RGM
TECNOLOGIA

Workshop LGPD

Gestão de Riscos, Incidentes e Notificações

Agenda

- **Riscos**
  - O que são riscos
  - Como gerenciar riscos
  - O relatório de análise de riscos e impactos da LGPD (DPIA)
- **Incidentes de segurança**
  - O que são incidentes de segurança e privacidade
  - Como gerenciar incidentes de segurança e privacidade
- **Notificações de incidente**
  - O que são as notificações previstas na LGPD
  - Qual o canal para envio de notificações à ANPD

RGM TECNOLOGIA

Adilson Taub Junior

CIO/CTO
DPO certified

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

Contatos

/in/ataubjr/

adilsontj@rgm.com.br

Acadêmico

Master of Business Administration (MBA)
Gestão Estratégica de Negócios

Formação Executiva
Compliance Empresarial (FGV)

Pós-graduação
Engenharia de Software

Graduação
Processamento de Dados

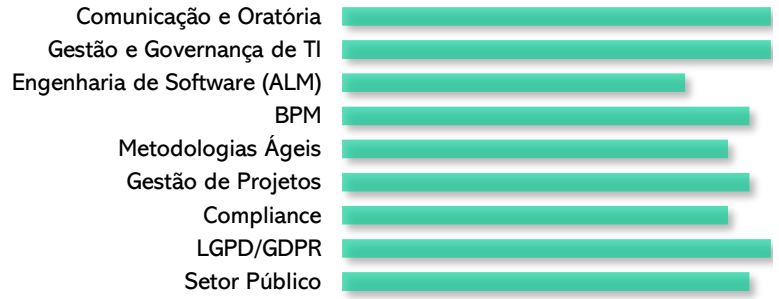
Certificações

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
IT Service Management (ISO/IEC 20.000)
ITIL V3 Fdn. Certified
COBIT 4.1 Fdn. Certified
ITIL V2 Fdn. Certified

Software Engineering
Professional Scrum Product Owner (PSPO I)
Professional Scrum Master (PSM I)
Certified Scrum Professional
Certified ScrumMaster
Kanban Foundation KIKF
IBM Certified Solution Designer (RUP)
Certified Expert in BPM

Mapa de habilidades



Riscos

O que é um Risco?

- Risco é toda a situação em que há probabilidade de os resultados serem diferentes do esperado devido a um ou outro motivo — já mapeados ou não —, de forma que se antecipa que algo pode ocorrer neste sentido. Isto nos dá a chance de evitar um dano ou consequência adversa. Resumindo, risco é uma probabilidade de uma ameaça explorar uma vulnerabilidade e causar um dano ou consequência
  - Riscos não são fatos ainda

RGM TECNOLOGIA

Como classificar um Risco?

- Um risco tem uma *Probabilidade* de ocorrer (percentual) e um *Impacto* previsto (baixo, médio ou alto). A combinação desses atributos mostra a *Criticidade* que devemos considerar ao tratá-lo. Uma sugestão é utilizar uma Matriz de Criticidade, como a seguir:

Probabilidade	Impacto: Baixo	Impacto: Médio	Impacto: Alto
100%	Alta	Urgente	Urgente
90%	Moderada	Urgente	Urgente
80%	Moderada	Alta	Urgente
70%	Moderada	Alta	Urgente
60%	Moderada	Alta	Alta
50%	Baixa	Alta	Alta
40%	Baixa	Moderada	Alta
30%	Baixa	Moderada	Moderada
20%	Baixa	Baixa	Moderada
10%	Baixa	Baixa	Moderada

Como gerenciar um Risco?

- Gerenciar riscos visa **diminuir a possibilidade do risco se tornar um fato** e, consequentemente, gerar os impactos esperados (ou não mapeados).

- Previsão na LGPD:
  - Os controladores e operadores poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os **mecanismos internos de supervisão e de mitigação de riscos** e outros aspectos relacionados ao tratamento de dados pessoais (LGPD, Art. 50)
  - O DPIA deve conter, entre outras coisas, os mecanismos de mitigação de risco utilizados pelo Controlador (LGPD, Art. 5º, inciso XVII)

RGM TECNOLOGIA

Estratégias de gestão de riscos

- Deve-se definir uma Estratégia para tratar cada risco. Os tipos possíveis de Estratégia para gestão de um risco são:
  - **Evitar**: O Controlador tomará medidas para impedir que o risco se torne um fato e gere um incidente
  - **Mitigar**: O Controlador tomará medidas para diminuir a probabilidade do risco ser disparado
  - **Compartilhar/Transferir**: O Controlador dividirá a responsabilidade de gestão do risco com um terceiro
  - **Aceitar**: O Controlador não tem como tomar medidas preventivas contra o risco e vai aceita-lo como ele é

RGM TECNOLOGIA

Exemplo de Risco

- **Risco**: "*Podemos ter perda de dados no sistema de Gestão Tributária por não termos backups atualizados. Se houver um problema do disco rígido do banco de dados, não haverá como garantir a recuperação das informações de arrecadação do IPTU do último mês.*"
- **Descrição do impacto**: "*Tornar o Portal da Transparência desatualizado e gerar problemas contábeis associados aos valores de receitas orçamentárias, dificultando a prestação de contas ao TCE.*"
- **Probabilidade**: 60% | **Impacto**: Alto | **Criticidade**: Alta
- **Tipo de estratégia**: Mitigar
- **Descrição da estratégia**: Atualizar o processo de *backup* do servidor XPTO, incluindo backup incremental diário em ambiente externo na nuvem. Realizar atividades quinzenais de teste de *restore* do servidor.
- **Responsável por gerenciar o risco**: João da Silva
- **Status**: Detectado [*Disparado, Encerrado, Cancelado*]
- **Data de cadastro:** 10/04/2022

RGM TECNOLOGIA

Relatório de impacto

Relatório de impacto de proteção de dados

- O Relatório de Impacto de Proteção de Dados, também conhecido como **Data Protection Impact Assessment** (DPIA), é um documento definido na LGPD que demonstra que o Controlador gerencia riscos de privacidade:
  - *"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."* (LGPD, Art. 5º, inciso XVII)
  - Deve ser emitido/gerenciado pelo DPO
  - Será a primeira evidência a ser analisada pela ANPD
  - 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.*" (LGPD, Art. 38, parágrafo único)

RGM TECNOLOGIA

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 TECNOLOGIA

Quando emitir o DPIA

De acordo com a 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 para o DPO

- Sempre quando houver:
  - Grande volume de tratamento de dados
  - Tratamento de Dados Sensíveis
  - Tratamento de Dados de Crianças e Adolescentes
  - Tratamento de Dados por Legítimo Interesse do Controlador
  - Compartilhamento de Dados Pessoais com terceiros
  - Tratamento de Dados Pessoais realizados de forma automatizada, sem verificação humana
  - Riscos de privacidade detectados com criticidade URGENTE ou ALTA

RGM TECNOLOGIA

Etapas da gestão de riscos na LGPD

Analisar website corporativo

- Verificar se o website realiza adequadamente o tratamento de cookies
- Verificar a publicação da Política de Privacidade
- Verificar a publicização do DPO e do canal para atender Titulares de Dados

Elencar riscos

- Inventariar riscos de acordo com a situação atual
- Classificar o grau de impacto e a probabilidade de ocorrência de incidente
- Associar processos, ativos e tratamento de dados aos riscos
- Definir responsáveis e estratégias para cada risco

Emitir o primeiro DPIA

- Emitir o primeiro DPIA da empresa
- O documento será guardado como baseline do projeto e contará com as informações pré-adequação

Criar o Plano de Ação

- Definir todas as alterações operacionais, jurídicas e tecnológicas que a organização deverá implementar para completar sua adequação
- *Envolvimento dos times jurídico e TI*

RGM TECNOLOGIA

Incidentes

O que é um Incidente?

- Sempre que houver uma ocorrência (fato), ilícita ou acidental, proveniente ou não de um risco previamente detectado, que gere *destruição*, *perda*, *alteração*, *comunicação* ou qualquer forma de *tratamento inadequado ou ilícito* sobre informações, temos um *incidente de segurança*
- Quando as informações associadas ao incidente são Dados Pessoais, temos um *incidente de privacidade*

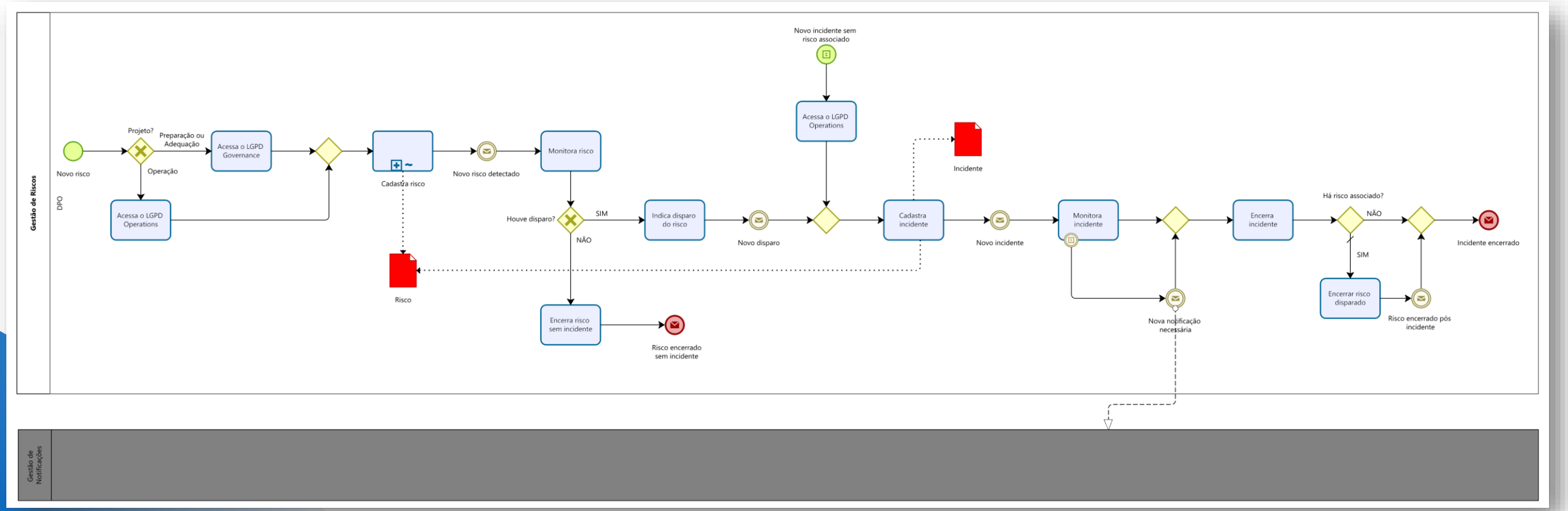
RGM TECNOLOGIA

Como tratar um Incidente?

- A melhor maneira de se evitar incidentes de privacidade é executar uma boa Gestão de Riscos, aliada à implementação de mecanismos de segurança que implementem os conceitos de *privacy by default* e *privacy by design*
  - **Privacy by design**: garanta que tudo o que a organização faz, ela pensa na privacidade desde o início
  - **Privacy by default**: não exija nenhuma ação do seu titular de dados para que a privacidade de seu produto ou serviço seja "ativada"
- É responsabilidade do Controlador evitar e gerenciar incidentes de privacidade
  - Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término (LGPD, Art. 47)
  - Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares (LGPD, Art. 49)

RGM TECNOLOGIA

Processo para gestão de riscos e incidentes



Notificações

O que é uma Notificação?

- Um incidente de privacidade deve ser comunicado à ANPD
  - 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. A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional (LGPD, Art. 48)
- Cabe ao Controlador e sua análise de impacto (inclusive o DPIA), analisar se o incidente pode acarretar risco ou dano relevante aos titulares. Essa análise ainda não foi regulamentada, mas podemos considerar os seguintes parâmetros para essa classificação
  - Volume da Dados Pessoais, Volume de Titulares de Dados associados e características dos Dados Pessoais (Dados Sensíveis, por exemplo)
- Canal oficial previsto pela ANPD
  - A ANPD definiu em maio/23 que o canal para enviar notificações ao órgão é o SUPER.BR, e inclusive providenciou um formulário padrão para a criação do artefato (https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis)

RGM TECNOLOGIA

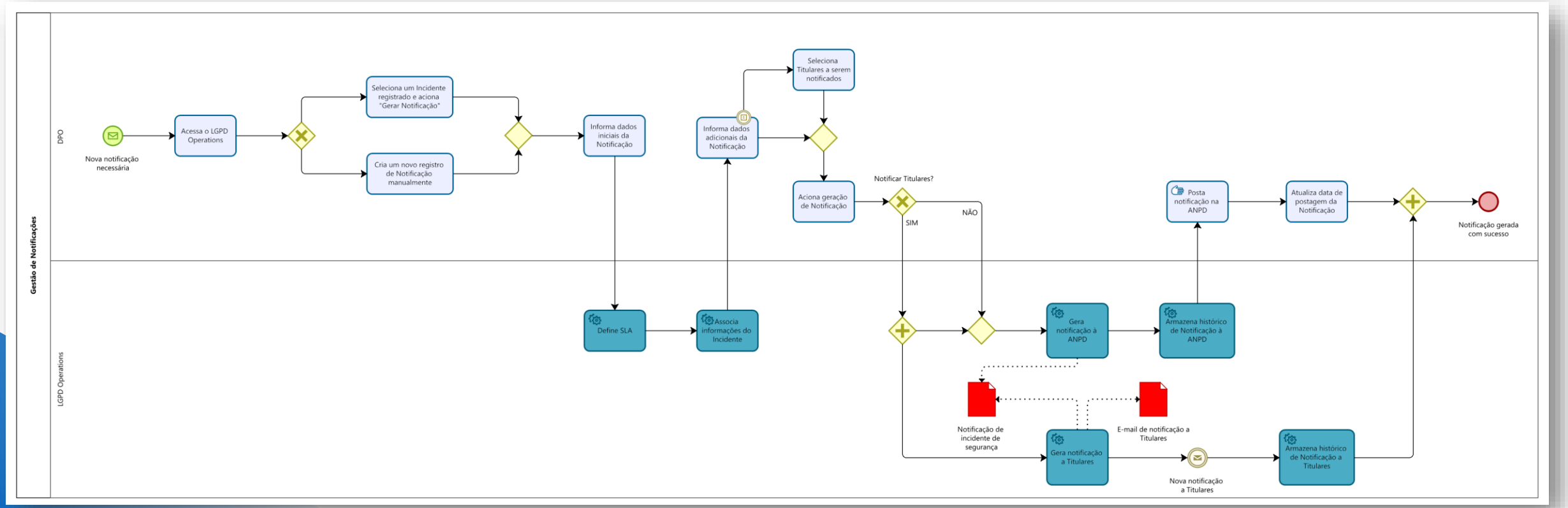
Parâmetros de uma Notificação

- Ao notificar a ANPD quando da ocorrência de um incidente que possa acarretar risco ou dano relevante aos Titulares, devem ser informado o seguinte:
  - A descrição da natureza dos dados pessoais afetados
  - As informações sobre os titulares envolvidos
  - A indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial
  - Os riscos relacionados ao incidente
  - Os motivos da demora, no caso de a comunicação não ter sido imediata
  - As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo

(LGPD, Art. 48)

RGM TECNOLOGIA

Processo para emissão de notificação



RGM TECNOLOGIA

Obrigado!

Adilson Taub Jr.

https://www.linkedin.com/in/ataubjr/

RGM Tecnologia

www.rgm.com.br

SCAN ME