titulares, a Ouvidoria Geral do Distrito Federal, por meio da Circular n.º 6/2021 - CGDF/OGDF, estabeleceu um Procedimento Operacional Padrão - POP, a ser realizado por todos os órgãos do GDF.
Esse procedimento orienta que as demandas que versem sobre assuntos ligados à Lei Geral de Proteção de Dados (LGPD) sejam registradas presencialmente nas Ouvidorias de cada órgão ou por intermédio do Sistema de Ouvidoria (OUV-DF) ou no Sistema Eletrônico de Informações ao Cidadão (e-SIC)
Está estabelecido também que as demandas deverão ser analisadas quanto à competência de tratamento por parte do órgão/entidade, sendo imprescindível a imediata correção de fluxo via sistema, conforme a necessidade. Após a admissão, ambos os tipos de demandas deverão ser incluídos em processo eletrônico SEI, com nível de acesso RESTRITO, e encaminhada ao Encarregado Setorial com vistas ao tratamento do mérito. O prazo de resposta é de 15 (quinze) dias, contados a partir da data de registro.
A Terracap deverá disciplinar internamente esse procedimento por meio de norma a ser aprovada pela direção da empresa.
Abaixo, temos o canal e o fluxo de atendimento aos direitos dos titulares criado pela Circular n.º 6/2021 - CGDF/OGDF, com um Procedimento Operacional Padrão. Basta acessar o canal http://www.lgpd.df.gov.br/index.html.

10. Norma sobre permissão de acesso aos processos administrativos

O acesso aos processos administrativos pelos interessados e/ou terceiros é disciplinado pela Instrução de Serviço SEI-GDF n.º 1/2018 - TERRACAP/PRESI e pela Norma Interna nº 1.5.2-A, sobre informações de acesso restrito.
Será necessária a atualização desses normativos já existentes adequando-os à LGPD, que deverá disciplinar os canais e a análise dos pedidos de acesso aos processos administrativos, em consonância com:

Lei nº 12.527/2011 – Lei Federal de Acesso à Informação;
Decreto regulamentador nº 7.724 de 16/05/2012;
Lei nº 4.990, de 12/12/2012 - Lei Distrital de Acesso à informação;
Decreto nº 34.276/2013 – Regulamenta a Lei distrital de acesso à informação;
Lei nº 4.896, de 31/07/2012, sobre o Sistema de Gestão de Ouvidorias SIGO-DF;
Lei Federal nº 13.460, de 26/06/2017, direitos do usuário dos serviços públicos;
Lei Geral de Proteção de Dados Pessoais - Lei nº 13.709/2018
Decreto Distrital nº 42.036 de 27 de abril de 2021.

11. Monitoramento e controle das soluções de segurança da informação

A Política de Segurança da Informação na Terracap - POSIC, institucionalizado pela Norma de Segurança da Informação – TIS 03, estabelece critérios para o monitoramento e controle das soluções de segurança da informação no âmbito da Terracap. Nela, estão regulamentados os critérios de acesso aos sistemas corporativos e as regras de acesso a colaboradores externos à Terracap.

O monitoramento de segurança da informação envolve atividades proativas que visam identificar riscos e vulnerabilidades de TI em estágios iniciais. É uma medida de extrema importância, visto que, o quanto antes as ações maliciosas são descobertas, maiores são as chances de diminuir os seus danos e a quantidade de dados sequestrados.

Atualmente a Terracap possui soluções gratuitas e pagas, que visam fornecer análises recorrentes sobre o ambiente da Companhia, apontando falhas e vulnerabilidades antes de serem notadas pelos usuários.

Nesse sentido, com a necessidade de adequação à LGPD, algumas iniciativas devem ser tomadas, visando aprimorar esse monitoramento: contratação de solução de análise de vulnerabilidade dos sistemas externos da empresa, contratação de uma análise cibernética da infraestrutura de TI da Terracap, contratação de um software de VPN com requisitos avançados de segurança, entre outras.

12. Implementação de LOG'S de auditoria nas tabelas de dados críticos

Os logs de auditoria fornecem um histórico das mudanças feitas em objetos no sistema. Na Terracap, os logs de auditoria permitem rastrear as ações executadas em um sistema de informação, oferecendo informações específicas sobre cada atividade executada em um software, como: data, usuário, ação, dados alterados, etc.

A maioria das tabelas críticas no Banco de Dados da Terracap já possui logs de auditoria, restando uma revalidação envolvendo a ASINF e as áreas negociais sobre quais informações críticas ainda não possuem essa funcionalidade.

13. termos de confidencialidade

Com o avanço da tecnologia e a facilidade de acesso às informações tornou-se comum ouvir notícias de vazamento de dados sigilosos ou restritos. Com a edição da Lei Geral de Proteção de Dados Pessoais (LGPD), a garantia dos direitos fundamentais de liberdade e de privacidade sobre os dados pessoais ganhou maior relevância no cenário das empresas.

E, para proteger as informações sigilosas ou restritas, o termo de confidencialidade da LGPD passou a ser o principal instrumento de preservação da integridade dos dados dos titulares.

O termo de confidencialidade configura o acordo de não divulgação e tem como objetivo manter o sigilo sobre as informações das partes envolvidas na relação jurídica. Por ser um documento de importância legal é, constantemente, empregado para afastar vazamento de informações ou de espionagem, e pode gerar aos envolvidos várias consequências no âmbito da responsabilidade civil, penal e administrativa.

Esse tipo de documento declara a obrigação de que haja sigilo em relação aos dados, ao uso deles e ao acesso a eles e o colaborador assume parte da responsabilidade pelo vazamento de dados ou por fragilizar um sistema, tornando-o passível de invasões.

Portanto, propomos que o termo de confidencialidade seja exigido de todos os empregados e terceirizados da empresa, bem como aos novos contratados.

A LGPD não determina expressamente sobre a exigência de assinatura de termo de confidencialidade entre os empregados e a empresa sendo, porém, salutar que a empresa desenvolva uma cultura de integridade e boas práticas por todos os empregados públicos que possuírem acesso a bases de dados pessoais com acesso restrito, sendo uma decisão da alta direção da empresa sobre a necessidade ou não da obrigatoriedade desse documento.

14. Adequação dos contratos

A LGPD traz a previsão sobre a necessidade da adequação dos contratos com terceiros realizados pela empresa, nos artigos 39, 42, 44 e 50 da Lei Geral de Proteção de Dados Pessoais (LGPD). Em seu artigo 42, ela afirma que a responsabilidade por qualquer dano ou violação referente ao tratamento de dados pessoais é de responsabilidade solidária entre o controlador e operador de dados pessoais. Ou seja, em qualquer contrato que haja o compartilhamento de dados pessoais, ambas as partes podem responder solidariamente por qualquer violação da LGPD.

Esta disposição legal faz com que seja essencial, no momento da elaboração dos contratos, a observação de cláusulas contratuais e demais disposições, delimitando as responsabilidades de cada pessoa jurídica contratante relativo ao tratamento de dados pessoais presente no fluxo de informações para execução daquele determinado processo.

Além da inclusão de cláusulas da LGPD nos contratos, essa adequação nos levará, também aos processos de compra realizados pela GECOP, aos editais licitatórios realizados pela CPLIC, passando pelos editas de licitação de imóveis e editais de Venda Direta, os quais, todos terão que se adequar aos princípios da LGPD, sendo necessário, também, que seja informado aos titulares de dados sobre o tratamento realizado.

Para isso, será necessária a realização de um levantamento completo dos contratos em vigor no contexto da empresa, separando por categoria, aqueles que contém os maiores riscos, os que dispõem do compartilhamento de um volume maior de dados pessoais, aqueles que tratam do compartilhamento de dados sensíveis, aqueles que são contratos de rotina, etc., objetivando a priorização baseada nos riscos apresentados.

Algumas cláusulas que tornam o contrato mais transparente são:

- Cláusula sobre como a empresa coleta os dados e quais dados são coletados;
- Cláusula apresentando os direitos dos titulares na LGPD e, no contexto do contrato, como estes direitos podem ser garantidos pelos titulares;
- Cláusula sobre a possibilidade da revogação do consentimento e sobre os resultados desta decisão no contexto do contrato;
- Cláusula sobre os procedimentos para a correção, bloqueio ou eliminação de dados (retificação);
- Cláusula sobre o procedimento para que o titular exerça seu direito de acesso aos dados coletados;
- Cláusulas que apresentem a estrutura de governança referente ao tratamento de dados, apresentando os atores e partes responsáveis (controlador, operador, encarregado, órgãos internos das empresas, diretoria, etc.)

15. Minutas padrão de contratos

A Lei Geral de Proteção de dados - LGPD impôs uma série de disposições acerca da manipulação dos dados, e na contratação de fornecedores é prudente a inclusão de disposições específicas a respeito da proteção de dados, por intermédio de cláusulas contratuais específicas, considerando a necessidade de uniformização dos procedimentos administrativos tendentes à adequação aos normativos da Lei.
Ao estabelecer um contrato, os controladores e operadores:

- declaram que cada um cumpre as normas de proteção de dados pessoais;
- protegem os dados pessoais dos clientes, funcionários, terceiros ou qualquer outro;
- garantem que ambas as partes entenderam claramente seu papel em relação aos dados pessoais que estão sendo tratados.

Sendo assim, existe a necessidade de criação de minutas padrão de contratos, tendo por base a necessidade de uniformização dos procedimentos administrativos em relação à LGPD.

16. Norma de anonimização de dados pessoais

A Lei Geral de Proteção de Dados Pessoais cita ainda que o dado anonimizado é aquele que, originariamente, era relativo a uma pessoa, mas que passou por etapas que garantiram a desvinculação dele a essa pessoa.
Se um dado for anonimizado, então a LGPD não se aplicará a ele. Vale frisar que um dado só é considerado efetivamente anonimizado se não permitir que, via meios técnicos e outros, se reconstrua o caminho para "descobrir" quem era a pessoa titular do dado - se de alguma forma a identificação ocorrer, então ele não é, de fato, um dado anonimizado e sim, apenas, um dado pseudonimizado e estará, então, sujeito à LGPD.
Na realização do mapeamento dos dados, a empresa irá analisar a necessidade de normatizar o processo de anonimização de dados pessoais no âmbito interno para garantir o perfeito cumprimento da Lei.

17. Plano de respostas a incidentes de segurança

O Plano de respostas a incidentes de segurança é o processo que descreve como uma organização deverá lidar com um incidente de segurança de TI, seja ele um ataque cibernético, uma violação de dados, a presença de um aplicativo malicioso (como um vírus), uma violação das políticas e padrões de segurança da empresa, dentre outros exemplos.
O objetivo é minimizar os danos que poderiam ser causados pelo incidente, reduzir o tempo de ação e os custos de recuperação. A Lei Geral de Proteção de dados – LGPD, em seu art. 48, informa que o controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.
Art. 48, § 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:

I - a descrição da natureza dos dados pessoais afetados;
II - as informações sobre os titulares envolvidos;
III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
IV - os riscos relacionados ao incidente;
V - os motivos da demora, no caso de a comunicação não ter sido imediata; e
VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

Considerando a posição das empresas brasileiras como alvo para ataques e violações de segurança, é importante que a Terracap, além de outras medidas preventivas, tenha definido um plano de ação que prepare a empresa para um eventual incidente de segurança de privacidade. Este plano de ação é o Plano de Respostas a Incidentes.

O Plano de Respostas a Incidentes deve conter:

- A definição de incidente para a empresa;
- Descrição dos procedimentos a serem executados quando um incidente ocorrer;
- As ferramentas, tecnologias e recursos a serem utilizados em caso de incidentes;
- Descrição dos colaboradores que fazem parte do processo e quais são suas responsabilidades e ações.

O Plano de Respostas a Incidentes consiste de um documento interno da empresa que deve ser amplamente conhecido por todos os funcionários e que dispõe sobre as medidas que devem ser tomadas no caso de um incidente de segurança em dados pessoais.
Vale destacar que na Política de Segurança da Informação na Terracap – POSIC já consta item intitulado "RESPOSTAS A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO", porém, devendo ser atualizado nos termos da LGPD.

18. Comitê de Proteção em Privacidade de Dados - CPRID

O comitê de proteção em privacidade de dados é um grupo multissetorial formado por representantes das Diretorias e da Presidência, que irá fomentar a cultura de proteção de dados dentro da empresa.
A formação de um comitê para deliberações sobre privacidade e proteção de dados pessoais é considerado um importante marco para alcançar a conformidade, considerando-se a transdisciplinaridade da LGPD. Dessa forma, a composição do comitê deve ser multissetorial.
Além disso, o comitê deverá ser responsável juntamente com o encarregado setorial pela implantação e monitoramento das ações de conformidade a serem executadas pelas unidades. Suas ações deverão ser guiadas pelas decisões aprovadas pela direção da empresa sobre o tema e principalmente no Programa de Governança e Privacidade - PGP.
A criação de um Comitê de Proteção em Privacidade de Dados Pessoais contitui uma boa prática e um importante instrumento facilitador da promoção de uma cultura de proteção aos dados pessoais dentro da empresa, no sentido de:

1. Gerenciar as atividades relativas ao tratamento de dados;
2. Fiscalizar os processos que envolvem tratamento de dados pessoais;
3. Acompanhar os indicadores e planos de ação do Programa de Governança em Privacidade;
4. Discutir e propor políticas sobre novas atividades de tratamento de dados pessoais, e conscientização de todos os envolvidos com tratamento de dados pessoais.

19. Treinamentos internos sobre a LGPD

Após a implantação de todos os instrumentos necessários à adequação, chega o momento de treinamento de todos os colaboradores, a fim de estabelecer uma cultura de proteção de dados pessoais no agente de tratamento.
Não basta que a empresa esteja em conformidade com a LGPD. É necessário também que todos os empregados, inclusive os terceirizados, estejam envolvidos no tratamento de dados pessoais, tomem conhecimento e sejam capacitados em LGPD. Isso pode ser feito por meio de um plano de capacitação, que contemple treinamentos internos que sensibilizem todos os empregados quanto a essa nova mudança de cultura e que envolva tanto a gestão de pessoas quanto a área de comunicação.

20. Comunicação interna para divulgação da LGPD

Apesar de parecer que os maiores efeitos da Lei estão atrelados às áreas de tecnologia ou jurídica, todos os departamentos sofrem algum tipo de impacto com a chegada da LGPD.
Sendo assim, como uma boa prática, o trabalho feito pela comunicação interna também precisa ser revisto em seus detalhes, a fim de manter a empresa adequada à Lei, cumprindo, assim, o princípio da transparência com a divulgação máxima de informações sobre as boas práticas a serem utilizadas pelos empregados.

21. Nomeação de DPO (Encarregado setorial de dados)

O Encarregado setorial de dados é a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD, conforme previsão expressa no art. 5º VIII.
Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.
§ 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.

ATRIBUIÇÕES:

• Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
• Receber comunicações da autoridade nacional e adotar providências;
• Orientar os funcionários e os contratados da entidade a respeito das práticas em relação à proteção de dados pessoais; e
• Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

22. Concepção de novos produtos (principio de privacy by design)

O privacy by design é uma metodologia que visa resguardar a privacidade do usuário, desde a concepção de um produto ou serviço que envolva o tratamento de dados pessoais.
Sua previsão está no artigo 46 da LGPD:
"Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.
§ 2º: "As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução".
Isso significa que quando a empresa for desenvolver um novo produto ou serviço, e eles envolverem a coleta e tratamento de dados pessoais, ela já deve pensar na privacidade e proteção de dados pessoais quando estiver desenvolvendo o projeto.
Nesse caso existe a necessidade, na concepção de novos produtos ou serviços, que a empresa realize controles internos para verificar a conformidade à LGPD nos seguintes casos:

- Na etapa de planejamento de novos projetos e iniciativas que possuem em seu escopo dados pessoais;
- Antes de realizar alterações significativas em processos que tratam dados pessoais que estejam em produção;
- Antes de realizar alterações sistêmicas significativas.

GT/LGPD - Portaria nº 037/2021 - PRESI

COMPOSIÇÃO

EMPREGADOS	MATRÍCULA	FUNÇÃO
LÍLIAN DE OLIVEIRA MILHOMEM	2077-0	Coordenadora
CECÍLIA MAGALHÃES CAMILO	2407-4	Suplente
PAULO SÉRGIO DIAS PEREIRA	1772-8	Membro
MARIA DO AMPARO GOMES VILELA	1658-6	Membro
RAFAEL SCOFIELD SARDENBERG	2785-5	Membro
RODRIGO TEIXEIRA DOS SANTOS	2388-4	Membro
NÚBIA DE SOUZA G F DE CASTRO	2731-6	Membro
RICARDO MIORIN GOMES	2763-4	Membro
DANIEL COSTA DE OLIVEIRA	2808-8	Membro
MARCELO LIBERATO SOUZA	2425-2	Membro
MARIA MERCEDES DE ALBUQUERQUE	2923-8	Membro
VIVIANE MELCHIOR DE SOUZA ANTERO	2831-2	Membro

REFERÊNCIAS BIBLIOGRÁFICAS

1. Lei nº 13.709, de 14 de agosto de 2018- Lei Geral de Proteção de Dados Pessoais – LGPD;

2. Governo Federal: Guias operacionais para adequação à LGPD: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias-operacionais-para-adequacao-a˜lei-geral-de-protecao-de-dados-pessoais-lgpd;

3. Governo Federal: Guia de Boas Práticas - Lei Geral de Proteção de Dados Pessoais (LGPD) https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guia-boas-praticas-lgpd;

4. Decreto Distrital nº 42.036, de 27 de abril de 2021;

5. Manual GDF da Lei Geral de Proteção de dados (LGPD) - http://lgpd.df.gov.br/Manual1.pdf;

6. Cartilha GDF - http://lgpd.df.gov.br/CartilhaGDF.pdf

7. LGPD - MANUAL DE IMPLEMENTAÇÃO, ED. REVISTA DOS TRIBUNAIS (THOMSON REUTERS), 2021 2ª. Edição – Viviane Maldonado

8. Proteção de Dados Pessoais - 3ª Edição 2021 - Patrícia Peck Pinheiro

9. RESOLUÇÃO CD/ANPD Nº 1, DE 28 DE OUTUBRO DE 2021 https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-1-de-28-de-outubro-de-2021-355817513

COMPOSIÇÃO DA DIRETORIA DA TERRACAP

IZIDIO SANTOS JÚNIOR
Presidente

HAMILTON LOURENÇO FILHO
Diretor Técnico

JÚLIO CESAR DE AZEVEDO REIS
Diretor de Comercialização

EDWARD JOHNSON GONÇALVES DE ABRANTES
Diretor de Administração e Finanças

KALINE GONZAGA COSTA
Diretora de Novos Negócios

LEONARDO HENRIQUE MUNDIM MORAES OLIVEIRA
Diretor de Regularização Social e Desenvolvimento Econômico

FERNANDO ASSIS BONTEMPO
Diretor Jurídico

Terracap
Agência de Desenvolvimento do Distrito Federal