Governança de dados aplicada

Módulo 3

Análise e Ciência de Dados

EV.G
Uma iniciativa ENAP

Fundação Escola Nacional de Administração Pública

Diretoria de Desenvolvimento Profissional

Conteudista/s
Priscilla Regina da Silva (Conteudista, 2021).

Enap, 2021
Fundação Escola Nacional de Administração Pública
Diretoria de Desenvolvimento Profissional
SAIS - Área 2-A - 70610-900 — Brasília, DF

Sumário

Módulo

3 Governança de dados aplicada

Unidade 1. A gestão de dados aplicada

Objetivo de Aprendizagem:
Aplicar as etapas para o *compliance* à Lei Geral de Proteção de Dados Pessoais.

1.1 Encarregado em ação

De acordo com artigo 5º da LGPD, considera-se encarregado, a 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.

Pode-se acrescentar ao rol de atribuições do encarregado, por determinação do controlador (inciso IV antes referido), o que é sugerido no Guia de Elaboração de Programa de Governança em Privacidade do Governo Federal:

1. **Apoiar** a definição de diretrizes de construção do inventário de dados pessoais relativos ao registro das operações de tratamento de dados pessoais determinados pelo artigo 37 da LGPD;
2. **Conduzir** ou aconselhar a elaboração do relatório de impacto à proteção de dados pessoais, de acordo com casos previstos pela LGPD em que tal documento é necessário;
3. **Conduzir** ou aconselhar a implementação de regras de boas práticas e de governança especificadas pelo artigo 50 da LGPD.

O encarregado pode ser responsável por cumprir o princípio da responsabilização e prestação de contas, previsto no art. 6º, inciso X, da LGPD, gerando evidências de conformidade, como relatórios de impacto à proteção de dados, geração de indicadores, registro das atividades de tratamento, atas de reunião do Comitê de Privacidade, dentre outras.

Com vistas a otimizar o processo de indicação de escolha do encarregado, no Poder Público, a Secretaria de Governo Digital do Ministério da Economia publicou, no dia 22 de outubro de 2020, a Instrução Normativa DEGDI nº 100, de 19 de outubro de 2020, definindo, entre outras questões, o perfil do encarregado que deve ser indicado pelos órgãos do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP. Compõem o SISP os órgãos da administração direta, autárquica e fundacional do Poder Executivo Federal.

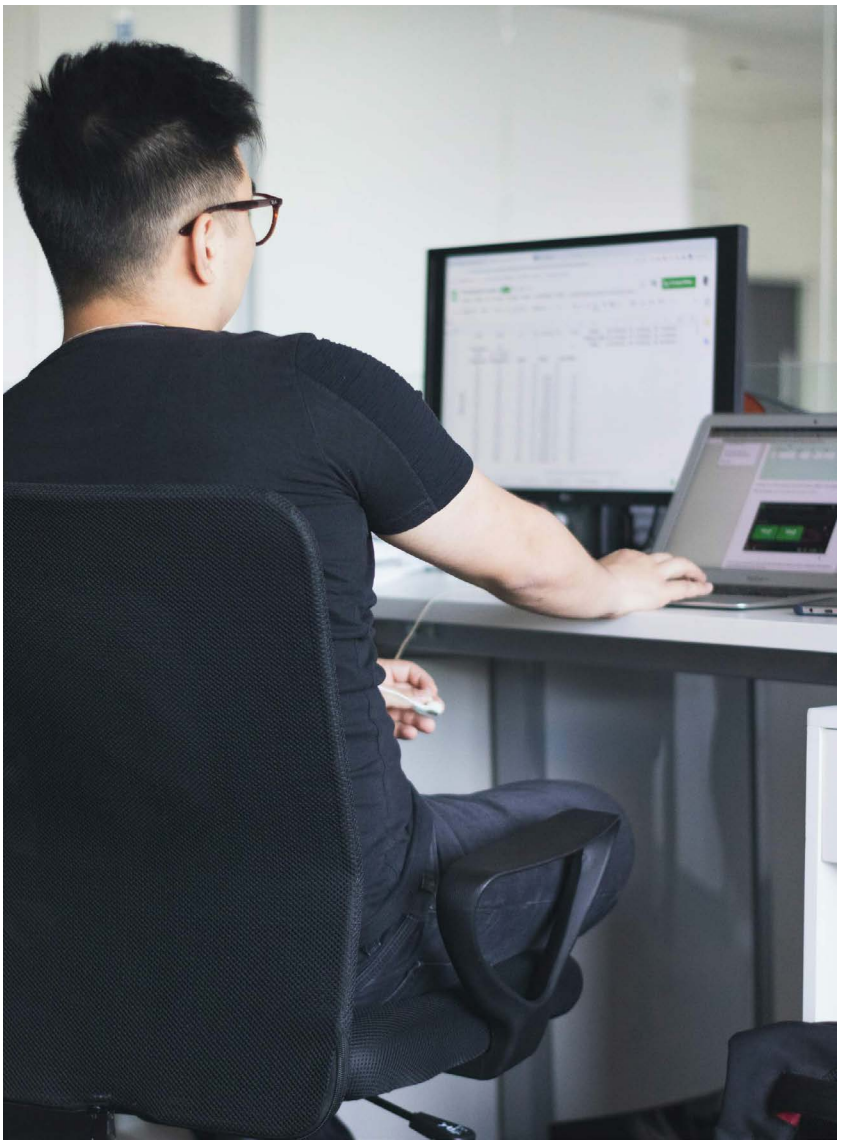
Segundo estabelecem os incisos do §1º do artigo 1º da referida Instrução, o encarregado deve possuir como requisitos mínimos: a) experiência na análise e elaboração de respostas de pedido(s) de acesso à informação pelo Serviço de Informação ao Cidadão e/ou Ouvidoria; b) conhecimentos multidisciplinares essenciais à sua atribuição, incluindo as áreas de gestão, segurança da informação, gestão de riscos, tecnologia da informação, proteção da privacidade e governança de dados; e c) conclusão dos cursos de Proteção de Dados no Setor Público e Governança de Dados ou equivalente, quando disponíveis na Escola Virtual de Governo.

Na esfera municipal, ressaltam-se as iniciativas elaboradas pelas prefeituras municipais de São Paulo e Porto Alegre, quanto à necessidade de conformidade com a legislação de proteção de dados. O município de São Paulo elaborou o Decreto nº 59.767, de 15 de setembro de 2020, regulamentando a LGPD no âmbito da administração direta e indireta municipal. Preconiza o art. 5 do referido decreto que o controlador-geral do município assumirá a posição de encarregado pelo tratamento de dados pessoais. Já, em Porto Alegre, instaurou-se um Comitê Gestor de Proteção de Dados, por meio do Decreto nº 20.777, de 28 de outubro de 2020, visando a definir e formular estratégias, diretrizes e procedimentos para adequação com a LGPD.

IMPORTANTE

O encarregado pode ser um colaborador da instituição ou um terceiro contratado, inclusive, uma empresa. No entanto, é importante evitar o conflito de interesses das atribuições do encarregado com outras funções que ele eventualmente exerça na instituição. Assim, o princípio da segregação de funções deve ser observado para evitar conflitos de interesses na designação do encarregado de dados, de forma que ele não acumule posições na instituição que o leve a determinar os propósitos e meios relacionados ao tratamento de dados pessoais.

Figura 10. Gestão de dados aplicada.



Fonte: Articulate Rise.

1.2 *Data mapping*

O mapeamento de dados, ou ainda, o *data mapping, data flow* ou inventário de dados é o primeiro passo para a adequação à LGPD.

Refere-se a apuração multisetorial de quais dados são coletados, o local onde estão armazenados e respectivo formato, políticas de acesso, justificativa para a respectiva coleta, usos dos dados, tempo de armazenamento, identificação quanto à transferência ou compartilhamento dos dados.

Um mapeamento de dados deve ser elaborado em conjunto pelos múltiplos setores da entidade. Alguns pontos essenciais devem estar contidos no mapeamento de dados:

Tipo de Dados	Classificar as categorias de dados trafegadas nesse fluxo (ex: se dados pessoais, dados pessoais sensíveis, anonimizados etc.).
Volume de Dados	O volume de dados trafegados nesse fluxo e a frequência desse tráfego (ex: online ou física, com frequência diária, semanal, mensal etc.).
Etapas do fluxo de dados	Descrição das etapas de tratamento do fluxo (ex.: coleta, armazenagem, processamento, transferências, descarte).
Tecnologias	Apontar no mapeamento de dados as principais tecnologias utilizadas nesse fluxo de dados (ex: sistemas, aplicações, bancos de dados que suportam o fluxo etc.).
Locais de Armazenamento	Indicar os locais onde o dado é coletado, armazenado, tratado ou processado. Nesse momento, deve-se indicar se é internamente ou externamente (ex: uso de nuvem para armazenamento de dados).
Origem dos Dados	Indicar as principais origens dos dados (entradas) e canais de captura de dados (ex: site, aplicativos, estabelecimentos físicos etc.).
Compartilhamento de dados com terceiros	Indicar as principais entidades com as quais os dados são compartilhados (ex: escritório de contabilidade terceirizado, emissor de NF-e etc.).
Localidades do tratamento	Indicar os países, estados e localidade onde sua empresa possui atividade.
Transferência Internacional de dados	• Plataformas de cloud (ex: amazon aws, microsoft azure, google cloud); • Data centers terceirizados; • Software terceirizados; • Transferência de dados pessoais para outros países.
Base legal	Indicar a base legal para realização do tratamento de dados referente ao fluxo descrito.
Dados de menores de idade	Identificar se no fluxo analisado há a coleta de dados pessoais de menores de idade (18 anos incompletos). Verificar se todos os registros possuem data de nascimento informada e válida.
Retenção e extinção de dados	Identificar a política de retenção e extinção (descarte) dos dados. Caso não existente, avaliar as boas práticas do setor da empresa e por categoria de dados.
Segurança da Informação	Identificar os principais controles de segurança da informação estabelecidos para proteger os dados coletados, armazenados, processados, compartilhados e transferidos.
Direito dos Titulares	Avaliar se o fluxo permite que o titular do dado pessoal tratado exerça seus direitos previstos nas normas de proteção de dados.

1.3 Documentos necessários

Checklist mínimo de elementos essenciais para um projeto de adequação com a LGPD:

- Montar Estrutura de Governança (ex: apontar DPO, definir time de adequação ou comitê de governança de privacidade e proteção de dados);
- Política de atendimento de direitos dos titulares;
- Política de privacidade e avisos de privacidade;
- Política de gerenciamento de fornecedores (política de due dilligence);
- Política de segurança de informação e plano de resposta à incidentes;
- Política de recursos humanos e contratos de trabalho;
- Modelos de cláusulas contratuais de proteção de dados (operador-controlador e controlador-operador);
- Registro de atividades de processamento de dados.

VÍDEO

Desafios do setor público para a adequação.
https://cdn.evg.gov.br/cursos/491_EVG/videos/modulo03_video01.mp4

Referências Bilbiográficas

BRASIL. Ministério da Economia. Secretaria Especial de Desburocratização, Gestão e Governo Digital. **Guias Operacionais para adequação à LGPD**. Disponível em: 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. Acesso em 27/03/2021.

Unidade 2: A realidade do processo

Objetivo de aprendizagem:
Analisar *cases* relacionados à LGPD.

2.1 Uma estrutura permanente

A **LGPD** é uma lei exponencial, pois, apesar de tratar especificamente sobre proteção de dados, é uma lei, em termos de conteúdo, abrangente e principiológica. Deste modo – e como visto até aqui -, complementações à lei são necessárias, desde regulamentos específicos editados pela Autoridade Nacional de Proteção de Dados, até elaboração de regras internas para a consolidação de uma boa governança de dados.

Assim, uma estrutura permanente conforme à LGPD deverá abranger constantes esforços de revisão e constante trabalho de adequação e readequação à lei. Justamente por isso a LGPD tem capítulo dedicado à governança de dados.

A governança de dados pode ser entendida como uma maneira de definir, aplicar e monitorar regras para o correto funcionamento dos dados e processos dentro e entre organizações, garantindo integridade, consistência, segurança e qualidade de dados e de processos. Algumas das possíveis estratégias seriam entender como os recursos municipais são divididos ou então adotar um padrão a partir de objetivos e serviços.

O primeiro passo é conhecer os dados disponíveis, então classificá-los e avaliá-los para identificar quais os tratamentos necessários para cada conjunto.

Assim, vejamos checklists para uma boa adequação:

GOVERNANÇA

- Mapeamento dos Dados Pessoais (*data mapping*).
- Identificação de finalidades de atividades de processamento de dados.
- Identificação de bases legais para as atividades de processamento.
- Inventário dos Dados Pessoais (registros das atividades de tratamento).
- Elaboração de relatório de análise das não conformidades (gap analysis).
- Plano de ação para a fase de implementação das medidas.
- Estrutura do time responsável pela Gestão do Programa de Governança em Privacidade e Proteção de Dados.

- Estruturação de processos internos para revisão de processos, produtos e serviços.
- Desenvolver modelos de Relatório de Impacto à Proteção de Dados.

CONTRATOS

- Desenvolver cláusulas padrão de proteção de dados área da empresa.
- Desenvolver Anexo de Proteção de Dados para regular relações: Controlador - Operador / Controlador - Controlador / Operador - Operados.
- Adaptar cláusulas padrão para diferentes tipos de contratos e áreas da organização.
- Revisar contratos firmados com fornecedores e prestadores de serviços da área.
- Desenvolver contrato para a transferência de dados intragrupo.
- Desenvolver instrumentos jurídicos para validar a transferência internacional de dados.
- Desenvolver documentos internos como termos de confidencialidade, contratos de trabalho que deem enfoque ao tema.

MELHORES PRÁTICAS

- Desenvolver Política de Relacionamento com a Autoridade Nacional de Proteção de Dados e outros entes reguladores.
- Desenvolver Política de Relacionamento Público e com mídia e outros atores interessados sobre ações envolvendo dados pessoais tomadas pela organização.
- Construir relacionamento com a Autoridade Nacional de Proteção de Dados e outras autoridades reguladoras.
- Construir relacionamento com outros stakeholders, públicos e privados, como sociedade civil, associações, universidades, think tank.
- Revisar e adaptar as práticas de desenvolvimento de negócios, em relação às negociações comerciais que envolvam o tratamento de dados pessoais.
- Desenvolver mecanismos internos para dar transparência aos colaboradores sobre a forma de tratamento dos seus dados pessoais.
- Desenvolver avisos de privacidade para promover a transparência sobre o uso de dados pessoais.

EDUCAÇÃO

- Desenvolver Política de Treinamentos e Comunicação sobre Privacidade e Proteção de Dados.
- Conduzir treinamentos de privacidade e proteção de dados, adaptados às diferentes áreas da entidade.
- Desenvolver estratégias de interação e comunicação com os fornecedores e prestadores de serviço para conscientizá-los sobre as práticas do órgão.
- Desenvolver portal com perguntas frequentes sobre Privacidade e Proteção de Dados (FAQ).
- Organização de *workshops* e treinamentos para equipes estratégicas.
- Criar de grupos de discussão internos de privacidade e proteção de dados.

2.2 *Cases* e Recomendações

Decretos Municipais de adequação à LGPD

- Município do Rio de Janeiro: Decreto Nº 49558 DE 06/10/2021 de adequação à LGPD
- Município de São Paulo: Decreto Municipal nº 59.767, de 16 de setembro de 2020 de adequação à LGPD

Webinários LGPD

- Introdução à Proteção de Dados e Administração Pública
- LAI e LGPD: encontros e desencontros
- LGPD e Direito Sancionatório
- Proteção de Dados e Administração Pública
- Lei Geral de Proteção de Dados: desafios para os municípios

Glossário

Anonimização:
Utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.
Autodeterminação informativa:
O direito que cada indivíduo tem de controlar e proteger seus dados pessoais.
Autoridade Nacional de Proteção de Dados (ANPD):
Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.
Interoperabilidade:
Característica que se refere à capacidade de diversos sistemas e organizações trabalharem em conjunto (interoperar) de modo a garantir que pessoas, organizações e sistemas computacionais interajam para trocar informações de maneira eficaz e eficiente.
Pseudonimização:
Tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.
Relatório de impacto à proteção de dados pessoais:
Documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

Referências Bilbiográficas

STJ - BIBLIOGRAFIAS SELECIONADAS - LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD): https://bdjur.stj.jus.br/jspui/bitstream/2011/162324/bibliografia_lgpd.pdf. Acesso em 27/03/2021.

CRAVO, Daniela Copetti; CUNDA, Daniela Zago; RAMOS, Rafael. **Lei Geral de Proteção de Dados e o Setor Público**, 2021. Disponível em: https://lproweb.procempa.com.br/pmpa/prefpoa/pgm/usu_doc/ebook_lgpd_e_poder_publico_23052021.pdf.

BRASIL. Ministério da Economia. Secretaria Especial de Desburocratização, Gestão e Governo Digital. **Guias Operacionais para adequação à LGPD**. Disponível em: 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. Acesso em 27/03/2021.