WORKSHOP

Gestão de Riscos, Incidentes e Notificações como definido na LGPD

Estado do Piauí

Assembleia Legislativa

RGM

AGENDA

- Apresentação
- Riscos e como trata-los
- Incidentes e Notificações da LGPD
- Como gerar as Notificações da LGPD

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**

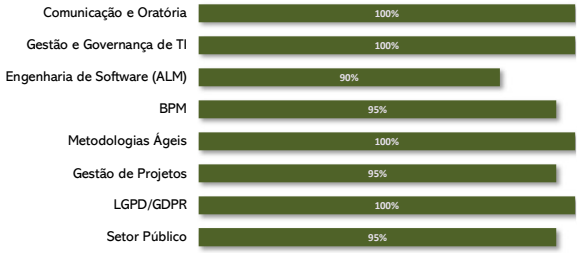
Certificações

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...

GERENCIAMENTO DE RISCOS DE PRIVACIDADE

E como isso afeta a adequação à LGPD

RGM

O QUE SÃO RISCOS

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.

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:

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

RGM

COMO GERENCIAR RISCOS

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)

- **Estratégias para gestão de riscos:**
  - ✓ **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

EXEMPLO DE RISCO

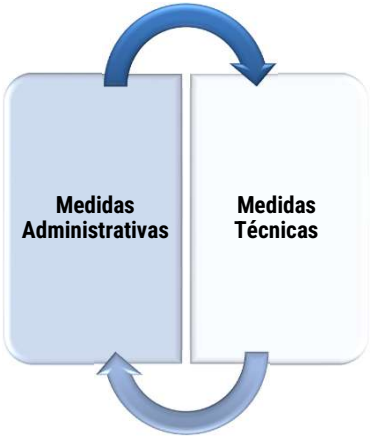
Podemos ter perda de dados pessoais no sistema Alepi por não termos backups atualizados. Se houver um problema no do banco de dados, não haverá como garantir a recuperação das informações dos Titulares de Dados.

- **Probabilidade:** 60%
- **Impacto** (Alto)**:**
  - ✓Tornar o acesso a plataforma Alepi indisponível para colaboradores, atrasando ciclos de capacitação importantes para o andamento de projetos.
- **Criticidade:** Alta
- **Estratégia** (Mitigar)**:**
  - ✓Atualizar o processo de backup do Alepi, incluindo backup incremental diário em ambiente externo na nuvem. Realizar atividades quinzenais de teste de *restore*.
- **Dados adicionais:**
  - ✓*Responsável atual por gerenciar o risco*: José Almeida
  - ✓*Data de cadastro do risco*: 13/05/23
  - ✓*Status atual*: Cadastrado

RGM

AS MEDIDAS DE SEGURANÇA

Diminuir a vulnerabilidade do controlador em relação à privacidade (diminuindo assim a quantidade de riscos que serão encontrados e deverão ser gerenciados) passa por implementar *medidas de segurança administrativas e técnicas*, que visem maximizar os níveis de segurança dos Dados Pessoais, pavimentando assim o caminho para garantir a privacidade dos Titulares de Dados.



RGM

MEDIDAS ADMINISTRATIVAS DE SEGURANÇA

Tudo se inicia com o estabelecimento de compromissos e guias que enderecem as boas práticas e os princípios que devem surgir já na governança corporativa do Controlador (Art. 50 da LGPD).

O comprometimento com a privacidade são documentados/obtidos através das **Medidas Administrativas de Segurança**:

Política de privacidade: Foco externo, demonstra as regras públicas de como o ente trata os Dados Pessoais e busca garantir a privacidade dos Titulares de Dados

Política de segurança: Foco interno, estabelece as regras a serem aplicadas pelo ente na implementação das Medidas Técnicas de Segurança

Cláusulas contratuais (e gestão de contratos): Estabelece diretrizes, limites e responsabilidades sobre os tratamentos de Dados Pessoais realizados no relacionamento entre as partes;

Treinamento, capacitação e conscientização: Prepara os colaboradores do ente a lidar com a privacidade, compartilha responsabilidades e documenta a ciência de todos perante os compromissos adotados pelo Controlador ou Operador

As **Medidas Administrativas de Segurança** devem:

- ✓ Estar integradas à governança corporativa
- ✓ Estabelecer relação de confiança com o Titular de Dados, por meio de atuação transparente e que assegure mecanismos de participação do Titular de Dados, incluindo canais para que eles exerçam seus direitos
- ✓ Definir mecanismos de supervisão do SGPD
- ✓ Prever as Medidas Técnicas de Segurança
- ✓ Estabelecer um ciclo de vida de atualização/manutenção das Medidas de Segurança adotadas
- ✓ Definir regras para a realização da gestão de riscos de segurança e privacidade
- ✓ Definir os parâmetros da gestão de incidentes e notificações
- ✓ Estabelecer regras para compartilhamento e transferência de Dados Pessoais
- ✓ Definir o papel e as responsabilidades do DPO
- ✓ Definir responsabilidades e regras a serem cumpridas pelo Controlador e seus Operadores
- ✓ Ser exequíveis

RGM

MEDIDAS
TÉCNICAS DE SEGURANÇA (1/2)

A garantia da privacidade dos dados é obtida através da implementação de Medidas Técnicas de Segurança, tal como previstas nas Medidas Administrativas de Segurança

RGM

MEDIDAS
TÉCNICAS DE SEGURANÇA (2/2)

Medidas técnicas de Confidencialidade

- Criptografia de dados
- Estrito controle de acesso físico e lógico: *Assegurar o nível de acesso apropriado e somente para as pessoas autorizadas*
- Classificação de dados: *Definir a que público os dados podem ser comunicados (Públicos? Sensíveis? Confidenciais?)*
- Treinamento de pessoal
- Segregação de funções: *Evitar que funções conflitantes sejam executadas pela mesma pessoa*
- Política de "mesa limpa"

Medidas técnicas de Integridade

- Padronizar caminho de acesso: *Por exemplo, não permitir atualização de dados "diretamente na Base de Dados"*
- Gravação de logs de usuários: *Garantir que possa ser determinado quem modificou a informação*
- Segregação de Função, posições e autoridade: *Ao menos duas pessoas serão necessárias para realizar mudanças que tenham graves consequências*
- Mudanças em sistemas e dados devem ser são autorizadas
- Padronizar terminologia: *Por exemplo, um incidente é sempre chamado de "incidente", logo, o termo "chamado" não pode ser inserido na base de dados*

Medidas técnicas de Disponibilidade

- Implementação de uma robusta solução de *backup* e *restore*
- Realizar rotinas de teste de restauração de ambientes
- Políticas de armazenamento gerenciado de dados: *Por exemplo, não permitir o armazenamento de dados em máquinas pessoais, dar preferência a sistemas de armazenamento centralizados, como servidores em rede interna ou cloud*
- Implementação do Gerenciamento de Disponibilidade da ITIL

RGM

GERENCIAMENTO DE INCIDENTES E NOTIFICAÇÕES

De acordo com as definições da LGPD

RGM

O QUE SÃO INCIDENTES

Incidente é uma ocorrência (fato) ilícita ou acidental, proveniente ou não de um risco previamente detectado, que gera destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito sobre informações.

Quando as informações associadas ao incidente são dados pessoais, temos um *Incidente de Privacidade:*

COMO TRATAR
INCIDENTES DE PRIVACIDADE

A melhor maneira de se evitar incidentes de privacidade é executar uma boa *Gestão de Riscos*, aliada à implementação de *Medidas de Segurança*.

- **A LGPD estabelece que 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

O QUE SÃO NOTIFICAÇÕES

Art. 48 O Controlador deverá comunicar à Autoridade Nacional e ao Titular de Dados a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

- Cabe ao Controlador analisar se o incidente pode acarretar risco ou dano relevante aos titulares, considerando aspectos como: volume de dados pessoais envolvidos, volume de titulares de dados associados e características dos dados pessoais (dados sensíveis, por exemplo)

- A ANPD definiu o canal para enviar notificações ao órgão: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca

RGM

COMPOSIÇÃO DE UMA NOTIFICAÇÃO DE INCIDENTE DE PRIVACIDADE

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
vi. As **medidas que foram ou que serão adotadas para reverter** ou mitigar os efeitos do prejuízo

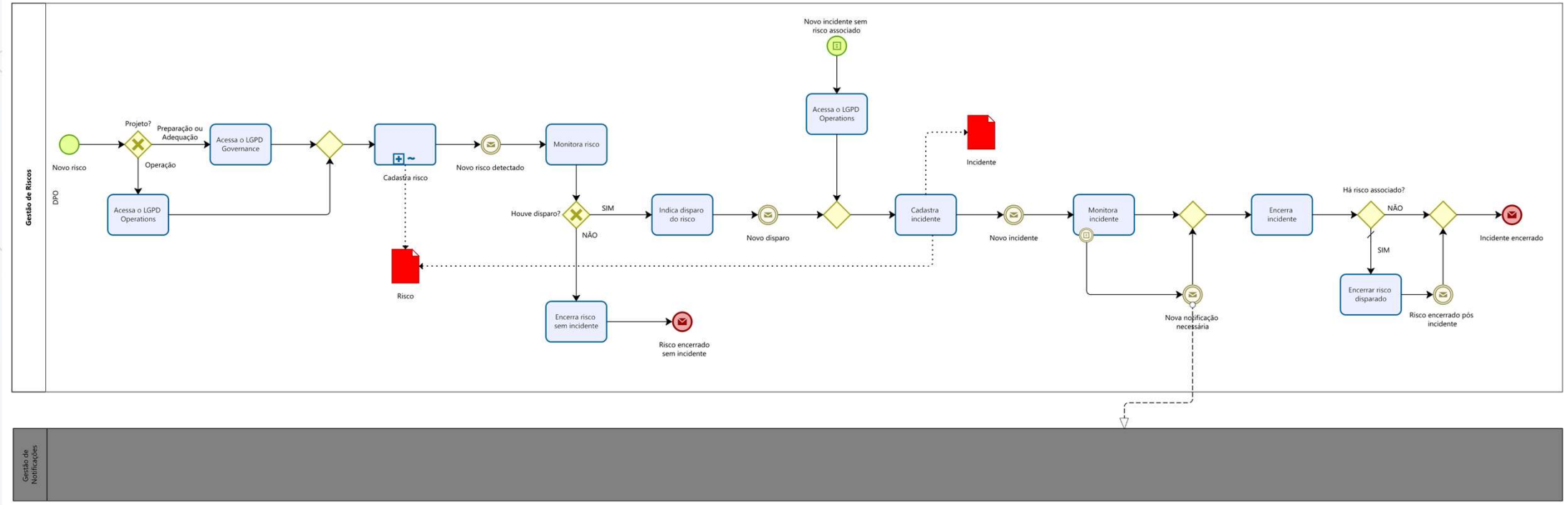
RGM

COMO TRATAR RISCOS, INCIDENTES E NOTIFICAÇÕES

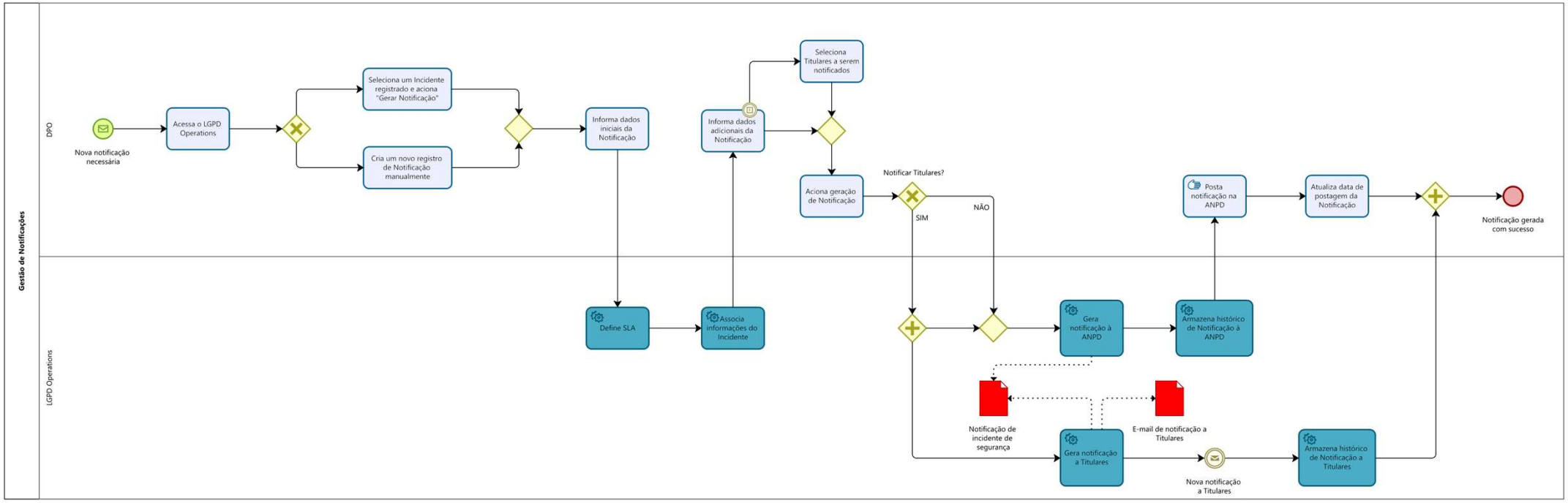
Fazendo uso das ferramentas Omnisblue

RGM

PROCESSO SUGERIDO PARA
GESTÃO DE RISCOS E INCIDENTES



PROCESSO SUGERIDO PARA
GESTÃO DE NOTIFICAÇÕES



RGM

DEMONSTRAÇÃO PRÁTICA

RGM

DÚVIDAS?

Agradecemos a atenção de todos!!!

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

RGM