

Business intelligence e o processo de gerenciamento de riscos em uma instituição pública

Business intelligence and the risk management process in a public institution

DOI:10.34117/bjdv8n10-209

Recebimento dos originais: 19/09/2022

Aceitação para publicação: 26/10/2022

Jorge Alberto dos Santos

Mestre em Psicologia Educacional pelo Centro de Ensino Unificado de Brasília (UNICEUB)

Instituição: Centro de Ensino Unificado de Brasília (UNICEUB)

Endereço: 707/907, Campus Universitário, Asa Norte, Brasília - DF, CEP: 70790-075

E-mail: ntjorge@gmail.com

Sebastião Ivaldo Carneiro Portela

Doutor em Educação para Ciência pela Universidade Estadual Paulista (UNESP)

Instituição: Universidade Estadual Paulista (UNESP)

Endereço: Vila Nova, Rio Claro - SP

E-mail: sebastiao.portela@gmail.com

Washington Fábio de Souza Ribeiro

Mestre em Gestão do Conhecimento em Tecnologia da Informação pela Universidade Católica de Brasília

Instituição: Universidade Católica de Brasília

Endereço: QS 07, Lote 01, Taguatinga Sul, Taguatinga, Brasília - DF, CEP: 71966-700

E-mail: washingtonfabio@gmail.com

Gilmar Severino Lucena de Souza

Mestre em Engenharia Biomédica pela Universidade de Brasília (UNB)

Universidade de Brasília (UNB)

Endereço: Brasília - DF, CEP: 70910-900

E-mail: gilmarlucena@gmail.com

Wilton Marinho Carneiro Souza

Mestre em Governança, Tecnologia e Inovação pela Universidade Católica de Brasília

Instituição: Universidade Católica de Brasília

Endereço: QS 07, Lote 01, Taguatinga Sul, Taguatinga, Brasília - DF, CEP: 71966-700

E-mail: wilton.marinho@gmail.com

David Rafael Ferreira da Silva

Graduado em Sistemas de Informação pelo Centro Universitário do Planalto Central
Apparecido dos Santos (UNICEPLAC)

Instituição: Centro Universitário do Planalto Central Apparecido dos Santos
(UNICEPLAC)

Endereço: SIGA Área Especial para Indústria Lote 2/3, Sca St. Leste Industrial, Gama,
Brasília - DF, CEP: 72445-020

E-mail: davidrafa01@gmail.com

Matheus Viana dos Santos

Graduado em Sistemas de Informação pelo Centro Universitário do Planalto Central
Apparecido dos Santos (UNICEPLAC)

Instituição: Centro Universitário do Planalto Central Apparecido dos Santos
(UNICEPLAC)

Endereço: SIGA Área Especial para Indústria Lote 2/3, Sca St. Leste Industrial, Gama,
Brasília - DF, CEP: 72445-020

E-mail: smatheus799vianna@gmail.com

Walyson Martins dos Santos

Graduado em Sistemas de Informação pelo Centro Universitário do Planalto Central
Apparecido dos Santos (UNICEPLAC)

Instituição: Centro Universitário do Planalto Central Apparecido dos Santos
(UNICEPLAC)

Endereço: SIGA Área Especial para Indústria Lote 2/3, Sca St. Leste Industrial, Gama,
Brasília - DF, CEP: 72445-020

E-mail: walyson10@gmail.com

RESUMO

O Gerenciamento de risco é uma área de conhecimento utilizada por muitas organizações públicas e privadas e proporciona a análise e o mapeamento de possíveis eventos, que possam gerar danos no ambiente organizacional. Neste trabalho, buscou-se o conceito de gestão de risco para caracterizar o funcionamento de um sistema de controle de uma empresa pública, que possui uma ferramenta de *Business Intelligence* (BI) que possibilita analisar e identificar as causas e o nível de risco do ambiente tecnológico. 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 de informações por meio de *dashboard* com gráficos e tabelas, auxilia de forma significativa a camada de apresentação para melhorar o processo de tomada de decisão dos gestores.

Palavras-chave: Gerenciamento de risco, *Business Intelligence*, ferramenta de BI.

ABSTRACT

Risk management is an area of knowledge used by many public and private organizations and provides an analysis and mapping of possible events that can cause damage in the organizational environment. The concept of risk management and the functioning of a control system of a public company were verified, which has a BI (Business Intelligence) tool that makes it possible to analyze and identify the causes and the level of risk of the technological environment. The management of processes involving the organization is carried out with the aim of preventing damage, attacks and financial losses. The study showed that the visualization of information through a dashboard with graphs and tables

significantly helps the presentation layer to improve the decision-making process of managers.

Keywords: risk management, *Business Intelligence*, BI tool.

1 INTRODUÇÃO

A gestão de risco é um tema 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 uma 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 maneira estruturada e gerida de forma apropriada, pode proporcionar para as empresas do setor público melhorias em seus processos organizacionais e tecnológicos, tendo como consequência positiva a elevação no desempenho dos serviços ofertados para a sociedade.

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 públicos ou privados são exemplos de negócios estritamente alinhados ao gerenciamento de risco, que divulgam dados acerca das exposições de crédito e de mercado. Assim, 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 (ARAÚJO; OLIVEIRA; MONTEIRO, 2017).

Com base nas primeiras ideias apresentadas, este estudo tem como problemática identificar quais elementos são essenciais para 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. Como objetivo geral busca-se articular o conhecimento teórico acerca do gerenciamento de riscos e a utilização do BI para analisar um cenário descaracterizado de uma empresa pública. O trabalho está

organizado da seguinte forma: 1) Introdução; 2) Apresentação do processo de gerenciamento de riscos; 3) Conceituação de Business Intelligence (BI); 4) Desenvolvimento; 5) Análise dos dados; 6) Considerações finais.

2 PROCESSOS DE GERENCIAMENTO E ANÁLISE DE RISCOS

Segundo o Instituto Brasileiro de Governança Corporativa (2021) – IBGC, "o gerenciamento de riscos não é uma prática nova, fazendo parte da rotina de qualquer empresário desde tempos muito remotos". Porém, o tema só começou a ganhar relevância no final do século vinte (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.

Na visão do IBGC (2021), "a indústria financeira teve incentivo para implementar o gerenciamento de riscos na década de 1980, devido à preocupação com a exposição dos bancos a operações não registradas em balanço." Ainda na temática gestão de riscos e na visão do autor Nascimento et al. (2022), a gestão de riscos tem encontrado crescente aplicabilidade nas contratações públicas, sendo considerada por alguns como ponto básico a ser observado nas decisões relacionadas a este processo, por possibilitar uma visão ampla do contexto garantindo mais eficiência, inibindo a falta de planejamento e o mau uso de recursos públicos. Ou seja, pelos relatos dos autores apresentados, percebe-se que o gerenciamento de riscos vem ganhando cada vez mais espaço no ambiente organizacional das empresas públicas brasileiras.

Apesar da temática de riscos não ser algo novo, a imersão do assunto no ambiente das empresas públicas e privadas é relativamente recente, o que pode indicar a falta de experiência na abordagem de alguns *players* de mercado.

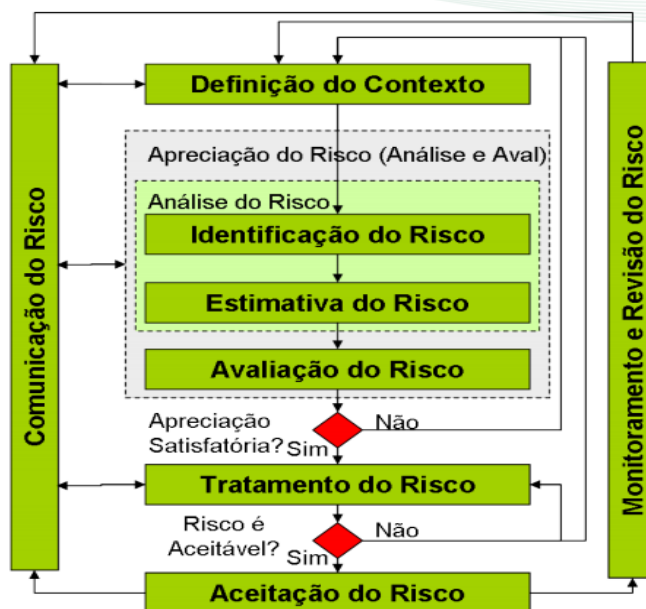
Nos processos de gestão de risco, o foco recai sobre a proteção dos ativos e na identificação das fontes de ameaça. Os ativos são os entes valorativos para as organizações, o que envolve tanto processos e atividades do negócio, informações, hardware, software, rede, pessoal, sítio e estrutura organizacional. Já as fontes das ameaças são caracterizadas por agentes que promovem ações com implicações danosas para a instituição. Podem ser classificadas em humanas intencionais, humanas acidentais e ambientais.

Segundo ISO/IEC 27005 (2021) as ameaças também pode ser classificadas com relação 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.

O processo de gerenciamento de risco envolve uma complexa dinâmica que engloba as etapas de apreciação e percepção do risco; delimitação do contexto e dimensão dos impactos; a análise do risco; tratamento, monitoramento e comunicação do risco e efetividade das medidas adotadas. A figura 1 ilustra as interconexões entre essas etapas (KONZEN; FONTOURA; NUNES, 2013).

Figura 1 – Processo de gerenciamento de riscos



Fonte: (KONZEN; FONTOURA; NUNES, 2013)

A definição do contexto, envolve a delimitação e alcance do problema através da identificação dos ativos em risco que envolve os eventos que possam causar impactos potenciais, tanto os negativos como os positivos. A estimativa de riscos, na visão do autor, "tem como objetivo atribuir o impacto e valores para as probabilidades e consequências de cada ameaça" (KONZEN; FONTOURA; NUNES, 2013).

Já na fase de avaliação do risco pode-se estabelecer o tratamento da vulnerabilidade. É neste momento que definimos se uma ameaça deve ser tratada ou não como uma prioridade. Ainda para o autor, no tratamento do risco "implementa-se controles para que possa reduzir, reter, transferir ou evitar os riscos. Uma vez que implementamos esse tratamento ele pode nos fornecer novos controles" (KONZEN; FONTOURA; NUNES, 2013). A etapa de aceitação de riscos, por sua vez, é a fase em que podemos compreender os registros o formal da decisão pelo aceite dos riscos residuais existentes na organização e se articula com a etapa de comunicação do risco que envolve "o fluxo de informações dentro de uma entidade, ou seja, quando desenvolvemos a comunicação dos riscos para garantir que todos tenham consciência sobre os riscos". (KONZEN; FONTOURA; NUNES, 2013).

Finalmente, o 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." (KONZEN; FONTOURA; NUNES, 2013). O processo de identificação e caracterização de riscos envolve a apreciação e análise das vulnerabilidades, probabilidades e os impactos.

2.1 ANÁLISE DE VULNERABILIDADES

A análise de vulnerabilidade pode ser uma abertura para a segurança da informação, pois elas acontecem de várias formas como, por exemplo, falhas no desenvolvimento de um sistema empresarial. 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 e 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.

2.2 ANÁLISE 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	Os controles de segurança para prevenir que a vulnerabilidade seja explorada são ineficazes.
Médio	A fonte de ameaça está motivada e possui conhecimento para o 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).

2.3 ANÁLISE E IMPACTO

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”. 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 significativa 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).

3 BUSINESS INTELLIGENCE

O uso de estratégias de BI para camada de apresentação dos dados inseridos no sistema de gestão de risco tem se intensificado, 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.

A sigla “BI” - *Business Intelligence*, em sua tradução para o português significa Inteligência de Negócios e para que comece a trazer benefícios para uma organização, é necessário, antes de qualquer outra coisa, que exista alguma base de dados (banco de dados, planilha de excel ou etc.), servindo como base para o processo de tomada de decisão. Os dados são fontes que contém valores/ativos que podem ser de bancos de dados entre outras fontes. Dessa quantidade de dados serão extraídas informações que servirão para o tratamento, transformando essas amostras de dados em conhecimentos que podem contribuir na tomada de decisão de valor agregado para uma organização (PRIMAK, 2008) e (SILVA FILHO, 2002).

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 Primak (2008), a dinâmica do *BI* está concentrada no ETL (*Extract, Transform, Load*) significa extração, transformação e carregamento. Na extração, os dados não tratados são coletados do banco de dados da organização. Na transformação, os dados são analisados e agrupados em um único formato. E no carregamento, as informações tratadas são enviadas para os seus respectivos destinos

Do ponto de vista prático, o BI pode fornecer 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. 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 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 na gestão de riscos em alguma instância gerencial ou operacional.

4 DESENVOLVIMENTO

A etapa de desenvolvimento e coleta dos dados foi realizada em uma empresa do setor público situada em Brasília-DF durante os meses de agosto e setembro de 2021. Os procedimentos consistiram em realizar prints de telas, com as devidas autorizações dos supervisores, por um dos autores do trabalho ao prestar serviço no órgão.

Por se tratar de um processo de gerenciamento de riscos de uma instituição pública, para fins de proteção de dados, não serão divulgados o nome da instituição pública e as telas sistêmicas não terão identificação total dos dados, sendo alguns dados descaracterizados. Para efeito de pesquisa utilizou-se a ferramenta *Power BI*, por questões institucionais, que serviu de apoio ao gerenciamento de risco para camada de apresentação, visualização e compreensão dos dados. De uma maneira direta foi analisado o processo de gestão de risco, com multiplicidades riscos, sendo externos ou internos, humano ou sistêmico, por exemplo.

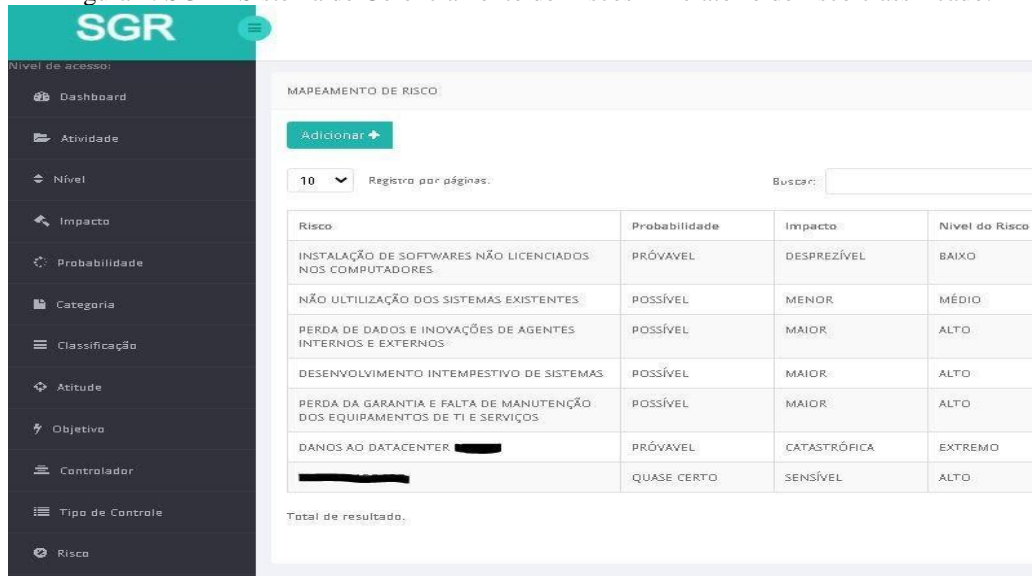
A ferramenta de BI contribui para o problema de pesquisa por meio da camada de apresentação das informações inseridas no sistema de risco, o SGR - “Sistema de Gerenciamento de Riscos” em que os dados registrados no gerenciamento de risco são usados para criação de *dashboards* para visualização e análise das informações.

5 ANÁLISE DE DADOS

5.1 MAPEAMENTO DO RISCO

O processo inicia-se com a identificação do risco por meio da análise de um evento com possibilidade de alterar ou danificar, colocar idoneidade física ou moral em risco. O controle do risco é realizado por meio de um sistema chamado de SGR. É relevante entender que um sistema permite levantar e filtrar as informações importantes para a organização na etapa de análise dos dados, verificar o sistema da empresa, interferência de comunicações internas, danos no funcionamento das estações de trabalho da organização, ataques aos serviços de TI e sistemas acomodados no *datacenter*, invasão de *hackers*, entre outros. A tela da figura 2 apresenta alguns dados descaracterizados do sistema de gestão de riscos:

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



Risco	Probabilidade	Impacto	Nível do Risco
INSTALAÇÃO DE SOFTWARES NÃO LICENCIADOS NOS COMPUTADORES.	PRÓVAVEL	DESPREZÍVEL	BAIXO
NÃO UTILIZAÇÃO DOS SISTEMAS EXISTENTES	POSSÍVEL	MENOR	MÉDIO
PERDA DE DADOS E INOVAÇÕES DE AGENTES INTERNOS E EXTERNOS.	POSSÍVEL	MAIOR	ALTO
DESENVOLVIMENTO INTEMPESTIVO DE SISTEMAS.	POSSÍVEL	MAIOR	ALTO
PERDA DA GARANTIA E FALTA DE MANUTENÇÃO DOS EQUIPAMENTOS DE TI E SERVIÇOS.	POSSÍVEL	MAIOR	ALTO
DANOS AO DATACENTER ██████████	PRÓVAVEL	CATASTRÓFICA	EXTREMO
██████████	QUASE CERTO	SENSÍVEL	ALTO

Fonte: Fonte: Dados internos de um sistema público do Governo Federal.

Na figura 2 observa-se os seguintes indicadores que caracterizam o risco:

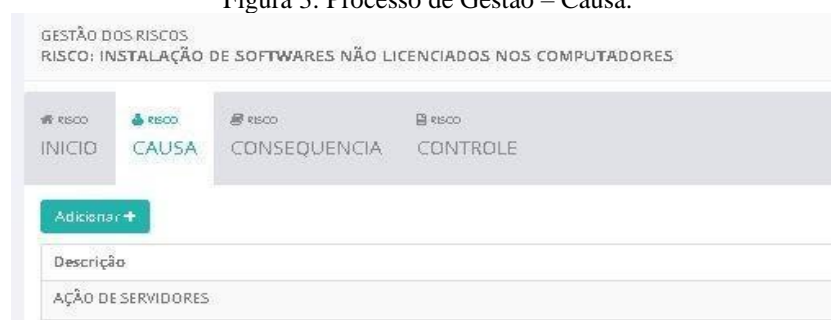
- 1) Risco: Levanta os dados do setor ou local onde foi identificado o risco, para o devido registro, observando as estimativas do risco, gerando uma base de relatório. Cada campo anterior ao Campo de Risco são informações que vão ser colocadas no preenchimento dos campos do sistema de risco.
- 2) Objetivo: onde, em qual setor ou demanda será feita a análise.
- 3) Atividade: registrar o que será feito em determinado setor ou demandas.
- 4) 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.
- 5) Tipo de risco: caracterização, se positivo, podendo agregar algo na empresa ou negativo, totalmente sem acréscimo.
- 6) Categoria: identificação por qual meio se deu aquele risco.
- 7) Nível do risco: informação do nível de gravidade, com essa informação é classificada se pode haver espera ou não para o tratamento.
- 8) Impactos do risco: essa informação mostra o nível de impactos na empresa.
- 9) Probabilidade do risco: ocorrência que pode tornar determinado risco acontecer novamente.
- 10) Atitude: o que foi feito ou o que será feito de imediato sobre o evento.
- 11) Controlador: responsável pela gerência do tratamento do risco.

5.2 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. A realização da gestão do risco é feita observando alguns tópicos para levantamento de informações: as causas, as consequências e os controles do risco.

Os *prints* das telas com esses parâmetros estão nas figuras 3, 4 e 5, com alguns dados reais descaracterizados de um ambiente corporativo.

Figura 3: Processo de Gestão – Causa.



Fonte: Dados internos de um sistema público do governo.

Figura 4: Processo de Gestão – Consequência.



Fonte: Dados internos de um sistema público do governo.

Figura 5: Processo de gestão – Controle.



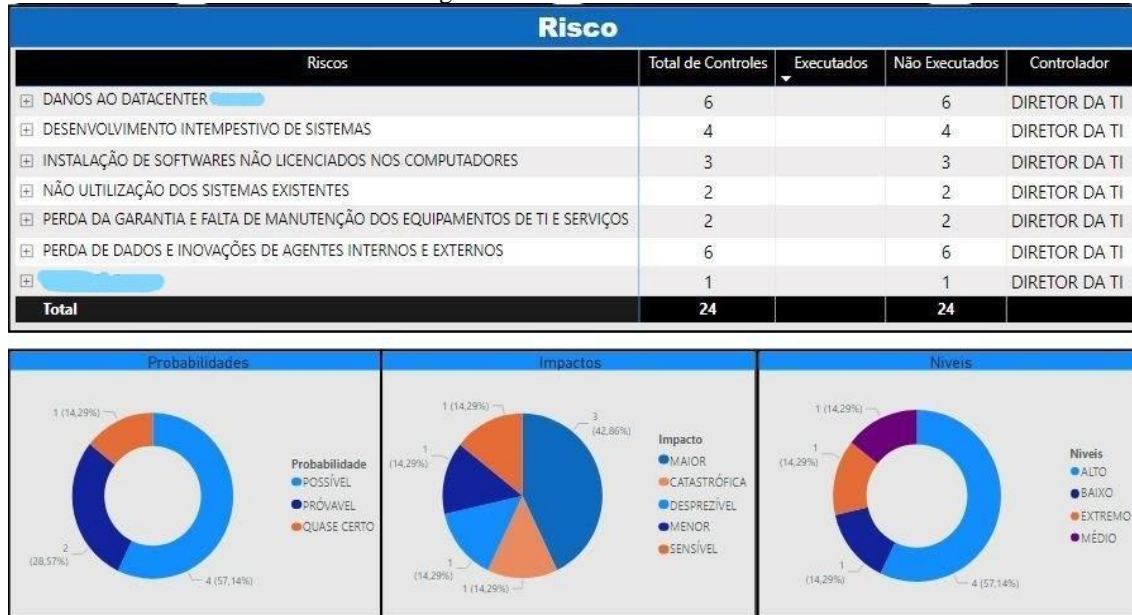
Fonte: Dados internos de um sistema público do governo.

Na figura 3, o processo de gestão de riscos aponta as causas dos riscos e a descrição dos motivos. Na figura 4, por meio da análise das causas, é evidenciado as consequências de determinado risco, tanto para a empresa quanto para as pessoas que geraram o risco. Na parte de controle (figura 5) são indicadas as medidas de tratamento dos riscos, com data de abertura para conhecimento interno. Nessa parte, as informações são classificadas em necessárias ou existentes. A primeira diz respeito a controles ainda não existentes ou em processo de solução. A segunda, por sua vez, se refere a controles que existem dentro do órgão e que estão em tratamento.

O sistema de gestão de risco não tem prazo para fechamento/finalização, pois, o intuito é tratar o risco o quanto antes e de forma contínua. 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. As informações ficam armazenadas no banco de dados para possível consulta, caso haja reincidência do mesmo.

A Ferramenta de BI tem a função de organizar a 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. A ferramenta Power BI é de fácil utilização e menos complexa entre as ferramentas de BI do mercado. Por meio dos *dashboard* são feitas visualizações e análises das estruturas dos dados exportados do banco de dados, como pode ser visto na figura 5.

Figura 6: Dashboard do SGR.



Fonte: Dados internos de um sistema público do governo.

Esta análise de risco e apresentação de dados realizada no *software* Power BI da empresa Microsoft proporciona maior segurança e controles contra os incidentes que podem acontecer, são dois sistemas de grande importância na organização e auxilia vários 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 Power BI apresenta-se a quantidade e as ações de gestão “não executadas” e “executadas”. O tratamento do risco é finalizado quando todos os controles são executados, a coluna no gráfico é para ciência dos gestores e controlador local, buscando atender as boas práticas de mercado em que um risco deve ser associado a uma pessoa ou área para que se tenha um responsável.

6 CONSIDERAÇÕES FINAIS

Tendo por premissa os itens apresentados neste trabalho foi possível concluir, a partir dos dados e da literatura adotada, que o objetivo geral foi atingido com a articulação

de conhecimentos teóricos acerca do gerenciamento de riscos com a prática real da utilização do BI para analisar uma situação no ambiente de uma empresa pública.

Os resultados permitiram indicar os elementos que 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.

O SGR, como sistema de gerenciamento de riscos utilizado no setor público, serve para melhor entendimento dos riscos identificados e os futuros casos que possam surgir, contribuindo com o gerenciamento de riscos de forma que seja eficiente e ágil para a tomada de decisão. Associada ao Power BI, agrega informações no banco de dados para poder realizar a apresentação através das análises, tratando dados de grandes quantidades e complexidades em soluções de fácil entendimento, ajudando no conhecimento interno e auxiliando nas decisões dos gestores da organização.

Este trabalho não tem a intenção de ser a única fonte de informações para o tema proposto e teve limitações por questões de natureza sanitárias do Brasil (pandemia), por ter sido realizada apenas em uma instituição pública e de maneira remota e por ter utilizado como base somente uma ferramenta de BI.

Como sugestão futura para outros trabalhos 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.

REFERÊNCIAS

ARAUJO, M., Oliveira, E., & Monteiro, S. (2017). **Avaliação de maturidade de processos de gestão de riscos de TI: ferramenta de apoio para a qualidade e eficiência do processo.** *Revista Brasileira De Computação Aplicada*, 9(2), 111-124. Disponível em <<https://doi.org/10.5335/rbca.v9i2.6099>>. Acesso em: 22 ago. 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.

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 - International Standardization Organization. Disponível em: <<https://www.iso.org/standard/75281.html>>. Acesso em: 10 ago. 2021.

KONZEN, M. P.; NUNES, R.C.; FONTOURA, L.M. **Gestão de Riscos de Segurança da Informação Baseada na Norma NBR ISO/IEC 27005 Usando Padrões de Segurança.** Anais do IX Simpósio de Excelência em Gestão de Tecnologia (IX SEGet). Resende/RJ, 2012.

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

Nascimento, A. M. H., Prudente, F. B., de Carvalho, K. M., & Silva, R. S. (2022). **A Cogovernança na Gestão de Riscos nas Grandes Contratações do Poder Judiciário / Co-Governance in Risk Management in Large Contracts of the Judiciary.** *Brazilian Journal of Development*, 8(1), 4393–4418. <https://doi.org/10.34117/bjdv8n1-292>

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

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

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=S010067622002000500014&lng=en&nrm=iso>. Acesso em 02 Maio 2021. <https://doi.org/10.1590/S0100-67622002000500014>.