Centro Universitário do Planalto Central Apparecido dos Santos - UNICEPLAC
Curso de Sistema de Informação
Trabalho de Conclusão de Curso

O uso de uma ferramenta de BI (Business Intelligence) aplicada ao processo de gerenciamento de risco em uma organização do setor público.

Gama-DF
2021

DAVID RAFAEL FERREIRA DA SILVA
MATHEUS VIANA DOS SANTOS
WALYSON MARTINS DOS SANTOS

O uso de uma ferramenta de BI (Business Intelligence) aplicada ao processo de gerenciamento de risco em uma organização do setor público.

Artigo apresentado como requisito para conclusão do curso de Bacharelado em Sistema de Informação pelo Centro Universitário do Planalto Central Apparecido dos Santos – Uniceplac.

Orientador: Prof. Me. Jorge Alberto dos Santos

Gama-DF

2021

DAVID RAFAEL FERREIRA DA SILVA
MATHEUS VIANA DOS SANTOS
WALYSON MARTINS DOS SANTOS

O uso de uma ferramenta de BI (Business Intelligence) aplicada ao processo de gerenciamento de risco em uma organização do setor público.

Artigo apresentado como requisito para conclusão do curso de Bacharelado em Sistema de Informação pelo Centro Universitário do Planalto Central Apparecido dos Santos – Uniceplac.

Gama, 14 de Junho de 2021.

Banca Examinadora

Prof. Me. Jorge Alberto dos Santos

Prof. Dr. Sebastião Ivaldo Carneiro Portela

Prof. Me. André Felix Freitas

O uso de uma ferramenta de BI (Business Intelligence) aplicada ao processo de gerenciamento de risco em uma organização do setor público.

David Rafael Ferreira da Silva
Matheus Viana Dos Santos
Walyson Martins dos Santos

Resumo:

O Gerenciamento de risco é uma área de conhecimento utilizada por muitas organizações públicas e privadas e proporciona uma análise e mapeamento de possíveis eventos, que possam gerar danos no ambiente organizacional. Neste trabalho acadêmico foi estudado o conceito de gestão de risco e observado o funcionamento de um sistema de controle de uma empresa pública, o qual possui uma ferramenta de BI (*Business Intelligence*) que possibilita analisar o passo a passo, identificar as causas e o nível de risco. A gestão dos processos que envolvem a organização é realizada com o objetivo de prevenir danos, ataques e prejuízos financeiros. O estudo demonstrou que a visualização por meio do dashboard com gráficos e tabelas, auxilia de forma significativa a camada de apresentação para melhores resultados e auxilia no processo de tomada de decisão.

Palavras-chave: Gerenciamento de Risco. *Business Intelligence.* Ambiente Organizacional. Empresa Pública.

Abstract:
Risk management is an area of knowledge used by many public and private associations and provides an analysis and mapping of possible events, which can cause damage to the organizational environment. In this academic work, the concept of risk management was studied and the functioning of a control system of a public company was observed, which has a BI (Business Intelligence) tool that makes it possible to analyze step by step, identify the causes and the level of risk. The management of the processes that involve an organization is carried out with the objective of preventing damages and financial losses. The study described that visualization through the panel with graphs and tables, significantly helps the presentation layer for better results and assists in the decision-making process.

Keywords: Risk Management. *Business Intelligence*, Organizational Environment. Public Company.

1. INTRODUÇÃO

A gestão de risco é um tópico emergente no atual cenário das empresas públicas, apresentando-se como uma área de conhecimento desafiadora do ponto de vista gerencial e técnico, uma vez que existe determinada necessidade organizacional para formular estratégias sólidas no sentido de identificar, registrar, tratar e administrar os riscos nas instituições da iniciativa pública.

O gerenciamento de riscos se aplicado de uma maneira estruturada e gerida de forma apropriada, pode proporcionar para as empresas do setor público uma possível melhoria em seus processos organizacionais, tendo como consequência positiva a elevação no desempenho dos serviços ofertados para a sociedade brasileira.

Na busca por atender as demandas crescentes das diversas áreas de negócio, mudanças nos serviços ou na estrutura organizacional podem ocorrer, acarretando riscos que podem colocar parcerias, contratos, investimentos, sistemas, serviços e produtos em situação vulnerável. No cenário apresentado, torna-se necessário estruturar um processo de gerenciamento de risco.

A gestão de riscos é um dos principais fatores para a sobrevivência de qualquer empresa, seja ela pública ou privada. Os bancos são exemplos de negócios estritamente alinhados ao gerenciamento de risco, que divulgam dados acerca das exposições de crédito e de mercado. Entretanto, também estão expostos a outros tipos de riscos, tais como o operacional e de imagem, os quais podem prejudicar, significativamente, seus negócios. Seguindo esta mesma linha de análise, as organizações da esfera pública precisam gerenciar seus riscos como medida de apoio ao atingimento de seus objetivos estratégicos.

Risco é a possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos. Pode ser uma oportunidade ou uma ameaça aos objetivos da organização, sendo que uma afeta negativamente e o outro, positivamente os objetivos do projeto (MONTEIRO, 2017).

O tema risco tornou-se uma preocupação atual entre empresas e organizações do setor público. Portanto, o problema de pesquisa deste trabalho está em torno de quais elementos são essenciais a serem considerados nos processos de gerenciamento de risco de uma empresa do setor público e como as ferramentas de *Business Intelligence* (BI) podem contribuir nesse processo.

Ao apresentar o problema de pesquisa, configura-se como objetivo geral articular o conhecimento teórico acerca do gerenciamento de riscos e sobre a utilização do BI para analisar uma situação prática dentro de uma empresa pública. Nesse sentido, esse trabalho acadêmico terá como referência os principais conceitos disponíveis na literatura sobre o processo de mapeamento, prevenção, identificação de causas e gestão de risco. Assim, o referido trabalho acadêmico está distribuído da seguinte forma: a) apresentação do processo gerenciamento de riscos e os detalhes pertinentes, b) conceituação de BI (Business Intelligence); c) análise dos dados; d) considerações finais.

2. GESTÃO DE RISCO

2.1 - Gerenciamento de Riscos

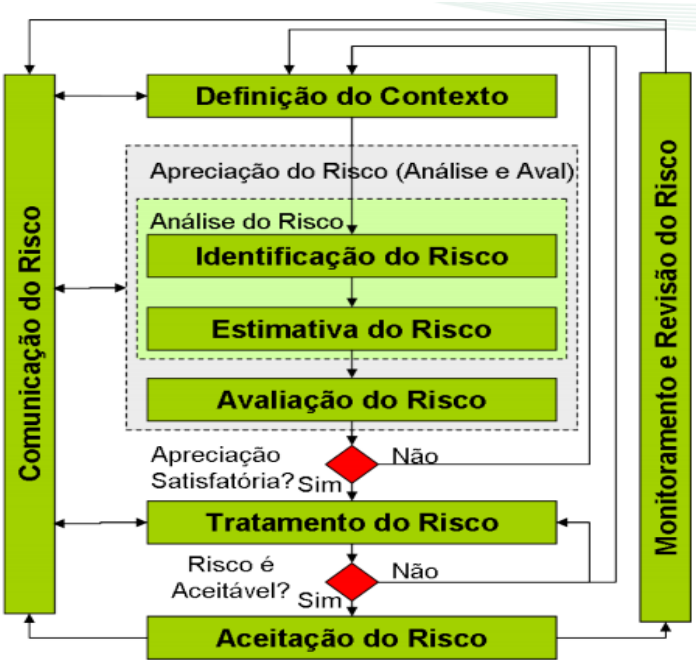
O gerenciamento de riscos não é uma prática nova e faz parte dos processos de negócios há muito tempo. Porém, o assunto começou a ganhar relevância em função da diversificação e

complexidade das atuais transações de negócios. Segundo o Instituto Brasileiro de Governança Corporativa - IBGC - (apud FRAPORTI et al., 2017)

> [...] o tema só começou a ganhar relevância no final do século XX, em virtude da globalização e do aumento da complexidade das companhias, instituições financeiras e organizações do terceiro setor. As práticas de gerenciamento de riscos, inicialmente, eram direcionadas à área de seguros, mas aos poucos foram se desenvolvendo como uma metodologia estruturada para as áreas de finanças, auditoria, estratégia e tecnologia da informação.

Entretanto, o processo de gestão de riscos de segurança tem ganhado uma nova configuração e maior destaque com as tecnologias da informação que disponibilizam sistemas capazes de identificar e comunicar com antecedência os momentos em que as instituições estão em ameaça. Além disso, os atuais sistemas são configurados dentro de uma estrutura lógica que avalia o risco e indica possíveis ataques. Conforme indicado na figura 1.

Figura 1 - Processo de gerenciamento de riscos



Fonte: Processo de gestão de riscos de segurança da informação (KONZEN, Marcos; FONTOURA, Lisandra; NUNES, Raul., 2012).

O detalhamento da figura 1 encontra-se nos próximos parágrafos.

Definição do Contexto

O entendimento do contexto de negócio da empresa é fundamental no processo de gestão de risco, pois garante o mapeamento do que é necessário ser protegido, seja uma informação, um produto, um software, dentre outros. Para Konzen et al (2012) o contexto define os objetivos, designa o escopo e os critérios de riscos, garantindo a identificação com precisão dos ativos que devem fazer parte da gestão de risco.

Identificação do Risco

Quando fazemos a listagem e mapeamento dos eventos de risco é necessário listar as possíveis causas e consequências de cada um desses eventos. Com base em Konzen et al(2012) “identificação do risco é identificar todos os eventos que possam causar grandes impactos potenciais, que possam trazer resultados negativos para atrapalhar e atrasar, ou melhorar o alcance dos objetivos.”

A identificação de riscos, de acordo com Wolmer (apud Fraporti et al., 2017) "requer a identificação de eventos indesejados, as suas causas e consequências (consequências no sentido de impacto que o risco poderá causar no objetivo)”. Então é um processo muito participativo, por que podem ser identificados novos riscos ao longo ciclo da organização.

Estimativa de Riscos

A estimativa de riscos tem uma combinação de repetições de eventos das hipóteses de acidentes e as suas decorrências. Na visão de Konzen (et al., 2012) “tem como objetivo atribuir o impacto e valores para as probabilidades e consequências de cada ameaça, no início da gestão de riscos, a estimativa do risco deve ser de alto nível, para evitar demora excessiva na apreciação”. Que inicialmente compreende pelo menos duas iterações para obter resultados satisfatórios, a norma apresenta algumas estratégias sobre como começar a realizar abordagem de alto nível na estimativa dos riscos.

Avaliação do Risco

Quando mensuram-se os eventos de riscos, é necessário ter medidas de tratamento para que sejam implementadas, sendo esses tratamentos: aceitar, mitigar, transferir, evitar. Do ponto

de Konzen (et al., 2012) “pode determinar a prioridade da ameaça, então com base nesta fase que podemos estabelecer o tratamento da vulnerabilidade, é neste momento que definimos se uma ameaça deve ser tratada ou não como uma prioridade”. Cada evento de risco precisa ser informado a forma de tratamento para que a organização tenha uma base do nível de risco.

Tratamento do Risco

De acordo com Konzen (et al., 2012) “o tratamento do risco é a fase da gestão de riscos, ela implementa controles para que possa reduzir, reter, transferir ou evitar os riscos. Uma vez que implementamos esse tratamento ele pode nos fornecer novos controles ou modificar os existentes”. As medidas de tratamento ela vem como uma sugestão do dirigente por sua implementação, são os gestores do risco.

Aceitação do Risco

Conforme a decisão de aceitação dos riscos seja tomada e justamente registrada em companhia com a responsabilidade pela decisão. Para Konzen et al(2012) "a aceitação de riscos é a fase em que podemos compreender os registros, o formal da decisão pelo aceite dos riscos residuais existentes na organização”. Então os riscos residuais formalmente aceitos pela empresa é uma forma para que possamos aprimorar um segundo plano para se obter todas as ações necessárias para resolver a situação.

Comunicação do risco

Para que as informações sobre riscos sejam compartilhadas entre o tomador de decisão e a todas as partes interessadas, tem como objetivo de atingir uma concordância sobre como os riscos devem ser tratados. Na visão de Konzen (et al., 2012):

> comunicação é o fluxo de informações dentro de uma entidade, ou seja, quando desenvolvemos a comunicação dos riscos para garantir que todos tenham consciência sobre os os riscos. É também um conjunto de atividades que são executadas, o objetivo da comunicação é fazer com que as informações sejam compartilhadas com os tomadores de decisão. Konzen (et al., 2012).

Monitoramento e Revisão do risco

O monitoramento é bastante importante na gestão de riscos, pois precisam ser monitorados todos os processos e analisados para que a empresa identifique novas oportunidades para o tratamento dos riscos.

Para Konzen (et al., 2012) “monitoramento e revisão do risco é a avaliação dos controles internos ao longo do tempo, sejam efetivos ou não. Podem ser contínuos ou pontuais, envolvendo autoavaliações, revisões e auditoria”.

Então todas as atividades de monitoramento e revisão de risco devem ser atualizadas para que possam ser feitas revisões para identificar modificações internas e externas que possam identificar modificar todo o contexto do processo da empresa.

2.2 Detalhamento da identificação de Risco

A (ABNT NBR ISO/IEC 27005) relata o detalhamento da identificação de risco como a “identificação do risco envolve a coleta de dados sobre vários elementos ou fatores e tem importância fundamental na gestão, que decompõe o risco em cinco fatores". Podendo avaliar os seguintes elementos:

A. Ativos;

B. Ameaças;

C. Vulnerabilidades;

D. Probabilidades;

E. Análise e impactos.

2.3 Ativos de Informação/Classificação

Conforme Konzen (et al., 2012) **“**um ativo é algo que tem valor para a organização e requer proteção”. onde há uma classificação entre ativos primários e suporte, onde os ativos primários de uma organização são:

A. Processos e Atividades do Negócio – onde agregam valores, executando o desempenho das funções.

B. Informações – onde são utilizadas para apoio dos processos.

A respeito das classificações de suporte, Conforme (FERNANDES, 2016) “As classificações de suporte são: hardware, software, rede, pessoal, sítio e estrutura organizacional”.

2.4 Análise de Ameaças

De acordo com a (ISO/IEC 27005) “uma fonte de ameaças é um agente ou condição que exercita ameaças. Ameaças podem ter como fonte os seres humanos e o ambiente.” Os seres humanos podem agir acidentalmente ou intencionalmente.

As origens das ameaças podem ser classificadas em:

A. humanas intencional;

B. humanas acidentais;

C. ambientais.

Com base na (ISO/IEC 27005):

As ameaças também podem ser organizadas quanto ao tipo:
A. Dano físico - Incidente com equipamento, tempo de uso.
B. Eventos naturais - Incidentes com fontes de água, do solo e ventos de ar;
C. Paralisação de serviços essenciais - Incidente em serviço de esgoto, água encanada, energia elétrica.
D. Interrupção por radiação - Incidentes causados por radiação térmica ou eletromagnética;
E. Ameaças da informação - Ataques, furto, cópia indevida, alteração de hardware ou software, destruição.
F. Falhas técnicas - Falhas, defeitos, saturação ou violação das condições de uso de equipamento em geral;
G. Ações não autorizadas – Utilização de máquinas ou equipamentos, cópia ou processamento ilegal de dados, acessos a dados;
H. Comprometimento de funções - Erro em utilização ou material, abuso de direitos, trabalho não realizado ou não concluído, indisponibilidade de pessoas.

2.5 Análise das Vulnerabilidades

Essa análise pode ser uma abertura na segurança, elas acontecem de várias formas falhas no desenvolvimento dos sistemas e etc. Para (Moreira, 2001) “a vulnerabilidade é o ponto onde qualquer sistema é suscetível a um ataque, ou seja, é uma condição encontrada em determinados recursos, processos, configurações etc.” Trata-se de uma condição causada, muitas vezes, pela ausência ou ineficiência das medidas de proteção utilizadas com o intuito de guardar os bens da empresa.

2.6 Análises de Probabilidades

Etapa que consiste em analisar as vulnerabilidades identificadas e determinar as probabilidades que irão ser exploradas.

Na (ISO/IEC 27005) “esses fatores podem contribuir na finalidade de ocorrer algum tipo de evento, e encontrar qual é a motivação da ameaça e a natureza da vulnerabilidade.” As classificações das vulnerabilidades podem ser, por exemplo: Alto, Médio, Baixo.

O quadro 1 a seguir detalha as classificações das vulnerabilidades apresentadas, sendo:

Quadro 1: Classificação dos níveis de vulnerabilidade

Nível	Definição
Alto	A fonte de ameaça está altamente motivada e possui conhecimento suficiente para a execução do ataque. Os controles de segurança para prevenir que a vulnerabilidade seja explorada são ineficazes.
Médio	A fonte de ameaça está motivada e possui conhecimento suficiente para execução do ataque. Os controles de segurança para prevenir que sejam eficazes.
Baixo	para execução do ataque. Os controles de segurança para prevenir que a vulnerabilidade seja explorada são eficazes.

Fonte: Ferreira; Araújo (2008, p.177).

2.7 Análise e Impactos

Para (STONEBURNER, 2002) “a análise de impacto é o passo principal do processo de avaliação de riscos e tem como objetivo determinar o resultado do impacto no negócio no caso de uma ameaça ter sucesso na exploração de uma determinada vulnerabilidade”.

Esta é uma importante etapa que estabelece uma determinação no impacto hostil, causado pelo invasor através de uma exploração de vulnerabilidades. As classificações dos impactos podem ser, por exemplo: Alto, Médio, Baixo.

O quadro 2 a seguir detalha as classificações dos impactos apresentadas, sendo:

Quadro 2: Classificação dos níveis de impacto

Nível	Definição
Alto	Perda significante dos principais ativos e recursos. Perda da reputação, imagem e credibilidade. Impossibilidade de continuar com atividades de negócio.
Médio	Perda dos principais ativos e recursos. Perda da reputação, imagem e credibilidade.
Baixo	Perda de alguns dos principais ativos e recursos. Perda da reputação, imagem e credibilidade.

Fonte: Ferreira; Araújo (2008, p.178).

Assim, é necessário conhecer a criticidade, o objetivo, e a sensibilidade dos sistemas e dos dados. Conforme (BARRETO, 2018)“todas estas informações podem ser obtidas em relatórios existentes na empresa, como, por exemplo, nos relatórios de validação de ativos críticos ou no relatório de análise de impacto no negócio”.

O impacto adverso de um evento pode ser descrito como a perda e/ou degradação da integridade, disponibilidade ou confidencialidade da informação. Impactos tangíveis podem ser mensurados quantitativamente utilizando-se uma unidade de medida conhecida, como: perda de

desempenhos, custos de manutenção ou tempo gasto para corrigir problemas. (BARRETO, 2018).

3. *BUSINESS INTELLIGENCE*

3.1. O que é BI

A sigla 'BI' - Business Intelligence, em sua tradução para o português significa Inteligência de Negócios, também chamada de inteligência empresarial, devido à sua vasta atuação dentro dos setores da empresa, entre eles o operacional, financeiro, marketing, entre outros, devido a sua funcionalidade. "*Business Intelligence* (BI), pode ser considerado como um conjunto de soluções" (TURBAN et al., 2009).

Segundo Borges (Apud LUCAS et al., 2016) *Business Intelligence* é um conceito amplo e que envolve diversas atividades e podem impactar nas estratégias das organizações, em suas próprias palavras:

> É o conjunto de atividades voltadas para a obtenção, para o processamento, a análise e a disseminação de informação acerca do ambiente de negócios de organizações de produção, com o objetivo de dar suporte à tomada de decisão e à definição estratégica. (BORGES Apud LUCAS et al, 2016).

Portanto, torna-se indispensável nos dias atuais o uso de estratégias de BI para camada de apresentação dos dados inseridos no sistema de gestão de risco, uma vez que a quantidade de informações e transações são grandes, o que reivindica um tratamento computacional adequado que o *Business Intelligence* é capaz de fornecer, através de ferramentas essenciais nas estratégias.

3.2 Ferramentas de *Business Intelligence*

Para efeito de pesquisa, esse artigo científico utilizou a ferramenta chamada de Power BI, por questões institucionais, onde servirá de apoio ao gerenciamento de risco para camada de apresentação e visualização dos dados para melhor compreensão. Nessa camada, encontram-se as ferramentas que dão feedback visual para as tratativas dos dados.

Atualmente há várias ferramentas de análise de dados no mercado, porém para efeito de objetivo de pesquisa e escopo do trabalho serão abordadas as seguintes: Power BI, Qlikview e Tableau.

3.2.1 Características

Qlikview: também chamada de Qlik sense têm uma característica que foi patenteada pela "Qlik, desenvolvedora das soluções" chamada tecnologia associativa, que traz para o gestor uma opção de construir gráficos com base em parâmetros desejados por ele, consumindo os dados do seu *Business Intelligence*, basicamente, ele consegue visualizar todos os produtos vendidos com os valores entre 100 a 200 reais, em um exemplo básico.

Tableau: É outra ferramenta de *Business Intelligence* que é muito utilizada no mercado de trabalho, alcançando o status de mais utilizada atualmente. Uma característica peculiar vinda apenas dela é a possibilidade de entender como o dado foi formado, trazendo para o gestor a possibilidade de compreender como aquele dado foi criado ao longo do tempo, a ferramenta nos mostra visualizações mostrando a história do dado e assim o gestor entende como a organização se comportou em determinado período, mostrando insides que vão possibilitar ao usuário identificar situações que em visões estáticas não serão possíveis.

Power BI: Uma característica exclusiva apenas para a ferramenta de *Business Intelligence* da Microsoft é a simplicidade, ela não é tão complicada de se aprender a usar comparada às outras

ferramentas já citadas, isso faz com que o gestor da organização não necessite de muito tempo para se ambientar com a nova ferramenta a ser utilizada e também auxilia as pessoas que só querem aprender através da ferramenta. Essa ferramenta consegue tratar todos os dados que as outras ferramentas não conseguem, mas de uma forma bem mais simples que as outras, essa simplicidade se deve graças à sua data de lançamento, 10 anos após o Tableau, isso fez com que os responsáveis da Microsoft pudessem estudar as outras ferramentas no mercado e elaborassem algo mais fácil e de melhor entendimento.

3.3 Funcionamento do *Business Intelligence*

Para que o *Business Intelligence* possa começar a trazer benefícios para uma organização, é necessário, antes de qualquer outra coisa, que haja alguma base de dados (banco de dados, planilha de excel ou etc.), servindo como base para o processo de tomada de decisão, uma vez que dessa quantidade de dados são extraídas informações que servirão para o tratamento, transformando essas amostras de dados, após tratados e visualizados, em valor agregado para uma organização pública, por exemplo.

Segundo Primak (2008), a arquitetura do *Business Intelligence* apresenta 3 partições: Dados, Informação e Conhecimento.

- **Conhecimento:** são informações consolidadas, onde pode-se tomar alguma decisão com base verídicas.
- **Informação:** Análise de dados tratados de interesse do órgão.
- **Dados:** São informações de fontes que contém valores/ativos que podem ser de bancos de dados entre outras fontes.

Ainda segundo Primak (2008):

> A arquitetura de um BI envolve diversos componentes, que vão desde servidores de alto desempenho, discos de grande capacidade de armazenamento a sistemas inteligentes que proporcionam a transformação de dados brutos em informações privilegiadas, disponibilizando-as aos usuários de acordo com os diversos níveis hierárquicos de uma organização (PRIMAK, 2008).

Para BEZERRA e SIEBRA, (Apud Turban et al., 2009) Business Intelligence (BI) ou Inteligência de Negócios, "é um termo que inclui arquiteturas, ferramentas, bancos de dados, aplicações e metodologias" que possui muitos recursos, ferramentas e técnicas que servem de base para a criação do conhecimento e dados relevantes para a organização.

Banco de dados: Local de armazenamento de dados, onde se localiza informações de um sistema ou setor de uma organização, sistema de administração de dados. "o modelo de banco de dados relacional possui a capacidade de lidar com grandes volumes de informações, eliminando dados redundantes."(SILVA FILHO, 2002).

ETL (*Extract, Transform, Load) significa* extração, transformação e carregamento, que é uma ferramenta de BI que faz a correção e sistematização dos dados. (PRIMAK, 2008) define ETL como uma ferramenta composta de 3 fases:

Extração: fase na qual os dados não tratados são coletados do banco de dados da organização.

Transformação: fase em que os dados são analisados e agrupados em um único formato.

Carregamento: fase onde as informações tratadas são enviadas para os seus respectivos destinos

O *Business Intelligence* é aplicado contribuindo para o processo de visualização dos dados, nesta camada que o resultado do processamento é observado por meio de gráficos,

relatórios ou outros recursos visuais. ou seja, após a finalização das análises, os resultados são apresentados para recursos de saída, que podem ser aplicativos, recursos do Software ou espectadores humanos.

3.4 Benefícios de *Business Intelligence*

Um procedimento moderno e no ambiente público é necessário conter algum benefício que chame a atenção para o seu uso, e é isso o que o *Business Intelligence* traz, benefícios em que se destaca a capacidade de demonstrar informações condensadas, objetivas e rápidas a respeito dos setores interessados dentro de uma empresa pública.

Turban et al.(2009) citam alguns benefícios do *Business Intelligence*, tais como:

1. Geração de relatórios mais rápida e precisa;
2. Melhoria na tomada de decisões;
3. Economia de tempo;
4. Versão única da verdade;
5. Melhoria das estratégias e dos planos;
6. Maior eficiência nos processos;
7. Economia de custos.

Com base na visão do autor Turban foi possível verificar que os benefícios do uso do *Business Intelligence* podem gerar impactos positivos para uma organização, uma vez que o *BI* atua tanto na economia do tempo quanto na geração de relatórios gerenciais e/ou operacionais para apoio ao processo de tomada de decisão.

O autor Primak (2008) aborda o assunto auxílio do *Business Intelligence* no processo de tomada de decisão, proporcionando alguns benefícios, sendo:

> Nos dias atuais, corporações de pequeno, médio e grande porte necessitam de BI para auxiliá-las nas mais diferentes situações para a tomada de decisão, otimizar o trabalho da organização, reduzir custos, eliminar a duplicação de tarefas, permitir previsões de crescimento da empresa como um todo e contribuir para a elaboração de estratégias. (PRIMAK, 2008, p. 06).

No tópico 4 o trabalho abordará a coleta e a análise dos dados para a conclusão do artigo.

3.5 *Business Intelligence* no âmbito do processo de gerenciamento de riscos

Uma vez que no tópico 2 (dois) deste trabalho acadêmico foram apresentados os conceitos primordiais do tema gerenciamento de riscos e no tópico 3 (três) o assunto BI (Business Intelligence) foi desenvolvido, este item tem a perspectiva de trazer a relação entre os assuntos demonstrados.

Conforme foi possível verificar no desenvolvimento do referencial teórico, o processo de gerenciamento de riscos requer atenção por parte das organizações públicas e privadas, principalmente, por parte dos gestores que precisam ter as informações dos riscos organizacionais disponíveis para que a tomada de decisão seja feita de maneira prática, de acordo com urgência necessária e a mais assertiva possível.

O BI em sua camada de apresentação pode proporcionar para o processo de gerenciamento de riscos as seguintes vantagens operacionais:

a) Dispor a informação de maneira estruturada e de acordo com a necessidade de cada gestor público;
b) Economia de tempo na apresentação das informações.

Percebe-se, por meio da literatura apresentada neste trabalho, que as duas áreas de conhecimento que são objetos de pesquisa, podem trabalhar em conjunto uma vez que o *Business Intelligence* busca auxiliar o processo a gestão de riscos em alguma instância gerencial ou operacional, fato este que será detalhado no tópico 4.

4. Análise dos dados

Esta pesquisa acadêmica foi realizada com base no processo de gerenciamento de riscos de uma instituição pública. Por questões de fins acadêmicos, objetivos de trabalho e por proteção de dados, não será divulgado o nome da instituição pública. Alguns dados informados no contexto do trabalho foram descaracterizados, sendo demonstrado o fluxo do processo para apoiar futuras pesquisas. Algumas das telas sistêmicas não terão identificação total dos dados, visando atender ao que preconiza este respectivo trabalho.

Os elementos utilizados nesta etapa de análise foram: a) sistema de gerenciamento de risco; b) Ferramenta de análise dados (Power BI da Microsoft); c) Bibliografias de estudos científicos utilizadas na etapa de desenvolvimento do trabalho. De uma maneira direta foi analisado o processo de gestão de risco, em que existe a possibilidade de haver vários riscos, sendo externos ou interno, humano ou sistêmico, por exemplo.

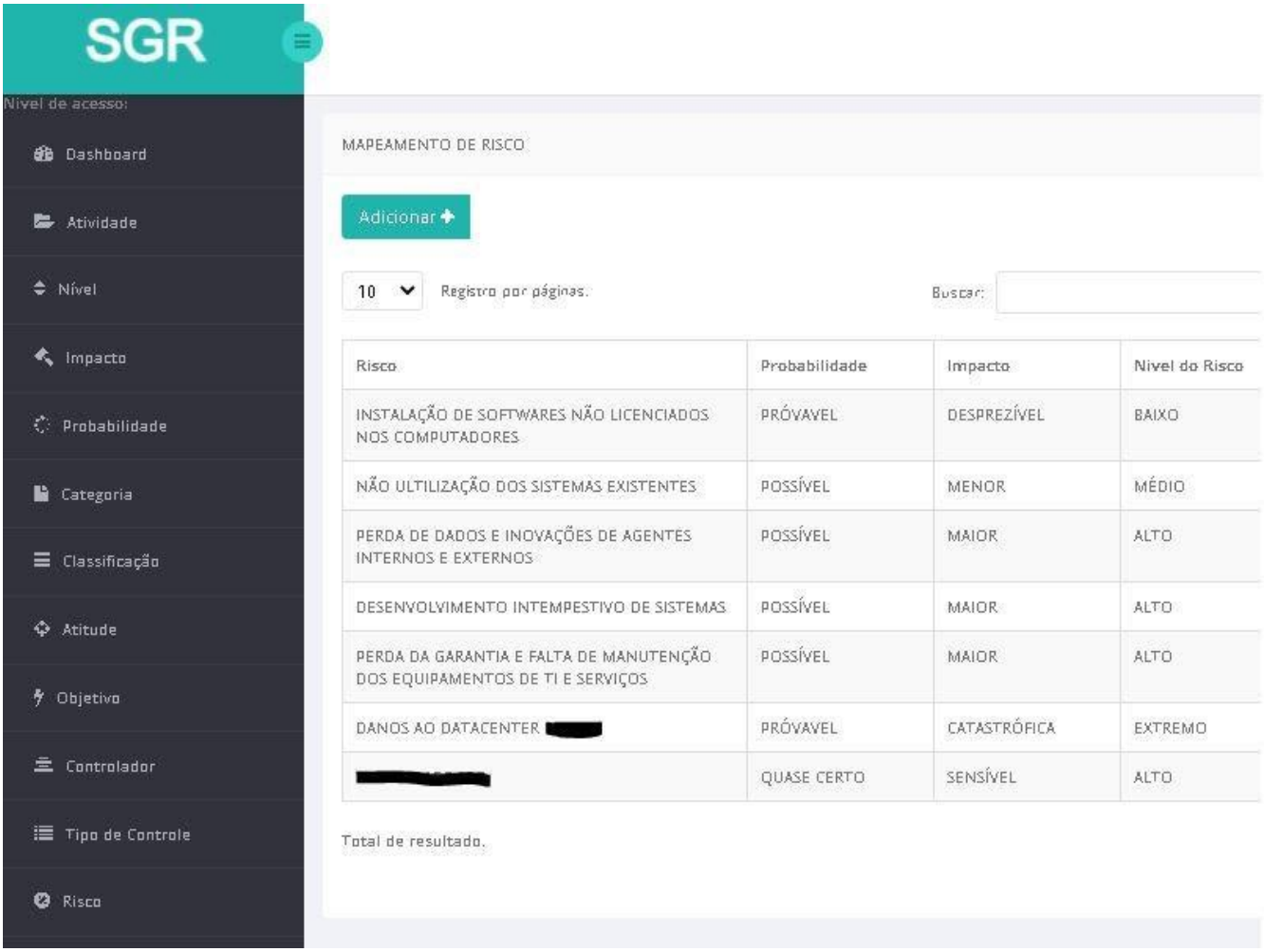
A ferramenta de BI contribui para o problema de pesquisa por meio da camada de apresentação das informações inseridas no sistema de risco, o SGR - “Sistema de Gerenciamento de Riscos” onde todos os dados encontrados e registrados no gerenciamento de risco são usados para criação dos gráficos e tabelas para visualização e análise das informações.

4.1 Mapeamento do risco

O processo começa com a identificação do risco por meio da análise de algo que possa alterar ou danificar, colocar idoneidade física ou moral em risco, seja ele, administracao, imagem ou qualquer outro setor, levantando assim informações importantes como a realização de analisar os dados, analisar o sistema da empresa, interferência de comunicações internas, danos no funcionamento das máquinas da organização, ataques ao *datacenter*, invasão de *hackers*, entre outros meios de identificar o risco. Com o risco identificado, é realizado o mapeamento do risco, uma análise do que pode afetar ou prejudicar a empresa.

A tela da figura 2 apresenta alguns dados descaracterizados de um sistema de gestão de riscos do ambiente de uma empresa pública.

Figura 2: SGR - Sistema de Gerenciamento de Riscos - Relatório de risco classificado.



Fonte: Dados internos de um sistema público do governo.

Na figura 2 os campos são os seguintes:

Campo Risco: Levantar todos os dados do setor ou local onde foi identificado o risco, para que seja registrado, observando as estimativas do risco, gerando uma base de relatório, cada

campo anterior ao Campo de Risco são informações que vão ser colocadas no preenchimento dos campos do sistema de Risco. O que deve ser observado nas estimativas de risco?

- Objetivo: onde, em qual setor ou demanda será feita a análise.
- Atividade: registrar o que será feito em determinado setor ou demandas.
- Descrição do risco: essa informação é muito importante para o mapeamento e gestão do risco, pois ao ser informado deve conter informações claras e diretas.
- Tipo de risco: caracterização, se positivo, podendo agregar algo na empresa ou negativo, totalmente sem acréscimo.
- Categoria: identificação por qual meio se deu aquele risco;
- Nível do risco: informação do nível de gravidade, com essa informação é classificada se pode haver espera ou não para o tratamento.
- Impactos do risco: essa informação mostra o nível de impactos na empresa;
- Probabilidade do risco: ocorrência que pode tornar determinado risco acontecer novamente.
- Atitude: o que foi feito ou o que será feito de imediato sobre o evento.
- Controlador: responsável pela gerência do tratamento do risco.

Todas as informações são gerenciadas e lançadas no campo Risco, pois faz parte do mapeamento.

4.2 Gestão de risco com uso do SGR e a ferramenta de BI

A ferramenta de BI faz parte de um ciclo básico de tratamento de dados, que busca se conectar ao banco de dados (BD), em que atuará na camada de apresentação das informações que serão inseridas no mapeamento do risco e gestão do risco, pois tem grande importância conforme (Ribeiro, 2020), “todos esses fenômenos: ciência aberta, dados abertos, junto aos avanços tecnológicos, emerge a ciência de dados que vem impactar em diversas áreas atuação.“

A realização da gestão do risco é feita observando alguns tópicos para levantamento de informações - as causas, consequências e os controles do risco, que podem ser um ou vários em um mesmo risco.

- Causas: o que causou o risco, motivos.

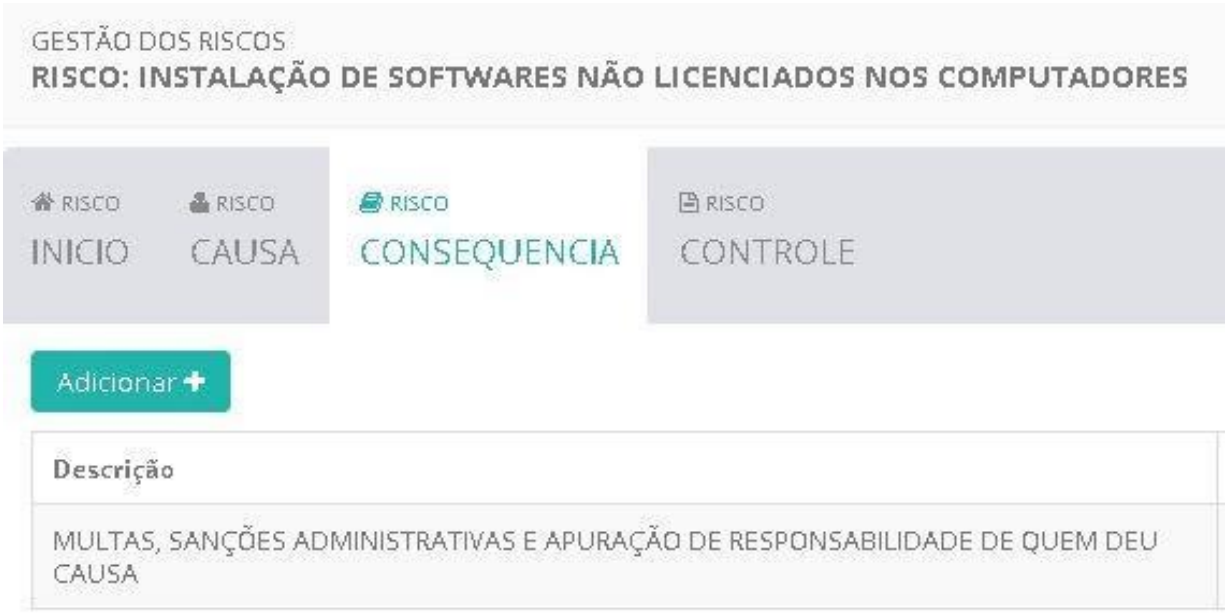
As telas das figuras 3, 4, 5 e 6, com alguns dados reais descaracterizados de um ambiente corporativo.

Figura 3: Processo de Gestão – Causa.

Fonte: Dados internos de um sistema público do governo.

- Consequências: através da análise de causas, qual consequência determinado risco gerou ou danificaram na empresa, nos contratos, lucros, etc.

Figura 4: Processo de Gestão – Consequência.



Fonte: Dados internos de um sistema público do governo.

- Controles: medidas de tratamento dos riscos, com data de abertura para conhecimento interno; Nessa parte, as informações devem ser classificadas em: Necessárias ou Existentes.
  - Necessárias: controles ainda não existentes ou em processo de solução.
  - Existentes: controles que existem dentro do órgão e que está em tratamento.

Figura 5: Processo de gestão – Controle.


GESTÃO DOS RISCOS
RISCO: INSTALAÇÃO DE SOFTWARES NÃO LICENCIADOS NOS COMPUTADORES

RISCO INICIO | RISCO CAUSA | RISCO CONSEQUENCIA | RISCO CONTROLE

Adicionar +

Descrição	Tipo de controle	Data de Criação	Data de Execução
CONTROLE DE PERMISSÕES E ACESSOS DOS SERVIDORES	EXISTENTES	18/01/2021	Controle Não Executado
REVISÃO PERIÓDICAS DOS SOFTWARES INSTALADOS	EXISTENTES	18/01/2021	Controle Não Executado
IMPLEMENTAÇÃO DE AUDITORIA NOS SOFTWARES INSTALADOS	NECESSÁRIOS	18/01/2021	Controle Não Executado

Fonte: Dados internos de um sistema público do governo.

O sistema de gestão de risco não tem prazo para fechamento/finalização, pois o intuito é tratar o risco o quanto antes. A data de finalização indica que o risco foi totalmente tratado e feito com todos os controles necessários para minimizar os impactos ou solucionar de forma eficiente o risco, todas informações ficam armazenadas no banco de dados para possível consulta caso haja reincidência do mesmo.

A apresentação dos dados do SGR é mostrada em uma ferramenta de BI. Por questões institucionais foi feita o contrato com as ferramentas da Microsoft, o Power BI, onde se conecta com o banco de dados, exportando uma cópia das tabelas do banco que foi selecionada, que será

feito o processo de analisar e transformar dados comuns em soluções, gerando uma informação em tabela ou gráficos para visualização. O Power BI é uma ferramenta de muitas utilidades, porém a finalidade é apresentar os dados, ajudar nas definições de melhores resultados, informações claras e ajudar nas decisões em todos os aspectos.

A Ferramenta de BI tem a função de auxiliar na apresentação dos dados, auxiliar nos resultados do órgão, levantar dados gerais ou parciais do sistema, informar as medidas feitas ou propostas, levantar informações da quantidade de riscos, informar quantidade de controles tratados e não tratados, o responsável pela gestão, as classificações de cada risco, entre outros recursos que a ferramenta pode proporcionar por ser de fácil utilização e menos complexas entre outras ferramentas de BI do mercado, através dos dashboard são feitas visualizações e as análises das estruturas dos dados exportados do banco de dados.

Figura 5: *Dashboard* do SGR.

Risco

Riscos	Total de Controles	Executados	Não Executados	Controlador
DANOS AO DATACENTER	6		6	DIRETOR DA TI
DESENVOLVIMENTO INTEMPESTIVO DE SISTEMAS	4		4	DIRETOR DA TI
INSTALAÇÃO DE SOFTWARES NÃO LICENCIADOS NOS COMPUTADORES	3		3	DIRETOR DA TI
NÃO ULTILIZAÇÃO DOS SISTEMAS EXISTENTES	2		2	DIRETOR DA TI
PERDA DA GARANTIA E FALTA DE MANUTENÇÃO DOS EQUIPAMENTOS DE TI E SERVIÇOS	2		2	DIRETOR DA TI
PERDA DE DADOS E INOVAÇÕES DE AGENTES INTERNOS E EXTERNOS	6		6	DIRETOR DA TI
[redacted]	1		1	DIRETOR DA TI
Total	**24**		**24**	

Fonte: Dados internos de um sistema público do governo.

Esta análise de risco e apresentação de dados realizada no Power BI proporciona maior segurança e controles contra os incidentes que podem acontecer, são dois sistemas de suma importância na organização e auxilia todos os setores nas ações internas e externas das atividades governamentais.

Com base nas análises realizadas, de acordo com o escopo da pesquisa e com as informações levantadas, foi possível identificar que cada ferramenta tem uma função distinta, porém integrada, onde o gerenciamento de risco previne e realiza tratativas para melhorias e soluções da organização. Já a ferramenta Power BI gera apresentação de resultados e informações sobre os riscos identificados, realizando análises de quantidades de riscos, controles, impactos, níveis, entre outros que são essenciais para a gestão da instituição pública.

No dashboard da ferramenta do Power BI apresenta a quantidade e as ações de gestão "não executados" e "executados". O tratamento do risco é finalizado quando todos os controles são executados, essa coluna no gráfico é para ciência dos gestores e controlador local.

5. CONSIDERAÇÕES FINAIS

Tendo por premissa os itens apresentados neste trabalho acadêmico, é possível concluir que o objetivo proposto do trabalho foi atingido, uma vez que este busca articular o conhecimento teórico acerca do gerenciamento de riscos e sobre a utilização do BI para analisar uma situação prática dentro de uma empresa pública. A articulação proposta pode ser constatada com a apresentação dos tópicos 2 e 3 do trabalho, além da análise realizada no item 4 - análise de dados.

Com o objetivo geral do trabalho alcançado, o problema de pesquisa que visa analisar quais elementos são essenciais a serem considerados nos processos de gerenciamento de risco de uma empresa do setor público e como as ferramentas de Business Intelligence (BI) podem contribuir nesse processo, é respondido quando se percebe que:

a) É essencial que um processo de gerenciamento de riscos possua um sistema computacional para apoiar e melhorar o processo;

b) É relevante o uso de uma ferramenta de BI para otimizar o tempo de apresentação das informações dos riscos para os gestores poderem tomar suas respectivas decisões.

O SGR o sistema de gerenciamento de riscos é utilizado em um setor público, servindo para que tenha um melhor entendimento sobre os riscos identificados e os futuros casos que possam surgir, trazendo dificuldades para os profissionais do setor onde foi identificado, para que, assim possam se adequar a seus processos, contribuindo com o gerenciamento de riscos de forma que seja eficiente e ágil para a tomada de decisão do setor público.

O BI é uma ferramenta que auxilia na visualização dos dados inseridos no sistema SGR, onde o Power BI agrega na busca informações no banco de dados para poder realizar a apresentação através das análises e tratativas de dados, tratando dados de grandes quantidades e complexidades em soluções de fácil entendimento, ajudando no conhecimento interno e auxiliando nas decisões dos gestores da organização. Portanto acima de tudo, é importante um planejamento amplo, bem realizado, adequado ao contexto da organização e aos objetivos da organização.

Este trabalho científico não tem a intenção de ser a única fonte de informações para o tema proposto. A partir do assunto em referência, outras pesquisas acadêmicas podem ser realizadas. A pesquisa feita teve suas limitações devidas: a) questões sanitárias do Brasil (pandemia); b) ter sido realizada apenas em uma instituição pública e de maneira remota; c) utilizou-se como base uma ferramenta de BI.

Como sugestão futura para outras pesquisas propõe-se as seguintes problemáticas: 1) Que componentes do BI podem otimizar o processo de gerenciamento de riscos em uma empresa do setor privado? 2) Quais camadas do BI são relevantes no contexto do processo de gerenciamento de riscos em uma instituição da iniciativa pública?

6. REFERÊNCIAS

ABNT NBR ISO/IEC 27005. **Tecnologia da informação - Técnicas de segurança - Gestão de riscos de segurança da informação**, Associação Brasileira de Normas Técnicas. Rio de Janeiro: ABNT, 2008.

BARRETO, Jeanine; FRAPORTI, Simone. **Gerenciamento de Riscos**. 2018.

BEZERRA, Alessandro; SIEBRA, Sandra. **Implantação e Uso de Business Intelligence: Um Relato de Experiência no Grupo Provider.** 2015. Disponível em: https://periodicos.ufpe.br/revistas/gestaoorg/article/viewFile/22121/18486. https://periodicos.ufpe.br/revistas/gestaoorg. Acesso em: 13 de Maio de 2021.

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Márcio Tadeu de Araújo; **Política de Segurança da Informação: guia prático para elaboração e implementação**. Rio de Janeiro: Ciência Moderna, 2008, 259p.
FERNANDES, Jorge. **Introdução à Gestão de Riscos de Segurança da Informação** 2021.

FREITAS, Eduardo. **GESTÃO DE RISCOS APLICADA A SISTEMAS DE INFORMAÇÃO**. https://bd.camara.leg.br/. 2009. Disponível em: http://bd.camara.gov.br/bd/handle/bdcamara/3564 Acesso em: 17 de novembro de 2020.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Gerenciamento de riscos corporativos: evolução em governança e estratégia.** São Paulo: IBGC, 2017. (Série Cadernos de Governança Corporativa, 19.

ISO/IEC. ISO/IEC FDIS 27005 - **Information technology** - Security Techniques - Information security risk management. [S.l.], 2007.

KONZEN, Marcos; FONTOURA, Lisandra; NUNES, Raul. **Gestão de Riscos de Segurança da Informação Baseada na Norma ISO/IEC 27005 Usando Padrões de Segurança**. https://www.aedb.br, 2012, Disponível em: https://www.aedb.br/seget/arquivos/artigos12/57616827.pdf , Acesso em: 17 de fevereiro de 2021.

LUCAS, Alexandre; CAFE, Ligia Maria Arruda; VIERA, Angel Freddy Godoy. **Inteligência de negócios e inteligência competitiva na ciência da informação brasileira: contribuições para uma análise terminológica.** Perspect. ciênc. inf., Belo Horizonte , v. 21, n. 2, p. 168-187, Junho 2016 . Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1413-99362016000200168&lng=en&nrm=iso>. Acesso: 15 Maio de 2021.

MONTEIRO, M. S. **A importância da gestão de riscos**. Belém: CONACI, 2017.

MOREIRA, Nilton Stringanci. **Segurança mínima: uma visão corporativa da segurança de informação.** Rio de Janeiro: Axcel Books, 2001.

PRIMAK, F. V. **Decisões com BI (Business Intelligence)**. Rio de Janeiro: Ciência Moderna, 2008.

RIBEIRO,nivaldo. **BIG DATA EM PERIÓDICOS DA ÁREA DE CIÊNCIA DA INFORMAÇÃO: uma abordagem voltada para a ciência aberta e a ciência de dados.** https://periodicos.ufrn.br/informacao; Disponivel em: https://periodicos.ufrn.br/informacao/article/view/22452/13544. Acesso em: 18 de Abril de 2021.

SILVA FILHO, Demóstenes Ferreira da et al . **Banco de dados relacional para cadastro, avaliação e manejo da arborização em vias públicas**. **Rev. Árvore**, Viçosa , v. 26, n. 5, p. 629-642, Oct. 2002 . Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0100-67622002000500014&lng=en&nrm=iso>. Acesso em 02 Maio 2021. https://doi.org/10.1590/S0100-67622002000500014.

STONEBURNER, G.;GOGUEN, A,; FERINGA, A. **Risk Management Guide for Information Technology Systems**. Gaithersburg: NIST - National Institute of Standars and Technology, July 2002. 54 p. (Special Publication 800-30).

TURBAN, E. et al. **Business Intelligence: um enfoque gerencial para a inteligência do negócio**. Porto Alegre: Bookman, 2009**.** Acesso: em 02 de maio de 2021.

WOLMER, L. G. S. **Diálogo público para melhoria da governança pública**. São Paulo: TCU, 2013.

Agradecimentos

Ao professor Jorge com o seu apoio e incentivo ao nosso trabalho final, pela alta disponibilidade e empenho para a construção da melhor forma possível deste trabalho de Conclusão de Curso. Ao professor Sebastião pelas horas de ensino sobre como poderíamos elaborar este trabalho da forma correta. Aos demais professores da UNIVERSIDADE DO PLANALTO CENTRAL que foram os responsáveis pelo nosso crescimento intelectual e também agradecemos a todos os alunos envolvidos neste trabalho, pelo empenho e esforço, com muita dedicação na realização do artigo. Obrigado!