WORKSHOP

O Relatório de Impacto de Privacidade (DPIA) previsto na LGPD

Estado do Piauí

Assembleia Legislativa

RGM

AGENDA

- Apresentação
- O que é o DPIA
- Quando emitir o DPIA
- Como emitir o DPIA

Anderson Mattiuci

Design Think | Compliance |
Cobit | Scrum | LGPD | GDPR
Exin DPO certified

27+ years of experience, helping companies solve problems with the right tools

Contatos

Anderson Mattiuci

Anderson.mattiuci@rgm.com.br

Acadêmico

- **Processamento de Dados**
- **TGTI**
- **Especializações**

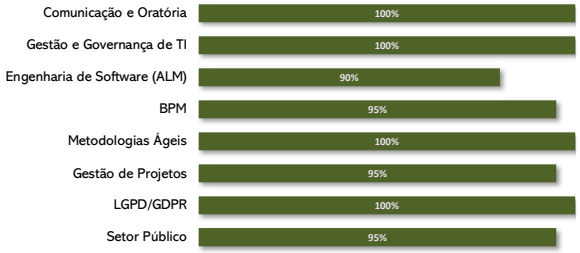
Certificações

Privacy & Security Management
Data Protection Officer (DPO)
Privacy and Data Protection Practitioner
Privacy and Data Protection Foundation
Information Security (ISO/IEC 27.001)

IT Governance and Service Management
ITIL V3 Fdn. Certified
COBIT 4.1 Fdn. Certified
SCRUM
Design Think
Compliance - FGV

Software Engineering
Certified Scrum Professional
Certified ScrumMaster
Kanban Foundation KIKF

Mapa de habilidades



Estado do Piauí

Assembleia Legislat

E VOCÊS SÃO...

RELATÓRIO DE IMPACTO DE PROTEÇÃO DE DADOS

O “DPIA” da LGPD

RGM

O QUE É O DPIA

Art. 5º (inciso XVII) 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. 38 Deve conter a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados .

- *Data Protection Impact Assessment* (DPIA)
- *Relatório de Impacto à Proteção de Dados* (RIPD)
- Deve ser emitido pelo DPO

MODELO PARA O DPIA

Uma sugestão para composição do relatório é detalhar todos os inventários relacionados à LGPD do Controlador e destacar a associação de suas entidades aos riscos levantados e às medidas administrativas e técnicas atualmente em uso que visam mitigar impactos à privacidade dos Titulares de Dados:

i. **identificação** do controlador, do DPO, e do estágio atual do SGPD;
ii. **inventário dos tratamentos de dados pessoais** realizados pelo controlador e seus detalhes como: bases legais/hipóteses, detalhamento sobre processos de consentimento envolvidos, classificação dos dados, indicação de processos de negócio e ativos de informação associados a cada tratamento de dados pessoais etc.;
iii. **detalhamento dos riscos conhecidos** associados ao tratamento de dados pessoais e estratégias de gestão desses riscos**;**
iv. **listagem das medidas administrativas e técnicas de segurança** atualmente em uso, associadas ao ativos de informação;

RGM

QUANDO DEVEMOS EMITIR O DPIA

De acordo com a LGPD e com as melhores práticas do mercado

RGM

QUANDO DEVEMOS EMITIR UM DPIA

Como está definido na LGPD

Sempre que o tratamento de dados *representar alto risco à garantia dos princípios gerais de privacidade dos Titulares de Dados:*

- Obrigação dos Controladores (LGPD, Art. 50, parágrafo 2º, inciso I, alínea d)
- Solicitação da ANPD para exceções à LGPD (LGPD, Art. 4º, parágrafo 3º)
- Solicitação da ANPD para justificar Legítimo Interesse (LGPD, Art. 10, parágrafo 3º)
- Solicitação da ANPD para agentes do Poder Público (LGPD, Art. 32)
- Solicitação da ANPD ao Controlador (LGPD, Art. 38)

Melhores práticas

Quando o DPO ou o Comitê de Governança, Privacidade e Segurança da informação detectarem um ou mais dos seguintes parâmetros:

- Grande volume de tratamento de dados
- Tratamento de Dados Sensíveis
- Tratamento de Dados de Crianças
- Uso do Legítimo Interesse do Controlador
- Tratamento de Dados Pessoais realizados de forma automatizada, sem verificação humana
- Riscos de privacidade detectados com criticidade URGENTE ou ALTA

RGM

PLANEJAMENTO PARA
EMISSÃO DO DPIA

Planejamento: Sugere-se que o DPO mantenha um histórico de emissão do DPIA para eventuais auditorias internas ou externas, e que emissão seja feita de forma cíclica e também pontual, de acordo com os seguintes critérios:

i. **DPIA de preparação:** após a conclusão da etapa de Preparação;
ii. **DPIA de adequação**: após a conclusão da etapa de Implementação;
iii. **DPIA pós-adequação:** A cada 6 (seis) meses após emissão do DPIA de adequação (emissão de 2 relatórios);
iv. **Período de maturidade:** 1 (uma) vez por ano) após a emissão do 4º relatório;
v. **DPIA pontual:** Sempre que o Controlador passar por mudanças que afetem o SGPD e, principalmente, atendam a algum critério das melhores práticas listadas anteriormente.
vi. **DPIA sob demanda:** Sempre que a ANPD ou um operador solicitar.

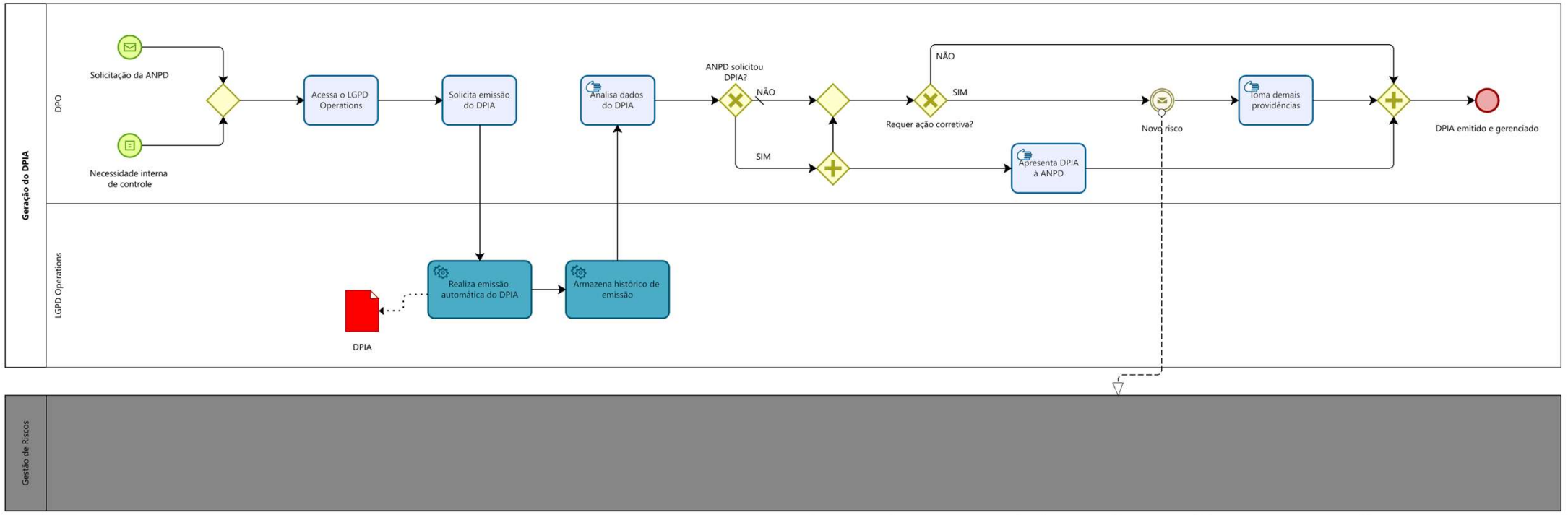
RGM

COMO EMITIR O RELATÓRIO DE IMPACTO DE PRIVACIDADE

Fazendo uso das ferramentas Omnisblue

RGM

PROCESSO SUGERIDO PARA
EMISSÃO DO DPIA



DEMONSTRAÇÃO PRÁTICA

RGM

DÚVIDAS?

Agradecemos a atenção de todos!!!

/anderson-mattiuci-3a659854/
+55 (11) 98078-2875
Anderson.mattiuci@omnisblue.com

RGM