 <i>Uso Interno</i>	Tipo de Documento:	Especificação Técnica
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Requisitos de Segurança da Informação – PowerBI

Sumário

1.	OBJETIVO.....	1
2.	ÂMBITO DE APLICAÇÃO	1
3.	DEFINIÇÕES.....	1
4.	DOCUMENTOS DE REFERÊNCIA.....	1
5.	RESPONSABILIDADES	1
6.	REGRAS BÁSICAS	2
7.	CONTROLE DE REGISTROS.....	31
8.	ANEXOS.....	31
9.	REGISTRO DE ALTERAÇÕES	31

1.OBJETIVO

Apresentar os requisitos de segurança da informação obrigatórios e recomendáveis para todos os serviços que utilizam o PowerBI pelo Grupo CPFL, ou empresas do Grupo, provendo orientações técnicas para os colaboradores.

2.ÂMBITO DE APLICAÇÃO

2.1.Empresa

Todas as empresas do Grupo CPFL.

2.2.Área

Todas as áreas Grupo CPFL.

3.DEFINIÇÕES

Não aplicável.


4.DOCUMENTOS DE REFERÊNCIA

Diretrizes Segurança da Informação (GED14369).
Classificação da Informação (GED 18744)

5.RESPONSABILIDADES

Não aplicável.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18711	Instrução	1.1	Emerson Cardoso	01/04/2022	1 de 31

 <i>Uso Interno</i>	Tipo de Documento:	Especificação Técnica
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Requisitos de Segurança da Informação – PowerBI

6. REGRAS BÁSICAS

6.1. INTRODUÇÃO

O Power BI é uma plataforma de business intelligence líder de mercado, que oferece uma estrutura completa para a implementação de soluções de BI em qualquer negócio. A suíte é capaz de capturar dados de variadas fontes, transformá-los e gerar dashboards interativos e automatizados que apoiam a tomada de decisão estratégica para a empresa, além disso é uma coleção de serviços de software, aplicativos e conectores que trabalham juntos para transformar suas fontes de dados não relacionadas em informações coerentes, visualmente envolventes e interativas.

Principais benefícios e características de utilização do Power BI:

A suíte de business intelligence da Microsoft oferece aplicativos integrados para auxiliar o usuário em todo o processo de obtenção de informações por meio de dados. O Power BI inclui extração, preparação, análise, visualização e governança de dados – tudo em uma solução.

- **Suporte na tomada de decisões**

Não é eficiente trabalhar com dados desorganizados, espalhados em centenas de planilhas que precisam ser atualizadas manualmente e demandam horas – ou até dias e semanas – de trabalho repetitivo.

Em um mundo rápido, complexo, em constante transformação e que gera cada vez mais dados por segundo, as Gerências e Administração das empresas precisa de agilidade e confiabilidade. E, para isso, é indispensável desenvolver soluções capazes de guiar e oferecer suporte à tomada de decisão. O Power BI, por meio de suas inúmeras funcionalidades, possibilita a construção de relatórios interativos, completos e confiáveis.


Com esse recurso, gestores podem tomar decisões com mais segurança e até antecipar problemas.

- **Autonomia**

Durante muito tempo, as áreas de negócio eram totalmente dependentes da TI para obter qualquer tipo de dado. E isso tem uma razão de ser: é muito perigoso fornecer acesso irrestrito a usuários não técnicos. Um simples deslize pode tirar toda a sua produção de operação, causando prejuízos gigantescos.

Com o Power BI – construído com uma interface intuitiva para que o usuário consiga fazer quase tudo com cliques – o analista tem mais autonomia para desenvolver soluções, monitorar resultados e propor melhorias. Isso traz autossuficiência para as áreas de negócios que, em poucas semanas, podem começar a trabalhar com dados sem grandes dificuldades. Por consequência, melhoram o acesso aos indicadores mais relevantes, a produtividade e a busca por novas soluções.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18711	Instrução	1.1	Emerson Cardoso	01/04/2022	2 de 31

 <i>Uso Interno</i>	Tipo de Documento:	Especificação Técnica
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Requisitos de Segurança da Informação – PowerBI

• Fácil compartilhamento de relatórios

De nada adianta ter terabytes de dados armazenados se eles não podem ser apresentados de modo claro e intuitivo a um número significativo de pessoas dentro da organização. Com o Power BI, é possível compartilhar relatórios com qualquer pessoa, de maneira segura, através dos navegadores, do recurso de embedding e do aplicativo para celular.

É muito comum a visão de que apenas a alta liderança precisa de acesso a dados para a tomada de decisão – e isso é verdade em casos de dados mais sensíveis e estratégicos – mas uma cultura realmente data driven se preocupa com a democratização dos dados dentro da empresa.

Do estagiário ao CEO – todos podem obter insights importantes a partir de dados. Quando todos têm acesso às informações relevantes para sua área ou cargo, o trabalho se torna mais estratégico e relevante para a empresa como um todo.

• Trabalho em nível colaborativo

Como um desdobramento da função de compartilhamento, a possibilidade de trabalho em nível colaborativo é outro grande benefício da ferramenta. Adotando algumas boas práticas de desenvolvimento em equipe, vários desenvolvedores podem trabalhar em conjunto para construir um relatório do zero.

Através dos workspaces do Power BI, conseguimos incluir usuários para que eles possam gerenciar relatórios, conjuntos de dados, pastas de trabalho, fazer versionamento etc. É possível ainda controlar permissões e níveis de acesso.

Na prática, essa flexibilidade facilita a integração entre departamentos, enriquece as análises e oferece toda a base que os gestores precisam para tomar decisões respaldadas por dados concretos.

• Dados protegidos e com acesso restrito


O grande objetivo de uma aplicação como o Power BI é tornar os dados acessíveis a quem precisa deles – mas é preciso de muito cuidado com qualquer tipo de tratamento de dados, afinal trabalhamos com informações muitas vezes sensíveis.

Compartilhar arquivos na nuvem para que outras pessoas acessem não quer dizer que qualquer um poderá vê-los. E os recursos de segurança do Power BI dão conta de resolver esse problema.

O Power BI possibilita o compartilhamento seguro de dados por meio de recursos de:

- ✓ Classificação e rotulação de dados como confidenciais
- ✓ Governança de dados
- ✓ Controle de permissões
- ✓ Monitoramento e proteção da atividade dos usuários

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18711	Instrução	1.1	Emerson Cardoso	01/04/2022	3 de 31

 <i>Uso Interno</i>	Tipo de Documento:	Especificação Técnica
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Requisitos de Segurança da Informação – PowerBI

É possível, ainda, combinar os recursos do Power BI com boas práticas de gestão de tecnologia, como a implantação de um modelo de Gerenciamento de Nível de Serviço (Service Level Management – SLM) – um conjunto de rotinas que têm como objetivo guiar o suporte em tecnologia, oferecer melhor atendimento ao cliente e garantir proteção e segurança.

Com estes recursos, conseguimos, por exemplo, compartilhar relatórios em nuvem com permissão para que apenas os colaboradores da área de marketing possam visualizar e fazer alterações. O mesmo pode ser feito de maneira ainda mais segmentada, selecionando apenas pessoas autorizadas.

• Integração com diversas fontes de dados

Com o Power BI, é muito simples conectar e obter dados de uma quantidade incrível de fontes. Atualmente, a ferramenta dá suporte à conexão a arquivos em diversas extensões, aos sistemas baseados em nuvem e muitos outros.

O Power BI desempenha um papel fundamental ao disponibilizar informações de dados para todos em uma organização. No entanto, à medida que os dados se tornam mais acessíveis para a tomada de decisões informadas, aumenta o risco de compartilhamento excessivo acidental ou de uso indevido de informações críticas para os negócios.

Os recursos de proteção de dados Power BI baseia-se nos pontos fortes da Microsoft em segurança e permitem que os clientes capacitem todos os usuários com Power BI e protejam melhor seus dados, independentemente de como ou onde eles são acessados.

Os pilares dos Power BI de proteção de dados da sua empresa e como eles ajudam a proteger os dados confidenciais da sua organização estão listados abaixo:


• Proteção de Informações da Microsoft rótulos de sensibilidade

- **Classificar e rotular dados do Power BI como confidenciais** usando os rótulos de confidencialidade da Proteção de Informações da Microsoft usados no Office e em outros produtos da Microsoft.
- **Impor políticas de governança mesmo quando o conteúdo do Power BI é exportado** para o Excel, PowerPoint, PDF e outros formatos com suporte, a fim de ajudar a garantir que os dados sejam protegidos mesmo quando saírem do Power BI.

• Microsoft Defender for Cloud Apps

- **Monitore e proteja a atividade do** usuário em dados confidenciais em tempo real com alertas, monitoramento de sessão e correção de risco usando o Defender para Aplicativos de Nuvem.
- **Capacitar administradores de segurança que** usam relatórios de proteção de dados e funcionalidades de investigação de segurança com o Defender para Aplicativos de Nuvem para aprimorar a supervisão organizacional.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18711	Instrução	1.1	Emerson Cardoso	01/04/2022	4 de 31

 <i>Uso Interno</i>	Tipo de Documento:	Especificação Técnica
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Requisitos de Segurança da Informação – PowerBI

- **Microsoft 365 de perda de dados**

- **As políticas de prevenção** contra perda de dados Power BI permitem que as equipes de segurança central usem Microsoft 365 de prevenção contra perda de dados para impor as políticas de DLP da organização Power BI. As políticas de DLP para Power BI atualmente dão suporte à detecção de rótulos de sensibilidade em conjuntos de dados e podem disparar ações automáticas de correção de risco, como alertas para administradores de segurança no portal de conformidade do Microsoft 365 e dicas de política para usuários finais.

6.2. MODOS DE CONJUNTO DE DADOS

Esse tópico fornece uma explicação técnica dos modos de conjunto de dados do Power BI. Essas informações se aplicam a conjuntos de dados que representam uma conexão dinâmica a um modelo de Analysis Services hospedado externamente e a modelos desenvolvidos no Power BI Desktop.

Os três modos de conjunto de dados são:

- **Modo Importação**


O modo de importação é o modo mais comum usado para desenvolver conjuntos de dados. Ele proporciona um desempenho extremamente rápido graças à consulta na memória. Ele também oferece flexibilidade de design para modeladores e suporte para recursos de serviço Power BI específicos (QA&, Insights rápido etc.). Devido a esses pontos fortes, ele é o modo padrão quando cria uma nova solução do Power BI Desktop.

É importante entender que os dados importados são sempre armazenados em disco. Quando consultados ou atualizados, os dados devem ser totalmente carregados na memória da capacidade do Power BI. Uma vez na memória, os modelos de Importação podem obter resultados de consulta muito rapidamente. Também é importante entender que não há nenhum conceito de modelo de Importação que seja carregado parcialmente na memória.

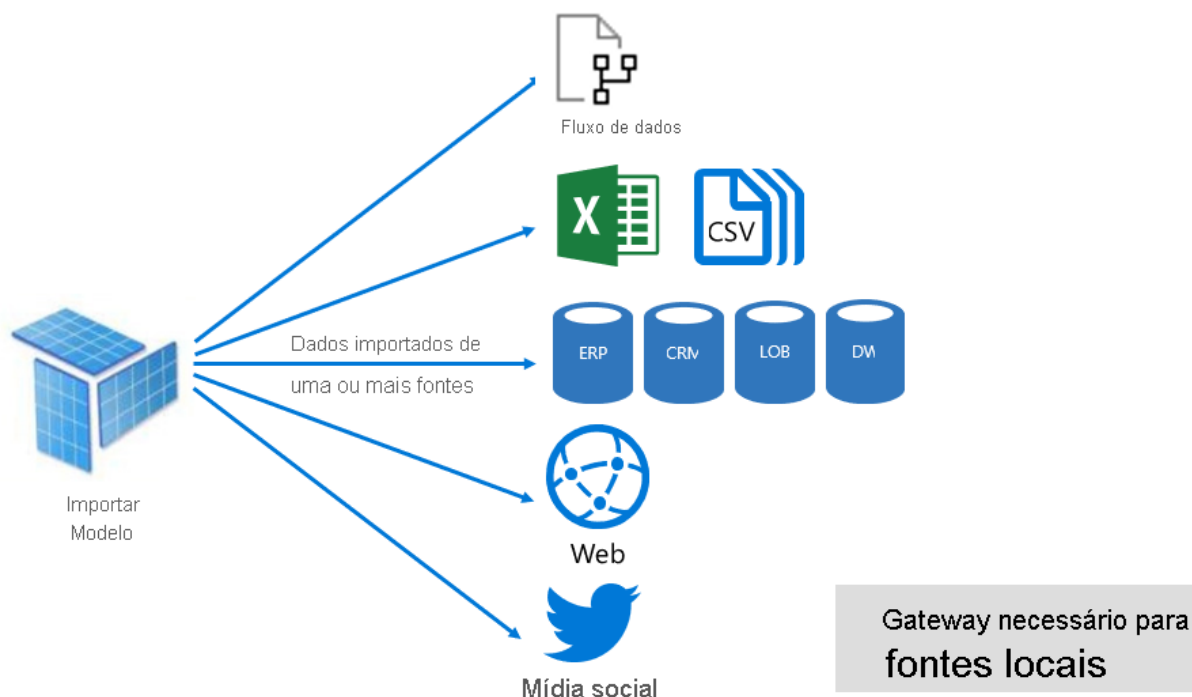
A flexibilidade de design pode ser obtida de três maneiras. Os modeladores de dados podem:

- ✓ Integrar dados armazenando dados em cache de fluxos de dados e fontes externas, independentemente do tipo ou formato da fonte de dados;
- ✓ Utilizar o conjunto inteiro das funções de Linguagem de fórmula de consulta do Power Query (informalmente chamado de M) ao criar consultas de preparação de dados;
- ✓ Utilizar todo o conjunto de funções de DAX (Data Analysis Expressions) ao aprimorar o modelo com lógica de negócios. Há suporte para colunas calculadas, tabelas calculadas e medidas.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18711	Instrução	1.1	Emerson Cardoso	01/04/2022	5 de 31

 Uso Interno	Tipo de Documento:	Especificação Técnica
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Requisitos de Segurança da Informação – PowerBI

Conforme mostrado na imagem a seguir, um modelo de Importação pode integrar dados de diversos tipos de fonte de dados com suporte.




Porém, embora haja vantagens atraentes associadas aos modelos de Importação, também há desvantagens:

- ✓ O modelo inteiro deve ser carregado na memória antes que o Power BI consulte o modelo, o que poderá causar uma pressão nos recursos de capacidade disponíveis, especialmente à medida que o número e o tamanho dos modelos de Importação forem crescendo;
- ✓ Os dados do modelo são apenas aqueles vigentes na atualização mais recente e, portanto, os modelos de Importação precisam ser atualizados, em geral, periodicamente;
- ✓ Uma atualização completa removerá todos os dados de todas as tabelas e os recarregará a partir da fonte de dados. Essa operação pode ser dispendiosa em termos de tempo e recursos para o serviço do Power BI e as fontes de dados.

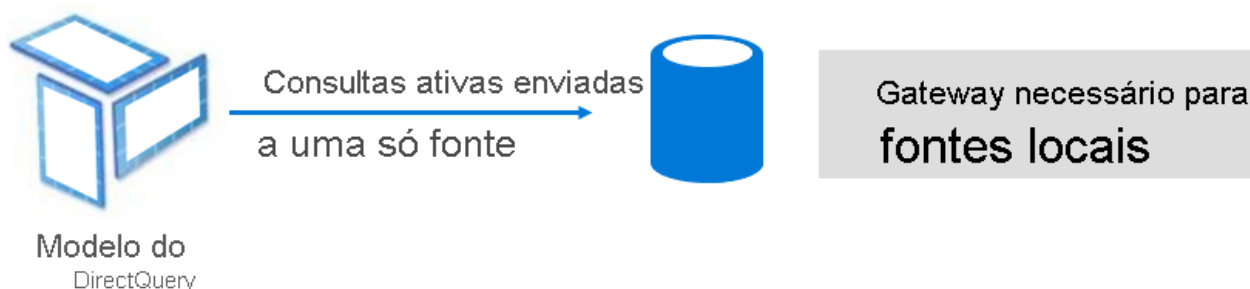
Da perspectiva de um recurso do serviço do Power BI, os modelos de Importação exigem:

- ✓ Memória suficiente para carregar o modelo quando ele é consultado ou atualizado;
 - ✓ Processamento de recursos e recursos de memória adicionais para atualizar os dados.
- **DirectQuery**

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18711	Instrução	1.1	Emerson Cardoso	01/04/2022	6 de 31

 Uso Interno	Tipo de Documento:	Especificação Técnica
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Requisitos de Segurança da Informação – PowerBI

O modo DirectQuery é uma alternativa ao modo de Importação. Os modelos desenvolvidos no modo DirectQuery não importam dados. Em vez disso, eles contêm apenas metadados que definem a estrutura do modelo. Quando o modelo é consultado, as consultas nativas são usadas para recuperar os dados da fonte de dados subjacente.



Há dois motivos principais para considerar desenvolver um modelo DirectQuery:

- ✓ Quando os volumes de dados são muito grandes (mesmo quando são aplicados métodos de redução de dados) para carregar em um modelo ou para uma atualização prática
- ✓ Quando os relatórios e painéis precisam fornecer dados "quase em tempo real", para além do que pode ser obtido dentro dos limites de atualização agendada. (Os limites de atualização agendada ocorrem oito vezes por dia para a capacidade compartilhada e 48 vezes por dia para a capacidade Premium.)

Há diversas vantagens associadas aos modelos DirectQuery:


- ✓ Os limites de tamanho do modelo de Importação não se aplicam;
- ✓ Os modelos não exigem a atualização de dados agendada;
- ✓ Os usuários de relatórios verão os dados mais recentes ao interagirem com segmentações e filtros de relatório. Além disso, os usuários de relatórios podem atualizar o relatório inteiro para recuperar dados atuais;
- ✓ Os relatórios em tempo real podem ser desenvolvidos usando o recurso atualização automática de página;
- ✓ Os blocos de painel, quando baseados em modelos DirectQuery, podem ser atualizados automaticamente, a cada 15 minutos.

No entanto, há algumas limitações associadas aos modelos do DirectQuery:

- ✓ Power Query/Mashup só podem funções que podem ser transpostas para consultas nativas compreendidas pela fonte de dados.
- ✓ As fórmulas DAX são limitadas a usar apenas funções que podem ser transpostas para consultas nativas compreendidas pela fonte de dados. Não há suporte para tabelas calculadas.
- ✓ Não há Insights recursos rápidos.

Da perspectiva de um recurso do serviço do Power BI, os modelos DirectQuery exigem:

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18711	Instrução	1.1	Emerson Cardoso	01/04/2022	7 de 31

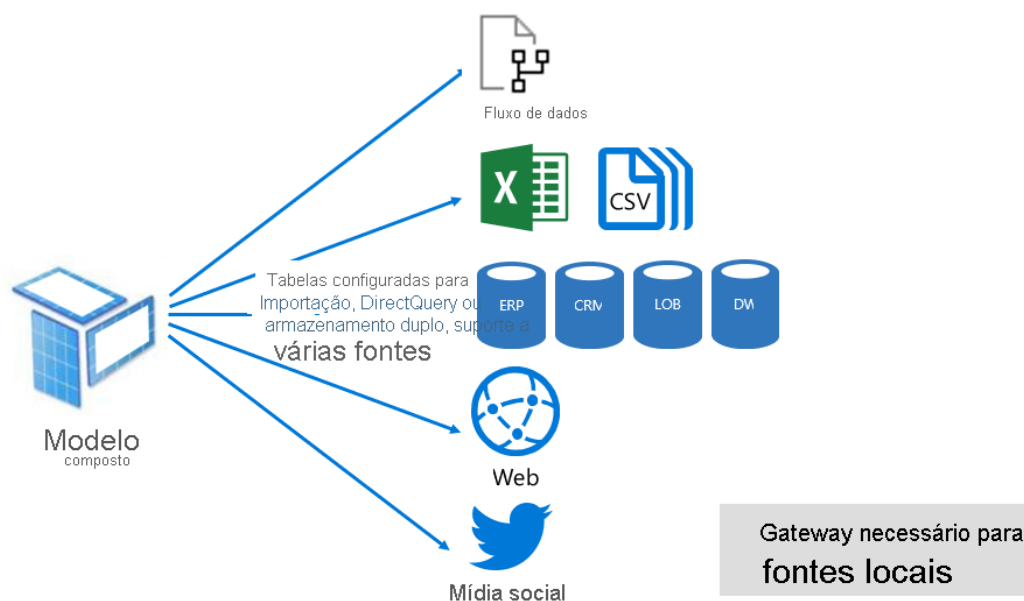
 Uso Interno	Tipo de Documento:	Especificação Técnica
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Requisitos de Segurança da Informação – PowerBI

- ✓ Memória mínima para carregar o modelo (somente metadados) quando ele for consultado.
- ✓ Às vezes, o serviço do Power BI deve usar recursos significativos do processador para gerar e processar consultas enviadas à fonte de dados. Quando essa situação ocorre, pode afetar a taxa de transferência, especialmente quando há usuários consultando o modelo ao mesmo tempo.

• Composto

O modo Composto pode combinar os modos de Importação e DirectQuery ou integrar várias fontes de dados DirectQuery. Os modelos desenvolvidos no modo Composto dão suporte à configuração do modo de armazenamento para cada tabela de modelo. Esse modo também oferece suporte a tabelas calculadas (definidas com DAX).

O modo de armazenamento de tabela pode ser configurado como Importação, DirectQuery ou Dual. Uma tabela configurada como modo de armazenamento Dual é ao mesmo tempo de Importação e DirectQuery, e essa configuração permite que o serviço do Power BI determine o modo mais eficiente a ser usado de acordo com cada consulta.




Os modelos Compostos oferecem o melhor dos modos de Importação e DirectQuery. Quando configurados adequadamente, eles podem combinar o alto desempenho de consultas de modelos na memória com a capacidade de recuperar dados de fontes de dados quase que em tempo real.

Pode otimizar sua solução em diferentes camadas de arquitetura. As camadas incluem:

- ✓ As fontes de dados
- ✓ O modelo de dados
- ✓ Visualizações, incluindo dashboards, relatórios do Power BI e relatórios paginados do Power BI

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18711	Instrução	1.1	Emerson Cardoso	01/04/2022	8 de 31

 <i>Uso Interno</i>	Tipo de Documento:	Especificação Técnica
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Requisitos de Segurança da Informação – PowerBI

✓ O ambiente, incluindo capacidades, gateways de dados e a rede

Otimizar modelos de dados

O modelo de dados dá suporte à experiência inteira de visualização. Os modelos de dados são hospedados externa ou internamente e, no Power BI, são chamados de conjuntos de dados. É importante entender suas opções e escolher o tipo apropriado de conjunto de dados para sua solução. Os três modos de conjunto de dados são: Importação, DirectQuery e composto. para obter mais informações, consulte conjuntos de dados no serviço Power BI e modos de conjunto de dados no serviço Power BI.

Otimizar visualizações

As visualizações do Power BI, incluindo dashboards, relatórios do Power BI e relatórios paginados do Power BI. Cada uma tem diferentes arquiteturas e, portanto, suas próprias diretrizes.

Dashboards


É importante entender que o Power BI mantém um cache para os blocos de dashboard, exceto para blocos de relatório em tempo real e blocos de streaming. Caso seu conjunto de armazenamento imponha a RLS (Segurança em Nível de Linha) dinâmica, entenda as implicações de desempenho, pois os blocos serão armazenados em cache por usuário.

Quando fixa blocos de relatório em tempo real em um painel, eles não são alimentados a partir do cache de consulta. Em vez disso, eles se comportam como relatórios e consultam os núcleos de back-end em tempo real.

Como o nome sugere, a recuperação de dados do cache proporciona um desempenho melhor e mais consistente do que confiar na fonte de dados. Uma maneira de aproveitar essa funcionalidade é ter painéis como a primeira página de aterrissagem para seus usuários. Fixe os visuais usados com frequência e altamente solicitados aos dashboards. Dessa forma, os dashboards se tornam uma valiosa "primeira linha de defesa", que oferece um desempenho consistente sem sobrecarregar a capacidade. Os usuários ainda podem clicar no relatório para analisar os detalhes.

Para conjuntos de dados de conexão dinâmica e do DirectQuery, o cache é atualizado periodicamente ao consultar a fonte de dados. Por padrão, a atualização ocorre a cada hora, embora possa configurar uma frequência diferente nas configurações do conjunto de dados. Cada atualização de cache envia as consultas à fonte de dados subjacente para atualizar o cache. O número de consultas geradas depende do número de visuais fixados nos dashboards que dependem dessa fonte de dados. Observe que se a segurança em nível de linha estiver habilitada, as consultas serão geradas para cada contexto de segurança diferente. Por exemplo, considere que haja duas funções diferentes que categorizem os usuários, com duas exibições diferentes dos dados. Durante a atualização do cache de consulta, o Power BI gera dois conjuntos de consultas.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18711	Instrução	1.1	Emerson Cardoso	01/04/2022	9 de 31

 Uso Interno	Tipo de Documento:	Especificação Técnica
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Requisitos de Segurança da Informação – PowerBI

Aplicar os filtros mais restritivos

Quanto mais dados um visual precisar exibir, mais lentamente esse visual será carregado. Embora esse princípio pareça óbvio, é fácil esquecer. Por exemplo: suponha que tenha um grande conjunto de dados. Sobre esse conjunto de dados, cria um relatório com uma tabela. Os usuários finais usam segmentações na página para obter as linhas que desejam e, normalmente, só estão interessados em algumas dezenas de linhas.

Adicionar URLs do Power BI à lista de permitidos

O serviço do Power BI requer conectividade com a Internet. Os pontos de extremidade listados nas tabelas devem ser acessíveis para clientes que usam o serviço do Power BI.

Para usar o serviço do Power BI, é necessário conseguir se conectar aos pontos de extremidade marcados como obrigatórios nas tabelas abaixo e aos pontos de extremidade marcados como obrigatórios nos sites vinculados. Se o link para um site externo se referir a uma seção específica, será necessário apenas analisar os pontos de extremidade nessa seção.

Os pontos de extremidade marcados como opcionais também podem ser adicionados às listas de permissões para habilitar uma funcionalidade específica.

O serviço do Power BI requer apenas que a porta TCP 443 seja aberta para os pontos de extremidade listados.

Caracteres curinga (*) representam todos os níveis sob o domínio raiz, e usaremos N/D quando as informações não estiverem disponíveis. A coluna Destino(s) lista os nomes de domínios e os links para sites externos que contêm mais informações sobre o ponto de extremidade.


Autenticação

O Power BI depende dos pontos de extremidade necessários nas seções de identidade e autenticação do Microsoft 365. Para usar o Power BI, conecte-se aos pontos de extremidade no site vinculado abaixo.

Linha	Finalidade	Destino(s)	Porta(s)
1	Obrigatório: Autenticação e identidade	Confira a documentação com as URLs do Microsoft 365 Common e do Office Online	N/D

Uso geral do site

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18711	Instrução	1.1	Emerson Cardoso	01/04/2022	10 de 31

 Uso Interno	Tipo de Documento:	Especificação Técnica
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Requisitos de Segurança da Informação – PowerBI

Para o uso geral do Power BI, conecte-se aos pontos de extremidade na tabela e nos sites vinculados abaixo.

Linha	Finalidade	Destino(s)	Porta(s)
1	Obrigatório: APIs de back-end	api.powerbi.com	TCP 443
2	Obrigatório: APIs de back-end	*.analysis.windows.net	TCP 443
3	Obrigatório: APIs de back-end	*.pbidedicated.windows.net	TCP 443
4	Obrigatório: CDN (Rede de Distribuição de Conteúdo)	content.powerapps.com	TCP 443
6	Obrigatório: Portal	*.powerbi.com	TCP 443
7	Obrigatório: Telemetria do serviço	dc.services.visualstudio.com	TCP 443
8	Opcional: Mensagens informativas	arc.msn.com	TCP 443
9	Opcional: pesquisas NPS	nps.onyx.azure.net	TCP 443

Obtendo dados

Para obter dados de fontes de dados específicas, como o OneDrive, você deve ser capaz de se conectar aos pontos de extremidade na tabela abaixo. O acesso a URLs e domínios de Internet adicionais pode ser necessário para fontes de dados específicas usadas na sua organização.


Linha	Finalidade	Destino(s)	Porta(s)
1	Obrigatório: AppSource (aplicativos internos ou externos no Power BI)	appsource.microsoft.com *.s-microsoft.com	TCP 443
4	Opcional: vídeo de tutorial do Power BI em 60 segundos	*.doubleclick.net *.ggpht.com *.google.com *.googlevideo.com *.youtube.com *.ytimg.com fonts.gstatic.com	TCP 443

Visuais do Power BI

O Power BI depende de determinados pontos de extremidade para exibir e acessar visuais. Você deve poder se conectar aos pontos de extremidade na tabela e nos sites vinculados abaixo

Linha	Finalidade	Destino(s)	Porta(s)
-------	------------	------------	----------

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18711	Instrução	1.1	Emerson Cardoso	01/04/2022	11 de 31

 Uso Interno	Tipo de Documento:	Especificação Técnica
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Requisitos de Segurança da Informação – PowerBI


Linha	Finalidade	Destino(s)	Porta(s)
1	Obrigatório: Importar um visual personalizado da interface do Marketplace ou de um arquivo	*.azureedge.net *.blob.core.windows.net *.osi.office.net *.msecnd.net store.office.com web.vortex.data.microsoft.com store-images.s-microsoft.com	TCP 443
2	Opcional: Bing Mapas	bing.com platform.bing.com *.virtualearth.net	TCP 443

Sites externos relacionados

O Power BI contém links para outros sites relacionados. Esses sites hospedam documentação, suporte, solicitações de novos recursos e muito mais. O acesso a esses sites não afetará a funcionalidade do Power BI, portanto, adicioná-los à lista de permissões é opcional.

Linha	Finalidade	Destino(s)	Porta(s)
1	Opcional: Site da comunidade	community.powerbi.com oxcrx34285.i.lithium.com	TCP 443
2	Opcional: Site de documentação	docs.microsoft.com img-prod-cms-rt-microsoft-com.akamaized.net statics-uhf-eas.akamaized.net cdnssl.clicktale.net ing-district.clicktale.net	TCP 443
3	Opcional: Site de download (para o Power BI Desktop etc.)	download.microsoft.com	TCP 443
4	Opcional: Redirecionamentos externos	aka.ms go.microsoft.com	TCP 443
5	Opcional: Site de comentários sobre ideias	ideas.powerbi.com powerbi.uservoice.com	TCP 443
6	Opcional: site do Power BI – página de aterrissagem, links para saber mais, site de suporte, links de download, demonstração do parceiro e assim por diante.	powerbi.microsoft.com	TCP 443
7	Opcional: Central de desenvolvedores do Power BI	dev.powerbi.com	TCP 443
8	Opcional: Site de suporte	support.powerbi.com s3.amazonaws.com *.olark.com	TCP 443

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18711	Instrução	1.1	Emerson Cardoso	01/04/2022	12 de 31

 Uso Interno	Tipo de Documento:	Especificação Técnica
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Requisitos de Segurança da Informação – PowerBI

Linha	Finalidade	Destino(s)	Porta(s)
		logx.optimizely.com mscom.demdex.net tags.tiqcdn.com	

Roteiro de adoção do Power BI: governança

A governança de dados é um tópico amplo e complexo. Ele identifica ações importantes a serem tomadas ao adotar o Power BI.

O foco principal da governança não são os próprios dados, mas o controle do *que as pessoas fazem com os dados*.

Quando focamos business intelligence de autoatendimento, os principais objetivos da governança são:

- Capacitar a comunidade de usuários internos a ser produtiva e eficiente.
- Estar em conformidade com os regulamentos do setor, do governo e contratuais da organização.
- Cumprir os requisitos internos da organização.

O equilíbrio ideal entre o controle e a capacitação será diferente entre as organizações. Também é provável que ele seja diferente entre diferentes unidades de negócios em uma organização. Com uma plataforma como o Power BI, você será mais bem sucedido quando enfatizar ao máximo a capacitação do usuário quanto ao esclarecer seu uso prático dentro de limites estabelecidos.


Estratégia de governança

Ao considerar a governança de dados em qualquer organização, o melhor ponto de partida é definir uma estratégia de governança. Ao focar primeiro as metas estratégicas de governança de dados, todas as decisões detalhadas ao implementar políticas de governança e processos podem ser informadas pela estratégia. Por sua vez, a estratégia de governança será definida pela cultura de dados da organização.

Decisões de governança são implementadas com diretrizes, políticas e processos documentados. Os objetivos da governança de uma plataforma de BI como o Power BI incluem:

- Capacitar as pessoas em toda a organização a usar dados e tomar decisões dentro dos limites definidos.
- Garantir que o uso de dados seja apropriado para as necessidades dos negócios.
- Garantir que a propriedade de dados e as responsabilidades de administração sejam claras.
- Aprimorar a experiência do usuário fornecendo diretrizes claras e transparentes (com o mínimo de fricção) sobre quais ações são permitidas, por quê e como.
- Aprimorar a consistência e a padronização do trabalho que usa dados entre limites organizacionais.
- Reduzir o risco de vazamento de dados e de uso indevido de dados.
- Atender aos requisitos regulatórios, industriais e internos para o uso adequado dos dados.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18711	Instrução	1.1	Emerson Cardoso	01/04/2022	13 de 31

 Uso Interno	Tipo de Documento:	Especificação Técnica
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Requisitos de Segurança da Informação – PowerBI

Fatores de sucesso de governança


A governança não é bem recebida quando se trata de mandatos de cima para baixo que se concentram mais em controle do que em capacitação. O controle do Power BI é mais bem-sucedido quando:

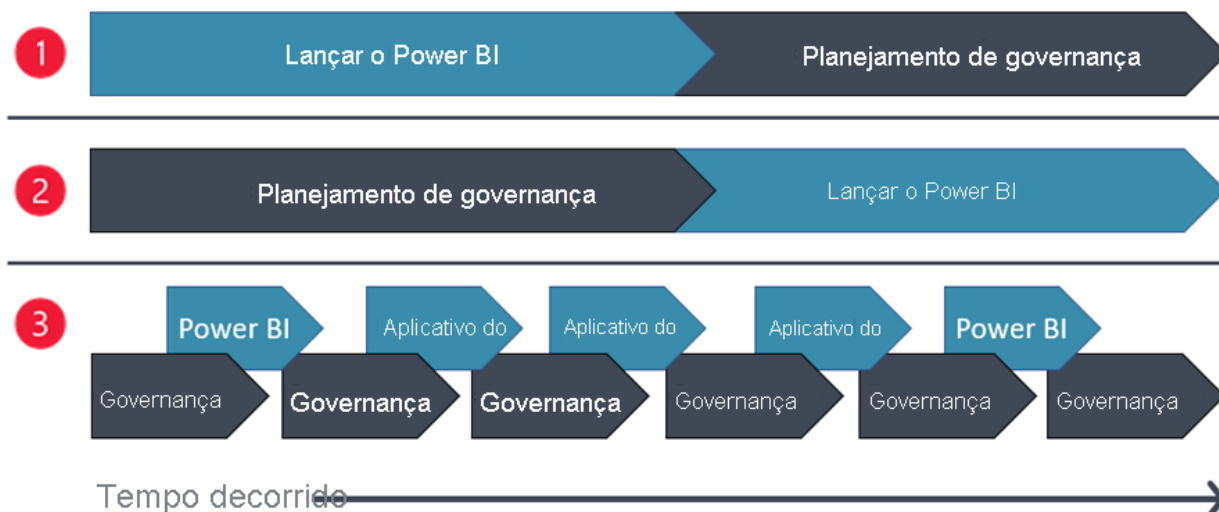
- O modelo de governança mais leve que atinge os objetivos necessários é usado.
- A governança é abordada de modo iterativo e não impede significativamente a produtividade.
- Uma abordagem de baixo para cima para formular diretrizes de governança é usada sempre que viável. O COE (centro de excelência) e/ou a equipe de governança de dados observam comportamentos bem-sucedidos que estão ocorrendo e, em seguida, executam ações para formalizar e escalar esses métodos com base nas lições aprendidas.
- As decisões de governança são definidas com a contribuição de diferentes unidades de negócios antes que elas sejam aplicadas. Embora haja ocasiões em que uma diretiva específica é necessária (particularmente em setores altamente regulamentados), as determinações devem ser a exceção, não a regra.
- As necessidades de governança são equilibradas com flexibilidade e a capacidade de serem produtivas.
- Os requisitos de governança podem ser cumpridos como parte do fluxo de trabalho regular dos usuários, tornando mais fácil para as pessoas fazerem a coisa certa do jeito certo com pouco conflito.
- A resposta a novas solicitações de dados não tem "não" como padrão, mas "sim e", com regras claras, simples e transparentes quanto a quais são os requisitos de governança para acesso, uso e compartilhamento de dados.
- Os usuários que precisam de acesso aos dados têm incentivo para fazer isso por meio de canais normais, em conformidade com os requisitos de governança, em vez de contorná-los.
- Decisões de governança, políticas e requisitos para os usuários seguir estão alinhados com metas de cultura de dados organizacionais, bem como outras iniciativas de governança de dados.
- Decisões que afetam o que os usuários e criadores podem e não podem fazer não são compostas unicamente por um administrador nem de modo isolado.

Introdução à governança para sua organização

Há três métodos de tempo principais que as organizações adotam ao introduzir a governança do Power BI para uma organização.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18711	Instrução	1.1	Emerson Cardoso	01/04/2022	14 de 31

 <i>Uso Interno</i>	Tipo de Documento:	Especificação Técnica
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Requisitos de Segurança da Informação – PowerBI



Os métodos no diagrama acima incluem:

Método Estratégia seguida

Distribuir o Power BI primeiro e depois introduzir governança: o Power BI é disponibilizado amplamente para os usuários da organização como uma nova ferramenta de BI de autoatendimento. Em seguida, em algum momento no futuro, um esforço de governança começa. Esse método prioriza a agilidade.

Primeiro planejamento de governança total, depois, distribuir o Power BI: o amplo planejamento de governança ocorre antes de permitir que os usuários comecem a usar o Power BI. Esse método prioriza o controle e a estabilidade.

Planejamento de governança iterativa com distribuições do Power BI em fases: de início, ocorre apenas o planejamento de governança suficiente. Depois o Power BI é distribuído de modo iterativo em fases para equipes individuais enquanto os aprimoramentos de governança iterativo ocorrem. Esse método prioriza igualmente a agilidade e a governança.

Escolha o método 1 quando o Power BI já estiver sendo usado para cenários de autoatendimento e você estiver pronto para começar a trabalhar da maneira mais eficiente.


Escolha o método 2 quando sua organização já tiver uma abordagem bem estabelecida para governança que pode ser prontamente expandida para incluir o Power BI.

Escolha o método 3 quando você quiser fornecer o maior grau de flexibilidade e agilidade. Essa abordagem equilibrada é a melhor opção para a maioria das organizações e cenários.

Método 1: distribuir o Power BI primeiro

O método 1 prioriza a agilidade e a velocidade. Ele permite que os usuários comecem a criar soluções rapidamente. Esse método ocorre quando o Power BI se tornou amplamente disponível para os usuários da organização como uma nova ferramenta de BI de autoatendimento. Ganhos rápidos e alguns sucessos são alcançados. Em algum momento no futuro, um esforço

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18711	Instrução	1.1	Emerson Cardoso	01/04/2022	15 de 31

 Uso Interno	Tipo de Documento:	Especificação Técnica
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Requisitos de Segurança da Informação – PowerBI

de governança começa, geralmente para levar ordem a um nível inaceitável de caos, já que a população de usuário de autoatendimento não recebeu diretrizes suficientes.

Vantagens:

- Mais rápido para começar.
- Usuários altamente capacitados podem concluir as tarefas rapidamente.
- Ganhos rápidos são obtidos.

Desvantagens:

- Maior esforço para estabelecer governança, já que o Power BI é usado predominantemente em toda a organização.
- Resistência de usuários de autoatendimento que são solicitados a alterar o que eles estavam fazendo.
- Na ausência de um plano estratégico, os usuários de autoatendimento são obrigados a descobrir as coisas por conta própria.

Método 2: planejamento de governança aprofundado primeiro

O método 2 prioriza o controle e a estabilidade. Ele está na extremidade oposta do espectro do método 1. O método 2 envolve o amplo planejamento de governança antes da distribuição do Power BI. É mais provável que essa situação ocorra quando a implementação do Power BI é conduzida pela TI. Também é provável que ocorra quando a organização opera em um setor altamente regulamentado ou quando existe um painel de controle de dados que impõe pré-requisitos e requisitos significativos.

Vantagens:

- Mais bem preparado para atender aos requisitos regulatórios.
- Mais bem preparado para dar suporte à comunidade de usuários.

Desvantagens:

- Favorece a BI corporativo mais do que a BI de autoatendimento.
- Mais lento para permitir que a população do usuário comece a obter valor e melhore a tomada de decisões.
- Incentiva os hábitos e as soluções alternativas insatisfatórias quando há um atraso significativo na permissão de uso de dados para tomada de decisões.

Método 3: governança iterativa com distribuições


O método 3 busca um equilíbrio entre agilidade e governança. É um cenário ideal que faz o planejamento de governança apenas *suficiente*. Melhorias de governança frequentes e contínuas ocorrem de modo iterativo ao longo do tempo junto com projetos de desenvolvimento do Power BI que agregam valor.

Vantagens:

- Dá igual prioridade à governança e à produtividade do usuário.
- Enfatiza uma mentalidade de *aprendizado durante o processo*.
- Incentiva a distribuição para grupos em fases.

Desvantagens:

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18711	Instrução	1.1	Emerson Cardoso	01/04/2022	16 de 31

 <i>Uso Interno</i>	Tipo de Documento:	Especificação Técnica
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Requisitos de Segurança da Informação – PowerBI

- Requer que um alto nível de comunicação seja bem-sucedido com as práticas de governança Agile.
- Esse nível de agilidade requer mais disciplina para manter a documentação e o treinamento atualizados.
- A introdução de novas diretrizes de governança e políticas muitas vezes causa um certo nível de interrupção do usuário.

Desafios da governança

Se sua organização tiver implementado o Power BI sem uma abordagem de governança ou uma direção estratégica (conforme descrito acima pelo método 1), poderá haver vários desafios que exigem atenção. Dependendo da abordagem que você executou e do seu estado atual, alguns dos desafios a seguir podem ser aplicáveis à sua organização.

Desafios de estratégia

- Ausência de uma estratégia de controle de dados coesa alinhada com a estratégia de negócios.
- Ausência de suporte executivo para o controle de dados como um ativo estratégico.
- Planejamento de adoção insuficiente para aprimorar a adoção e o nível de maturidade da BI e da análise.

Desafios de pessoas

- Ausência de prioridades alinhadas entre equipes centralizadas e unidades de negócios.
- Ausência de líderes identificados com conhecimento e entusiasmo suficientes em todas as unidades de negócios para impulsionar os objetivos de adoção organizacional.
- Ausência de conscientização quanto às melhores práticas de autoatendimento.
- Resistência a seguir as diretrizes e políticas de governança que acabam de ser introduzidas.
- Esforço duplicado gasto em unidades de negócios.
- Ausência de responsabilidade, funções e atribuições claras.


Desafios do processo

- Ausência de processos claramente definidos, resultando em caos e inconsistências.
- Ausência de padronização ou repetição.
- Capacidade insuficiente para se comunicar e compartilhar lições aprendidas.
- Ausência de documentação e excesso de confiança no conhecimento de tribal.
- Incapacidade de cumprir os requisitos de segurança e privacidade.

Desafios de qualidade de dados e gerenciamento de dados

- Acúmulo de dados e relatórios.
- Dados imprecisos, incompletos ou desatualizados.
- Ausência de confiança nos dados, especialmente para conteúdo de autoatendimento.
- Relatórios inconsistentes produzidos sem validação de dados.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18711	Instrução	1.1	Emerson Cardoso	01/04/2022	17 de 31

 Uso Interno	Tipo de Documento:	Especificação Técnica
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Requisitos de Segurança da Informação – PowerBI

- Dados valiosos não usados ou difíceis de acessar.
- Conjuntos de dados fragmentados, em silos e duplicados.
- Ausência de catálogo de dados, inventário, glossário ou linhagem.
- Falta de clareza na propriedade e na administração de dados.

Desafios de habilidades e conhecimento de dados

- Níveis variados de capacidade para interpretar, criar e se comunicar com os dados de modo eficaz.
- Níveis variados de habilidades técnicas e lacunas de habilidades.
- Ausência de capacidade para gerenciar com segurança a diversidade e o volume de dados.
- Subestimar o nível de complexidade do desenvolvimento e do gerenciamento de soluções de BI em todo o ciclo de vida.
- Curta permanência com contínuas transferências e rotatividade da equipe.
- Lidar com a velocidade da mudança para serviços de nuvem.

Planejamento de governança

Para organizações que implementaram o Power BI sem uma abordagem de governança ou direção estratégica (conforme descrito acima pelo método 1), o esforço para iniciar o planejamento de governança pode ser assustador.

Se um corpo de governança formal não existir atualmente em sua organização, o foco do planejamento de governança e dos esforços de implementação será mais amplo. No entanto, se houver um painel de governança de dados existente na organização, seu foco será principalmente a integração às práticas existentes e personalizá-las para acomodar os objetivos de BI de autoatendimento e BI corporativa.

Importante

A governança é uma grande tarefa e nunca está totalmente *concluída*. Priorizar e iterar de modo incansável as melhorias tornará o escopo mais gerenciável. Se você acompanhar seu progresso e realizações a cada semana e a cada mês, ficará surpreso com o decorrer do tempo.


Algumas atividades possíveis de planejamento de governança e saídas que você pode considerar importantes são descritas a seguir.

Estratégia

Principais atividades:

- Avaliar o estado atual da cultura de dados, da adoção e das práticas de BI.
- Realizar uma série de sessões de coleta de informações para definir o estado futuro desejado, a visão estratégica, as prioridades e os objetivos para a cultura de dados, a adoção e as práticas de BI. É uma abordagem útil se você ainda não tem um método estruturado para a coleta de informações.
- Validar o foco e o escopo do programa de governança.
- Identificar iniciativas de baixo para cima em andamento.
- Identificar dificuldades, problemas e riscos imediatos.
- Instruir a liderança sênior sobre governança e verificar se o suporte executivo é suficiente para sustentar e expandir o programa.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18711	Instrução	1.1	Emerson Cardoso	01/04/2022	18 de 31

 <i>Uso Interno</i>	Tipo de Documento:	Especificação Técnica
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Requisitos de Segurança da Informação – PowerBI

- Esclarecer como o Power BI se encaixa na estratégia geral de dados e análise para a organização.
- Avaliar fatores internos, como preparação organizacional, níveis de maturidade e desafios importantes.
- Avaliar fatores externos como risco, exposição, regulamentação e requisitos legais, incluindo diferenças regionais.

Principais resultados:

- Caso de negócios com análise de custo/benefício.
- Objetivos de governança, foco e prioridades aprovados que estão em alinhamento com os objetivos de negócios de alto nível.
- Planejar objetivos e prioridades de curto prazo. Eles são ganhos rápidos.
- Planejar metas e prioridades de longo prazo e adiadas.
- Critérios de sucesso e KPIs (indicadores chave de desempenho).
- Riscos conhecidos documentados com um plano de mitigação.
- Planejar os requisitos do setor de reuniões, governamentais, contratuais e regulatórios que afetam o BI e a análise na organização.
- Plano de financiamento.

Pessoas

Principais atividades:

- Estabelecer um conselho de governança e identificar as principais partes interessadas.
- Determinar o foco, o escopo e um conjunto de responsabilidades para o conselho de governança.
- Estabelecer um COE.
- Determinar o foco, o escopo e um conjunto de responsabilidades para o COE.
- Funções e responsabilidades.
- Confirmar quem tem autoridade para tomada de decisão, aprovação e veto.

Principais resultados:


- Estatuto do conselho de governança.
- Estatuto do COE.
- Plano de alocação de equipe.
- Funções e responsabilidades.
- Matriz de responsabilidade e tomada de decisão.
- Plano de comunicação.
- Plano de gerenciamento de problemas.

Políticas e processos

Principais atividades:

- Analisar dificuldades imediatas, problemas, riscos e áreas para melhorar a experiência do usuário.
- Priorizar as políticas de dados a serem resolvidas por ordem de importância.
- Identificar os processos em vigor que funcionam bem e podem ser formalizados.
- Determinar como novas políticas de dados serão socializadas.
- Decidir até que ponto as políticas de dados podem ser diferentes ou personalizadas para grupos diferentes.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18711	Instrução	1.1	Emerson Cardoso	01/04/2022	19 de 31

 <i>Uso Interno</i>	Tipo de Documento:	Especificação Técnica
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Requisitos de Segurança da Informação – PowerBI

Principais resultados:

- Processo de como as políticas de dados e a documentação serão definidas, aprovadas, comunicadas e mantidas.
- Planejar a solicitação de exceções e desvios válidos de políticas documentadas.

Gerenciamento de projeto

A implementação do programa de governança deve ser planejada e gerenciada como uma série de projetos.

Principais atividades:

- Estabelecer uma linha do tempo com prioridades e marcos.
- Identificar iniciativas e dependências relacionadas.
- Identificar e coordenar as iniciativas de baixo para cima existentes.
- Criar um plano de projeto iterativo alinhado com priorização de alto nível.
- Obter aprovação e fundos de orçamento.
- Estabelecer uma forma tangível de acompanhar o progresso.

Principais resultados:

- Projetar o plano com iterações, dependências e sequenciamento.
- Ritmo para retrospectivas com foco em melhorias contínuas.

Políticas de governança


Critérios de decisão

Todas as decisões de governança devem estar alinhadas com as metas estabelecidas para a adoção organizacional. Depois que a estratégia for clara, mais decisões de governança tática precisarão ser tomadas, o que afetará as atividades diárias da comunidade de usuários de autoatendimento. Esses tipos de decisões táticas se correlacionam diretamente às políticas de dados criadas.

A maneira como vamos tomar decisões de governança depende de:

- **Quem detém e gerencia o conteúdo de BI?** Quem detém e gerencia o conteúdo tem um impacto significativo nos requisitos de governança.
- **Qual é a área do titular dos dados?** Os dados em si, incluindo seu nível de sensibilidade, são um fator importante. Alguns domínios de dados inerentemente exigem controles mais rígidos. Por exemplo, PII (informações de identificação pessoal) ou dados sujeitos a regulamentos devem estar sujeitos a requisitos de governança mais rígidos do que dados menos confidenciais.
- **Os dados e/ou a solução de BI são considerados críticos?** Se você não puder tomar uma decisão informada facilmente sem esses dados, você está lidando com elementos de dados críticos. Determinados relatórios e aplicativos podem ser considerados críticos porque atendem a um conjunto de critérios predefinidos. Por exemplo, o conteúdo é entregue aos executivos. Critérios predefinidos para o que é considerado *crítico* ajudam todos a ter expectativas claras. Os dados críticos geralmente estão sujeitos a requisitos de governança mais rígidos.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18711	Instrução	1.1	Emerson Cardoso	01/04/2022	20 de 31

 <i>Uso Interno</i>	Tipo de Documento:	Especificação Técnica
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Requisitos de Segurança da Informação – PowerBI

Principais decisões de governança do Power BI

À medida que você explorar suas metas e objetivos e buscar decisões mais táticas de governança de dados, conforme descrito acima, será importante determinar quais são as prioridades mais altas. Decidir em que concentrar seus esforços pode ser um desafio.

A seguinte lista inclui itens que você pode optar por priorizar ao introduzir governança para Power BI:

- Recomendações e requisitos para propriedade de conteúdo e propriedade.
- Recomendações requisitos para o escopo de entrega de conteúdo.
- Recomendações requisitos para distribuição e compartilhamento de conteúdo com colegas, bem como para usuários externos, como clientes, parceiros ou fornecedores.
- Atividades permitidas contendo dados regulamentados e dados altamente confidenciais.
- Permitido o uso de fontes de dados não verificadas desconhecidas pela TI e/ou recomendações para fontes de dados que recebem manutenção manual.
- Como gerenciar workspaces com eficiência.
- Quem pode ser um administrador do Power BI.
- Requisitos de segurança, privacidade e proteção de dados e ações permitidas para artefatos de dados atribuídos a cada rótulo de confidencialidade.
- Uso permitido ou incentivado de gateways pessoais.
- Uso permitido ou incentivado de compra por autoatendimento de licenças de usuário.
- Requisitos para quem pode certificar artefatos de dados, bem como requisitos que devem ser atendidos.
- Gerenciamento do ciclo de vida do aplicativo para gerenciar conteúdo durante todo o ciclo de vida, incluindo fases de desenvolvimento, teste e produção.
- Requisitos adicionais aplicáveis ao conteúdo crítico, como verificações de qualidade de dados e documentação.
- Requisitos para usar dados mestres padronizados e dados comuns para garantir a consistência.
- Recomendações e requisitos para uso de ferramentas externas.


Se você não tomar decisões de governança e comunicá-las corretamente, as pessoas usarão os próprios critérios para saber como as coisas devem funcionar, e isso geralmente resulta em abordagens inconsistentes para tarefas comuns. Embora nem todas as decisões de governança precisem ser tomadas com antecedência, é importante identificar as áreas de maior risco na organização. Em seguida, implemente incrementalmente políticas e processos de governança que proporcionarão mais impacto.

Funções e responsabilidades

Quando tiver uma noção da estratégia de governança, as funções e as responsabilidades deverão ser definidas para estabelecer expectativas claras.

A estrutura da equipe de governança, as funções (incluindo a terminologia) e as responsabilidades variam muito entre as organizações. Funções muito generalizadas são


N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18711	Instrução	1.1	Emerson Cardoso	01/04/2022	21 de 31

 <i>Uso Interno</i>	Tipo de Documento:	Especificação Técnica
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Requisitos de Segurança da Informação – PowerBI

descritas abaixo. Em alguns casos, a mesma pessoa pode atender a várias funções. Por exemplo, o CDO (diretor de dados) também pode ser o responsável executivo.

Função	Descrição
Diretor de dados ou diretor de análise	Define a estratégia para uso de dados como um ativo corporativo. Supervisiona políticas e diretrizes de governança de toda a empresa.
Quadro de governança de dados	Comitê de capacitação com membros de cada unidade de negócios que, como proprietários de domínio, são capacitados a tomar decisões de governança corporativa. Eles tomam decisões em nome da unidade de negócios e no melhor interesse da organização. Fornece aprovações, decisões, prioridades e direção para a equipe de governança de dados corporativos e os comitês de trabalho.
Equipe de governança de dados	Cria políticas de governança, padrões e processos. Fornece supervisão e otimização de dados de toda a empresa, confiabilidade, privacidade e usabilidade. Colabora com o COE para fornecer educação, suporte e orientação de governança para proprietários de dados e criadores de conteúdo.
Comitês de trabalho de governança de dados	Equipes temporárias ou permanentes que se concentram em tópicos de governança individuais, como segurança ou qualidade de dados.
Conselho de gerenciamento de alterações	Coordena os requisitos, os processos, as aprovações e o agendamento para processos de gerenciamento de versão com o objetivo de reduzir o risco e minimizar o impacto das alterações em aplicativos críticos.
Gerenciamento de projeto	Gerencia projetos de governança individuais e o programa de governança de dados em andamento.
Responsável executivo do Power BI	Promove a adoção e o uso bem-sucedido do Power BI. Garante ativamente que decisões sobre o Power BI estejam consistentemente alinhadas com objetivos de negócios, princípios orientadores e políticas entre limites organizacionais.
Centro de excelência	Orienta a comunidade de criadores e consumidores para promover o uso efetivo do Power BI para tomada de decisões. Fornece coordenação entre departamentos de atividades do Power BI para melhorar as práticas, aumentar a consistência e reduzir as ineficiências.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18711	Instrução	1.1	Emerson Cardoso	01/04/2022	22 de 31

 <i>Uso Interno</i>	Tipo de Documento:	Especificação Técnica
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Requisitos de Segurança da Informação – PowerBI

Função	Descrição
Líderes do Power BI	Um subconjunto de criadores de conteúdo encontrado nas unidades de negócios que ajudam a promover o avanço da adoção do Power BI. Eles contribuem para o crescimento da cultura de dados ao defender o uso de melhores práticas e ajudar ativamente colegas.
Administradores do Power BI	Responsabilidades diárias de supervisão do sistema para dar suporte a processos internos, ferramentas e pessoas. Lida com monitoramento, auditoria e gerenciamento.
Tecnologia da Informação	Fornecer assistência ocasional para administradores do Power BI para serviços relacionados ao Power BI, como Azure Active Directory, Microsoft 365, Teams, SharePoint ou OneDrive.
Gerenciamento de riscos	Examina e avalia o compartilhamento de dados e os riscos de segurança. Define padrões e políticas de dados éticos. Comunica requisitos regulatórios e legais.
Auditoria interna	Auditoria de conformidade com requisitos regulatórios e internos.
Administrador de dados	Colabora com o comitê de governança e/ou o COE para garantir que os dados organizacionais tenham níveis aceitáveis de qualidade de dados.
Todos os criadores e consumidores de BI	Adere às políticas para garantir que os dados estejam seguros, protegidos e bem gerenciados como um ativo organizacional.


6.3. Recomendações de Segurança

As recomendações de segurança descritas neste documento serão separadas em diferentes tópicos. Cada um deles será explorado a fim de que o leitor possa entender e consiga utilizar as recomendações no projeto no qual foi designado.

Abaixo são descritos os tópicos:

- Melhores Práticas de Segurança
- Gestão de Acessos
- Compartilhamento e armazenamento
- Gestão de Riscos
- Registros de Auditoria e Monitoração
- Worspace, Espaço de Trabalho
- DLP
- CASB
- Gateways de fontes de dados
- Integração

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18711	Instrução	1.1	Emerson Cardoso	01/04/2022	23 de 31


 <i>Uso Interno</i>	Tipo de Documento:	Especificação Técnica
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Requisitos de Segurança da Informação – PowerBI

6.4. Melhores Práticas de Segurança

Visando garantir um maior nível de segurança na utilização da ferramenta, recomendamos que minimamente seja realizado, siga e comprove as melhores práticas de mercado, sendo elas:

- a. Classificar e rotular dados do Power BI como Confidenciais, caso tenha dúvidas sobre como tratar esse tipo de informação, consultar a GED 18744 - Classificação da Informação.
- b. Impor políticas de governança mesmo quando o conteúdo do Power BI é exportado para Excel, PPT ou PDF.
- c. Monitore e proteja a atividade do usuário em dados confidenciais em tempo real, incluído com alertas.
- d. Capacite os administradores de segurança que usam relatórios de proteção de dados.
- e. Considere o seu público-alvo, procure desenvolver um painel dinâmico e com foco.
- f. Conte uma história em uma tela, tente inserir todas as informações necessárias em tela única.
- g. Ao apresentar o dashboard, exiba-o no modo de tela inteira, sem distrações.
- h. Destaque as informações mais importantes utilizando tamanhos de fontes diferenciados.
- i. Tenha definido um key User por área de negócio que responsável por criar os workspaces da área;
- j. Para conceder acesso no relatório e/ou dashboard do Power BI deve sempre especificar nominalmente as pessoas que deverão possuir acesso, para não ocorrer acesso indevido nas informações. Crie grupos para facilitar o permissionamento;
- k. É proibido publicar relatórios e dashboards do Power BI para a Internet e usuários externos, devido aos riscos de segurança da informação;
- l. Considere desativar o recurso de exportação de dados em seu relatório ou dashboard, a menos que seja extremamente necessário com as pessoas que deverão possuir acesso;
- m. Publicar apenas o dado que será utilizado. Antes de utilizar dados pessoais ou confidenciais em suas atividades de negócio ou de acessá-las, busque sempre

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18711	Instrução	1.1	Emerson Cardoso	01/04/2022	24 de 31

 <i>Uso Interno</i>	Tipo de Documento:	Especificação Técnica
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Requisitos de Segurança da Informação – PowerBI

minimizar os dados, ou seja, utilizar somente dados necessários para atingir a finalidade;

- n. A ferramenta possui mecanismos de proteção em que identifica comportamentos suspeitos e gera alertas de riscos.

6.4.1. Gestão de Acessos


Este tópico visa abordar os requisitos mínimos recomendáveis para garantir o bom funcionamento do ciclo de vida da identidade de um usuário ao Power BI e, além disso, garantir um nível de segurança adequado no acesso à console:

- a. Autenticação multifatorial (MFA) estar ativado;
- b. Restringir acesso de usuários de dispositivos não corporativos, conforme rollout Intune.
- c. Toda e qualquer atividade de solicitação, aprovação, criação, alteração, bloqueio, desbloqueio e deleção da dados na solução deverá ser registrada em logs de auditoria para posteriormente ser consumido pela ferramenta de SIEM da CPFL;
- d. A solução deverá possuir de maneira previa, uma segregação de funções para a administração e uso das funcionalidades da própria solução;
- e. A solução deve garantir o conceito de Least Privilege, ou seja, privilégio mínimo para os usuários, sendo esses da área contratante ou do provedor;
- f. A solução deverá implementar mecanismos que permita a utilização do modelo Just-In-Time Access garantindo o acesso privilegiado temporário para usuários previamente autorizados;
- g. Não devem ser utilizados mecanismos de autenticação considerados abertos (open), tais como Open Id ou Open Authentication;

6.4.2. Compartilhamento e armazenamento

- a. Desativar a configuração 'Compartilhar conteúdo com usuários externos' no Portal de administração - se essa opção for deixada ativada, seus relatórios do Power BI serão liberados para o público externo;
- b. Desabilitar a configuração 'Publicar na web' também - se for deixada ativada, o Power BI publicará seus relatórios na Internet. Considere desativar a publicação para toda a organização. Ter grupo de exceção;

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18711	Instrução	1.1	Emerson Cardoso	01/04/2022	25 de 31

 Uso Interno	Tipo de Documento:	Especificação Técnica
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Requisitos de Segurança da Informação – PowerBI


- c. Restringir exportar dados, considere desativar o recurso de 'exportação de dados', a menos que seja extremamente necessário;
- d. Monitorar os dados exportados;
- e. Qual tipo de filtro o relatório e/ou dashboard terá, será ou não de forma dinâmica.
- f. Compartilhar dentro da organização deve especificar as pessoas;
- g. Compartilhamento externo para fora da organização irá ocorrer quando o usuário tiver permissão para compartilhar externo, mas deverá especificar as pessoas nominalmente;
- h. Bloquear acessos de convidados.
- i. As informações classificadas como Confidencial/Uso Interno não devem estar disponíveis ao acesso público;
- j. Deve-se adotar criptografia de dados armazenados em backup.
- k. Deve-se garantir que haja a segregação adequada dos dados armazenados e processados;
- l. Os dados de produção não devem ser replicados ou utilizados em ambientes que não sejam de produção, como por exemplo, homologação e desenvolvimento;
- m. Deve-se garantir processo de homologação de novos aplicativos ou serviços e este deve ser documentado;

6.4.3. Gestão de Riscos

Este tópico refere-se à análise e a gestão de risco que deve ser realizada periodicamente pelas equipes de segurança da informação da CPFL. Nestes casos, a área que utiliza a ferramenta deve ter conhecimento e ler atentamente a normativa de Gestão de Riscos vigente. Abaixo serão descritos algumas diretrizes para auxiliar na análise.

- a. Não criar workspace sem a permissão do responsável pela área (Key User);
- b. Não publicar dashboards com link público;
- c. Não conectar em bases de dados usando o gateway local;
- d. Não compartilhar dashboards usando o workspace pessoal;
- e. Não armazenar seu arquivo pbix em sua máquina local. Sempre usar o Azure (Key User);

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18711	Instrução	1.1	Emerson Cardoso	01/04/2022	26 de 31

 Uso Interno	Tipo de Documento:	Especificação Técnica
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Requisitos de Segurança da Informação – PowerBI

- f. Não consumir dados locais como Excel, arquivos de texto e outros para construir dashboards;
- g. Não compartilhar arquivos pbix, nem internamente e nem externamente.

6.4.4. Registros de Auditoria e Monitoração

- a. Configurar o registro de auditoria para rastreabilidade;
- b. Configurar a retenção dos logs de maneira on-line por pelo menos 6 (seis) meses;
- c. Devem estar legíveis para análise ou auditoria, ou seja, os arquivos de logs devem fornecer informações completas sobre origem e destino do usuário, a data/hora precisam estar corretas e sincronizadas com todos os sistemas/aplicações no qual fazem parte. Devem fornecer completa rastreabilidade entre os respectivos usuários;
- d. Os administradores não devem possuir permissão para realizar a exclusão ou desativação dos registros de log;

6.4.5. Worspace, Espaço de Trabalho

- a. Adicionar por grupos de usuários aos espaços de trabalho, ou por usuário;
- b. Atribuir aos usuários suas funções e privilégios como visualizador, contribuidor, membro ou administrador;
- c. Implementar um modelo de "least-privilege administrative".


6.4.6. DLP

- a. Configurar a ativação das regras de DLP;
- b. Configurar que os rótulos de confidencialidade fiquem ativados.
- c. Deve-se verificar a possibilidade de integração com sistemas de correlação de eventos, DLP, IDS/IPS, SOC (Security Operation Center) da CPFL.

6.4.7. CASB

- a. Criar políticas de sessão para monitorar atividades do Power BI;
- b. Alerta de compartilhamento suspeito e de exportação de relatórios no Power BI.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18711	Instrução	1.1	Emerson Cardoso	01/04/2022	27 de 31

 <i>Uso Interno</i>	Tipo de Documento:	Especificação Técnica
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Requisitos de Segurança da Informação – PowerBI

6.4.8. Gateways de Fontes de Dados

- Ter um gateway para gerenciar as fontes de dados;
- Capacidade de publicar um único relatório para sua base de usuários, mas expõe os dados de maneira diferente para cada pessoa.
- As permissões dessas fontes de dados podem ser gerenciadas pelo administrador do gateway;
- Segurança em Nível de Linha (RLS) e/ou Segurança em Nível de Objeto (OLS) podem ser implementados na fonte de dados, para permitir que os usuários exibam dados que têm privilégios para acessar;
- Para importar uma cópia dos dados das fontes de dados, garantir criptografia ativa nos armazenamentos: Armazenamento do Azure, Bancos de Dados SQL do Azure e Armazenamento de Blob do Azure.


6.4.9. Integração

- Utilização da conta de serviço O365;
- Usar para conectar o Power BI com a fonte de dados/sistema;
- Este usuário é responsável por gerenciar que outros usuários e grupos podem acessar os dados;
- Ativar MFA, mas precisa deixar com algum usuário essa validação de duplo fato de autenticação, com o gestor da área de negócio;
- Irá importar uma cópia dos dados para Power BI ou conectar-se diretamente à fonte de dados ? Analisar se aplica configurar separação do que cada tipo de usuário poderá visualizar nos relatórios (RLS - Row Level Security, regras podem ser aplicadas no workspace ou no relatório);
- Não possibilitar publicar para internet, e nem convidar usuários externos. Somente dentro da organização, domínio CPFL;
- Restringir download/exportar de relatórios/dados;
- Conceder permissão de acesso nominalmente as pessoas (governança).

6.5. Quais dados posso utilizar?

Basicamente qualquer tipo de dados de negócio. No entanto, deve-se ter cautela com as informações Confidenciais e em especial aos dados pessoais, tais como Nome, Documentos, Endereço, Código de Identificação tanto de colaboradores quanto de

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18711	Instrução	1.1	Emerson Cardoso	01/04/2022	28 de 31

 Uso Interno	Tipo de Documento:	Especificação Técnica
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Requisitos de Segurança da Informação – PowerBI

clientes, para não infringir a Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018 e as normas e procedimentos internos do **Grupo CPFL**.

Para maiores orientações das regras de segurança, consulte o Guia em: [Guia de Segurança da Informação.pdf \(cpfl.com.br\)](#)

6.6. Na tabela abaixo encontram-se os requisitos de segurança para o PowerBI.

Requisitos	Usuário restrito	Usuário adm	Usuário executivo	Prestador	Exceção	Porque
Somente visualização de dashboards	Sim	sim	Não	sim	sim	Evitar acesso indevido e vazamento de informações
Acesso somente dentro da Org.	Sim	sim	Sim	sim	NA	Evitar acesso indevido e vazamento de informações
Ativar MFA	Sim	sim	Sim	sim	NA	Melhorar as boas práticas de segurança
Download pro device corporativo, com MDM	Sim	sim	Sim	sim	NA	Melhorar as boas práticas de segurança
Desativar compartilhamento externo para fora da organização.	Sim	sim	Sim	sim	NA	Evitar acesso indevido e vazamento de informações
Restringir recurso de exporting data, liberar somente aos administradores	Sim	sim	Não	sim	NA	Evitar vazamento de informações
Ativar recurso de Row-Level Security (RLS) para restringir acesso dos usuários.	Sim	sim	Sim	sim	NA	Evitar acesso indevido e vazamento de informações
Ativar criptografia informações confidenciais em trânsito.	Sim	sim	Sim	sim	NA	Evitar vazamento de informações

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18711	Instrução	1.1	Emerson Cardoso	01/04/2022	29 de 31




Uso Interno

Tipo de Documento:	Especificação Técnica
Área de Aplicação:	Segurança da Informação
Título do Documento:	Requisitos de Segurança da Informação – PowerBI

Ativar criptografia dados confidenciais em repouso.	Sim	sim	Sim	sim	NA	Evitar vazamento de informações
Ativar log de auditoria.	Sim	sim	Sim	sim	NA	Para análise de segurança e tratamento de incidente
Ativar retenção do armazenamento de log para 90 dias.	Sim	sim	Sim	sim	NA	Para análise de segurança e tratamento de incidente
Ativar encaminhamento dos logs do Power BI para o SIEM.	Sim	sim	Sim	sim	NA	Para análise de segurança e tratamento de incidente
Restringir a implantação dos recursos por meio do Azure Policy.	Sim	sim	Sim	sim	NA	Melhorar as boas práticas de segurança
Ativar políticas de detecção de anomalias e transferência não autorizada de dados confidenciais no Microsoft Cloud App Security para o PowerBI.	Sim	sim	Sim	sim	NA	Para análise de segurança e tratamento de incidente
Ativar acesso privilegiado JIT (just-in-time) para as contas de administrador do Power BI.	Não	não	Não	não	sim (contas administrativas)	Melhorar as boas práticas de segurança
Ativar controle por chaves criptográficas no Power BI pelo Key Vault.	Sim	sim	Sim	sim	NA	Melhorar as boas práticas de segurança
Ativar rótulos de confidencialidade	Sim	sim	Sim	sim	s	Melhorar as boas práticas

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18711	Instrução	1.1	Emerson Cardoso	01/04/2022	30 de 31

 <i>Uso Interno</i>	Tipo de Documento:	Especificação Técnica
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Requisitos de Segurança da Informação – PowerBI

da Proteção de Informações para os seus relatórios, dashboards, conjuntos de dados e fluxos de dados para proteger o seu conteúdo confidencial contra acesso a dados não autorizado e vazamentos.						de segurança
---	--	--	--	--	--	--------------

7.CONTROLE DE REGISTROS

Identificação	Armazenamento e Preservação	Proteção (acesso)	Recuperação e uso	Retenção	Disposição
Requisitos de SI	Eletrônico (GED)	Restrição de acesso	Por tema ou título	Até a próxima atualização do documento	Substituição

8.ANEXOS

Não aplicável.

9.REGISTRO DE ALTERAÇÕES

9.4.Colaboradores

Empresa	Área	Nome
Paulista	EIS	Mateus Rocha

9.5.Alterações

Versão Anterior	Data da Versão Anterior	Alterações em relação à Versão Anterior
Não aplicável	Não aplicável	Documento em versão inicial
1.0	30/03/2022	Revisão geral do documento

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18711	Instrução	1.1	Emerson Cardoso	01/04/2022	31 de 31