# Matriz de Risco de exposição à LGPD para bancos de dados Shadow IT em PME

- Fabio Netto Pinheiro Grande
- https://www.linkedin.com/in/fabio-netto/

- Luis Ramirez
- https://www.linkedin.com/in/luisacramirez/

This Photo by Unknown author is licensed under CC BY.

# O que trataremos

- Conceitos LGPD
- Mostrar como montar parâmetros para confecção de uma matriz de risco de exposição à LGPD
- Montar um Escore para exposição LGPD baseado na matriz de risco
- Mecanismo de controle do progresso das adequações
- Demonstração de Recursos do SQL Server que mitigam a exposição LGPD

# PORQUE SE IMPORTAR?

- O mundo dos dados
- Temos um avatar digital
- Proteger os dados
- Garantir a privacidade
- Controlar as informações pessoais
- Adequação às legislações estrangeiras e nacionais

# E CHEGOU A LGPD

- Conhecer, entender e aplicar
- Objetivo
- Fundamentos e Princípios
- Conceitos Básicos
- Medidas de Segurança

# PASSANDO PARA A PRÁTICA

- LGPD é mais do que é possível ver acima da linha d'água
- Projetos de adequação
- Diagnóstico
- Tratamento de dados
- Mapeamento de dados
- Bancos de dados

# Definição – Shadow IT

- São sistemas de tecnologia sob controle de departamentos e estão fora do controle da TI central da empresa, costumam endereçar deficiências dos sistemas centralizados.
- Em PME representam muitas vezes com a própria atividade principal da empresa por não possuírem departamentos de TI estururados.
- Em muitas empresas de médio e até grande porte existe Shadow IT espalhadas pelos departamentos.

# Problemas frente a chegada LGPD na Shadow IT

- Exposição dados pessoais
- Multas pesadas violação LGPD
- Ausência de identificação dos tipos de dados pessoais
- Controle de usuários e acessos descentralizado quando existe
- Desconhecimento LGPD
- Equipes limitadas em recursos
- Mercado aquecido que dificulta expansão das equipes envolvidas
- **Restrições orçamentárias para compra de ferramentas/consultoria**

# Adequação a LGPD

LGPD não é um desafio apenas da TI
Adequação LGPD é um desafio para ser vencido com envolvimento de todos

# Desafio

- Adequação que não necessite grande investimento
- Permita uma priorização na diminuição do risco de exposição a LGPD
- **Envolver todos na empresa para melhorias dos processos**
- **Instituir melhores práticas permanentes no sistemas SGBD**
- **Não interromper o negócio/atividades da empresa**

Dividir em passos/etapas
Questionários TI e Usuários
Matriz de Risco
Escore de Risco
Priorização
Adequações
Acompanhamento

# Fase 1 Pesquisa dados da TI

- Mapear todos os Bancos Existentes dentro da Empresa que se qualifiquem como Shadow TI
- Levantar as informações relativas aos bancos de dados
  - Tamanho da base (Segmentar)
  - Tipo de Solução de Banco de Dados(Sql Server,Postgres,Myql, etc)
  - Versão do banco de dados
  - Quantidade de usuários com acesso
  - Quantidade de usuários com perfis administrativos
- Mapear os responsáveis pelo seu uso para poder fazer a fase 2 das informações

# Fase 2 Levantamento dados com usuários SGBD

- Mandar questionários para os responsáveis(usuários) do SGBD para melhor entender os dados
- O questionário pode ser feito via email, Google Forms, Microsoft Forms, a ferramenta que a empresa adote
  - **Existência de dados pessoais**
  - **Existência de dados pessoais sensíveis(possui um maior risco)**
  - Uso interno/Externo(Intranet/Internet)
  - Compartilhamento com outros setores/areas dentro da empresa
  - Usuários que precisam ter acesso
  - Forma de recebimento das bases

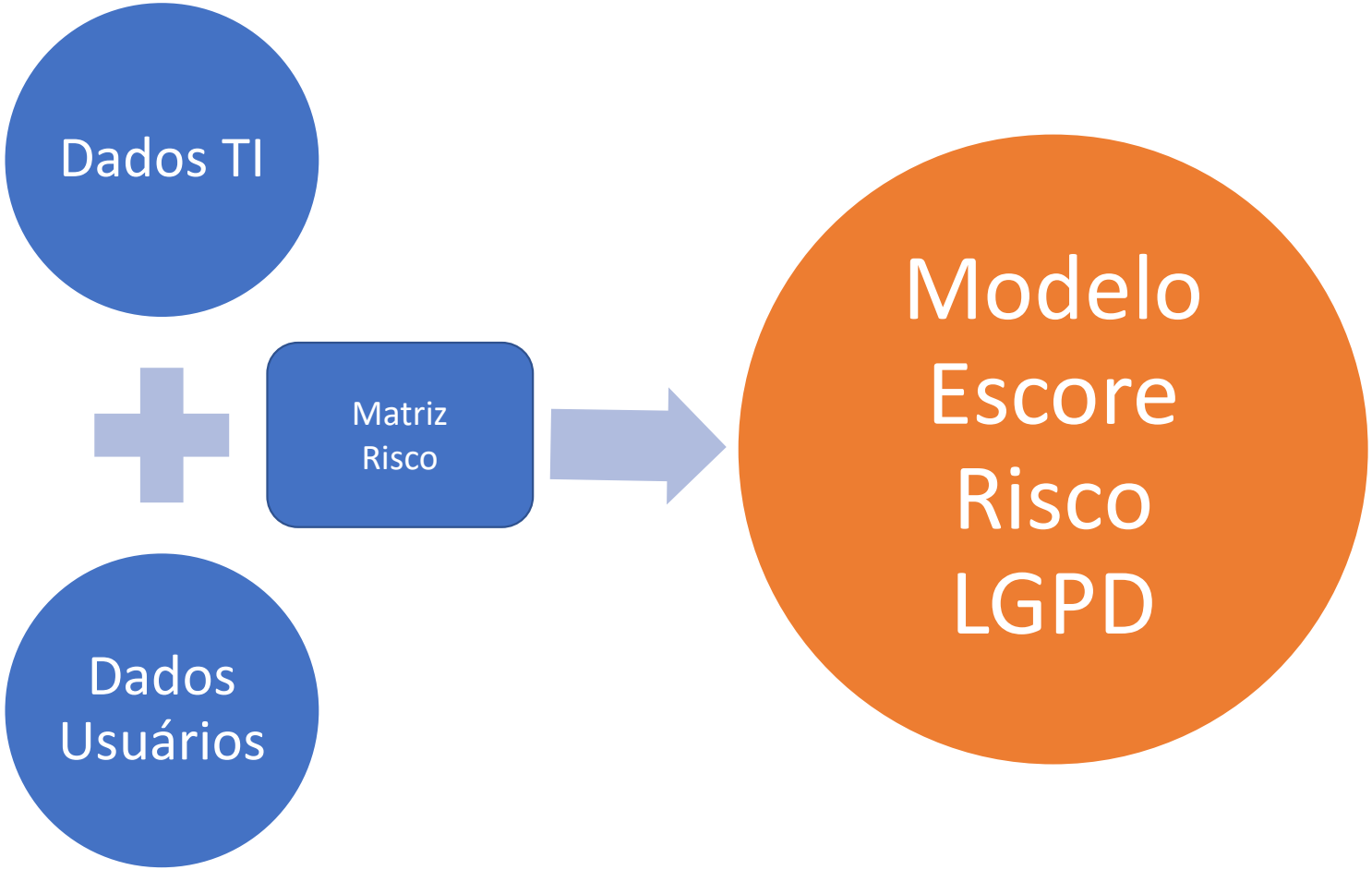
# Fase 3
# Montagem
# Matriz de Risco

- Com as respostas dos formulários faremos
- A validação das respostas
- Montagem dos pesos e detalhamento da Matriz de risco

| Evento | Mapeamento | Descrição | Unidade | Peso |
|---|---|---|---|---|
| Tamanho da base | TI | Tamanho ocupado pela base | GB | 0.1 |
| Tipo de Solução de Banco de Dados | TI | Peso 100 para solução SGBD sem suporte a LGPD | Sim/Não | |
| Versão do banco de dados | TI | Peso 100 para versões sem suporte a LGPD | Sim/Não | 100 |
| Quantidade de usuários com acesso ao SGBD | TI | | Qtde | 1 |
| Quantidade de usuários com perfis administrativos no SGBD | TI | | Qtde | 5 |
| Existência de dados pessoais | Usuarios | | Qtde | 10 |
| Existência de dados pessoais sensíveis(possui um maior risco) | Usuarios | | Qtde | 50 |
| Uso interno/Externo(Intranet/Internet) | Usuarios | Peso 100 para uso Internet | Sim/Não | 100 |
| Compartilhamento com outros setores/areas dentro da empresa | Usuarios | Peso 100 para compartilhamento com outros setores | Sim/Não | 100 |
| Usuários que precisam ter acesso | Usuarios | | Qtde | 1 |
| Forma de recebimento das bases | Usuarios | Peso 100 para arquivos txt em areas compartilhadas | Sim/Não | 100 |

# Matriz de Risco(exemplo)

# Fase 4  Montagem Escore Risco



# Quanto maior o escore maior o risco e maior a priorização no tratamento

# Fase 4 Retirada de acesso de usuários

- No Cruzamento dos usuários mapeados na TI com os indicados pelo usuário da informação, será possível retirar todos os que não constarem na lista
- Retirada de todos os usuários não constantes mais no quadro de empregados
- Revisar os acessos de terceiros

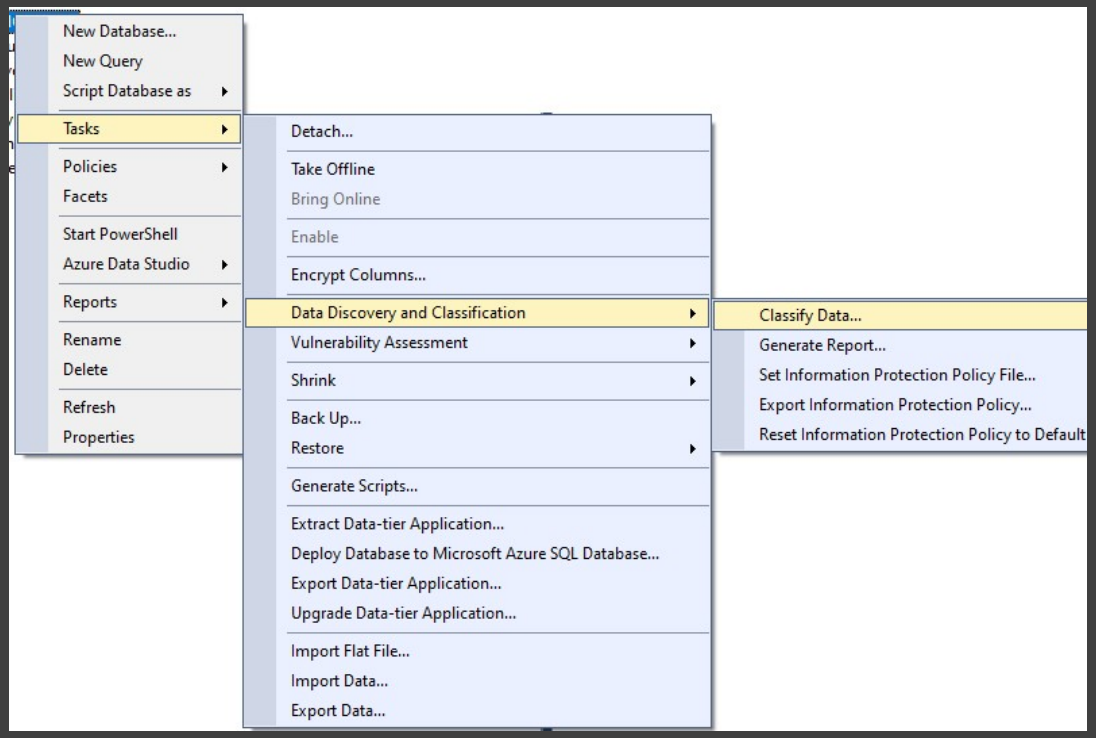
# Fase 5 Nivelamento versão SGBD

- Verificar a versão minima do banco que tenha suporte a ferramentas GDPR/LGPD
- No caso do Microsoft SQL Server a versão minima é o 2016
- Já existem recursos de mapeamento de informações pessoais a partir desta versão
- Elaborar o cronograma de atualização baseado no Escore de Risco
- Mapear os responsáveis pelo seu uso para poder fazer a fase 2 das informações

# Fase 6 Mapeamento Informações Pessoais

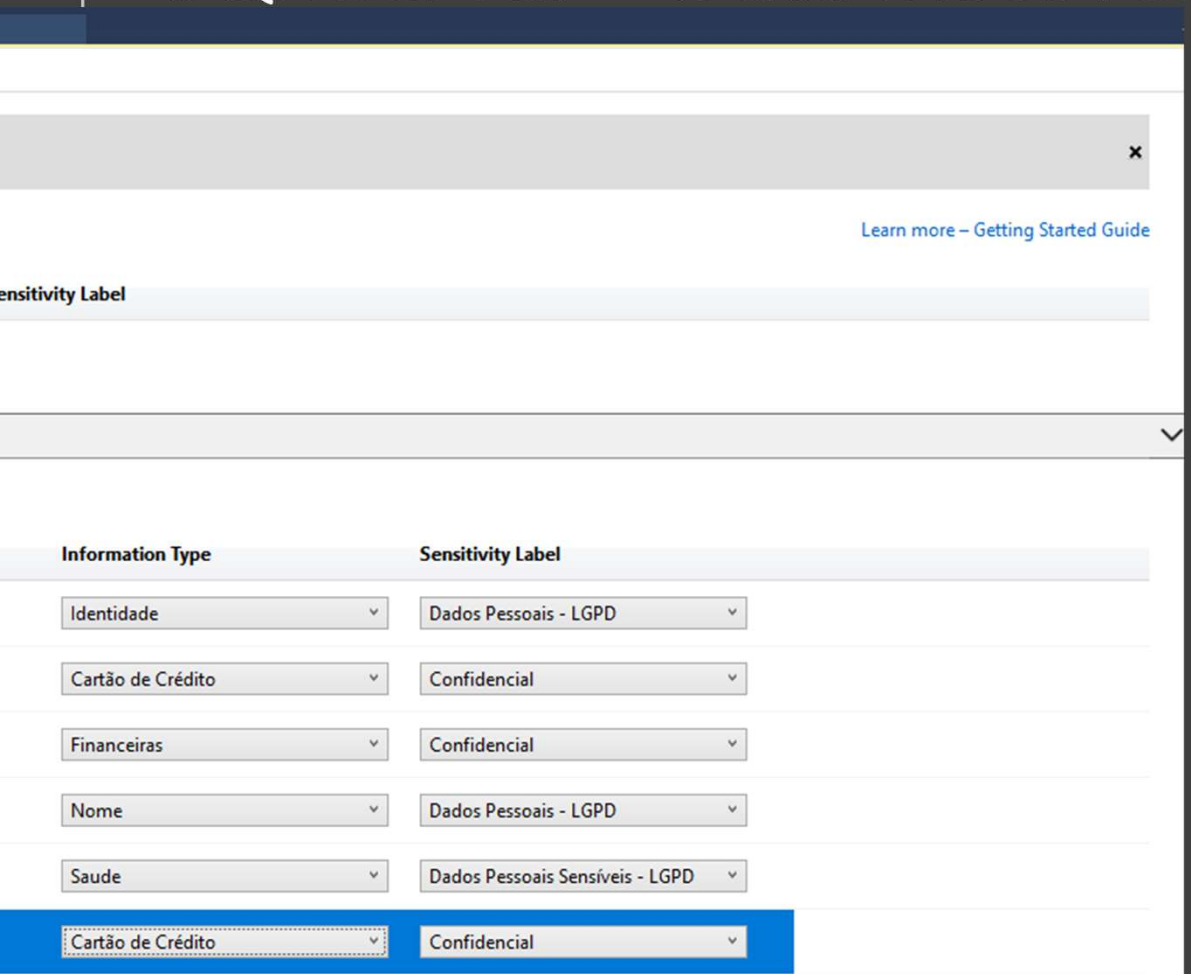
- Focaremos no caso específico do SQL Server 2016 em diante
- Já existem campos específicos para classificar tipos de dados e sua sensitividade em relação a proteção de dados
- Mapear os responsáveis pelo seu uso para poder fazer a fase 2 das informações

# SQL Server – Data Discovery and Classification

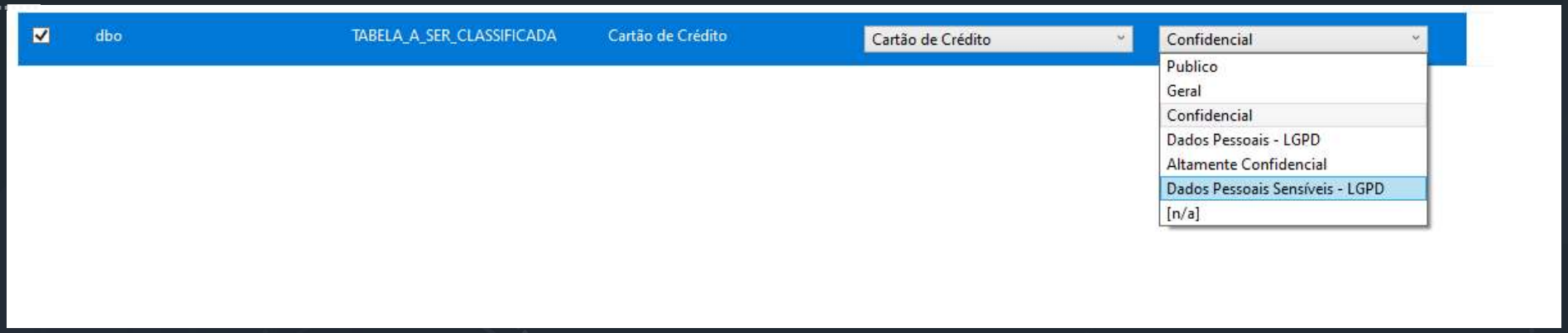



- Descoberta e classificação de dados(Classify Data)
- Ajuda a atender os padrões de privacidade de dados

# SQL Server – Data Discovery and Classification




- Modo Automático
- Arquivo Customizado contendo parâmetros LGPD – Brasil
- Também existem modos manuais




# SQL Server – Data Discovery and Classification

- Information Protection Policy
- Arquivo customizável contendo parâmetros para a LGPD – Brasil
- Necessita do SSMS(Management Studio) na versão 18.4, trata-se da ferramenta local para acesso ao Sql Server
- Pode ser usada pelo usuário que tem conhecimento das informações no banco para facilitar a classificação
- Permite mudar e adequar classificações de informações

# Aproveitar o momento de classificação de dados pessoais para também melhorar a governança de todas as informações

# Fase 7
# Acompanhamento
# Indicadores

- Uso do Escore Original para acompanhar a evolução das adequações
- % informações em bancos mapeadas

# Fase 8
# Adequações SGBD

- DDM - Dynamic Data Masking
- RLS - Row Level Security

# SQL Server – DDM(Dynamic Data Masking)

- Mascara de Dados Dinâmicos
- Limita a visualização de dados sensíveis a usuários sem privilégio de visualização
- Permite o cruzamento de informações
- A partir do mapeamento dos dados será possível mapear os campos com dados pessoais e pessoais sensíveis para uso do filtro
- Baixo impacto no funcionamento do banco de dados

# SQL Server RLS (Row Level Security)

- Segurança a nível de linha
- Permite configurar para grupos ou context de execução o acesso a linhas em uma tabela
- Exemplos práticos
  - Dentro do SQL Server o setor contábil precisa apenas dos dados financeiros, não necessitando ter acesso aos dados pessoais para elaboração de seus relatórios
  - Uma filial consegue visualizer apenas os seus clientes, evitando acesso a base inteira

# Espaço aberto a perguntas

- https://www.linkedin.com/in/fabio-netto/

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