**Documentação do Projeto de RLS e PLS no Power BI**

**Tomás Torre**

**OBJETIVO**

O objetivo deste projeto é demonstrar a aplicação prática de **RLS (Row-Level Security)** e **PLS (Page-Level Security)** em um modelo de dados no Power BI, voltado para ambientes corporativos.  
A ideia central é mostrar como implementar controles de segurança e restrição de acesso a dados em relatórios e dashboards, garantindo que cada usuário visualize apenas as informações que lhes são pertinentes.

No cenário que vamos ver, é um modelo criado para relatórios versionados entre a central e as filiais da corporação, podendo ser aplicado às áreas e subáreas dentro da central e dentro de cada filial também, apenas ajustando algumas coisas.

**METODOLOGIA**

**1. RLS (Row-Level Security)**

* O RLS foi configurado para filtrar automaticamente os dados com base no **usuário logado** no serviço do Power BI.
* Foram criadas regras que utilizam a função USERPRINCIPALNAME() para identificar o usuário autenticado.
* A partir disso, aplicam-se filtros de linha que restringem as informações de acordo com o perfil de acesso ou grupo de usuários.
* Assim, um usuário da filial X só visualiza os dados correspondentes à sua filial.

**2. PLS (Page-Level Security)**

* O PLS foi configurado para controlar a **navegação e visualização de páginas** dentro do relatório.
* A lógica compara o perfil de acesso do usuário com a página que ele tenta acessar.
* Usuários com perfil **restrito** só conseguem acessar páginas específicas, enquanto usuários com perfil **administrador** têm acesso a todas as páginas.
* Essa configuração geralmente é feita com **botões de navegação** e **condições DAX** aplicadas à visibilidade de elementos visuais.

**FUNCIONAMENTO DO MODELO**

1. **Usuário acessa o relatório no Power BI Service.**
2. O Power BI identifica o e-mail corporativo via USERPRINCIPALNAME().
3. As regras de RLS aplicam automaticamente os filtros de linha para restringir os dados.
4. As regras de PLS controlam a navegação, exibindo somente as páginas permitidas ao perfil do usuário.
5. O usuário tem, então, uma experiência personalizada, segura e alinhada ao seu nível de permissão.

**BENEFÍCIOS DA IMPLEMENTAÇÃO**

* **Segurança de dados**: cada usuário acessa apenas o que lhe é devido.
* **Governança corporativa**: alinhamento às regras internas de controle de informação.
* **Escalabilidade**: modelo facilmente aplicável a diferentes áreas, regionais e perfis.
* **Experiência do usuário**: interface ajustada conforme a necessidade de cada colaborador.

**ESTRUTURA DO PROJETO**

* **Dataset**: modelo de dados preparado para suportar filtros de segurança.
* **Tabela de Controle (PLS\_RLS)**: armazena os perfis de usuário e regras de acesso.
* **Regras DAX**: implementadas tanto no RLS quanto na lógica de navegação (PLS).
* **Relatórios e Páginas**: configurados para variar conforme o perfil do usuário.

**GERENCIAMENTO DE RELACIONAMENTOS**

Tabela

O conteúdo gerado por IA pode estar incorreto.

**Relacionamento entre a tabela de RLS\_PLS e a de apoio**

Interface gráfica do usuário, Texto, Aplicativo, chat ou mensagem de texto

O conteúdo gerado por IA pode estar incorreto.

**Modelagem – relacionamento entre tabelas**

Diagrama

O conteúdo gerado por IA pode estar incorreto.

**EXEMPLOS**

**1) Usuário 1 – Cargo presidente – central – acesso completo**Interface gráfica do usuário, Texto, Aplicativo, chat ou mensagem de texto

O conteúdo gerado por IA pode estar incorreto.Gráfico, Gráfico de barras

O conteúdo gerado por IA pode estar incorreto.Gráfico, Gráfico de barras

O conteúdo gerado por IA pode estar incorreto.

**2) Usuário 17 – Cargo coordenador – filial 3 – acesso restrito**

Interface gráfica do usuário, Texto, Aplicativo

O conteúdo gerado por IA pode estar incorreto.Gráfico, Gráfico de barras

O conteúdo gerado por IA pode estar incorreto.Interface gráfica do usuário, Texto, Aplicativo

O conteúdo gerado por IA pode estar incorreto.