



UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE INFORMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

ANDERSON FRANÇA FERREIRA

**Aplicando a Análise *Bow Tie* no Gerenciamento do Risco de Perda de Eficiência Energética
em um *Data Center* de uma Instituição Federal de Ensino Superior**

Recife
2021

ANDERSON FRANÇA FERREIRA

Aplicando a Análise *Bow Tie* no Gerenciamento do Risco de Perda de Eficiência Energética em um *Data Center* de uma Instituição Federal de Ensino Superior

Dissertação apresentada ao Programa de Mestrado Profissional em Ciência da Computação do Centro de Informática da Universidade Federal de Pernambuco, como requisito parcial para a obtenção do grau de Mestre em Ciência da Computação.
Área de concentração: Sistema de Informação

Orientadora: Prof^a. Dr.^a Patricia Cabral de Azevedo Restelli Tedesco

Recife
2021

Catálogo na fonte
Bibliotecário Cristiano Cosme S. dos Anjos, CRB4-2290

F383a Ferreira, Anderson França
Aplicando a análise Bow Tie no gerenciamento do risco de perda de eficiência energética em um Data Center de uma Instituição Federal de Ensino Superior / Anderson França Ferreira. – 2021.
97 f.: il., fig., tab.

Orientador: Patrícia Cabral de Azevedo Restelli Tedesco.
Dissertação (Mestrado) – Universidade Federal de Pernambuco. CIn, Ciência da Computação, Recife, 2021.
Inclui referências e apêndices.

1. Sistemas de Informação. 2. Data Center. 3. Energia. 4. Eficiência energética. I. Tedesco, Patrícia Cabral de Azevedo Restelli (orientadora). II. Título.

681.3 CDD (23. ed.) UFPE - CCEN 2021 – 80

Anderson França Ferreira

“Aplicando a Análise *Bow Tie* no Gerenciamento do Risco de Perda de Eficiência Energética em um *Data Center* de uma Instituição Federal de Ensino Superior”

Dissertação apresentada ao Programa de Pós-Graduação Profissional em Ciência da Computação da Universidade Federal de Pernambuco, como requisito parcial para a obtenção do título de Mestre Profissional em 23 de fevereiro de 2021.

Aprovado em 23 de fevereiro de 2021.

BANCA EXAMINADORA

Profa. Carina Frota Alves
Centro de Informática / UFPE

Prof. Jorge da Silva Correia Neto
Universidade Federal Rural de Pernambuco

Profa. Patrícia Cabral de Azevedo Restelli Tedesco
Centro de Informática / UFPE
(Orientadora)

Dedico este trabalho primeiramente a Deus, que esteve sempre presente em minha vida proporcionando sempre o melhor, em seguida, a minha família e, amigos que souberam caminhar comigo na construção deste trabalho.

AGRADECIMENTOS

Agradeço ao meu bom e justo Deus que me concedeu a oportunidade de chegar tão longe.

Aos meus pais, João Ferreira Neto e Nerister França Ferreira que não se encontram neste plano terreno, mas que souberam com muito louvor transmitir educação e amor que considero base primordial para esta escrita e de lá, do plano superior, sei que estão orando e torcendo por mim.

À minha noiva e companheira de todos os momentos, Danúba Karen Sena Queiroz, dando-me incentivos para não desistir da escrita.

Ao meu irmão Adelson França Ferreira, minha cunhada Lidiane e sobrinho Lucas pelo carinho e amor que sempre me deram.

A minha querida tia e segunda mãe Maria de Lourdes Ferreira Leandro pelos incentivos constantes na minha educação.

Aos meus sogros Marconi Tavares de Queiroz e Núbia Goretti Sena Lins de Queiroz por me acolher tão bem me deixando muito a vontade e seguro nesta nova família.

Aos meus avôs paternos (Sr. Celso e Sra. Laura) e maternos (Sr. Francisco e Sra. Mercedes) que também se encontram no plano superior, mas que me deixaram maravilhosas recordações e aprendizados.

À colega Bruna Tarcília Ferraz que desde o início do processo para concorrer a uma vaga ao programa de mestrado dando incentivo e ajuda, e ao professor de língua inglesa Heleno Seixas pela ajuda na construção desta pesquisa.

Ao IFPE Campus Igarassu que flexibilizou minhas atividades profissionais ao longo do curso.

Aos amigos Edmilson Jeronimo e família, Marcos Gomes e Pedrosa e Eugênia, por estarem ao meu lado quando mais precisei neste últimos 2 anos.

Aos colegas do IFPE Marco Eugênio Araújo e Inêz Manuele dos Santos por ajudarem muito neste trabalho.

À minha orientadora Patrícia Cabral de Azevedo Restelli Tedesco pelas valiosas orientações no trabalho pelas dicas em sala de aula e principalmente pela confiança depositada em mim.

À professora do CIn Carina Frotas Alves por enriquecer com informações na minha qualificação.

À secretária do CIn Joelma França que sempre soube tratar a todos com muita atenção, carinho e deixou claro que sua atitude profissional seria de muita relevância na formação de todos.

À turma do MPROF 2018 em Gestão que se mostrou uma família.

Enfim, a todos que durante esta jornada estiveram de forma direta ou indireta participando desta construção que será de grande importância para a sociedade.

“Normas têm sido desenvolvidas para oferecer diretrizes sólidas e unificadas para que a eficiência energética seja obtida”. (MARIN,2016, p. 13).

RESUMO

O monitoramento do consumo de energia elétrica nos data centers das Instituições Federais de Ensino Superior é de fundamental importância para o controle dos gastos públicos, pois é, através de respostas rápidas das consequências provenientes do risco da perda da eficiência energética nestes ambientes que auxiliam um atendimento de boa qualidade a população e ao cumprimento das leis e as normas ambientais vigentes. Este trabalho, vem propor o uso de uma metodologia para auxiliar a Gestão na Tomada de Decisões sobre os ativos de um *data center* através do monitoramento dos equipamentos, e assim, tornando-os eficientes quanto ao consumo de energia elétrica. A pesquisa é baseada na metodologia *Bow Tie*, que utiliza uma ferramenta visual para auxiliar na Gestão de Riscos de Segurança da Informação observando a norma da ABNT NBR ISO/IEC 27005 de 2019 – Tecnologia da Informação – Técnicas de Segurança – Gestão de Riscos de Segurança da Informação. O levantamento das causas e consequências da perda de eficiência energética foi feito em 15 *campi*, além da EAD e da Reitoria do Instituto Federal de Pernambuco (IFPE), de acordo com a realidade de cada unidade gestora e respondido pelos representantes da Gestão de Tecnologia da Informação destas unidades. Neste trabalho, foi observado que a metodologia proposta consegue demonstrar os possíveis cenários que envolvem uma tomada de decisão, para se evitar a perda de eficiência energética em um *data center* do IFPE. De posse dos resultados obtidos da análise das respostas do formulário que foi encaminhado às unidades gestoras do IFPE, verificou-se que a metodologia *Bow Tie* consegue auxiliar de forma prática, simples e visual, tanto a gestão quanto a eficiência energética de um *data center* do IFPE, quando comparada a outras metodologias tradicionais fornecendo informações antecipadas para tomada de decisão em momentos críticos. Este trabalho de pesquisa pode, de forma adaptável, ser empregado em outras instituições da Administração Pública Federal ligado à área de Tecnologia da Informação.

Palavras-chave: Data Center. Energia. Eficiência Energética. TI Verde. Bow Tie.

ABSTRACT

The monitoring of electric energy consumption in the data centers of federal institutions of higher education plays a major role towards the control of public expenditure since it is through quick responses to the consequences arising from the risk of loss of energy efficiency in these environments that assist the population with good quality service and compliance with current environmental laws and regulations. This paper proposes the use of a methodology to assist management in making decisions about the assets of a data center by monitoring the equipment, and thus, making them efficient as to electric energy consumption. The research is based on the Bow Tie methodology, which uses a visual tool to assist in Information Security Risk Management, observing the ABNT NBR ISO / IEC 27005 2019 standard - Information Technology - Security Techniques - Information Security Risk Management. The survey of the causes and consequences of the loss of energy efficiency was carried out in 15 campuses, at the long-distance learning center (EAD) and at the office of the Rectorate at IFPE, in accordance with the reality of each management unit and answered by representatives of the Information Technology Management of these units. In this paper, it was observed that the proposed methodology is able to demonstrate, in a clear and objective way, all scenarios that involve decision making, to avoid the loss of energy efficiency in an IFPE data center. Upon considering the results obtained from the answers in the form submitted to the IFPE management units, it was observed that the bow tie methodology can support in a practical, simple, visual way, both the administration and the energetic efficiency of an IFPE data center, when compared to other traditional methodologies providing advance information for decision making at critical moments. This research can, in an adaptable way, be used in other Federal Public Administration institutions associated to the Information Technology area.

Keywords: Data Center. Energy. Efficiency Energy. Green IT. Bow tie.

LISTA DE FIGURAS

Figura 1 – Exemplo da Metodologia HAZOP	20
Figura 2 – Exemplo da Metodologia <i>What-If</i>	21
Figura 3 – Princípios, Estrutura e Processos da Gestão de Riscos	25
Figura 4 – Princípios da Gestão de Riscos	26
Figura 5 – Estrutura da Gestão de Riscos	27
Figura 6 – Processo.....	28
Figura 7 – Processo de Gestão de Risco	29
Figura 8 – Processo de Gestão de Risco de Segurança da Informação.....	31
Figura 9 – A Atividade de Tratamento de Risco.....	33
Figura 10 – Diagrama de <i>Bow Tie</i>	36
Figura 11 – Modelo de Diagrama Genérico do <i>Bow Tie</i>	37
Figura 12 – Passos para a Construção do Diagrama de <i>Bow Tie</i>	38
Figura 13 – Organograma Geral do IFPE	50
Figura 14 – Ferramenta BowTieXP	67
Figura 15 – Diagrama de <i>Bow Tie</i> para Tomada de Decisão Evitando a Perda de Eficiência Energética no <i>Data Center</i> do IFPE.....	68
Figura 16 – Indicação para o Planejamento de Compras de Forma mais Eficiente e Justificada	70
Figura 17 – Alerta para a Indisponibilidade de Recursos Financeiros	71
Figura 18 – Indicação para a Necessidade de Capacitação de Servidores.....	72

LISTA DE QUADROS

Quadro 1 – Equipamentos da Carga Crítica do <i>Data Center</i> do IFPE <i>Campus</i> Igarassu .	54
Quadro 2 – Fator de Potência, Tensão e Corrente da Carga Crítica do <i>Data Center</i> do IFPE <i>Campus</i> Igarassu.....	55
Quadro 3 – Carga, Frequência, Potência, FC e FES da Carga Crítica do <i>Data Center</i> do IFPE <i>Campus</i> Igarassu.....	56
Quadro 4 – Equipamentos da Carga do Sistema UPS do <i>Data Center</i> do IFPE <i>Campus</i> Igarassu.....	56
Quadro 5 – Fator de Potência, Tensão e Corrente da Carga do Sistema UPS do <i>Data Center</i> do IFPE <i>Campus</i> Igarassu.....	57
Quadro 6 – Carga, Frequência e Potência da Carga do Sistema UPS do <i>Data Center</i> do IFPE <i>Campus</i> Igarassu.....	57
Quadro 7 – Equipamentos da Carga de Iluminação do <i>Data Center</i> do IFPE <i>Campus</i> Igarassu.....	57
Quadro 8 – Carga, Frequência, Potência Nominal e Potência da Carga de Iluminação do <i>Data Center</i> do IFPE <i>Campus</i> Igarassu.....	58
Quadro 9 – Equipamentos da Carga de Climatização do <i>Data Center</i> do IFPE <i>Campus</i> Igarassu.....	58
Quadro 10 – Fator de Potência, Tensão e Corrente, da Carga de Climatização do <i>Data Center</i> do IFPE <i>Campus</i> Igarassu.....	58
Quadro 11 – Carga, Frequência, Capacidade e Potência Nominal da Carga de Climatização do <i>Data Center</i> do IFPE <i>Campus</i> Igarassu.....	58

LISTA DE GRÁFICOS

Gráfico 1 – Consumo de Energia Média por dia do IFPE Campus Igarassu entre 2018 e 2019	60
Gráfico 2 – Causas.....	63
Gráfico 3 – Barreiras Preventivas.....	64
Gráfico 4 – Fator de Escalonamento para Causas	64
Gráfico 5 – Barreiras Secundárias para Causas.....	65
Gráfico 6 – Consequências.....	65
Gráfico 7 – Barreiras Protetivas	66
Gráfico 8 – Fatores de Escalonamento para Consequências	66
Gráfico 9 – Barreiras Secundárias para Consequências	67

LISTA DE TABELAS

Tabela 1 – Valores de Referência do PUE e DCiE	44
Tabela 2 – Resultado da Busca dos Trabalhos Relacionados	46
Tabela 3 – Contribuições das Pesquisas.....	48
Tabela 4 – Valores do PUE e DCiE do <i>Data Center</i> do IFPE <i>Campus</i> Igarassu entre 2018 e 2019	59
Tabela 5 – Consumo Elétrico do <i>Data Center</i> do IFPE <i>Campus</i> Igarassu.....	59

LISTA DE ABREVIATURAS E SIGLAS

A3P	Agenda Ambiental na Administração Pública
ABNT	Associação Brasileira de Normas Técnicas
ANSI	American National Standards Institute
BICSI	Building Industry Consulting Service International
CAPES	Coordenação de Aperfeiçoamento de Pessoal de Nível Superior
CGTI	Coordenação de Gestão de Tecnologia da Informação
CGU	Controladoria Geral da União
Ci	Consequências de Acidentes
CO2	Dióxido de Carbono
CONSUP	Conselho Superior
CTI	Coordenação de Tecnologia da Informação
CTIC	Coordenação de Tecnologia da Informação e Comunicação
DADT	Diretoria de Avaliação e Desenvolvimento de Tecnologia
DCE	Data Center Effectiveness
DCiE	Data Center Infrastructure Effectiveness
DCIM	Data Center Infrastructure Management
DGTI	Departamento de Gerencia de Tecnologia da Informação
EAD	Educação a Distância
ECO-92	Conferência das Nações Unidas sobre o Meio Ambiente e o Desenvolvimento
EDC	Energia Data Center
ETI	Equipamentos de Tecnologia da Informação
EUA	Estados Unidos da América
FC	Fator de Crescimento
FES	Fator de Espaço de Suporte
FMEA	Failure Mode and Effect Analysis

HAZOP	Hazard and Operability Study
IEC	International Electrotechnical Commission
IEi	Eventos Intermediários
IFPE	Instituto Federal de Educação, Ciência e Tecnologia de Pernambuco
I/O	Input / Output
ISO	International Organization for Standardization
ISO/IEC	International Organization of Standardization / International Electrotechnical Commission
IT	Information Technology
KVA	Kilovolt-ampere
KW	Kilowatt
MP	Ministério Público
NBR	Norma Brasileira
NGRis	Núcleo de Gestão de Riscos
OBS	Observação
PEi	Eventos Primários
PROPESQ	Pró-Reitoria de Pesquisa, Pós-Graduação e Inovação
PUE	Power Usage Effectiveness
SBi	Barreiras de Segurança
SGSI	Sistema de Gestão de Segurança da Informação
TE	Evento Topo
TI	Tecnologia da Informação
TIA	Telecommunications Infrastructure Standard
TIC	Tecnologia da Informação e Comunicação
UPS	Uninterruptable Power Supply
UTI	Unidade de Terapia Intensiva

XX

Século 20

XXI

Século 21

SUMÁRIO

1	INTRODUÇÃO	18
1.1	DESCRIÇÃO DO PROBLEMA E MOTIVAÇÃO.....	21
1.2	OBJETIVOS	22
1.2.1	Objetivo Geral.....	22
1.2.2	Objetivo Específico	22
1.3	ORGANIZAÇÃO DO TRABALHO.....	22
2	FUNDAMENTAÇÃO TEÓRICA	24
2.1	GESTÃO DE RISCOS.....	24
2.2	GESTÃO DE RISCOS DE TI	28
2.3	<i>BOW TIE</i>	34
2.3.1	Definição	34
2.3.2	Estrutura	35
2.4	TIC	39
2.5	TI VERDE	39
2.6	SUSTENTABILIDADE	40
2.7	<i>DATA CENTER VERDE</i>	42
2.8	EFICIÊNCIA ENERGÉTICA PARA <i>DATA CENTERS</i>	43
2.9	CONSIDERAÇÕES	44
3	TRABALHOS RELACIONADOS.....	45
3.1	CRITÉRIOS DE ANÁLISES DOS TRABALHOS	45
3.2	DESCRIÇÃO DOS TRABALHOS	46
3.3	CONSIDERAÇÃO DO CAPÍTULO.....	48
4	MATERIAIS E MÉTODOS	49
4.1	CARACTERIZAÇÃO DA PESQUISA.....	49
4.2	UNIDADE DE ESTUDO	50
4.3	PROCEDIMENTO PARA COLETA DE DADOS	51
4.4	ASPECTOS ÉTICOS	51
4.5	ANÁLISE DOS DADOS.....	52
4.6	CONSIDERAÇÃO DO CAPÍTULO.....	52
5	RESULTADOS	54
5.1	<i>POWER USAGE EFFECTIVENESS E DATA CENTER INFRASTRUCTURE EFFECTIVENESS</i>	54
5.2	GESTÃO DE RISCO DA PERDA DA EFICIÊNCIA ENERGÉTICA NOS <i>DATA CENTERS</i> DO IFPE.....	60

5.3	CONSIDERAÇÃO DO CAPÍTULO.....	72
6	CONCLUSÃO.....	74
6.1	PRINCIPAIS CONTRIBUIÇÕES.....	75
6.2	AMEAÇAS E LIMITAÇÕES.....	75
6.3	TRABALHOS FUTUROS	76
	REFERÊNCIAS.....	77
	APÊNDICE A – QUESTIONÁRIO	80
	ANEXO A – DESPACHO DO TERMO DE ANUÊNCIA DA PESQUISA	95
	ANEXO B – TERMO DA ANUÊNCIA DA PESQUISA	97

1 INTRODUÇÃO

A busca constante por atender à necessidade crescente da sociedade para entregar produtos e serviços, de forma eficiente e eficaz, vem crescendo desde a Revolução Industrial. Desse modo, para atender e acompanhar esta demanda, o uso de recursos naturais, através do consumo de energia elétrica produzida pelas diversas categorias de matrizes energéticas espalhadas pelo mundo, cresce de forma proporcional e sem o devido controle a cada ano.

Com este consumo desordenado, o impacto ambiental trouxe consequências indesejáveis, produzidas pelas organizações, que viriam a ocorrer nos anos seguintes. Desta forma, os problemas de ordem ambiental acabaram redirecionando a competitividade na década passada, com as mudanças nos valores sociais e o desenvolvimento de novas tecnologias, no surgimento de produtos ecologicamente corretos. Assim, tiveram início os novos movimentos “verdes”, tendo como principais objetivos a redução da poluição e da energia no desenvolvimento de produtos e serviços (QUEIRÓS, 2019).

A geração de energia ou matriz energética, muitas vezes, não consegue conciliar a produção com os aspectos ambientais, devido às condições climáticas ou de relevo de uma determinada região, só é possível produzir energia de uma fonte. Percebe-se que nos Estados Unidos a queima de carvão mineral representa ainda a maior fonte de energia consumida e, conseqüentemente, a principal fonte de emissão de gás carbônico daquele país (MARIN, 2016). Há uma relação entre o consumo de energia elétrica e a emissão de Dióxido de Carbono (CO₂) na atmosfera. Essa relação será mais ou menos importante dependendo da forma como a energia elétrica é gerada em uma determinada região geográfica (MARIN, 2016). No Brasil, a maior parte da geração de energia elétrica é produzida pelas centrais de usinas hidrelétricas, considerada uma das formas de matriz energética mais limpa se comparada a de carvão mineral, mas mesmo assim, não podemos ignorar o impacto ambiental de uma construção deste porte numa área que antes abrigava animais e pessoas.

O avanço científico e tecnológico das últimas décadas, segundo Salles e colegas (2013), desconsiderou a conexão entre economia e ecologia, tendo como resultado negativo a degradação ambiental. A diminuição de reservas de recursos não renováveis, o aumento de resíduos sólidos *per capita* e a redução de espaço para o seu armazenamento são exemplos de consequências de um desenvolvimento não sustentável. As práticas de gestão ambiental começaram a surgir em algumas empresas no século XXI, não apenas de forma reativa, mas também proativa. A produção começou a conciliar os resultados positivos financeiros esperados com termos ambientais exigidos pelos órgãos de controle, com isso foi possível verificar a redução de desperdícios de recursos (SALLES et al., 2013). O melhor aproveitamento da matéria prima e insumos repercutiram na produção até chegar no consumidor final com descartes lançados no meio ambiente.

As grandes empresas começaram a se preocupar com os recursos naturais, sabendo que eles não são inesgotáveis (MORETTI, 2010). Para Salles e colegas (2013), cada vez mais as

questões relacionadas à sustentabilidade e o meio ambiente têm se destacado, tanto no meio acadêmico como no meio empresarial. Pensando assim, não é mais possível para as empresas ignorarem as leis e regras ambientais, adequando sua maneira de conduzir a sua produção de forma a não prejudicar meio ambiente. Boa parte das organizações possui uma grande interação com o ambiente e as comunidades do entorno da área de suas operações, demandando, entretanto, elevados investimentos financeiros para implementar ações ambientalmente corretas (MARTIN, 2018).

As construções começaram a seguir o caminho sustentável, tanto na sua produção como em conceitos arquitetônicos. Os *Data Centers* experimentaram nos últimos anos um crescimento exponencial em sua capacidade de processamento, aumentando significativamente também o consumo de energia, tanto para os servidores, como para a infraestrutura elétrica e de refrigeração (GOLDHAR, 2009). De maneira análoga os *data centers* verdes surgiram com o propósito de estimular a preservação ambiental procurando diminuir o impacto causado ao meio ambiente e o consumo excessivo de energia elétrica. Para isso, foi preciso aplicar técnicas e ferramentas disponíveis no mercado, escolhendo meios eficazes, para minimizar essas decorrências. Assim, algumas alternativas foram propostas, tais como o de concentrar no gerenciamento de data center os serviços e dispositivos de TI, de climatização, de energia, de estrutura física e de monitoramento. Implementar algumas alternativas como: virtualização e consolidação de servidores, desativar servidores sem uso, aquisição de servidores energeticamente eficientes, *layout* e confinamento de corredores quentes e frios, dispositivos de gerenciamento do fluxo de ar, ajustes de temperatura e umidade de entrada, economizadores a ar e a água (GUIRARDI; FEITOZA, 2019).

Muitos métodos de avaliação de risco foram projetados ao longo da história para auxiliar as organizações na continuidade do seu negócio. Algumas Metodologias de Análise de Risco, como *Hazard and Operability Study* (HAZOP) ou “Estudo de Perigos e Operabilidade” é uma técnica de identificação de perigos durante a operação de um processo que consiste em identificar desvios de variáveis em relação a valores estabelecidos como normais (OLIVEIRA et al., 2011). A metodologia *What-If* é uma técnica que consiste em detectar perigos utilizando questionamento aberto promovido pela pergunta E se. . . ? O objeto da *What-If* pode ser um sistema, processo, equipamento ou evento (MARTINS; SIMÕES JUNIOR; MENEZES, 2010). Tanto a metodologia HAZOP quanto a metodologia *What-If* apresentam seus dados de forma textual em tabelas sendo pouco eficiente quando existem uma grande informação de dados, conforme exemplificados nas figuras 1 e 2. Outro método que pode ser usado para avaliar todos os tipos de riscos é a análise *bow tie* (JACINTO; SILVA, 2009). O método de *bow tie*, que é uma combinação de análise de árvore de falhas e análise de árvore de eventos, é muito popular porque incorpora as causas e consequências do cenário do acidente através de um diagrama. Segundo Afefy (2015), o diagrama *bow tie* é usado para avaliação de risco, gerenciamento de risco e comunicação de risco. Esta metodologia fornece uma visão geral melhor da situação dos riscos e ajuda as pessoas

a entender a relação entre os riscos e os eventos organizacionais.

Figura 1 – Exemplo da Metodologia HAZOP

Sistema: Caldeira / Vaso de Pressão					
Parâmetro: Pressão (Vapor)					
Nó: 03					
Palavra Guia	Desvio	Causas	Deteção	Consequências	Providências
Mais	Pressão	<ul style="list-style-type: none"> • Não abertura do registro de purga (RE-2) (falha do operador); e • Entupimento do sistema de purga e descarga. 	<ul style="list-style-type: none"> • Manômetro do vaso de pressão (M-2); e • Visual (saída do purgador sem sinal de vapor). 	<ul style="list-style-type: none"> • Acúmulo de água no vaso de pressão ocasionando perdas produtivas; • Risco de acidente no momento de acionar manualmente o purgador (queima por vapor); • Gastos com manutenção corretiva; e • Atraso na produção. 	<ul style="list-style-type: none"> • Elaboração de procedimento operacional (manual); • Instalação de saída auxiliar para casos de emergência; • Manutenção periódica preventiva; • Capacitação do operador; e • Elaboração de procedimento de emergência em caso de acidente.
Menos	Pressão	<ul style="list-style-type: none"> • Descarga (RE-3) aberta durante operação (falha do operador); e • Vazamento na tubulação 	<ul style="list-style-type: none"> • Manômetro do vaso de pressão (M-2); e • Visual (vazamento de vapor). 	<ul style="list-style-type: none"> • Risco de acidente no caso de vazamento de vapor; • Gastos com manutenção corretiva; e • Atraso na produção. 	<ul style="list-style-type: none"> • Elaboração de procedimento operacional (manual); • Manutenção periódica preventiva; • Capacitação do operador; e • Elaboração de procedimento de emergência em caso de acidente.

Fonte: Oliveira et al. (2011).

Figura 2 – Exemplo da Metodologia *What-If*

E se...? Identificação de Perigos		
Objeto da análise: Festa de aniversário		Folha:
Executado por: Maria Pereira		Data:
E se...???	Perigo/ Consequência	Medidas de controle de risco e emergência
Vierem mais pessoas que o esperado?	Falta de espaço, falta de bebidas	Avaliar a possibilidade de comparecerem mais convidados e prever alimentos e bebidas com folga
As pessoas não encontrarem o local da festa?	Desagradar amigos, criar clima de insatisfação, não receber presentes, perda de alimentos	Anexar mapa aos convites, acrescentando número do telefone
Chover ?	Dificuldades na chegada, pessoas com roupa molhadas	Adquirir guarda-chuva grande para ajudar as pessoas a deslocarem-se do carro à porta de casa

Fonte: Martins et al. (2010).

1.1 DESCRIÇÃO DO PROBLEMA E MOTIVAÇÃO

Diante dos cortes no orçamento em 2019, feitos pelo Governo Federal, o Instituto Federal de Pernambuco (IFPE), assim como outros órgãos, precisou ajustar seus gastos de forma que pudesse chegar ao final do ano com as contas pagas em dia. Diversas medidas foram tomadas para reduzir custos, entre elas a economia de energia elétrica, através do uso racional, em todos os *campi*, reitoria e na Educação a Distância (EAD).

Antes mesmo desse cenário conturbado, os órgãos públicos já precisavam estar atentos a questões similares, abordadas pelo artigo 22 da Lei 8.078, de 11 de setembro de 1990, que se refere à proteção do consumidor, onde informa que eles são obrigados a fornecer serviços adequados, eficientes e seguros.

Não menos importante, a Agenda 21 Brasileira como afirmam CARLOS e colegas (2002), é um processo e instrumento de planejamento participativo para o desenvolvimento sustentável, e que tem como eixo central a sustentabilidade, compatibilizando a conservação ambiental, a justiça social e o crescimento econômico. Este documento é resultado de uma grande consulta à população brasileira, sendo construída a partir das diretrizes da Agenda 21 global (CARLOS et al., 2002). Trata-se, assim, de um instrumento fundamental para a construção da democracia participativa e da cidadania ativa no País.

Entender o impacto de novas aquisições para suportar o crescimento operacional devido ao aumento da demanda, pode parecer inicialmente que a instituição está bem, mas se não houver um estudo detalhado e um planejamento consciente nas aquisições de novos equipamentos, o resultado ao longo do tempo será de uma ineficiência energética crescente e como consequência aumento do consumo de energia elétrica.

A partir do cenário descrito, pode ser levantando o seguinte questionamento: Como gerenciar o Risco de Perda de Eficiência Energética em um *data center* no IFPE?

Para responder ao questionamento principal da pesquisa, será necessário responder a outras questões mais específicas, como:

- Como manter um monitoramento constante dos ativos de um *data center* de forma eficaz e eficiente?
- Como manter uma equipe bem treinada e com conhecimento técnico sempre atualizado para que possam desempenhar suas funções de forma que evitem ou diminuam o desperdício de energia nestes ambientes?

1.2 OBJETIVOS

1.2.1 Objetivo Geral

Propor um Modelo de Gestão de Risco de Tecnologia da Informação no IFPE em um ambiente de Data Center, utilizando a metodologia visual Bow Tie.

1.2.2 Objetivo Específico

Para alcançar o objetivo geral será necessário obter os resultados dos objetivos específicos listados abaixo em cada unidade gestora do IFPE de acordo com a realidade de cada unidade:

- Levantar o *Power Usage Effectiveness* (PUE) e o *Data Center Infrastructure Effectiveness* (DCiE);
- Definir o Contexto em que está inserido o *Data Center* da pesquisa e Identificar os Riscos (Ameaças e Consequências) de acordo com a Associação Brasileira de Normas Técnicas (ABNT) Norma brasileira (NBR) *International Organization for Standardization/International Electrotechnical Commission* (ISO/IEC) 27005:2019;
- Validar junto aos Diretores e Coordenadores de TI de cada unidade gestora do IFPE as prioridades na tomada de decisão sobre os aspectos de ameaça (causa) e efeito diante de um cenário de perda de eficiência energética no *data center* do IFPE;
- Representar o Diagrama de *Bow Tie* de acordo com a validação das prioridades apresentadas no estudo.

1.3 ORGANIZAÇÃO DO TRABALHO

O presente trabalho está organizado em 6 capítulos, além desta introdução. O capítulo 2, descreve a fundamentação teórica, apresentando os conceitos que servirão de base para esta

pesquisa. O capítulo 3, apresenta os critérios de análises dos trabalhos adotados nesta pesquisa de dissertação. No capítulo 4, é apresentada a metodologia que foi utilizada para o alcance do objetivo do trabalho. O capítulo 5, apresenta os resultados obtidos. O capítulo 6 apresenta as contribuições deste trabalho, ameaças à validade, limitações e sugestões para trabalhos futuros.

2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo são apresentados os conceitos que fundamentaram esta pesquisa, a saber: Gestão de Risco, Gestão de Risco de TI, *Bow Tie*, TIC, TI Verde, Sustentabilidade, *Data Center* Verde e Eficiência Energética para *Data Centers*. Espera-se que desta forma fique mais claro para o leitor as ideias, ao longo da leitura desta dissertação através das referências de outros autores.

2.1 GESTÃO DE RISCOS

Inicialmente cabe compreender que riscos estão presentes em todas as atividades humanas, em todos os lugares e em todos os níveis de atividades corporativas, mesmo que em diferentes graus de intensidade, representando a incerteza sobre um estado futuro ou a incerteza sobre o alcance de um objetivo (TRIVELATO; MENDES; DIAS, 2018). A gestão de riscos é uma das funções primordiais dos conselhos de administração dentro de um processo de governança corporativa (SILVEIRA, 2010).

A gestão de riscos são trabalhos e esforços direcionados com o intuito de manter o controle no que se refere a riscos. Ela é formada por uma estrutura que fornecem os fundamentos e os arranjos organizacionais para a concepção, implementação, monitoramento, análise crítica e melhoria contínua da gestão de riscos através de toda uma organização. O propósito da gestão do risco é a criação e proteção de valor melhorando o desempenho e encorajando a inovação, bem como apoiando o alcance de objetivos, de acordo com ABNT NBR ISO 31000:2018.

A Gestão de Risco fornece uma abordagem simples para gerenciar qualquer tipo de riscos, podendo ser usado durante a vida de diversas organizações sendo aplicado a qualquer atividade, incluindo a tomada de decisões em todos os níveis de uma organização.

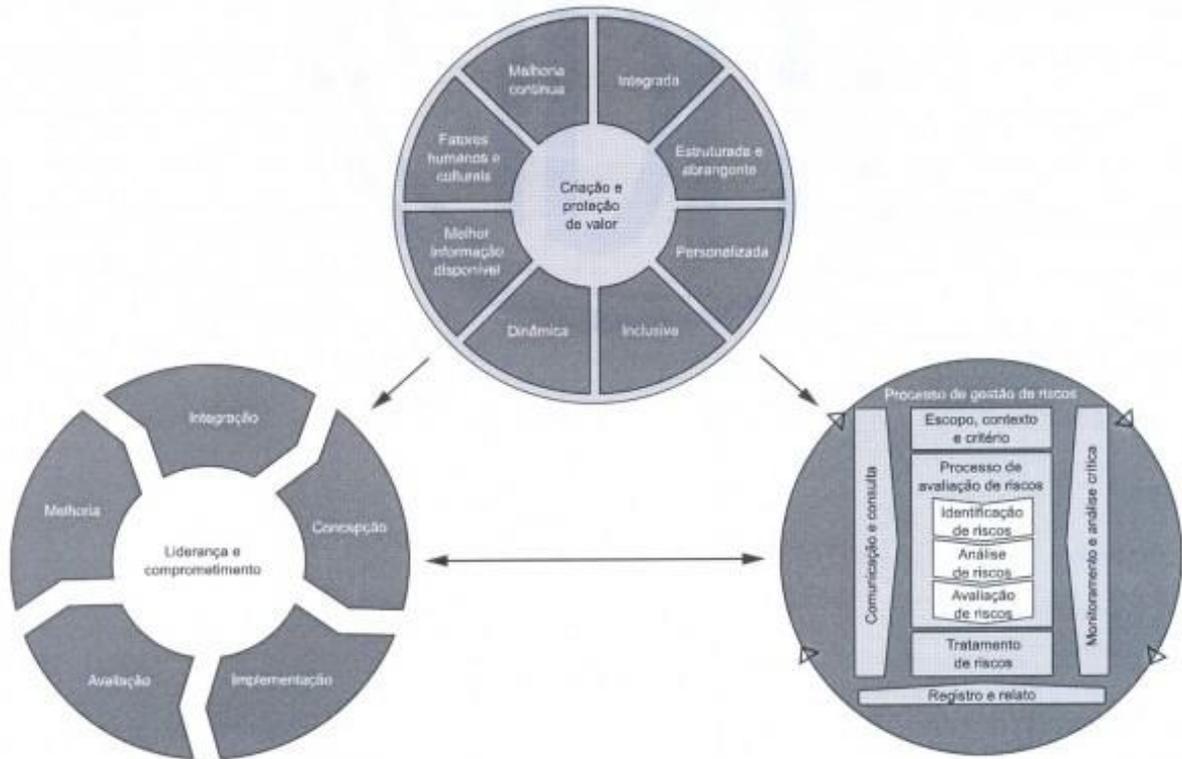
As organizações de diversos portes, como informa a ABNT NBR ISO/IEC 27005: 2019, enfrentam fatores e influências tanto externas, quando se busca o controle dos riscos nos negócios sob a ótica da segurança da informação, como internas, quando as atividades são formalizadas e coordenadas para controlar e dirigir um conjunto de instalações e pessoas com relações e responsabilidades entre si. A gestão dos riscos é iterativa e auxilia estas organizações na definição da estratégia, objetivos e na tomada de decisões. É parte da governança e liderança, sendo considerada fundamental para a maneira de como a organização é gerenciada em todos os níveis, contribuindo para a melhoria constante dos sistemas de gestão organizacional.

A gestão de riscos, segundo a ABNT NBR ISO/IEC 27005: 2019, está inserida nas atividades associadas a uma organização, onde inclui a interação com as partes interessadas. Considera-se ainda o contexto externo e interno da organização, incluindo aspectos humanos e os fatores culturais da empresa.

A gestão de risco baseia-se nos princípios, estrutura e processo, conforme ilustrado na figura 3. Tais princípios podem já existir de forma total ou parcial numa organização, porém, eles

podem precisar ser adaptados ou melhorados para que o gerenciamento do risco seja eficiente, eficaz e consistente.

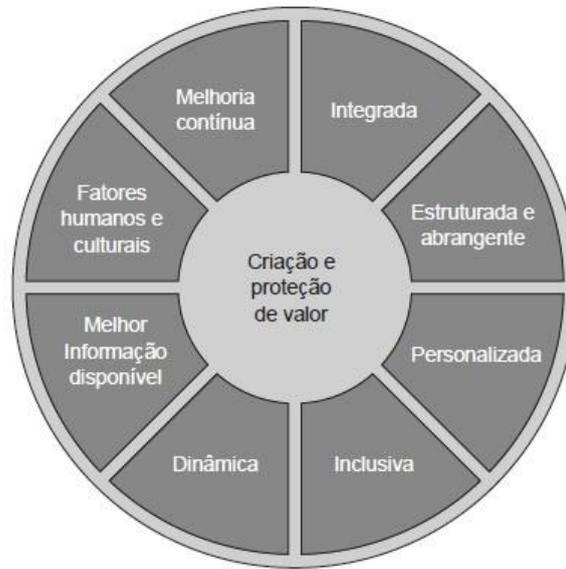
Figura 3 – Princípios, Estrutura e Processos da Gestão de Riscos



Fonte: ABNT NBR ISO 31000 (2018).

Os princípios fornecem orientações sobre as características da gestão de riscos de forma eficaz e eficiente, comunicando seu valor e explicando sua intenção e propósito. Os princípios são a base para gerenciar riscos, desta maneira, eles devem ser aceitos quando forem estabelecidos a estrutura e os processos de gestão de riscos da empresa. Estes princípios possibilitarão que as empresas possam gerenciar os efeitos de incertezas em seus objetivos, conforme demonstrado na figura 4.

Figura 4 – Princípios da Gestão de Riscos



Fonte: ABNT NBR ISO 31000 (2018).

O propósito da estrutura da gestão de riscos é apoiar a organização na integração da gestão de riscos em atividades significativas e em algumas funções. Ou seja, a eficácia da gestão de riscos dependerá de sua integração na governança e em todas as atividades da empresa, incluindo a tomada de decisão, requerendo com isso o apoio das partes envolvidas e interessadas, como, por exemplo, a alta gestão da organização. Fazem parte desta estrutura: integração, concepção, implementação, avaliação e melhoria da gestão de riscos. A estrutura da gestão de riscos é representada na figura 5.

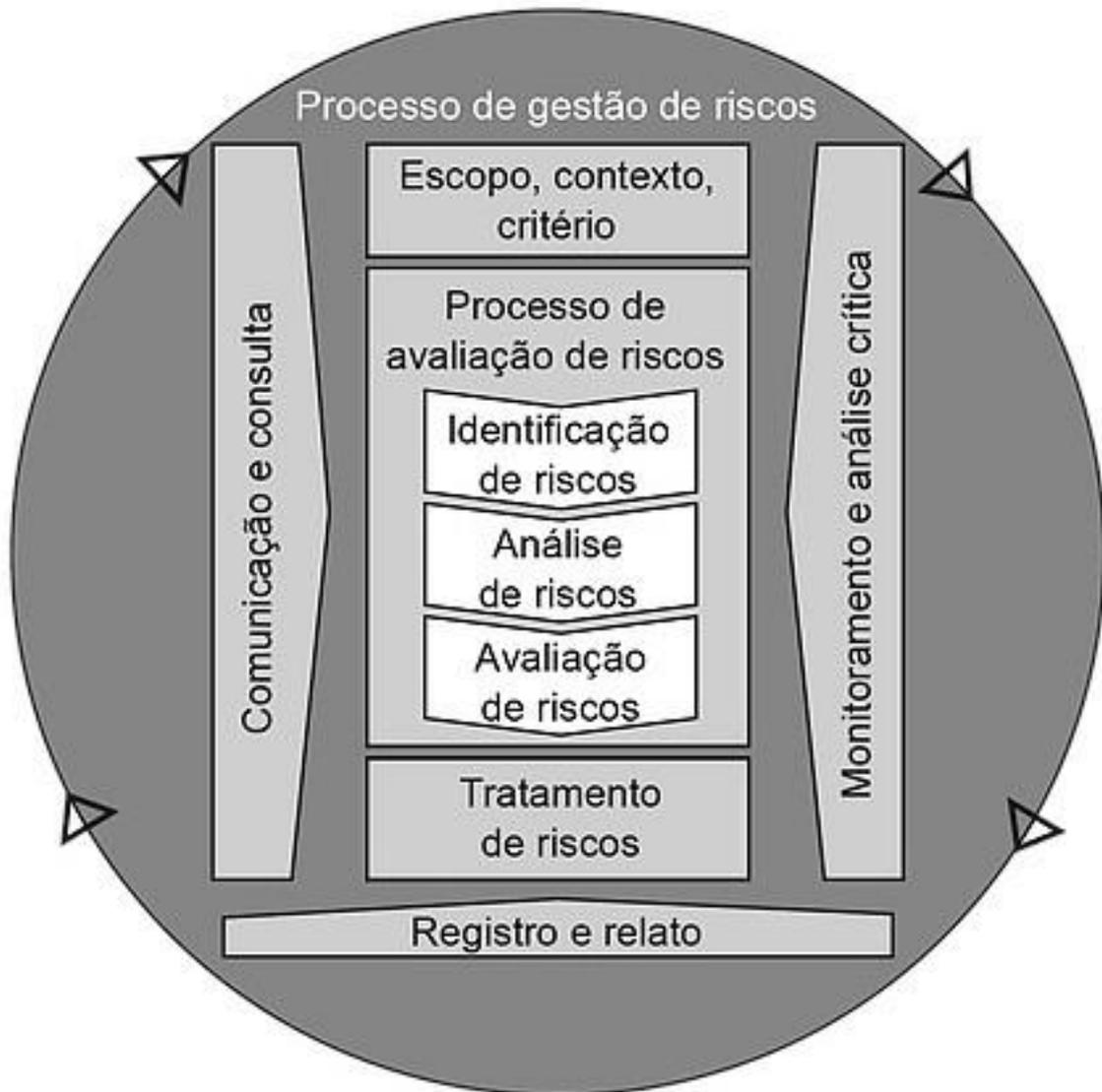
Figura 5 – Estrutura da Gestão de Riscos



Fonte: ABNT NBR ISO 31000 (2018).

O processo de gestão de riscos relaciona-se com a aplicação sistemática de políticas, procedimentos e práticas para as atividades de contexto, processo de avaliação e riscos (Identificação, Análise e Avaliação), tratamento, monitoramento e comunicação de forma iterativa. O processo de gestão de riscos é demonstrado na figura 6.

Figura 6 – Processo

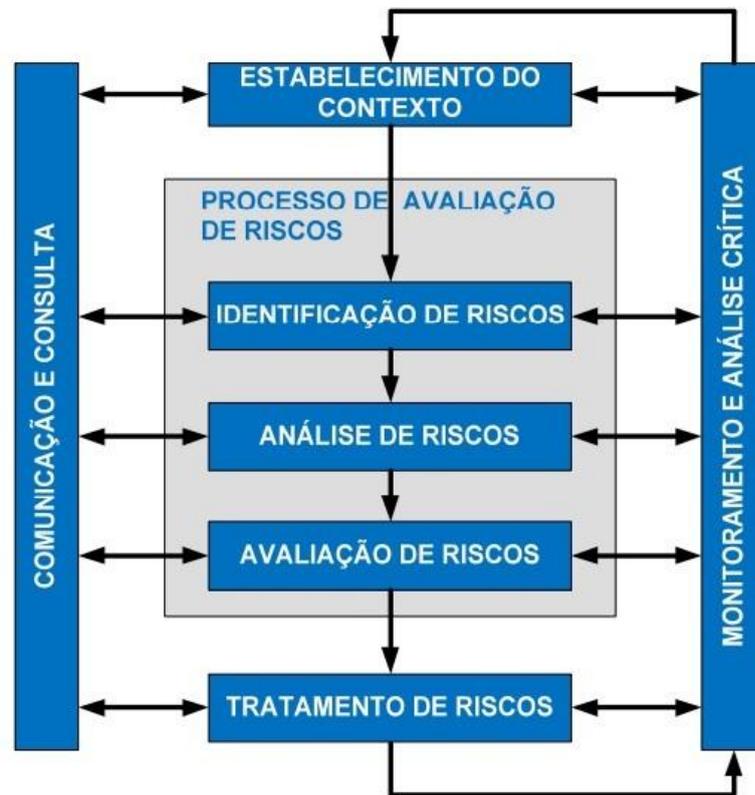


Fonte: ABNT NBR ISO 31000 (2018).

2.2 GESTÃO DE RISCOS DE TI

A tecnologia da informação possui papel fundamental nas organizações, figurando como um componente estratégico para seus processos de negócio. A aplicação da gestão de riscos no contexto da governança de TI é fator crítico de sucesso para o alcance dos objetivos estratégicos das organizações (ARAÚJO; OLIVEIRA; MONTEIRO, 2017). Como demonstrado na figura 7, os conceitos de processos observados na Gestão de Riscos pela norma ABNT NBR ISO 31000:2018 são absorvidos no ambiente de Tecnologia da Informação. Portanto, no mundo corporativo, ela visa administrar os riscos inerentes à propriedade, ao envolvimento, à operação, à influência, à adoção e ao uso de TI como parte dos negócios da organização.

Figura 7 – Processo de Gestão de Risco



Fonte: ABNT ISO/IEC 27005 (2019).

O processo de gestão de risco da segurança da informação inicia-se quando o contexto é identificado, seguido de um processo de avaliação de riscos. Portanto, quando as informações são suficientes para que se determine de forma eficaz as ações necessárias para reduzir os riscos, a um nível aceitável, então a tarefa está concluída e o tratamento do risco já pode ser realizado. Caso contrário, se as informações forem insuficientes, deve-se proceder com uma outra iteração do processo de avaliação de riscos, revisando-se o contexto (por exemplo: os critérios de avaliação de riscos, de aceitação do risco ou de impacto), possivelmente em partes limitadas do escopo. A figura 8 demonstra o processo de gestão de risco da segurança da informação.

A eficácia no tratamento do risco vai depender dos resultados do processo de avaliação de riscos. Destaca-se que o tratamento do risco envolve um processo cíclico para: avaliar um tratamento do risco, decidir se os níveis de risco residual são aceitáveis, gerar um novo tratamento do risco se os níveis de risco não forem aceitáveis e avaliar a eficácia do tratamento.

Entretanto, pode ocorrer que o tratamento do risco não resulte em um nível de risco residual aceitável e diante desta situação, será necessária uma outra iteração do processo de avaliação de riscos, com mudanças nas variáveis do contexto (por exemplo: os critérios para o processo de avaliação de riscos, de aceitação do risco e de impacto), seguida por uma fase adicional de tratamento do risco.

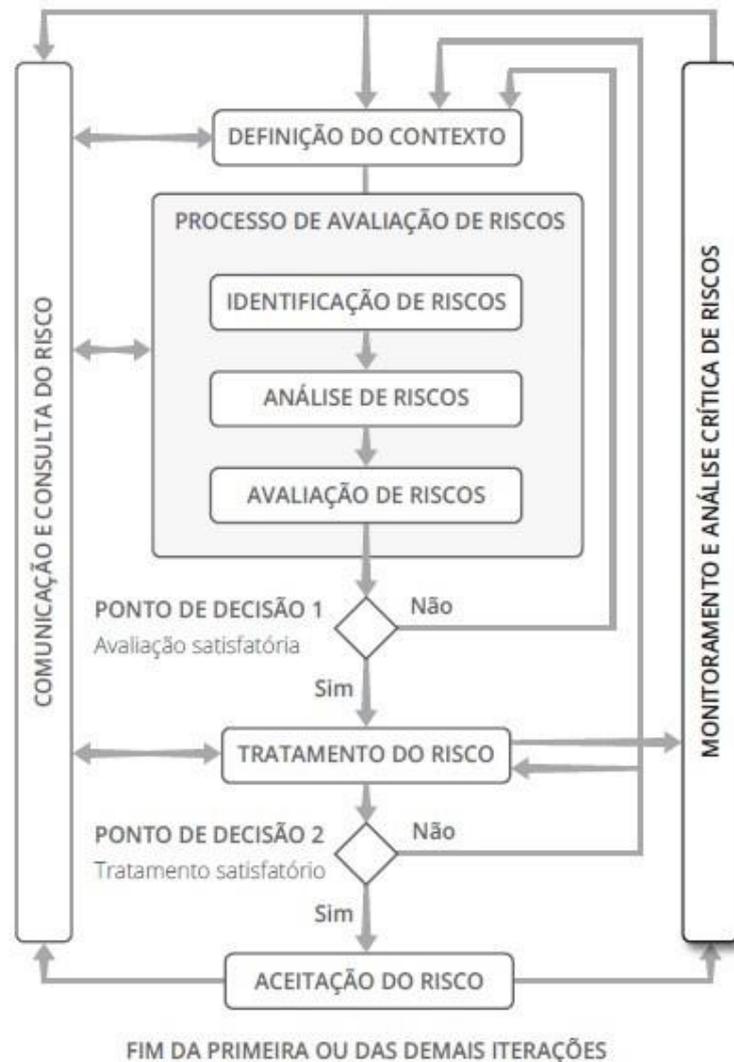
Na aceitação do risco é preciso assegurar que os riscos residuais sejam explicitamente

aceitos pelos gestores da organização, pois é muito importante em uma situação em que a implementação de controles é omitida ou adiada, tal como, devido aos altos custos. Durante o processo de gestão de riscos de segurança da informação, os riscos e a forma com que são tratados sejam comunicados ao pessoal das áreas operacionais e gestores apropriados de forma prioritária.

Mesmo antes do tratamento do risco, históricos sobre riscos identificados podem ser muito úteis para gerenciar incidentes e ajudar a reduzir possíveis prejuízos. A conscientização dos gestores e pessoal em relação aos riscos, à natureza dos controles aplicados para mitigá-los e às áreas definidas como de interesse pela organização, auxiliam a lidar com os incidentes e eventos não previstos da maneira mais efetiva.

Os resultados minuciosos de cada atividade do processo de gestão de riscos de segurança da informação, bem como as decisões sobre o processo de avaliação de riscos e o tratamento do risco, precisam ser documentados para possíveis revisões ou dados históricos. A norma ISO/IEC 27001 especifica que os controles implementados no escopo, limites e contexto do Sistema de Gestão de Segurança da Informação (SGSI), devem ser fundamentados em risco.

Figura 8 – Processo de Gestão de Risco de Segurança da Informação



Fonte: ABNT ISO/IEC 27005 (2019).

O tratamento do risco deve ter como base o resultado do processo de avaliação de riscos, no custo esperado para implementação deste tratamento e nos benefícios previstos. Assim, quando ocorrer uma grande modificação do risco a custo relativamente pequeno e desejável todas as implementações devem ser feitas, caso contrário, deve-se fazer uma análise precisa para verificar suas justificativas.

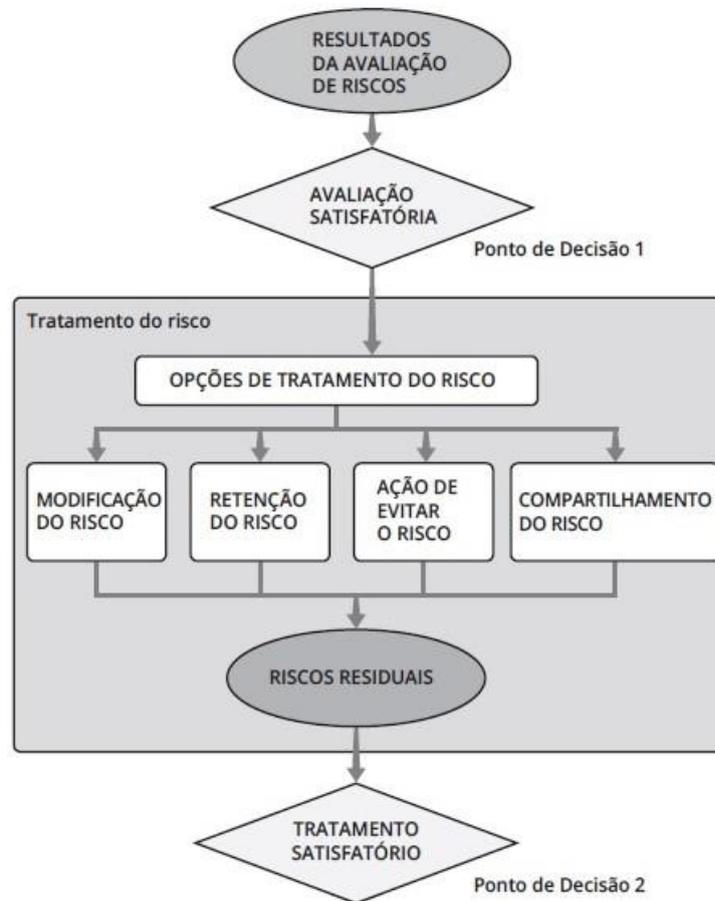
Em geral, as consequências adversas do risco devem ser reduzidas o máximo possível, independentemente de qualquer critério absoluto. Os gestores devem ainda considerar os riscos improváveis de forma grave, pois os controles que não forem justificáveis do ponto de vista estritamente econômico, podem precisar ser implementados. As quatro opções para o tratamento do risco, conforme figura 9 não são mutuamente exclusivas, pois muitas empresas podem se beneficiar de uma combinação de opções, como a redução da probabilidade do risco, a redução de suas consequências e o compartilhamento ou retenção dos riscos residuais. Algumas outras formas de tratamento do risco podem utilizar mais de um risco de forma efetiva, como por

exemplo: um treinamento e a conscientização em segurança da informação. Para isso, deve ser definido um plano de tratamento do risco, identificando de forma clara a ordem de prioridades, assim como os prazos de execução. As prioridades podem ser estabelecidas usando várias categorias técnicas, incluindo a ordenação dos riscos e a análise de custo-benefício. Cabe aos gestores da empresa o equilíbrio dos custos da implementação dos controles e o orçamento.

A identificação de controles existentes pode levar a uma falsa ideia de que estes excedem as necessidades atuais em função da comparação de custos, incluindo a manutenção. Se a remoção de controles redundantes é desnecessária e tiver que ser considerada, especialmente se os controles têm alto custo de manutenção, devem-se considerar a segurança da informação e os fatores de custo. Devido à influência que os controles exercem uns sobre os outros, a remoção de controles redundantes pode reduzir a segurança em vigor na totalidade. Talvez inclusive, seja até menos dispendioso deixar controles com redundância ou desnecessários do que removê-los. O processo de gestão de riscos de TI permite a uma organização, além de identificar o seu nível atual de maturidade, conhecer os caminhos para evolução de seus processos de governança de TI, através do monitoramento e análise crítica em busca da melhoria contínua de seu processo de gestão de riscos (ARAÚJO; OLIVEIRA; MONTEIRO, 2017).

Outro cuidado que se deve ter sobre como o risco é percebido pelas partes afetadas e sobre as formas mais apropriadas de comunicação entre as partes envolvidas. É importante que todas as restrições organizacionais, técnicas, estruturais; identificadas durante a atividade de definição de contexto, sejam levadas em conta durante o tratamento do risco. Uma vez que o plano de tratamento do risco tenha sido definido, os riscos residuais precisam ser analisados novamente, posto que isso envolve uma atualização do processo de avaliação de riscos, considerando-se os efeitos já previstos do tratamento do risco que foi proposto anteriormente. Caso o risco residual ainda não satisfaça aos critérios para a aceitação do risco da organização, uma nova iteração do tratamento do risco poderá ser necessária antes de prosseguir à aceitação do risco.

Figura 9 – A Atividade de Tratamento de Risco



Fonte: ABNT NBR ISO/IEC 27005 (2019).

Alguns conceitos utilizados na Gestão de Riscos de TI:

- Ameaça: é todo e qualquer evento que possa explorar alguma vulnerabilidade;
- Vulnerabilidade: é qualquer fraqueza que possa ser explorada de forma a comprometer a segurança de sistemas ou informações. Pode ser entendido ainda como a fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças;
- Risco: é a combinação da probabilidade (chance da ameaça se concretizar) de um evento indesejado ocorrer e de suas consequências para a organização;
- Impacto: é a mudança adversa no nível obtido dos objetos de negócios. É a consequência avaliada dos resultados com a ocorrência de um evento em particular, em que determinada vulnerabilidade foi explorada, uma ameaça ocorreu e uma ameaça se concretizou;
- Estimativa de Riscos: é o processo utilizado para atribuir valores à probabilidade, as consequências negativas, ou ambas, associadas a um risco;

- Identificação dos Riscos: é o processo para localizar, listar e caracterizar elementos de risco;
- Ação de Evitar o Risco: é a decisão de não se envolver ou agir de forma a mitigar uma situação de risco;
- Estimativa de Riscos: é o processo utilizado para atribuir valores à probabilidade e consequências de um risco;
- Ações de Modificação do Risco: são ações tomadas para reduzir a probabilidade, as consequências negativas, ou ambas, associadas a um risco;
- Comunicação do Risco: é a troca ou compartilhamento de informações sobre o risco entre o tomador de decisão e outras partes interessadas;
- Ação de Evitar o Risco: é a decisão de não se envolver ou agir de forma a mitigar uma situação de risco;
- Retenção de Risco: é a aceitação do ônus da perda ou do benefício do ganho associado a um determinado risco;
- Compartilhamento do Risco: é o compartilhamento com outra entidade do ônus da perda ou do benefício do ganho associado a um risco.

2.3 BOW TIE

2.3.1 Definição

A metodologia *Bow Tie* (o diagrama tem o formato de uma gravata borboleta *bow tie* em inglês, daí o nome), onde oferece uma boa visão geral de um cenário de evento adverso. Em um *Bow Tie* completo é possível representar todos os cenários possíveis, com todos os caminhos e barreiras identificados (ABDI et al., 2016).

Com o diagrama de *Bow Tie* é possível efetuar a avaliação de risco, a gestão de risco e a comunicação de risco de forma simples e visual. A metodologia de *Bow Tie* oferece recursos para o entendimento da relação entre os riscos e os eventos de uma organização. Como uma ferramenta gráfica é possível entender todo o contexto de um cenário de acidente desde as causas até suas consequências e com isso pode-se evitar que um determinado risco possa ocorrer ou, caso ele ocorra, direcionar da melhor maneira seu desfecho.

O processo envolve a identificação sistemática de perigos e efeitos, a avaliação dos riscos associados e a especificação das medidas de controle e recuperação que devem ser implementadas e mantidas (AFEFY, 2015).

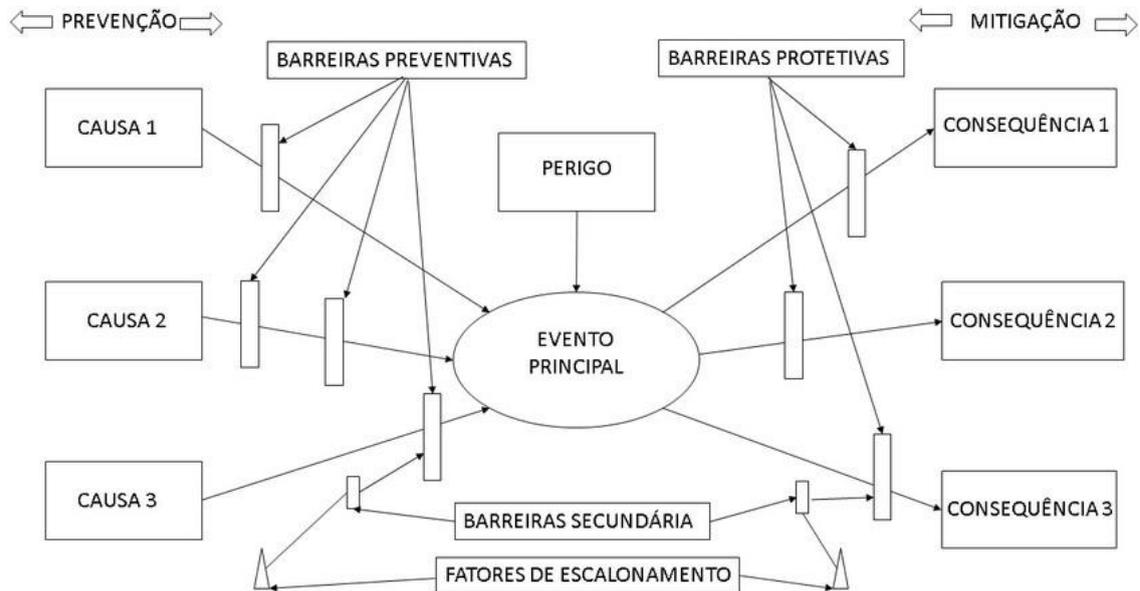
2.3.2 Estrutura

O primeiro passo na criação de um diagrama de *Bow Tie* é definir o evento principal ou simplesmente risco que se deseja evitar. O evento principal localiza-se no centro do diagrama de *Bow Tie* e servirá de parâmetro para a construção de todo o modelo. Um evento principal pode ser acionado por uma ou várias ameaças. As ameaças estão no lado esquerdo do evento principal no diagrama de *Bow Tie*. Num evento principal podem ocorrer uma série de consequências, que são colocadas ao lado direito no diagrama de *Bow Tie*. O próximo passo se concentra na identificação de barreiras preventivas (ou seja, as barreiras que irão impedir as ameaças, evitando assim sua inicialização) e barreiras protetoras (ou seja, as barreiras servirão para proteger ou mitigar as consequências indesejáveis após a ação do evento principal). As barreiras preventivas estão no lado esquerdo do risco e as barreiras protetoras estão no lado direito do risco.

Em seguida, devem ser determinados os fatores de escalonamento que podem levar a um risco aumentado, comprometendo a eficácia das barreiras preventivas e protetoras. Na próxima etapa, os mecanismos disponíveis usados para controlar os efeitos indesejáveis desses fatores de escalonamento serão as barreiras secundárias.

O diagrama de *Bow Tie* tradicional inclui, portanto, do seu lado esquerdo uma lista de perigos ou ameaças potenciais (*Threat*) que levam, através de diversos caminhos, a um risco (*Top Event*); do seu lado direito terá as diferentes consequências (*Consequence*) decorrentes da materialização do risco. Nesse processo são considerados ainda e as barreiras preventivas (*Preventive Barriers*) e barreiras protetivas (*Protective Barriers*). Os Fatores de Escalonamento (*Escalation Factors*) serviram para degradar as barreiras preventivas e protetivas e Barreiras Secundárias (*Secondary Barriers*) serviram para fortalecer as barreiras preventivas ou protetivas, minimizando ou anulando o impacto dos fatores de escalonamento.

Uma característica importante e útil é que esta análise de barreiras ajuda a identificar barreiras perdidas ou mal projetadas, o que é uma questão-chave na gestão de riscos (JACINTO; SILVA, 2009). Um exemplo é mostrado na Figura 10.

Figura 10 – Diagrama de *Bow Tie*

Fonte: Adaptado de Abdi et al. (2016).

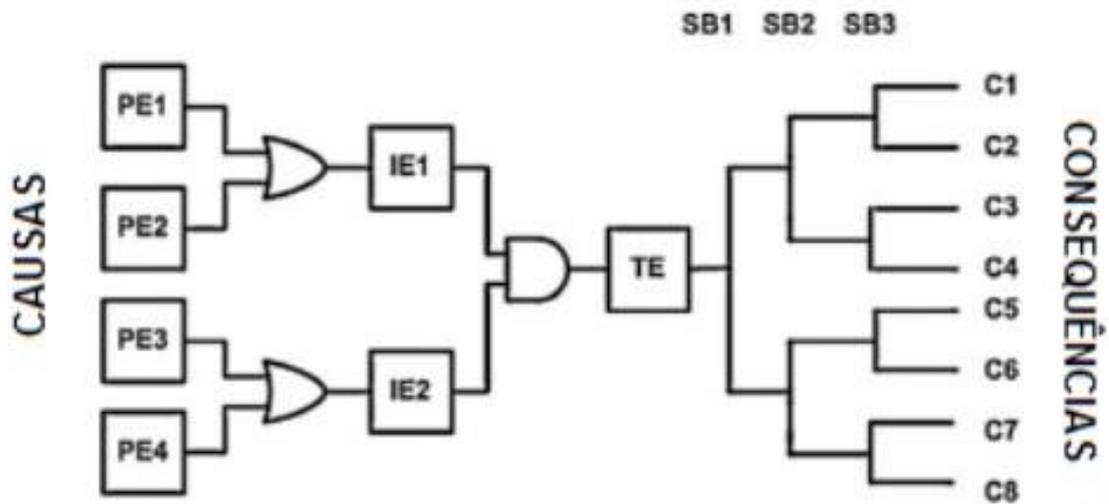
- O Perigo: este é o potencial (material ou atividade) para levar a um evento principal;
- Evento Principal: este é o evento que pode levar a resultados indesejados (geralmente perda de controle ou perda de contenção);
- Causas: estas são as categorias de desafios para os sistemas de segurança que, se não combatidas, levarão ao evento principal;
- Consequências: estas são as categorias de resultados indesejados que podem ocorrer se o evento a partir do evento principal não for combatido;
- Barreiras de Prevenção: estas são as barreiras/controles que podem barrar (ou reduzir a probabilidade) a causa antes que ela atinja o evento principal;
- Barreiras de Mitigação: estas são as barreiras/controles que podem prevenir uma sequência de eventos antes que ela atinja a consequência indesejada;
- Barreiras Secundárias: estas são para fortalecer as barreiras preventivas ou protetivas, minimizando ou anulando o impacto dos fatores de escalonamento;
- Fator de Escalonamento: razões que podem degradar a barreira do caminho principal e as barreiras utilizadas para evitar isso.

A dinâmica da metodologia consiste no conhecimento dos perigos e seus efeitos, em seguida avalia os riscos envolvidos, bem como suas especificações de recuperação e controle e que devem estar atualizadas e de fácil acesso.

O Diagrama de *Bow Tie* pode ser tornar complexo dependendo do seu tamanho e o quanto se queira analisar. Neste caso, se faz necessária a participação de uma equipe dedicada e especializada que possa alimentar constantemente os dados de forma confiável, com todas as frequências de eventos, bem como as novas probabilidades de falhas nas barreiras.

A Figura 11 mostra um Modelo de Diagrama Genérico do *Bow Tie* com os eventos primários (PE_i), os eventos intermediários (IE_i), o evento de topo (TE), as barreiras de segurança (SB_i) e as consequências de acidentes (C_i).

Figura 11 – Modelo de Diagrama Genérico do *Bow Tie*



Fonte: Barros (2019).

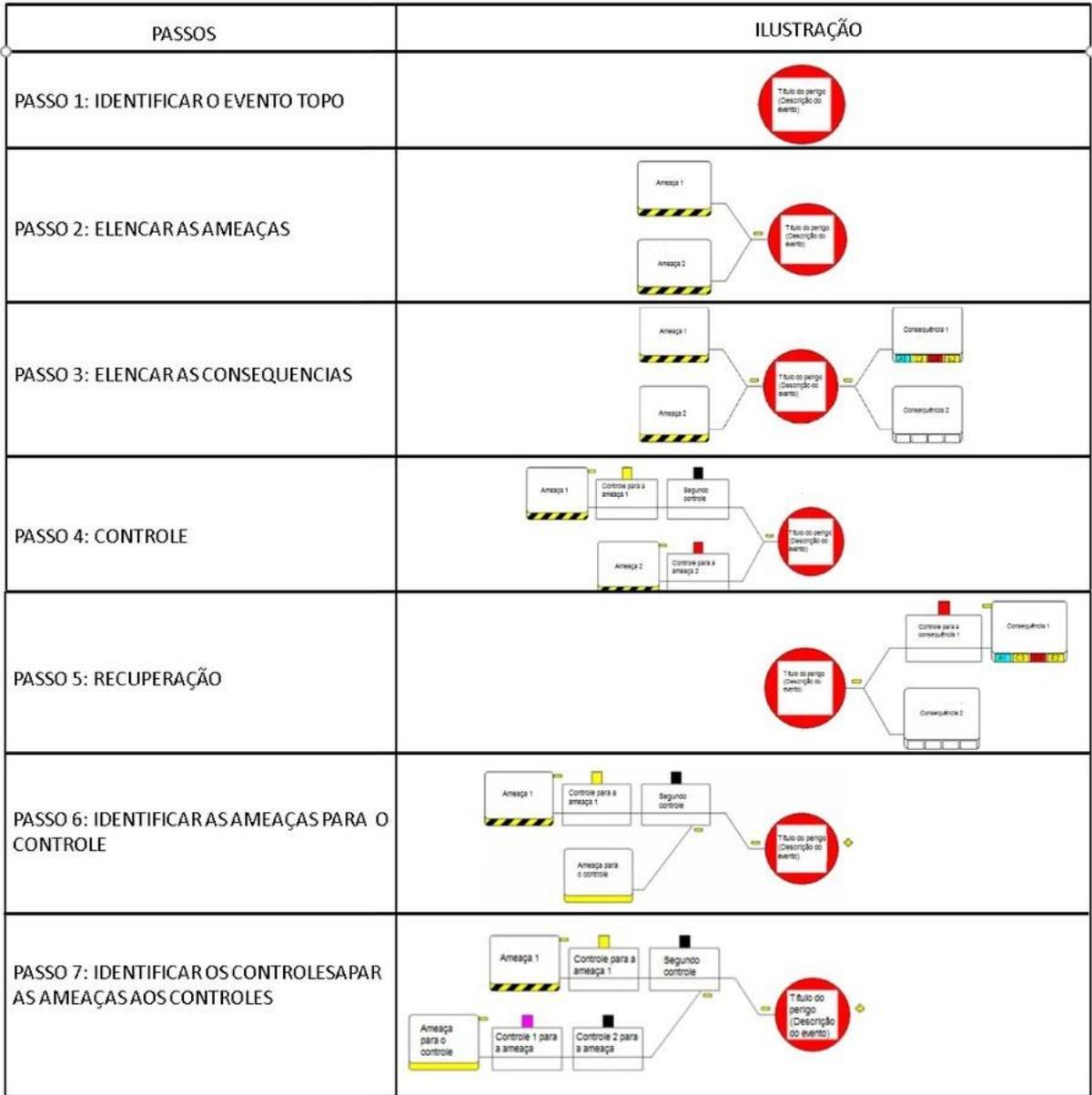
Este diagrama ajuda a entender qual combinação possível de eventos primários levará ao evento principal na árvore de falhas e quais falhas de função de segurança escalarão o evento principal para uma consequência específica na árvore de eventos. Por exemplo, a probabilidade de ocorrência da consequência C4 na Figura 11 pode ser avaliada como:

$$P(C4) = P(TE) * P(\overline{SB1}) * P(SB2) * P(SB3) \quad (2.1)$$

Onde $P(TE)$ é a probabilidade máxima de evento, e $P(\overline{SB1})$, $P(SB2)$ e $P(SB3)$ referem-se à probabilidade de não falha de e $\overline{SB1}$ à probabilidade de falha de SB2 e SB3, respectivamente (KHAKZAD; KHAN; AMYOTTE, 2013).

Os passos para construção do Diagrama *Bow Tie* estão listados na figura 12.

Figura 12 – Passos para a Construção do Diagrama de *Bow Tie*.



Fonte: Adaptado de Afefy (2015).

Onde:

- Passo 1: identifica o controle que se deve ter para se evitar um determinado evento;
- Passo 2: levantamento das possíveis ameaças que levaram ao evento não desejado;
- Passo 3: levantamento das consequências caso ocorra o evento não desejado;
- Passo 4: identificação de mecanismos de controle para as ameaças identificadas;
- Passo 5: identificação de mecanismos de recuperação para as consequências identificadas;

- Passo 6: levantamento de ameaças dos mecanismos de controle identificado no passo 4;
- Passo 7: identificar os controles para as ameaças dos mecanismos que foram listados no passo 6.

2.4 TIC

A Tecnologia da Informação e Comunicação (TIC), é a área que permeia em todos os meios técnicos usados para tratar a informação e auxiliar na comunicação, incluindo por exemplo: equipamentos físicos, redes e celulares. Em outras palavras, é todo e qualquer meio tecnológico seja físico (hardware) ou lógico (software) que pode auxiliar no negócio da organização (CHAHIN et al., 2004).

No Brasil, a partir do início do século XXI, os gestores públicos despertaram para o valor das TICs como instrumento na construção do futuro (PEREIRA; SILVA, 2010). A partir de então, políticas públicas foram criadas para que as novas tecnologias impulsionassem o desenvolvimento.

As modificações ocasionadas nos processos de desenvolvimento, e suas consequências na democracia e cidadania, convergem para uma sociedade caracterizada pela importância crescente dos recursos tecnológicos e pelo avanço das Tecnologias de Informação e Comunicação com impacto nas relações sociais, empresariais e nas instituições. É a denominada Sociedade da Informação e do Conhecimento que cogita uma capacidade constante de inovação (PEREIRA; SILVA, 2010).

Com a utilização das TICs, a Administração Pública passou a ter vários objetivos, através do meio da internet oferecendo serviços como: a melhoria contínua da qualidade, o aumento da eficácia e da eficiência, a transparência dos atos administrativos, a fiscalização das ações governamentais e a participação popular no exercício da cidadania. O Governo Eletrônico muda a interface entre o Estado e o cidadão, e isso pode levar à reforma das estruturas que sustentam a interface

2.5 TI VERDE

Conhecida também como Tecnologia da Informação Verde ou do inglês: *Green Information Technology*, é uma tendência mundial voltada para a redução do impacto dos recursos tecnológicos no meio ambiente.

Pode ser ainda descrita como o conjunto de práticas para tornar mais sustentável e menos prejudicial a utilização de tecnologia. Desta maneira, ela determina modos de compatibilizar a utilização de recursos naturais de forma adequada às políticas sustentáveis existentes dentro das empresas. De forma prática, temos como exemplo a sua aplicação quanto ao uso de recursos tecnológicos que consomem menos energia, o uso de matéria prima e substâncias menos tóxicas

em seus processos produtivos e o descarte responsável de seus produtos através da reciclagem e da reutilização de materiais.

A TI Verde abrange, entre outros, o cumprimento de leis ambientais e os levantamentos dos aspectos e impactos ambientais de atividades relacionadas à área da Tecnologia da Informação, acompanhando ou criando procedimentos e planos de ação com objetivos de eliminação, ou diminuição da agressão ambiental.

O nome TI Verde foi criado para transformar as empresas em empresas mais verdes, desde impressão de uma simples folha de papel até um gerenciamento de energia em *data centers* (DELVAZ; BOVÉRIO, 2011). O problema não é apenas das empresas e governos, mas também da sociedade de maneira geral, pois todos têm um papel importante no meio ambiente.

A adoção da TI Verde diferencia-se da adoção de uma TI qualquer, especialmente pela importância que as questões éticas e de sustentabilidade possuem no processo de tomada de decisão. Enquanto a adoção de uma TI é geralmente motivada pelos potenciais benefícios econômicos do uso dessa tecnologia, as práticas de TI Verde são motivadas por serem uma preocupação ecológica do planeta, mesmo que os benefícios econômicos possam não ser tangíveis no curto prazo.

Organizações que estão preocupadas com as suas responsabilidades sociais e ambientais, com a sustentabilidade dos negócios e a TI Verde, têm tratado essas questões elaborando políticas claras quanto à aquisição de equipamentos (com menor consumo de energia, materiais reciclados, materiais não poluentes, dentre outros), uso de computadores e impressoras (através de processos computacionais mais eficientes, virtualização, diminuição de impressões, remanufatura de cartuchos, uso de papel reciclado) e até mesmo a disposição dos computadores e *data centers* (menores, com menor consumo, melhor refrigeração e etc.) (LUNARDI; SIMÕES; FRIO, 2014).

2.6 SUSTENTABILIDADE

Pode ser definida como a capacidade do ser humano de interagir com o planeta, preservando o meio ambiente para não comprometer os recursos naturais das futuras gerações. É visto ainda como um conjunto de variáveis interdependentes, mas que consegue integrar as questões sociais, energéticas, econômicas e ambientais.

São ainda ações que utilizam os recursos naturais de maneira eficiente para que não comprometa o amanhã. Fica notável que as ações sustentáveis vividas hoje, podem garantir condições suficientes para manter a qualidade de vida da população no futuro (GUIRARDI; FEITOZA, 2019).

Um grande marco para a sustentabilidade mundial se deu em 1992 com a RIO-92 ou ECO-92, e teve como principal produto um programa de ação baseado num documento de 40 capítulos, onde 179 países participantes acordaram e assinaram a Agenda 21 Global, que constitui a mais abrangente tentativa já realizada para promover, em escala planetária, um novo padrão de desenvolvimento, denominado desenvolvimento sustentável. Esse nome se deu pensando nas

novas formas sustentáveis para o século XXI que estavam por vir.

O modelo da Agenda 21 Brasileira é um processo e instrumento de planejamento participativo para o desenvolvimento sustentável e que tem como eixo central a sustentabilidade, compatibilizando a conservação ambiental, a justiça social e o crescimento econômico. O documento é resultado de uma vasta consulta à população brasileira, sendo construída a partir das diretrizes da Agenda 21 global. Trata-se, portanto, de um instrumento fundamental para a construção da democracia participativa e da cidadania ativa no País. A Agenda se fundamenta nas recomendações do Capítulo IV da Agenda 21 que indica aos países o “estabelecimento de programas voltados ao exame dos padrões insustentáveis de produção/consumo e o desenvolvimento de políticas e estratégias nacionais de estímulo a mudanças nos padrões insustentáveis de consumo”; no Princípio 8 da Declaração do RIO-92 que afirma que “os Estados devem reduzir e eliminar padrões insustentáveis de produção e consumo e promover políticas demográficas adequadas”; e ainda na Declaração de Johannesburgo que institui a “adoção do consumo sustentável como princípio basilar do desenvolvimento sustentável”.

As instituições públicas, além de normatizar e fiscalizar as ações provenientes da iniciativa privada, no sentido de promover a sustentabilidade, deve também ser agente ativo nas ações que permitam o desenvolvimento sustentável. Assim, com base nesta premissa, o Governo Brasileiro, por meio do Ministério do Meio Ambiente criou a Agenda Ambiental da Administração Pública (A3P) (FREITAS; BORGERT; PFITSCHER, 2011). A A3P tem como princípios a inserção dos critérios ambientais; que vão desde uma mudança nos investimentos, compras e contratação de serviços pelo governo; até uma gestão adequada dos resíduos gerados e dos recursos naturais utilizados tendo como principal objetivo a melhoria na qualidade de vida no ambiente de trabalho. A A3P é uma decisão voluntária respondendo à compreensão de que o Governo Federal possui um papel estratégico na revisão dos padrões de produção e consumo e na adoção de novos referenciais em busca da sustentabilidade socioambiental. O programa tem como diretriz a sensibilização dos gestores públicos para as questões socioambientais, estimulando-os a incorporar princípios e critérios de gestão ambiental nas atividades administrativas, por meio da adoção de ações que promovam o uso racional dos recursos naturais e dos bens públicos, o manejo adequado e a diminuição do volume de resíduos gerados, ações de licitação sustentável/compras verdes e ainda no processo de formação continuada dos servidores públicos¹.

O Governo Federal publicou a portaria n.º 326, de 23 de julho de 2020, onde institui o Programa Agenda Ambiental na Administração Pública - Programa A3P e estabelece suas diretrizes. Neste programa os órgãos podem aderir voluntariamente, sem norma de imposição e tampouco sanção para quem não segue as suas diretrizes. A maior parte dos órgãos públicos já adota procedimentos considerados sustentáveis. Em diversas instituições, a coleta seletiva, por exemplo, é uma prática comum; em algumas foi adotado sistema para evitar o desperdício de água; outras estabeleceram que toda licitação será dentro de critérios de sustentabilidade. O que o Programa A3P fez foi sistematizar em eixos temáticos aquilo que é fundamental para um

¹ sitio: <https://sites.google.com/site/comprassustentaveis/governo-federal---cadmat>

projeto de sustentabilidade, hoje disperso em diversos órgãos. São seis eixos: Uso dos Recursos Naturais; Qualidade de Vida no Ambiente de Trabalho; Sensibilização dos Servidores para a Sustentabilidade; Compras Sustentáveis; Construções Sustentáveis; e Gestão de Resíduos Sólidos². Estes eixos são fundamentados pela política dos 5 R's: Repensar, Reduzir, Reaproveitar, Reciclar e Recusar o consumo de produtos que gerem impactos socioambientais negativos significativos.

Vale ressaltar que a responsabilidade socioambiental deixou de ser uma opção para as organizações, tornando-se uma questão de visão, de estratégia e, muitas vezes, de sobrevivência (QUEIRÓS, 2019). O uso ineficiente da TI, além de prejudicar o meio ambiente, pode resultar em maiores custos para as organizações, fato que pode fazê-las perder vantagens competitivas (MELVILLE, 2010). Colocar em prática a TI Verde exige algumas mudanças de comportamento e tecnologias, além de investimentos financeiros para viabilizar o processo de adoção dessas práticas (SALLES et al., 2013).

2.7 DATA CENTER VERDE

É um ambiente computacional que é inteiramente construído, gerenciado e operacionalizado sobre os princípios da TI Verde, que possui uma missão crítica que abriga equipamentos responsáveis pelo processamento e armazenamento de informações nas mais variadas categorias de organizações, como, por exemplo, empresas privadas, órgãos públicos, escolas, hospitais, entre outros.

Um *Data Center* Verde utiliza os recursos e capacidades de um *data center* convencional como sala de computadores, ar-condicionado/controle ambiental, distribuição elétrica e *Uninterruptable Power Supply* (UPS), detecção/supressão de incêndio, espaços de suporte, automação do edifício e segurança e controle; porém consome menos energia e espaço, e são menos poluentes ao meio-ambiente, criando desta maneira uma infraestrutura com sustentabilidade.

Os custos de energia dos *data centers* são uma grande preocupação da TI Verde, porque mais da metade de todos os custos de energia elétrica relacionada à TI são gerados pelos *data centers*. Os principais equipamentos de um *data center* são os servidores e os dispositivos de armazenamento de dados (LOPES; CARRERO, 2016). Eles consomem muita energia e necessitam de fontes de alimentação ininterruptas. Adicionalmente, um *data center* necessita de outros equipamentos que gastam energia, composta de uma estrutura de refrigeração dedicada e ventiladores.

² sitio: <https://www.proambientaltecnologia.com.br/o-que-e-a-a3p/>

2.8 EFICIÊNCIA ENERGÉTICA PARA DATA CENTERS

É uma atividade que busca utilizar de forma racional e com o mínimo de perda o uso das fontes de energia. A utilização que busca evitar maiores perdas de energia, consiste em usar mecanismos mais eficientes para o gerenciamento da fonte energética para se obter um determinado resultado. A questão dos impactos dos *Data Centers* tomou maiores dimensões quando a Agência de Proteção Ambiental Americana apresentou, em 2007, um relatório que mostrou que 1,5% de toda a energia gasta nos Estados Unidos da América (EUA) é utilizada em *Data Centers* e a tendência, na época, era somente aumentar (FABRO; RIVEROS; WONZOSKI, 2017). Quanto melhor for a relação entre a quantidade de energia empregada em uma atividade e aquela disponibilizada para sua realização, melhor será a sua Eficiência Energética.

Para definir eficiência Energética de um *Data Center* usa-se como métrica o *Power Usage Effectiveness* (PUE), ou, em português, Eficiência de Uso de Energia. Outra métrica que se aplica a *data centers*, é a *Data Center Infrastructure Effectiveness* (DCiE), em português, Eficiência da Infraestrutura do *Data Center* (OLIVEIRA, 2017). Ambas as métricas foram desenvolvidas pela organização industrial não lucrativa chamada *Green Grid*³. Para auxiliar toda a complexidade que envolve uma Gestão de Infraestrutura de *Data Centers*, são utilizados softwares específicos, conhecidos como *Data Center Infrastructure Management* (DCIM), em português, Gestão de Infraestrutura de *Data Center*.

Na equação (2.2), o numerador se refere à quantidade total de Energia que o *Data Center* (EDC) consome e, no denominador, somente o consumo dos Equipamentos de Tecnologia da Informação (ETI). No campo da teoria, um *Data Center* tem o PUE perfeito quando este é igual a 1, ou seja, toda a energia elétrica que entra é para alimentar as cargas de TI. Porém, no mundo real isso não acontece. Então, na prática, quanto mais próximo de 1 for o PUE mais eficiente será esse *Data Center*.

$$PUE = \frac{EDC}{ETI} \quad (2.2)$$

Na equação (2.3), temos o numerador se referindo ao consumo dos Equipamentos de Tecnologia da Informação (ETI) e o denominador como sendo a quantidade total de Energia que o *Data Center* (EDC) consome. Esta fórmula representa o inverso do PUE e quando multiplicamos o resultado por 100%, assim teremos a informação de quantos por cento a infraestrutura de um *data center* é eficiente naquele dado momento.

$$DCiE = (1/PUE) = (ETI/EDC) * (1/100) \quad (2.3)$$

A tabela 1 mostra os Valores de Referência do PUE e DCiE de acordo com 42U *Data Center Solutions*⁴.

³ sitio: <https://www.thegreengrid.org/>

⁴ <https://www.42u.com/measurement/pue-dcie.htm>

Tabela 1 – Valores de Referência do PUE e DCiE

PUE	DCiE	Descrição
3.0	33%	Muito Ineficiente
2.5	40%	Ineficiente
2.0	50%	Médio
1.5	67%	Eficiente
1.2	83%	Muito Eficiente

Fonte: Adaptado de 42u DATA CENTER SOLUTIONS (2019).

O DCIM são soluções de softwares, gratuitas ou pagas, que monitoram, medem, gerenciam e controlam o uso do *data center* e o seu consumo de energia de todos os equipamentos relacionados à TI como servidores, switches e rede, e componentes de infraestrutura como unidades de distribuição de energia e aparelhos de ar-condicionado da sala de computadores.

Com a ferramenta DCIM é possível obter alguns dados como: Localização de um determinado ativo no meu *data center*; Orientações sobre o melhor lugar para colocar um novo servidor; Informações sobre espaço, energia, refrigeração e conectividade de rede, como sendo suficiente para atender minhas necessidades para um determinado período; Informações sobre eventos no *data center* - o que aconteceu, quais serviços são afetados, onde os técnicos devem resolver o problema; Informações sobre recursos subutilizados no meu *data center*; Se tenho energia ou resfriamento suficiente em condições de falha, ou manutenção; entre muitas outras (UPTIME INSTITUTE, 2020).

Assim, diminuir o custo de energia dos *data centers* é uma tarefa muitas vezes difícil e complexa, visto que cada vez mais o número de equipamentos ligados a rede só cresce para atender a demanda de novos usuários ou clientes.

2.9 CONSIDERAÇÕES

Neste capítulo abordamos a importância e a amplitude de conceitos como Gestão de Risco, Gestão de Risco de TI, *Bow Tie*, TIC, TI Verde, Sustentabilidade, *Data Center Verde* e Eficiência Energética para *Data Centers*. O estreito relacionamento que estes conceitos têm direcionam para um tema tão vasto que é a sustentabilidade em *Data Centers*.

Diante disso a gestão de risco de TI se posiciona como a base normativa para manter as práticas em conformidade com as leis que as instituições estão sujeitas, ficando claro assim que o assunto se mostra um campo de oportunidades para desenvolvimento de novas pesquisas científicas. Este trabalho mostrará nos capítulos que se seguem respostas às lacunas envolvendo o tema.

3 TRABALHOS RELACIONADOS

Neste capítulo são apresentados os trabalhos utilizados para a composição desta pesquisa, bem como as *strings* (palavras, conceitos) de buscas utilizadas nas principais fontes de pesquisas para seleção das pesquisas correlatas.

3.1 CRITÉRIOS DE ANÁLISES DOS TRABALHOS

Foram coletados estudos realizados sobre o tema de Tomada de Decisão na Gestão de Riscos da TI evitando a Perda de Eficiência Energética em *Data Centers* através de ferramentas de busca on-line pelo Portal da CAPES e Google Acadêmico usando a combinação de *strings* na língua Portuguesa e Inglesa, pois são base fundamental para o desenvolvimento deste trabalho de dissertação.

Para escolher os artigos alusivos ao tema, definimos alguns critérios que satisfizessem os objetivos específicos descritos no Capítulo 1 deste trabalho:

- Identificar métodos para quantificar a Eficiência Energética em *Data Centers*;
- Aplicação de Modelos para o controle da Gestão de Riscos em TI, com foco na continuidade do negócio organizacional;
- Representação gráfica de fácil entendimento para tomada de decisão na Gestão de Riscos.

A *string* de busca foi definida a partir da escolha desses critérios, através de palavras chaves utilizadas com os operadores lógicos *AND* e *OR*:

String de Busca: (“Eficiência Energética” *OR* “*Energy Efficiency*”) *AND* (“Centro de Dados” *OR* “*Data Center*”) *AND* (“Gestão de Riscos de TI” *OR* “*IT Risk Management*”) *AND* (“Ferramenta Visual de Levantamento de Risco” *OR* “*Visual Risk Assessment Tool*”).

Na tabela 2 seguem os resultados obtidos após o resultado da aplicação da *string*. Foram realizadas algumas triagens para reduzir o quantitativo de trabalhos relacionados a serem analisados, visando o alinhamento com o tema, contemporaneidade e os objetivos desta pesquisa:

Tabela 2 – Resultado da Busca dos Trabalhos Relacionados

Cr�terios Aplicados	Quantidade de Trabalhos Resultantes
Aplic��o da String de busca na Capes e Google Acad�mico	67
Exclus�o de trabalhos com mais de 5 anos	34
Exclus�o trabalhos que n�o fa�am parte de ambientes organizacionais	10
Excluir trabalhos que n�o utilizem modelos de controle da Gest�o de Riscos em TI, com foco na continuidade do neg�cio organizacional	4

Fonte: O Autor (2020).

Conforme a tabela 2 foram selecionados 4 trabalhos de acordo com o crit rio inicial de exclus o, ou seja, somente trabalhos de 2015 em diante, e que tamb m atenderam ao crit rio inicial de inclus o que trata da aplica o dos modelos de Controle da Gest o de Risco em TI em ambientes organizacionais.

Durante a pesquisa outros trabalhos relevantes foram incorporados, como Plano de Gest o de Riscos e Controles do Instituto Federal de Pernambuco (2020), Tecnologia da Informa o — T cnicas de Seguran a — Gest o de Riscos de Seguran a da Informa o (2019) e Pol tica da Seguran a da Informa o e Comunica o do IFPE (2017), visto que o primeiro basea-se na norma geral de gest o de riscos, o segundo a norma espec fica da gest o de riscos de TI, e a terceira a aplica o da norma espec fica no servi o p blico federal.

Assim seguem os trabalhos que serviram de base para a constru o desta disserta o, s o eles:

3.2 DESCRI O DOS TRABALHOS

Para descri o dos artigos, foi necess rio escolher o tipo de revis o que mais se adequasse ao estudo dos trabalhos. Considerando o curto espa o de tempo para discuss o contextual do tema, foi ent o utilizada a revis o narrativa. Os artigos de revis o narrativa s o publica es amplas apropriadas para descrever e discutir o desenvolvimento ou o “estado da arte de um determinado assunto, sob o ponto de vista te rico ou conceitual (ROTHER, 2007), constitu do basicamente da an lise cr tica e interpreta o pessoal do autor a respeito dos artigos, livros, revistas para a avalia o dos trabalhos apresentados nesta se o.

A seguir s o elencados em ordem cronol gica os 7 trabalhos escolhidos como refer ncias para este trabalho de pesquisa com os seus respectivos t tulos, suas principais contribui es e lacunas:

- 1) Plano de Gest o de Riscos e Controles do Instituto Federal de Pernambuco (INSTITUTO FEDERAL DE PERNAMBUCO, 2020). Este documento apresenta os fundamentos e a estrutura do Plano de Gest o de Riscos do Instituto Federal de

Educação, Ciência e Tecnologia de Pernambuco (IFPE), com o objetivo de orientar as unidades a implementá-lo em conformidade com a Instrução Normativa Conjunta Ministério Público (MP)/ Controladoria Geral da União (CGU) nº 01/2016, o Decreto nº 9.203, de 22 de novembro de 2017, e a Política de Gestão de Riscos do IFPE, aprovada pela Resolução do Conselho Superior (CONSUP) nº 57 de 30 de novembro de 2018, que estabelece o Núcleo de Gestão de Riscos (NGRis) como a instância responsável pela implementação do presente Plano. Nesse contexto, o citado Plano tem o intuito de viabilizar o processo de implantação de um modelo de gestão de riscos no Instituto Federal de Educação, Ciência e Tecnologia de Pernambuco (IFPE), fortalecendo as unidades administrativas, facilitando a tomada de decisão e proporcionando mais segurança aos servidores e às servidoras na execução de suas atividades cotidianas, de modo a contribuir para o alcance dos objetivos institucionais.

- 2) Modelo Multicritério para Priorização de Ações no Gerenciamento de Riscos de Indisponibilidade de Estoques em Prateleiras com Base na Ferramenta *Bow-Tie*: Estudo de Caso no Setor Varejista (BARROS, 2019). Este trabalho teve como objetivo desenvolver um plano para redução da ocorrência de indisponibilidade em uma loja localizada na cidade de Caruaru-PE. A metodologia estruturada foi proposta com etapas que visam prevenir a ocorrência da indisponibilidade de estoque, foi utilizado o diagrama de *bow tie* que serviu para identificação das principais causas, consequências, barreiras e identificação de alternativas para os problemas identificados.
- 3) Tecnologia da Informação — Técnicas de Segurança — Gestão de Riscos de Segurança da Informação (ABNT NBR ISO/IEC 27005, 2019). Este documento fornece diretrizes para o processo de gestão de riscos de segurança da informação.
- 4) Política da Segurança da Informação e Comunicação do IFPE (INSTITUTO FEDERAL DE PERNAMBUCO, 2017). Este documento tem como propósito estabelecer diretrizes, normas, procedimentos e responsabilidades adequadas para o manuseio, tratamento, controle e proteção das informações pertinentes ao IFPE.
- 5) Propostas de Eficiência Energética em Infraestrutura para *Data Center* (OLIVEIRA, 2017). Este trabalho destaca de modo prático e direto os principais componentes necessários para esse ambiente crítico, chamado *data center*, funcionar de maneira adequada mesmo quando falhas venham a ocorrer.
- 6) *Data Centers* - Engenharia: Infraestrutura Física (MARIN, 2016). Esta obra abrange estudos de casos e exemplos de dimensionamentos, e abrange sistemas elétricos e de climatização, cabeamento estruturado, sistemas de segurança, proteção contra incêndio, DCIM e eficiência energética, apresentando as métricas mais utilizadas, seus significados e aplicações. Apresenta os conceitos de disponibilidade, confiabilidade e redundância de

forma ampla e com base em normas técnicas vigentes ABNT NBR, ISO, IEC, *American National Standards Institute (ANSI)*, *Building Industry Consulting Service International (BICSI)*, *Telecommunications Infrastructure Standard (TIA)*, *The Uptime Institute*, entre outras. A ocupação de um *data center* foi abordada com praticidade, fornecendo detalhes de planejamento dos espaços e de como se relacionam, aspectos construtivos da edificação, pisos elevados, cargas de piso e muito mais.

- 7) *Application of Bow-tie methodology to improve patient safety* (ABDI et al., 2016). O objetivo deste artigo foi aplicar a metodologia *Bow-tie*, uma técnica proativa de avaliação de risco baseada em abordagem sistêmica, para análise prospectiva dos riscos que ameaçam a segurança do paciente em Unidade de Terapia Intensiva (UTI). Projeto / metodologia / abordagem - A metodologia de *bow tie* foi usada para gerenciar os riscos clínicos que ameaçam a segurança do paciente por uma equipe multidisciplinar na UTI.

Tabela 3 – Contribuições das Pesquisas

	Fundamentação	Estudo de Caso
Plano de Gestão de Riscos e Controles do Instituto Federal de Pernambuco	✓	✗
Modelo Multicritério para Priorização de Ações no Gerenciamento de Riscos de Indisponibilidade de Estoques em Prateleiras com Base na Ferramenta Bow-Tie: Estudo de Caso no Setor Varejista	✓	✓
Tecnologia da Informação — Técnicas de Segurança — Gestão de Riscos de Segurança da Informação	✓	✗
Política da Segurança da Informação e Comunicação do IFPE	✓	✗
Propostas de Eficiência Energética em Infraestrutura para Data Center	✗	✓
Data Centers - Engenharia: Infraestrutura Física	✓	✗
Application of Bow-tie methodology to improve patient safety	✗	✓

Fonte: O Autor (2020).

3.3 CONSIDERAÇÃO DO CAPÍTULO

Neste capítulo foram identificados os trabalhos de pesquisa utilizados que auxiliaram nesta dissertação. Embora não haja nenhum trabalho que possa servir de parâmetro exato, as pesquisas aqui serviram como base para a construção e desenvolvimento de uma nova linha de pesquisa

4 MATERIAIS E MÉTODOS

Neste capítulo será apresentada a metodologia que foi utilizada para este trabalho de pesquisa. O capítulo está organizado desta forma: Caracterização da Pesquisa, Ambiente da Pesquisa, Fatores de Inclusão e Exclusão, Procedimentos para Coleta de Dados, Aspectos Éticos e Procedimento para Análise dos Dados.

4.1 CARACTERIZAÇÃO DA PESQUISA

A pesquisa exploratória tem como objetivo proporcionar maior familiaridade com o problema, com vistas a torná-lo mais explícito ou a constituir hipóteses (GIL, 2002). Assim, as pesquisas exploratórias têm como fundamento principal o aprimoramento de ideias ou a descoberta de intuições. A pesquisa descritiva exige do investigador, para que a pesquisa tenha certo grau de validade científica, uma precisa delimitação de técnicas, métodos, modelos e teorias que orientarão a coleta e interpretação dos dados (TRIVINOS, 1987). A pesquisa explicativa tem como preocupação central identificar os fatores que determinam ou que contribuem para a ocorrência dos fenômenos. Esse é o tipo de pesquisa que mais aprofunda o conhecimento da realidade, porque explica a razão, o porquê das coisas (GIL, 2002).

Esta pesquisa exploratória/explicativa caracteriza-se pelo levantamento do cenário atual de um *data center* quanto a eficiência energética, e ainda, da aplicação de um formulário eletrônico que será preenchido pelos representantes da TI da reitoria, de todos os *campi* e centro EAD do IFPE.

A metodologia empregada neste trabalho será a de estudo de caso, que é usado em muitas situações, para contribuir para o nosso conhecimento dos fenômenos individuais, grupais, organizacionais, sociais, políticos e relacionados (YIN, 2014). Este trabalho classifica-se ainda como estudo de caso único por não ter tido nenhum levantamento baseado nas características específicas deste estudo.

A abordagem da pesquisa define-se como sendo qualitativa, onde a realidade é subjetiva e múltipla, que ela é construída de modo diferente por cada pessoa. Assim, o pesquisador deve interagir com o objeto e sujeito pesquisado, de modo a dar vozes a eles para construir uma teia de significados (CHUEKE; LIMA, 2012).

Este trabalho tem como base a norma da ABNT ISO/IEC 27005:2019 - Gestão de Risco de Segurança da Informação, utilizando a Metodologia *Bow Tie* num ambiente de Infraestrutura de *Data Center* do IFPE para apresentar de forma clara e visual como uma Gestão de Risco pode atuar de forma eficiente e eficaz.

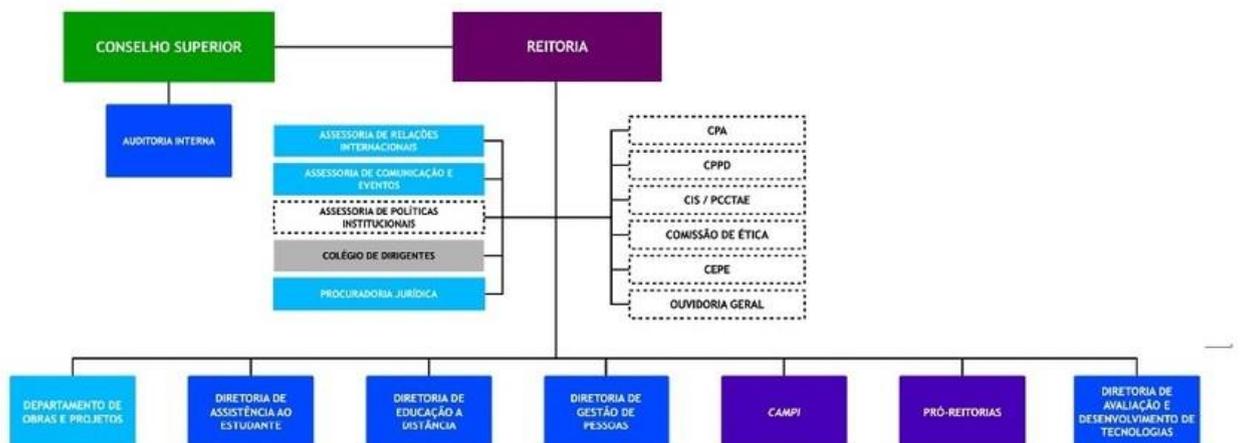
Este estudo irá analisar as causas e efeitos, bem como seus fatores de escalonamentos e barreiras preventivas, barreiras protetivas e barreiras secundárias, ligados a Perda de Eficiência Energética nos *Data Centers* nas unidades do IFPE.

4.2 UNIDADE DE ESTUDO

Este estudo foi realizado no Instituto Federal de Pernambuco, uma instituição centenária e, ao mesmo tempo, inovadora, quando foi criada em 1909, quando foi criada a Escola de Artífices do estado, e ao surgimento das escolas agrotécnicas federais ao longo da primeira metade do século XX. Vinculado à Rede de Educação Profissional e Tecnológica, criada em 2008 através da Lei n.º 11.892/08.

O IFPE conta com 16 *campi* distribuídos na região metropolitana do Recife, agreste e sertão pernambucano para atender 27.224 alunos matriculados em 282 cursos nas áreas de qualificação profissional, técnico, graduação e pós-graduação. E para suportar esta demanda, o IFPE possui 1.314 professores e 1024 técnicos administrativos (PLATAFORMA NILO PECANHA, 2020). O instituto possui ainda 01 reitoria e 01 centro EAD, como pode ser visto no organograma da figura 13.

Figura 13 – Organograma Geral do IFPE



Fonte: Adaptado do Portal IFPE (2020)

A estrutura de TI do IFPE é composta de 01 Diretoria de Avaliação e Desenvolvimento de Tecnologia (DADT) situado na reitoria; 01 Departamento de Gerência de Tecnologia da Informação (DGTI) situado no *Campus* Recife, 08 *campi* com Coordenação de Gestão de Tecnologia da Informação (CGTI), 01 Coordenação de Tecnologia da Informação (CTI) no centro EAD e 07 *campi* com Coordenação de Tecnologia da Informação e Comunicação (CTIC).

Em cada estrutura de TI do IFPE conta com um *data center*, que é o objeto do estudo, para atender suas demandas locais e que estão interligados entre por uma rede para atender serviços sistêmicos, ou seja, sistemas comuns que precisam estar funcionando em cada unidade do IFPE.

4.3 PROCEDIMENTO PARA COLETA DE DADOS

Inicialmente foram levantados, junto ao setor administrativo, os dados do Consumo de Energia Média por dia do IFPE Campus Igarassu entre 2018 e 2019. Neste mesmo *campus* foi levantado os dados de consumo energético da eficiência energética (PUE e DCiE) do *data center* no mesmo período.

Em seguida, foi feito o levantamento das principais ameaças e consequências indicadas por todos os coordenadores e/ou diretores da área de TI dos *campi* do IFPE, através de formulário de pesquisa eletrônico, dividido em três seções (dados pessoais do respondente, levantamento das causas e levantamento das consequências) entre os dias 10 e 16 de outubro de 2020 (Apêndice A) para ordenar de forma priorizada. O critério de seleção dos participantes da pesquisa foi baseado no conhecimento técnico e sua responsabilidade na área de TI de sua unidade gestora. A pesquisa baseou-se na infraestrutura de *data center* e tiveram como objetivo entender as prioridades, segundo a experiência de cada gestor de TI, sobre os aspectos de causa e efeitos diante de um cenário de perda de eficiência energética no *data center* de sua unidade gestora.

Com o tema: Pesquisa sobre Cenários do Gerenciamento da Perda da Eficiência Energética nos *Data Centers* dos *Campi* do IFPE foram abordadas 4 questões ligadas às causas na primeira seção e 4 questões ligadas a consequências na segunda seção.

Para auxiliar nas respostas foram explicados, no início de cada seção, alguns termos, baseados nos conceitos da Gestão de Risco de TI e no *Bow Tie* que foram explanados no capítulo da fundamentação teórica desta pesquisa. Foi ainda explicado o significado de Eficiência Energética de *Data Center* e como mensurar esta eficiência.

4.4 ASPECTOS ÉTICOS

O formulário de pesquisa deste trabalho foi submetido a avaliação pela Pró-Reitoria de Pesquisa, Pós-Graduação e Inovação (PROPESQ), que é o setor do IFPE responsável por planejar, supervisionar, coordenar, fomentar e acompanhar as atividades e políticas de pesquisa, integradas ao ensino e à extensão, bem como promover ações de intercâmbio com instituições e empresas na área de fomento à pesquisa, ciência, tecnologia e inovação tecnológica.

A PROPESQ orienta que pesquisadores, internos ou externos, atentem para que antes de iniciar qualquer atividade de pesquisa com dados da instituição, sejam esses dados obtidos através de entrevistas com membros da comunidade interna ou através de informações institucionais constantes em documentos fornecidos pelos servidores responsáveis, os mesmos devem abrir processo no protocolo para obter o termo de anuência de pesquisa.

Foi encaminhado então no dia 14/09/202, por e-mail o requerimento, termo de anuência

preenchido do IFPE e solicitação contendo informações do projeto de pesquisa, seguindo todas as orientações que constavam na resolução nº 29/2017/CONSUP/IFPE. Foi aberto o processo de n.º 23294.010706.2020-89 que transcorreu até o dia 09/10/2020, data que foi encaminhado o DESPACHO DO TERMO DE PESQUISA (ANEXO A) e o TERMO DE ANUÊNCIA DA PESQUISA (ANEXO B).

Assim, com os devidos cuidados empregados no decorrer da pesquisa, acredita-se que este trabalho esteja pautado em uma conduta moralmente correta atendendo os aspectos éticos esperados em um trabalho científico.

4.5 ANÁLISE DOS DADOS

Para a análise de dados desse estudo foi proposta a metodologia *Bow Tie* tendo como base nos conceitos da ABNT ISO/IEC 27005:2019 - Gestão de Risco de Segurança da Informação obtendo assim um cenário de risco para perda de eficiência energética em *data center* do IFPE de forma visual nos *campi* e reitoria.

Essa metodologia foi proposta por utilizar uma visualização prática e simples, porém, com grande amplitude de todos os possíveis cenários levantados na pesquisa que envolvem uma Gestão de Risco para perda de eficiência energética em um *data center*. Para aplicar a metodologia proposta foram seguidos os seguintes passos:

- 1) Levantamento do PUE e DCiE do *data center* do IFPE para entender o quanto está eficiente o ambiente de *data center* de um *campus* ou da reitoria através das equações (2.2) e (2.3);
- 2) De acordo com a norma da ABNT ISO/IEC 27005:2019 - Gestão de Risco de Segurança da Informação obter os seguintes dados que envolvem um *data center*: Contexto, Riscos, Ameaças, Controles, Vulnerabilidades, Barreiras Preventivas, Consequências, Barreiras Protetivas, Fatores de Escalonamento e Barreiras Secundárias;
- 3) Elaboração do Questionário Eletrônico dividido em três seções (dados pessoais do respondente, levantamento das causas e levantamento das consequências);
- 4) Aplicação do Questionário aos gestores de TI das unidades do IFPE para informar voluntariamente, segundo sua experiência, como compor um cenário de risco de perda de eficiência energética no *data center* de sua unidade sobre os aspectos de causa e consequência.

4.6 CONSIDERAÇÃO DO CAPÍTULO

Neste capítulo foi possível demonstrar as características da metodologia *Bow Tie* tendo como base nos conceitos da ABNT ISO/IEC 27005:2019 - Gestão de Risco de Segurança da Informação.

O ambiente da pesquisa são os *data centers* de toda a infraestrutura do IFPE, levantando informações através de formulário eletrônico a todos os gestores de TI.

5 RESULTADOS

Neste capítulo serão apresentados os dados e interpretação da pesquisa.

5.1 POWER USAGE EFFECTIVENESS E DATA CENTER INFRASTRUCTURE EFFECTIVENESS

Para contextualizarmos este trabalho foram levantados os dados entre 2018 e 2019 do *data center* do IFPE *Campus* Igarassu em busca dos valores do PUE e DCiE, não havendo necessidade de informações dos *data centers* das outras unidades, pois este primeiro levantamento serviu como referência para que pudéssemos entender, através de valores calculados do PUE e DCiE, como se encontra a eficiência energética de um possível objeto de estudo.

Inicialmente foram feitos levantamentos de todos os Equipamentos pertencentes à Carga Crítica do IFPE *Campus* Igarassu, conforme quadro 1. Estes equipamentos fazem parte do rol dos equipamentos que geralmente encontram-se dentro de um *rack*. Para esta pesquisa foram considerados os seguintes atributos: Equipamento, Tombamento, Fabricante, n.º de Série, Fator de Potência, Tensão, Corrente, Carga, Frequência, Potência, Fator de Crescimento e Fator de Espaço de Suporte.

Quadro 1 – Equipamentos da Carga Crítica do *Data Center* do IFPE *Campus* Igarassu

	EQUIPAMENTO	TOMBAMENTO	FABRICANTE	Nº DE SÉRIE
CARGAS CRÍTICAS	Firewall Cisco ASA 5505-K8	181958	Cisco	JMX1842Z08C
	Switch Cisco Catalyst 3750 -1G Tipo 1 Gigabit Ethernet Layer 3	181950	Cisco	FDO1836R1Y0
	Controlador Cisco Wireless 5508	181971	Cisco	FCW1842L0DR
	Switch Cisco SG300 Tipo 3 Gigabit POE 28 Portas	181952	Cisco	DNI18310J57
	Switch Cisco SG300 Tipo 3 Gigabit POE 28 Portas	181951	Cisco	DNI18310J24
	Switch Cisco SG300 Tipo 5 Gigabit POE 8 Portas	181956	Cisco	PSZ18291LBZ
	Switch Cisco SG300 Tipo 3 Gigabit POE 28 Portas	181953	Cisco	DNI18310J5D
	Gateways Analógico FXS AudioCodes MP-124D/FXS/AC	185882	Audio Codes	DT2222112
	Gateways Mediant 1000B MSBRChassis AudioCodes	185894/185897	Audio Codes	DT2337382
	KVM Console TFT7600 G2	187631	HP	2C445072KL
	Servidor PROLIANT DL380 GEN9	187629	HP	BRC51167XS
	Servidor PROLIANT DL380 GEN9	187630	HP	BRC51167XY
	Switch Cisco SG300 Tipo 5 Gigabit POE 8 Portas	181955	Cisco	PSZ18291LCR
	Router BOARD 2011UI AS-RM (Worldnet)	-	MikroTik	763207C9F4D0/728/r2
	Fiber Link 2100B (Embratel/Claro)	-	Parks	PRK500B4D009
	MSR1002-4 Router JG875A (Embratel/Claro)	-	HP	CN74K1W0FB

Fonte: O Autor (2019).

Boa parte das informações eram possíveis achar nos próprios equipamentos, que podiam estar numa etiqueta colada no chassi ou em manuais. Algumas informações referentes a energia elétrica quando não era possível encontrar descrita de forma fácil, era contornado através de fórmulas ou conversões com dados que se tinham disponíveis, como por exemplo:

P = Potência em KW

V = Tensão em Volts

I = Corrente em Amperes

C = Carga em kVA

F = Frequência em Hertz

Fp = Fator de Potência

Assim teremos:

a Potência é igual ao valor da Tensão multiplicado pelo valor da Corrente, o resultado divide por mil

$$P = (V * I)/1000 \quad (5.1)$$

a Tensão é igual ao valor da Potência dividido pelo valor da Corrente

$$V = P/I \quad (5.2)$$

a Corrente é igual ao valor da Potência dividido pelo valor da Tensão

$$I = P/V \quad (5.3)$$

a Carga é igual ao valor da Tensão multiplicado pelo valor da Corrente, o resultado multiplica pelo Fator de Potência, e o resultado divide por mil.

$$C = ((V * I) * Fp)/1000 \quad (5.4)$$

O quadro 2 e quadro 3 ilustram como ficou o resultado.

Quadro 2 – Fator de Potência, Tensão e Corrente da Carga Crítica do *Data Center* do IFPE *Campus* Igarassu

	EQUIPAMENTO	FATOR DE POTENCIA	TENSÃO (V)	CORRENTE(A)
CARGAS CRÍTICAS	Firewall Cisco ASA 5505-K8	0,6	220	1,8
	Switch Cisco Catalyst 3750 -1G Tipo 1 Gigabit Ethernet Layer 3	0,8	220	3
	Controlador Cisco Wireless 5508	0,8	220	0,523
	Switch Cisco SG300 Tipo 3 Gigabit POE 28 Portas	0,8	220	4
	Switch Cisco SG300 Tipo 3 Gigabit POE 28 Portas	0,8	220	4
	Switch Cisco SG300 Tipo 5 Gigabit POE 8 Portas	0,8	220	2
	Switch Cisco SG300 Tipo 3 Gigabit POE 28 Portas	0,8	220	4
	Gateways Analógico FXS AudioCodes MP-124D/FXS/AC	0,8	220	0,8
	Gateways Mediant 1000B MSBRChassis AudioCodes	0,8	220	2
	KVM Console TFT7600 G2	0,8	220	1,5
	Servidor PROLIANT DL380 GEN9	0,8	220	0,003
	Servidor PROLIANT DL380 GEN9	0,8	220	0,003
	Switch Cisco SG300 Tipo 5 Gigabit POE 8 Portas	0,8	220	2
	Router BOARD 2011Ui AS-RM (Worldnet)	0,8	220	1,2
	Fiber Link 2100B (Embratel/Claro)	0,8	220	2,5
	MSR1002-4 Router JG875A (Embratel/Claro)	0,8	220	0,8

Fonte: O Autor (2019).

O fator de crescimento não foi considerado nesta pesquisa, pois, os equipamentos já tinham mais de 6 anos de uso e como a expectativa de uma renovação da infraestrutura, não fazia sentido obter o cálculo deste dado.

Para cálculo do PUE e DCiE, iremos considerar apenas o Total do Kilovolt-ampere (kVA) de cada carga do *data center* do IFPE *Campus* Igarassu. O Fator de Crescimento (FC) é uma

estimativa dada em percentual e geralmente acordada com a gestão sobre o crescimento previsto para os próximos 5 anos, assim, havia uma expectativa de renovação de equipamentos por isso foi desconsiderado.

O Fator de Espaço de Suporte (FES), e a área destinada à manutenção ou suporte dos equipamentos com a carga crítica. Como o ambiente do *data center* do *Campus Igarassu* não era de grande porte, este dado não foi considerado como relevante por não existirem tais equipamentos. O resultado do Total do Kilowatt (KW) da carga crítica iremos utilizar mais adiante para informar o consumo do *data center* e fazer um comparativo com o consumo geral do *Campus Igarassu*.

Quadro 3 – Carga, Frequência, Potência, FC e FES da Carga Crítica do *Data Center* do IFPE *Campus Igarassu*

	EQUIPAMENTO	CARGA(kVA)	FREQUENCIA (Hz)	POTENCIA (KW)	FC-FATOR DE CRESCIMENTO(% em 5 anos)	FES-FATOR DE ESPAÇO DE SUPORTE (20%)
CARGAS CRÍTICAS	Firewall Cisco ASA 5505-K8	0,2376	60	0,396	0	1,044684288
	Switch Cisco Catalyst 3750 -1G Tipo 1 Gigabit Ethernet Layer 3	0,528	60	0,66		
	Controlador Cisco Wireless 5508	0,092048	60	0,11506		
	Switch Cisco SG300 Tipo 3 Gigabit POE 28 Portas	0,704	60	0,88		
	Switch Cisco SG300 Tipo 3 Gigabit POE 28 Portas	0,704	60	0,88		
	Switch Cisco SG300 Tipo 3 Gigabit POE 8 Portas	0,352	60	0,44		
	Switch Cisco SG300 Tipo 3 Gigabit POE 28 Portas	0,704	60	0,88		
	Gateways Analógico FXS AudioCodes MP-124D/FXS/AC	0,1408	60	0,176		
	Gateways Mediant 1000B MSBRChassis AudioCodes	0,352	60	0,44		
	KVM Console TFT7600 G2	0,264	60	0,33		
	Servidor PROLIANT DL380 GEN9	0,00048672	60	0,468		
	Servidor PROLIANT DL380 GEN9	0,00048672	60	0,468		
	Switch Cisco SG300 Tipo 5 Gigabit POE 8 Portas	0,352	60	0,44		
	Router BOARD 2011UJ AS-RM (Worldnet)	0,2112	60	0,264		
	Fiber Link 2100B (Embratel/Claro)	0,44	60	0,55		
	MSR1002-4 Router JG875A (Embratel/Claro)	0,1408	60	0,176		

Fonte: O Autor (2019).

Totalizando os valores do kVA e KW da Carga Crítica do *Data Center* do IFPE *Campus Igarassu* temos:

- TOTAL (kVA) = 5,22342144
- TOTAL (KW) = 7,56306

Em seguida foi levantada a Carga dos Equipamentos do Sistema UPS, visto no quadro 4. Fazem parte deste bloco os equipamentos como Geradores e *No-Breaks* e Banco de Baterias do IFPE *Campus Igarassu*. Para esta pesquisa foram considerados os seguintes atributos: Equipamento, Tombamento, Fabricante, n.º de Série, Fator de Potência, Tensão, Corrente, Carga, Frequência e Potência.

Quadro 4 – Equipamentos da Carga do Sistema UPS do *Data Center* do IFPE *Campus Igarassu*

	EQUIPAMENTO	TOMBAMENTO	FABRICANTE	Nº DE SÉRIE
CARGA DO SISTEMA DE UPS	Nobreak APC SURT10000XLI	185266	APC	QS1411272236
	Bateria APC SURT192XLBP	185266	APC	5S1406T00325
	Bateria APC SURT192XLBP	185266	APC	5S1406T03659
	PDU APC 2G para Rack AP8858	185266	APC	ZA1335001041
	PDU APC 2G para Rack AP8858	185266	APC	ZA1349007452

Fonte: O Autor (2019).

Da mesma forma que ocorreu no levantamento dos dados dos equipamentos da carga crítica. Aqui seguiu-se a mesma linha de raciocínio para a busca das informações para preenchimento da planilha, ou seja, se não estivesse disponível no equipamento ou manual, buscaram-se fórmulas para encontrar a informação energética conforme visto anteriormente. O quadro 5 e o quadro 6 mostram os resultados.

Quadro 5 – Fator de Potência, Tensão e Corrente da Carga do Sistema UPS do *Data Center* do IFPE *Campus* Igarassu

	EQUIPAMENTO	FATOR DE POTENCIA	TENSÃO (V)	CORRENTE(A)
CARGA DO SISTEMA DE UPS	Nobreak APC SURT10000XLI	0,8	220	50
	Bateria APC SURT192XLBP	0,8	220	0
	Bateria APC SURT192XLBP	0,8	220	0
	PDU APC 2G para Rack AP8858	0,8	220	16
	PDU APC 2G para Rack AP8858	0,8	220	16

Fonte: O Autor (2019).

Da mesma forma, para cálculo do PUE e DCiE, foi considerado apenas o Total do kVA e o Total do KW como será visto mais adiante, e desta forma, segue o mesmo raciocínio também o levantamento de carga dos equipamentos da carga de iluminação e de climatização.

Quadro 6 – Carga, Frequência e Potência da Carga do Sistema UPS do *Data Center* do IFPE *Campus* Igarassu

	EQUIPAMENTO	CARGA(kVA)	FREQUENCIA (Hz)	POTENCIA (KW)
CARGA DO SISTEMA DE UPS	Nobreak APC SURT10000XLI	8,8	60	11
	Bateria APC SURT192XLBP	0	60	0
	Bateria APC SURT192XLBP	0	60	0
	PDU APC 2G para Rack AP8858	2,816	60	3,52
	PDU APC 2G para Rack AP8858	2,816	60	3,52

Fonte: O Autor (2019).

Totalizando os valores do kVA e KW da Carga do Sistema UPS do *Data Center* do IFPE *Campus* Igarassu:

- TOTAL (kVA) = 14,432
- TOTAL (KW) = 18,04

Depois foram levantados os Equipamentos da Carga de Iluminação, apresentados no quadro 7. Aqui pertencem todos os equipamentos utilizados para iluminação do *Data Center* do IFPE *Campus* Igarassu.

Quadro 7 – Equipamentos da Carga de Iluminação do *Data Center* do IFPE *Campus* Igarassu

	EQUIPAMENTO	FABRICANTE	FATOR DE POTENCIA	TENSÃO (V)	CORRENTE(A)
CARGA DE ILUMINAÇÃO	Lampada de LED 40 6.500K	Taschiba	0,92	220	0,093
	Lampada de LED 40 6.500K	Taschiba	0,92	220	0,093

Fonte: O Autor (2019).

Para esta pesquisa foram considerados os seguintes atributos: Equipamento, Fabricante, Fator de Potência, Tensão, Corrente, Carga, Frequência, Potência Nominal e Potência, conforme quadro 8.

Quadro 8 – Carga, Frequência, Potência Nominal e Potência da Carga de Iluminação do *Data Center* do IFPE *Campus* Igarassu

	EQUIPAMENTO	CARGA(kVA)	FREQUENCIA (Hz)	POTENCIA NOMINAL (W)	POTENCIA (KW)
CARGA DE ILUMINAÇÃO	Lampada de LED 40 6.500K	0,0188232	60	20,50	0,02
	Lampada de LED 40 6.500K	0,0188232	60	20,50	0,02

Fonte: O Autor (2019).

Totalizando os valores do kVA e KW da Carga de Iluminação do *Data Center* do IFPE *Campus* Igarassu:

- TOTAL (kVA) = 0,0376464
- TOTAL (KW) = 0,04092

Depois foram levantados os Equipamentos da Carga de Climatização, apresentado no quadro 9. Aqui pertencem todos os equipamentos utilizados para resfriamento do *Data Center* do IFPE *Campus* Igarassu como *split*, ar-condicionado de janela, entre outros.

Quadro 9 – Equipamentos da Carga de Climatização do *Data Center* do IFPE *Campus* Igarassu

	EQUIPAMENTO	TOMBAMENTO	FABRICANTE	Nº DE SÉRIE
CARGA DE CLIMATIZAÇÃO	Split 42VFCA22M5 22.000 BTU/h	222637	Midea	1216B18739701/0000012

Fonte: O Autor (2019).

Para esta pesquisa foram considerados os seguintes atributos: Equipamento, Tombamento, Fabricante, n.º de Série, Fator de Potência, Tensão, Corrente, Carga, Frequência, Capacidade e Potência Nominal, de acordo com o quadro 10 e o quadro 11.

Quadro 10 – Fator de Potência, Tensão e Corrente, da Carga de Climatização do *Data Center* do IFPE *Campus* Igarassu

	EQUIPAMENTO	FATOR DE POTENCIA	TENSÃO (V)	CORRENTE(A)
CARGA DE CLIMATIZAÇÃO	Split 42VFCA22M5 22.000 BTU/h	0,92	220	8,8

Fonte: O Autor (2019).

Quadro 11 – Carga, Frequência, Capacidade e Potência Nominal da Carga de Climatização do *Data Center* do IFPE *Campus* Igarassu

	EQUIPAMENTO	CARGA(kVA)	FREQUENCIA (Hz)	CAPACIDADE (KW)	POTENCIA NOMINAL (W)	EFICIENCIA (W)	POTENCIA (KW)
CARGA DE CLIMATIZAÇÃO	Split 42VFCA22M5 22.000 BTU/h	1,78112	60	6,45	1.919	3,36	1,936

Fonte: O Autor (2019).

Totalizando os valores do kVA e KW da Carga de Climatização do *Data Center* do IFPE *Campus* Igarassu:

- TOTAL (kVA) = 1,78112
- TOTAL (KW) = 1,936

Com o levantamento das cargas feito, puderam ser efetuados os cálculos conforme a fórmula (2.2) para obter o valor do PUE e a fórmula (2.3) para obter o valor do DCiE, o resultado segue conforme a tabela 4.

Tabela 4 – Valores do PUE e DCiE do *Data Center* do IFPE *Campus* Igarassu entre 2018 e 2019

PUE	1,261391553
DCiE	79,27752469

Fonte: O Autor (2019).

Verificou-se que os resultados dos valores apresentados no PUE e DCiE do *Data Center* do IFPE *Campus* Igarassu entre 2018 e 2019 e comparados com os valores de referência da tabela 1, estão dentro de uma faixa de eficiência desejável.

Para concluir esta contextualização, buscou-se em seguida o resultado da soma do consumo elétrico de todas as Cargas analisadas neste estudo para o *Data Center* do IFPE *Campus* Igarassu, conforme tabela 5.

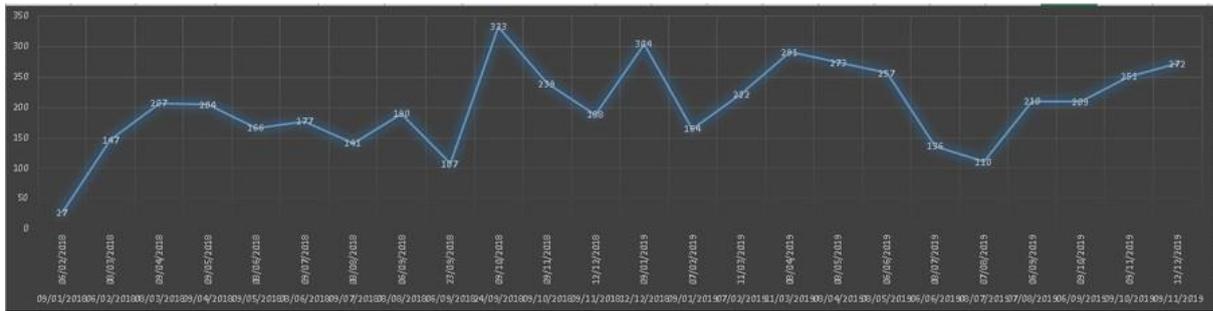
Tabela 5 – Consumo Elétrico do *Data Center* do IFPE *Campus* Igarassu

Total de Consumo no Data Center (kW)	27,58
---	--------------

Fonte: O Autor (2019).

De posse das faturas mensais de consumo de energia elétrica do *campus* Igarassu entre 2018 e 2019 foi criado o gráfico 1, onde comparando a tabela 5, verifica-se que o consumo do *Data Center* foi inferior a 26% do consumo geral do IFPE *Campus* Igarassu no dia 23/09/2018, data esta onde ocorreu o menor consumo de energia elétrica no *campus* se compararmos com todo os outros no período analisado.

Gráfico 1 – Consumo de Energia Média por dia do IFPE Campus Igarassu entre 2018 e 2019



Fonte: Adaptado do Setor Administrativo do IFPE Campus Igarassu (2019)

Ciente das normas, orientações e programas do governo federal quanto ao bom uso dos recursos públicos no que se refere ao consumo de energia elétrica nas instalações públicas, seguiu-se o experimento proposto por este trabalho, descrito a seguir.

5.2 GESTÃO DE RISCO DA PERDA DA EFICIÊNCIA ENERGÉTICA NOS DATA CENTERS DO IFPE

Este trabalho é fundamentado pela norma da ABNT ISO/IEC 27005:2019, porém limitando-se dentro do processo a Definição de Contexto e a Identificação dos Riscos, este último inserido no subprocesso de Avaliação de Riscos.

A definição do contexto diz respeito ao ambiente a que está sendo referido um determinado assunto, podendo ser externo, quando busca atingir seus objetivos fora dos limites físicos da instituição ou interno, quando atua dentro do seu espaço físico. Desta forma o nosso contexto está inserido no ambiente interno do IFPE.

O escopo deste trabalho, que descreve os limites desta pesquisa, que são os *data centers* do IFPE.

A identificação do risco consiste em relacionarmos eventos que podem causar uma perda potencial dentro de uma instituição. No ambiente do estudo, o ativo é caracterizado como sendo de suporte e infraestrutura por estarem relacionado: a elementos físicos que suportam processos (*hardware*), programas que contribuem para as operações de um sistema (*software*), dispositivos de telecomunicações (redes) e instalações físicas. Foi utilizada a expressão “Perda da Eficiência Energética no *Data Center* do IFPE“ para identificar o risco que devemos controlar.

Para a identificação das ameaças não foi encontrado um levantamento de prováveis ameaças ao ativo identificado como “Eficiência Energética do *Data Center* do IFPE“, assim, de acordo com a norma ABNT ISO/IEC 27005:2019, serão consideradas as informações coletadas nos catálogos externos de ameaças específicas dentro do escopo levantado e as principais ameaças em ambientes de *data centers* identificados no dia a dia que possam aumentar o consumo de energia elétrica em outras organizações. Para isso levou-se em conta os equipamentos ligados em suas respectivas atuações, como: a carga crítica, a carga de sistema UPS, a carga de iluminação

e a carga de climatização dos *data centers* do IFPE. Desta forma, foram obtidos as seguintes ameaças:

- Equipamentos antigos;
- Equipamentos de iluminação funcionando de forma precária;
- Temperatura do sistema de climatização oscilando;
- A carga do *no breaks*/geradores próximo ao limite da capacidade;
- Equipamentos de rede próximo ao limite da capacidade (roteadores, *switchs*, *hubs*, etc);
- Consumo de recursos dos servidores (constantemente picos de I/O) próximo ao limite da capacidade;
- Máquinas físicas ou virtuais ociosas.

As ameaças, segundo consta na tabela informativa da norma ABNT ISO/IEC 27005, podem ser identificados como sendo do tipo: Natural, Acidental ou Intencional. Já a fonte das ameaças pode ser de origem do tipo: *Hacker*, Criminoso Digital, Terrorista, Espionagem Industrial e Pessoal Interno.

Deste modo, ainda baseado na norma ABNT ISO/IEC 27005, chegamos às seguintes definições de ameaças levantadas quanto à sua identificação e fonte: Intencional e Pessoal Interno.

A finalidade da identificação dos controles existentes é tratar os riscos da ocorrência de um incidente de segurança através de mecanismos administrativos, físico ou operacional. Com base nas ameaças levantadas foram identificados os seguintes controles:

- Aquisição de novos equipamentos;
- Manutenção dos equipamentos;
- Configuração dos equipamentos;
- Desativação de equipamentos;
- Redistribuição de equipamentos (dentro do *campus*);
- Redistribuição de equipamentos (entre unidades de lotação);
- Melhoramento de *layout* e distribuição dos equipamentos.

A identificação da vulnerabilidade é uma fraqueza que pode ser explorada levando à realização de uma ameaça e assim comprometendo a segurança de sistemas ou informações. De acordo com os controles foram listadas as seguintes vulnerabilidades:

- Falta de recursos financeiro para investimentos;
- Equipamentos sem Garantias;
- Falta de equipe com conhecimento técnico;
- Falta de peças ou componentes sobressalentes (dentro do *campus* ou nas outras unidades de lotação);
- Falta de equipamentos (dentro do *campus* ou nas outras unidades de lotação).

A identificação das barreiras contra as vulnerabilidades servem para evitar ou minimizar as fraquezas, ou as vulnerabilidades que podem ser exploradas, levando ao comprometimento da segurança. Desta forma foram identificadas as seguintes barreiras:

- Captação de recursos financeiros;
- Melhoramento no planejamento de aquisições e serviços de TI;
- Capacitação técnica de servidores.

A identificação das consequências são os resultados de um incidente ou um evento que pode ter um impacto na organização, ou em um setor específico. Assim, foram identificadas as seguintes consequências de acordo com o risco proposto:

- Aumento no valor da conta de energia;
- O não cumprimento de normas e legislações em vigor quanto a eficiência e eficácia;
- Uso inadequado de recursos públicos.

A identificação das barreiras protetivas são barreiras que tendem a minimizar ou sanar os impactos das consequências. Assim, foram identificadas as seguintes barreiras protetivas:

- Avaliação periódica do consumo de energia elétrica dentro do *Data Center*;
- Planejamento de redução de consumo de energia dentro do *Data Center*;
- Atenção ao cumprimento de normas e legislações vigentes;
- Atenção ao uso adequado dos recursos públicos.

A identificação dos fatores de escalonamento estão relacionados a algumas atitudes que diminuem ou mesmo anulam as barreiras protetivas. Abaixo seguem os fatores de escalonamentos identificados:

- Falta de recursos humanos;

- Falta de pessoas comprometidas;
- Desconhecimento das normas e legislações vigentes.

A identificação das barreiras secundárias servem para impedir ou minimizar a ação do fator de escalonamento. As seguintes barreiras secundárias foram identificadas:

- Realizar campanhas de conscientização do uso racional de energia elétrica;
- Capacitação técnica de servidores;
- Captação de recursos humanos.

Foi elaborado um formulário eletrônico para ser respondido por cada representante que responda pelo setor de TI nas unidades do IFPE, conforme (Apêndice A).

As perguntas do formulário encaminhado basearam-se na infraestrutura de *data center* e tiveram como objetivo entender as prioridades, segundo a experiência de cada gestor de TI, sobre os aspectos de causa e efeitos diante de um cenário de perda de eficiência energética no *data center do campus*.

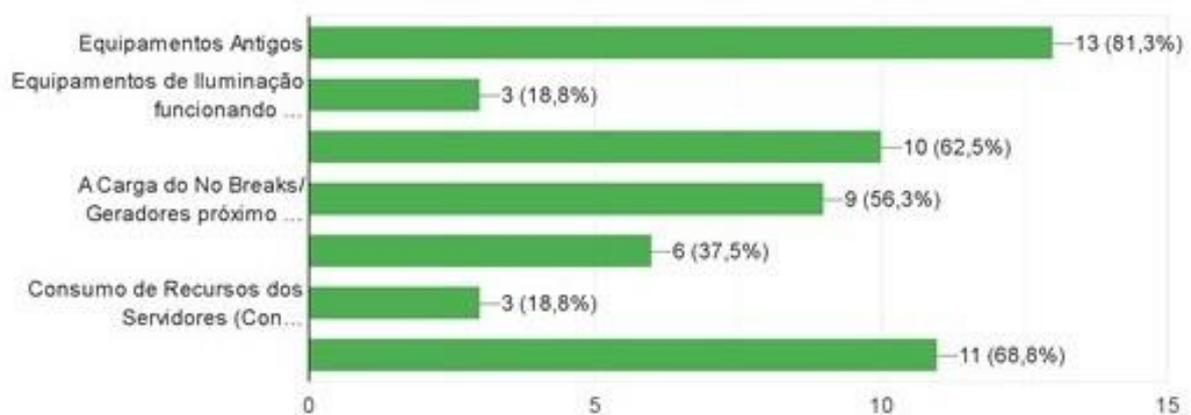
As perguntas tiveram como base a identificação do risco, as causas ou ameaças, controles existentes, vulnerabilidades e as consequências levantadas anteriormente.

O formulário eletrônico foi encaminhado voluntariamente para 18 gestores de TI do IFPE, representantes dos *campi*, reitoria e EAD, e destes obtivemos, 16 respostas completas, 1 não quis participar da pesquisa e 1 não respondeu dentro do prazo da pesquisa no período de 10 a 16 de outubro de 2020. Seguem as perguntas e as respostas abaixo informado pela maioria.

1. Com base em sua experiência e a realidade de sua unidade de lotação, gostaríamos que fosse(m) listado(s) a(s) CAUSA(S) que pode(m) levar ao risco de perda de eficiência energética do *data center*. (Pode registrar mais de uma opção).

Resposta: 13 (81,3%) informaram Equipamentos Antigos. Verificam-se todas as respostas no gráfico 2.

Gráfico 2 – Causas

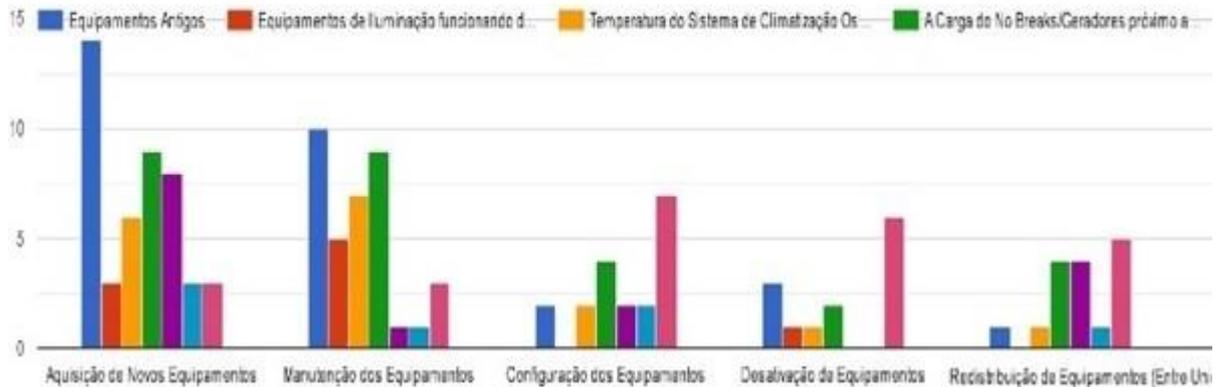


Fonte: O Autor (2020).

2. Para cada causa listada na pergunta anterior, liste a(s) BARREIRA(S) PREVENTIVA(S) que evite(m) a ocorrência desta(s) causa(s). (Pode registrar mais de uma opção).

Resposta: 14 (87,5%) informaram Aquisição de Novos Equipamentos. Verificam-se todas as respostas no gráfico 3.

Gráfico 3 – Barreiras Preventivas

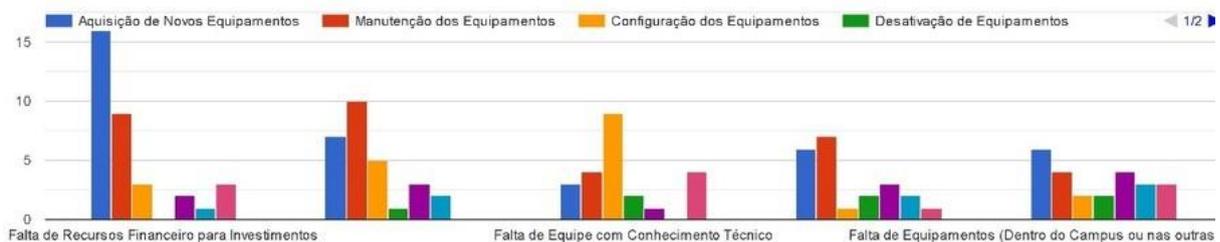


Fonte: O Autor (2020).

3. Para cada barreira preventiva na pergunta anterior, liste o(s) FATOR(ES) DE ESCALONAMENTO(S) que pode(m) anular a ação desta(s) barreira(s) preventiva(s). (Pode registrar mais de uma opção).

Resposta: 16 (100%) informaram Falta de Recursos Financeiro para Investimentos. Verificam-se todas as respostas no gráfico 4.

Gráfico 4 – Fator de Escalonamento para Causas

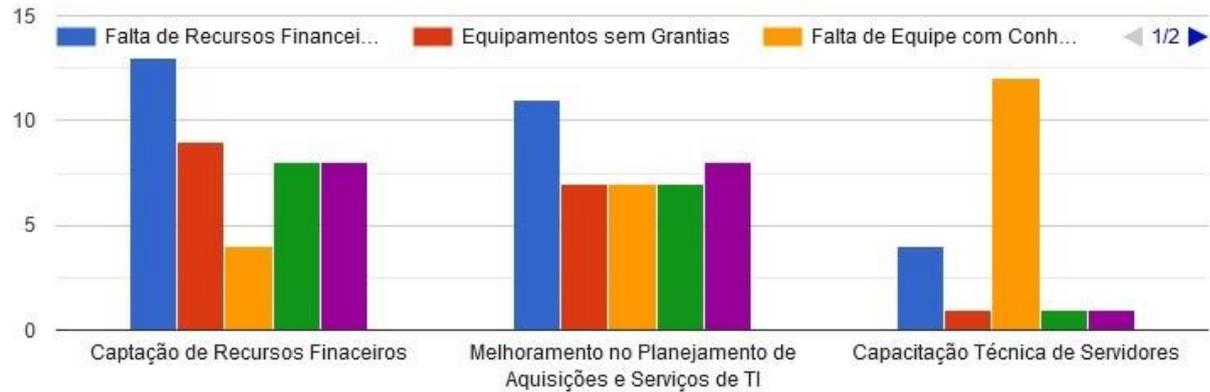


Fonte: O Autor (2020).

4. Para cada fator de escalonamento na pergunta anterior, liste a(s) BARREIRA(S) SECUNDÁRIA(S) que evite(m) a ocorrência deste(s) fator(es) de escalonamento(s). (Pode registrar mais de uma opção).

Resposta: 13 (81,3%) informaram Captação de Recursos Financeiros. Verificam-se todas as respostas no gráfico 5.

Gráfico 5 – Barreiras Secundárias para Causas



Fonte: O Autor (2020).

5. Com base em sua experiência e a realidade de sua unidade de lotação, gostaríamos que fosse(m) listado(s) a(s) CONSEQUÊNCIA(S) quando houver perda de eficiência energética do *data center* (Pode registrar mais de uma opção).

Resposta: 13 (81,3%) informaram Uso inadequado de recursos públicos. Verificam-se todas as respostas no gráfico 6.

Gráfico 6 – Consequências

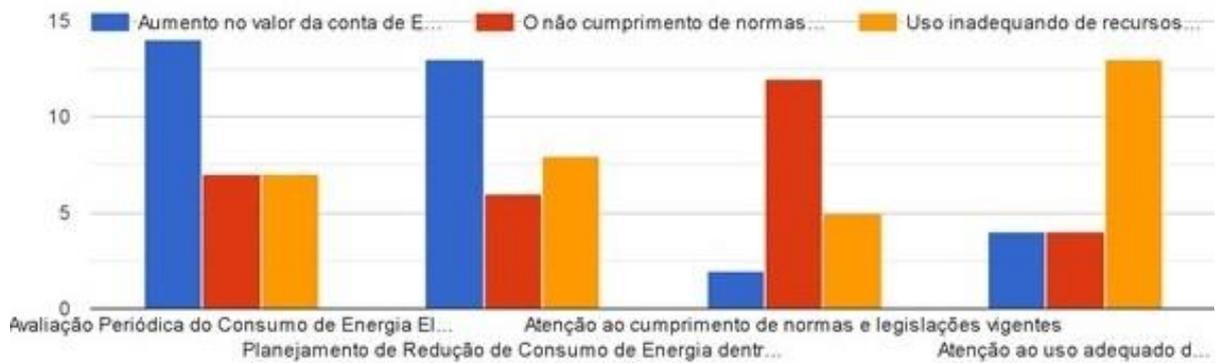


Fonte: O Autor (2020).

6. Para cada consequência listada na pergunta anterior, liste a(s) BARREIRA(S) PROTETIVA(S) que evite(m) a ocorrência desta(s) consequência(s). (Pode registrar mais de uma opção).

Resposta: 14 (87,5%) informaram Avaliação Periódica do Consumo de Energia Elétrica dentro do *Data Center*. Verificam-se todas as respostas no gráfico 7.

Gráfico 7 – Barreiras Protetivas



Fonte: O Autor (2020).

7. Para cada barreira protetiva na pergunta anterior, liste o(s) FATOR(ES) DE ESCALONAMENTO(S) que pode(m) anular a ação desta(s) barreira(s) protetiva(s). (Pode registrar mais de uma opção).

Resposta: 12 (75%) informaram Desconhecimento das normas e legislações vigentes. Verificam-se todas as respostas no gráfico 8.

Gráfico 8 – Fatores de Escalonamento para Consequências

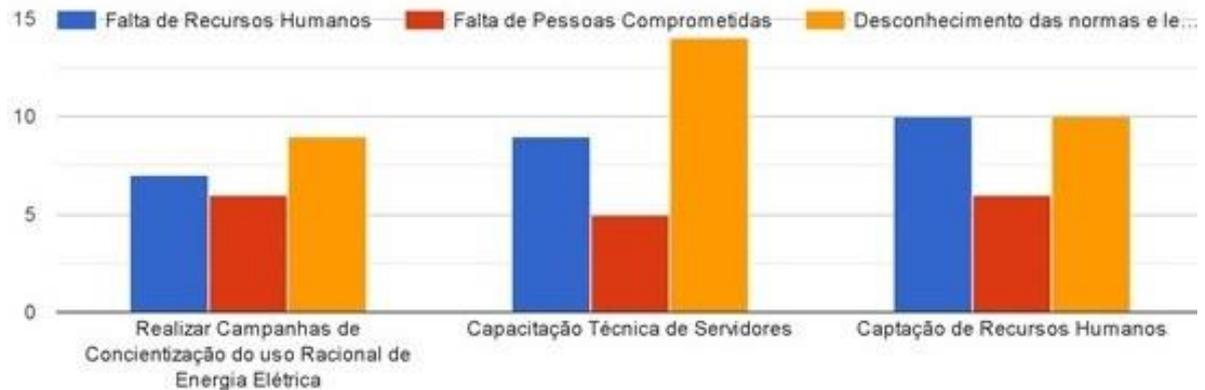


Fonte: O Autor (2020).

8. Para cada fator de escalonamento na pergunta anterior, liste a(s) BARREIRA(S) SECUNDÁRIA(S) que evite(m) a ocorrência deste(s) fator(es) de escalonamento(s). (Pode registrar mais de uma opção).

Resposta: 14 (87,5%) informaram Capacitação Técnica de Servidores. Verificam-se todas as respostas no gráfico 9.

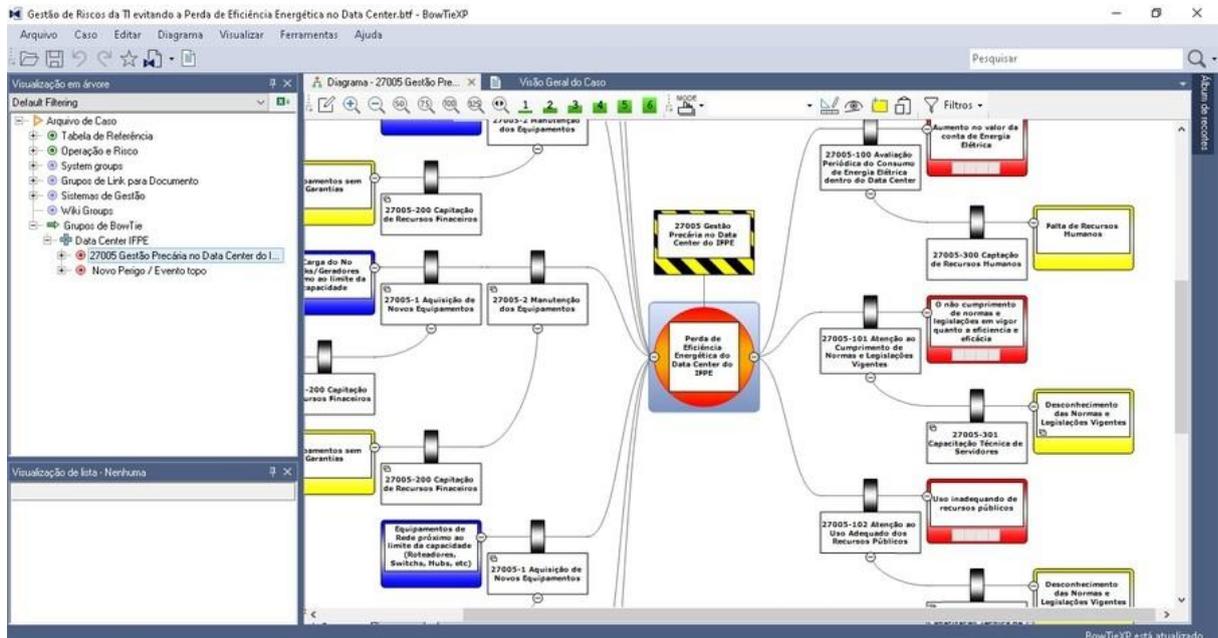
Gráfico 9 – Barreiras Secundárias para Consequências



Fonte: O Autor (2020).

Utilizando a ferramenta BowTieXP versão 10.0.6 para teste da CGE *Risk Management Solutions* foi possível construir uma representação visual do que foi levantado até o momento com os dados coletados, conforme figura 14.

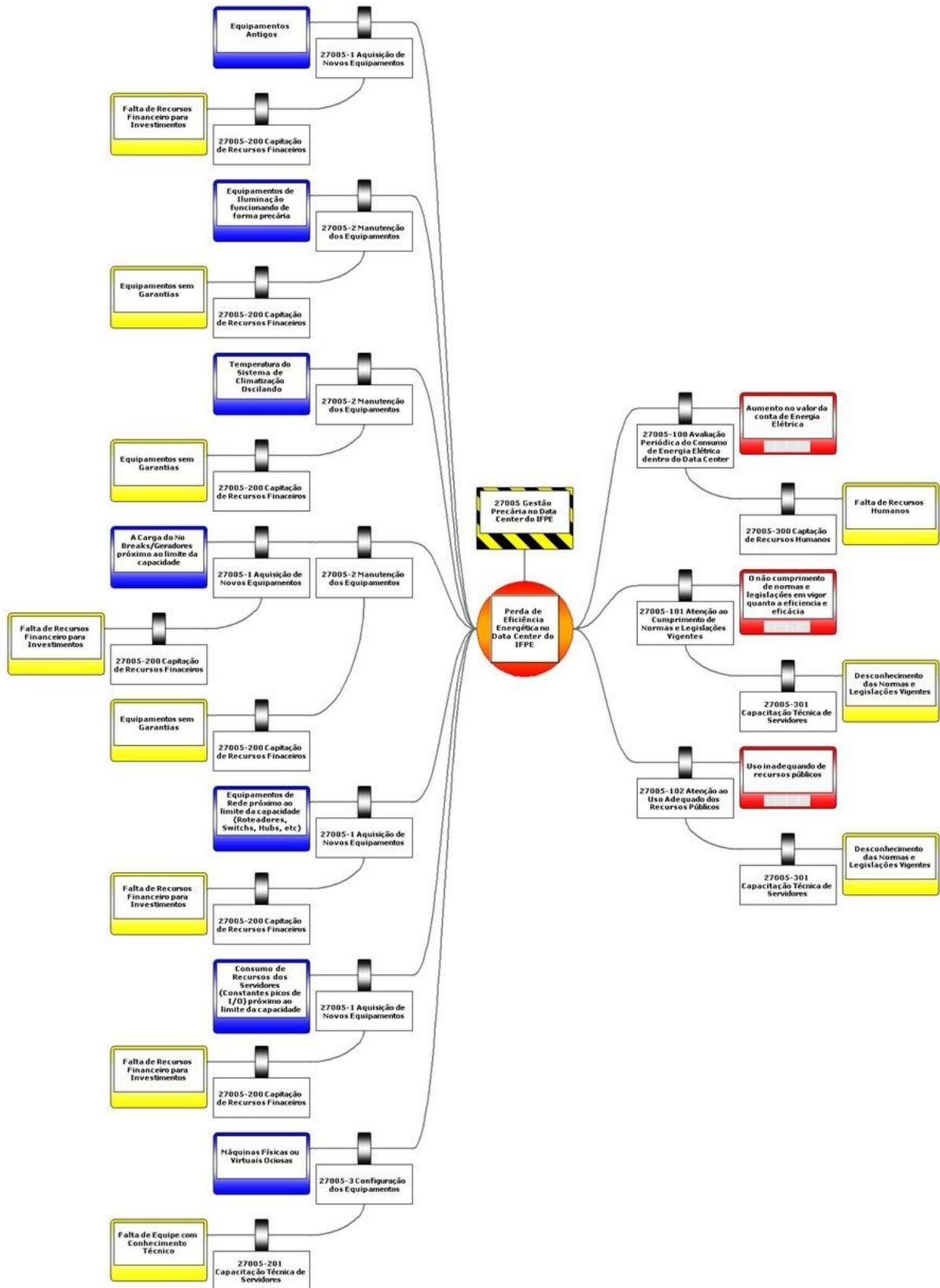
Figura 14 – Ferramenta BowTieXP



Fonte: O Autor (2020).

A representação final do Diagrama de *Bow Tie* para a Tomada de Decisão Evitando a Perda da Eficiência Energética no *Data Center* do IFPE de acordo com o levantamento dos *campi* e reitoria encontra-se na figura 15. A apresentação do diagrama traz uma visão ampla de todos os cenários que foram levantados para a Perda de Eficiência Energética em um *data center* com suas causas e consequências.

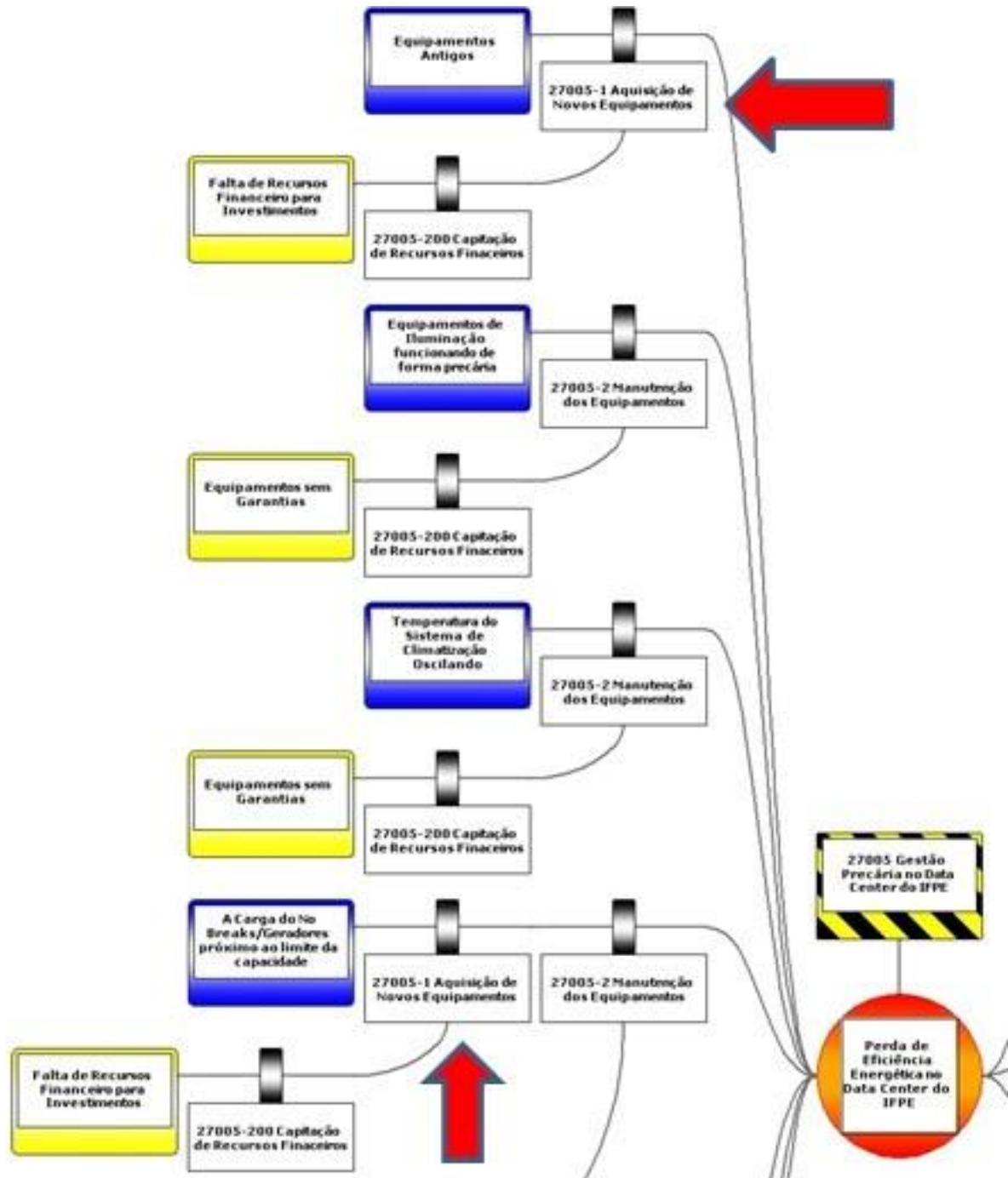
Figura 15 – Diagrama de *Bow Tie* para Tomada de Decisão Evitando a Perda de Eficiência Energética no *Data Center* do IFPE



Fonte: O Autor (2020)

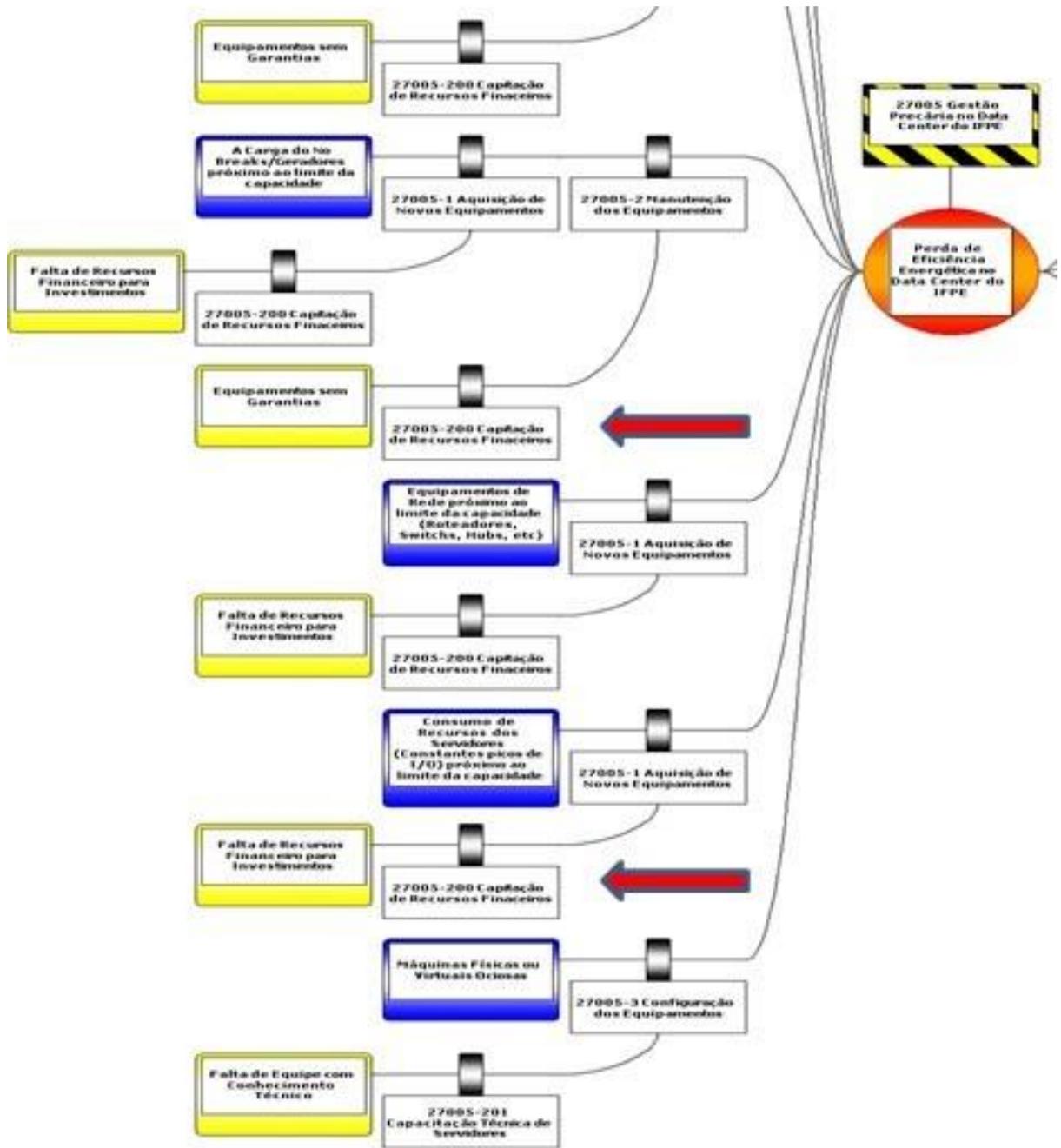
No diagrama ainda é possível identificar uma única ação comum que podem ser utilizadas em diversas causas para evitar a Perda de Eficiência Energética ou ainda, a utilização de um único recurso para minimizar diversas consequências do fato já ocorrido. Temos por exemplo: Para Causas “Equipamentos Antigos” e “A Carga do No-break/Geradores próximo ao limite da Capacidade”, tem a mesma Barreira Preventiva: “Aquisição de Novos Equipamentos”, indicando assim um planejamento de compras de forma mais eficiente e justificada, como mostra a figura 16. Podemos verificar ainda para os Fatores de Escalonamento “Equipamentos sem Garantias” e “Falta de Recursos Financeiros para Investimentos” a mesma Barreira Secundária: “Captação de Recursos Financeiros”, alertando para a indisponibilidade de recursos financeiros, como mostra a figura 17. Temos ainda no lado das Consequências, as Barreiras Protetivas: “Atenção ao Cumprimento de Normas e Legislações Vigentes” e “Atenção ao uso Adequado aos Recursos Públicos” o mesmo Fator de Escalonamento: “Desconhecimento das Normas e Legislações Vigentes”, indicação para a necessidade de capacitação de servidores, como mostra a figura 18 .

Figura 16 – Indicação para o Planejamento de Compras de Forma mais Eficiente e Justificada



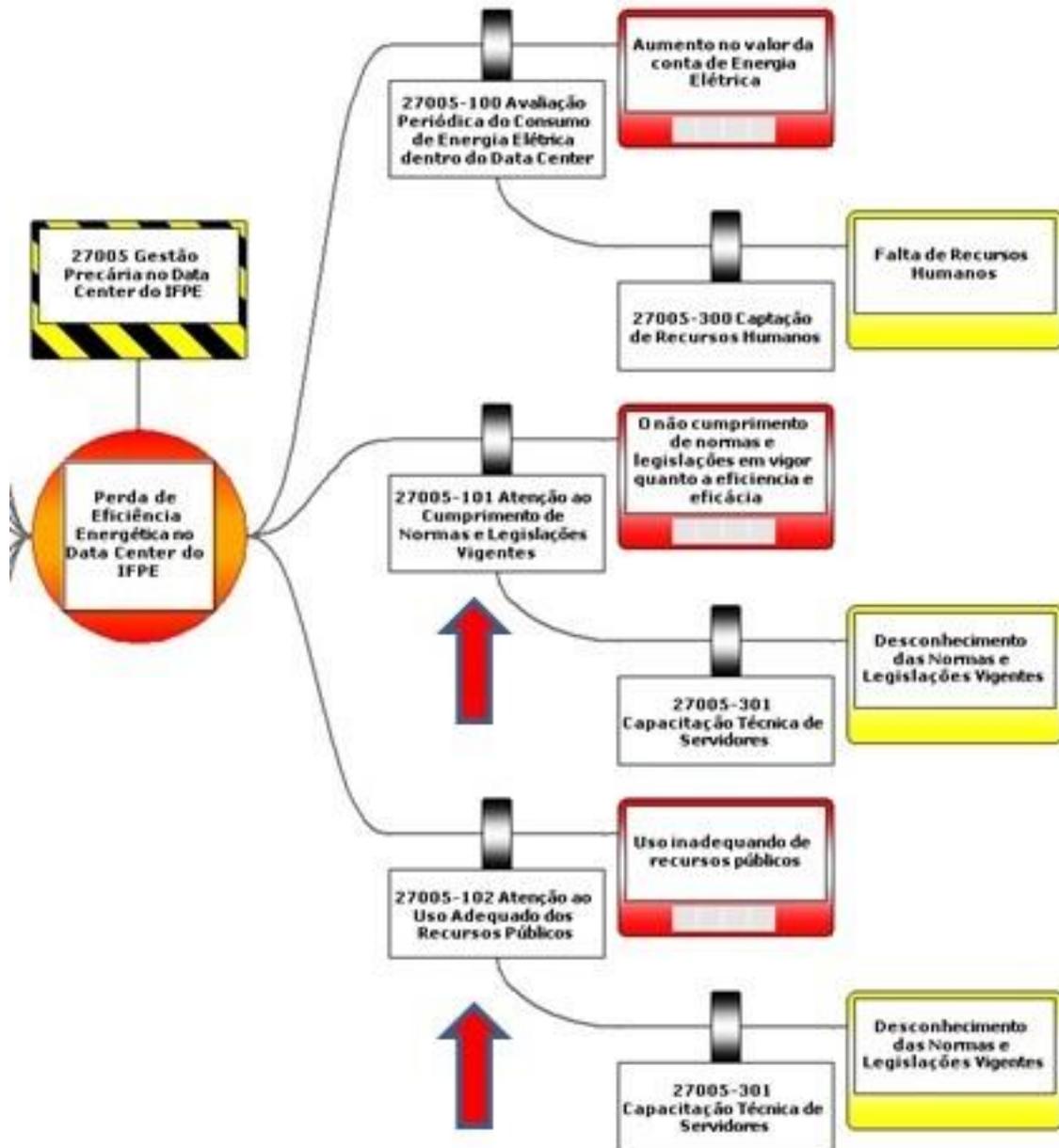
Fonte: O Autor (2020)

Figura 17 – Alerta para a Indisponibilidade de Recursos Financeiros



Fonte: O Autor (2020).

Figura 18 – Indicação para a Necessidade de Capacitação de Servidores



Fonte: O Autor (2020).

5.3 CONSIDERAÇÃO DO CAPÍTULO

Neste capítulo foram apresentados os resultados do PUE e do DCiE de acordo com o levantamento feito no IFPE *Campus* Igarassu no ano de 2019 envolvendo os equipamentos de carga crítica, carga do sistema de UPS, carga de iluminação e carga de climatização. Estes resultados, bem como o comparativo do consumo elétrico do *data center* e o consumo de energia médio do *campus* Igarassu no mesmo período, serviram de referência para o monitoramento da

eficiência energética do data center deste *campus*.

Em seguida, utilizando a norma ABNT ISO/IEC 27005:2019, foi levantados a definição de contexto e identificação do risco, este último inserido no subprocesso de avaliação de riscos. As ameaças foram identificadas e levantadas as fontes de acordo com o contexto interno do *data center* do IFPE. Foram identificados ainda os relacionamentos entre as ações e consequências, bem como os seus atributos internos como vulnerabilidades, barreiras e fatores de escalonamentos.

Por fim, foi apresentado o resultado do questionário aplicado a todos os gestores de TI das unidades do IFPE e com base nestes dados coletados foi construído o diagrama de *bow tie* que representa o objeto deste estudo.

6 CONCLUSÃO

Diante do crescimento dos meios digitais cada vez maior em instituições da administração pública federal para atender as demandas de usuários de maneira adequada, evitando a indisponibilidade dos serviços, alguns órgãos procuram soluções que possam auxiliar na continuidade de suas atividades. Neste contexto, formulou-se o problema da pesquisa: **Como gerenciar o Risco de Perda de Eficiência Energética em um *data center* no IFPE?** E para responder ao questionamento principal da pesquisa, será necessário responder ainda duas questões específicas:

- Como manter um monitoramento constante dos ativos de um *data center* de forma eficaz e eficiente?
- Como manter uma equipe bem treinada e com conhecimento técnico sempre atualizado para que possam desempenhar suas funções de forma que evitem ou diminuam o desperdício de energia nestes ambientes?

O propósito deste estudo fundamentou-se na observância da norma ABNT ISO/IEC 27005:2019 utilizando a metodologia *Bow Tie* para auxiliar no cumprimento de leis e legislações ambientais, eficiência energética de consumo de energia elétrica, prestação de serviço eficiente e eficaz ao consumidor final, ajustes para adequação de gastos financeiros na Administração Pública Federal e resposta rápida para problemas que possam surgir, no que se refere à Gestão de Risco de Segurança da Informação em *Data Center* do IFPE.

Este trabalho de pesquisa contribui com o estudo sobre análise de risco em um contexto de *data center*, propondo o uso de uma metodologia ainda não usada no ambiente de análise de risco de TI para mapeamento dos possíveis cenários de risco de perda de eficiência energética em um *data center*, em específico, no IFPE.

Através do trabalho de pesquisa realizado, evidencia-se a grande importância da adoção de medidas sustentáveis nas organizações públicas agregando informações relevantes a comunidade acadêmica, ao mesmo tempo, atua como ponto de alteração de diretrizes voltadas ao consumo sustentável dos recursos de tecnologias digitais de informação e comunicação.

Analisando os resultados do capítulo 5, o questionamento “Como manter um monitoramento constante dos ativos de um *data center* de forma eficaz e eficiente?” e respondido pela informação da figura 16 pois a indicação para o planejamento de compras antecipa a necessidade de forma mais eficiente e justificada. Para o questionamento “Como manter uma equipe bem treinada e com conhecimento técnico sempre atualizado para que possam desempenhar suas funções de forma que evitem ou diminuam o desperdício de energia nestes ambientes?” e perfeitamente atendida pela informação da figura 18 que indica a necessidade de capacitação de servidores em resposta a possíveis consequências de um fato não desejado.

Este estudo mostrou ainda que pode ser implementado em qualquer órgão da administração pública independente de qualquer região do Brasil. A sua fácil adaptabilidade permite a integração em qualquer departamento de TI, visto os problemas recorrentes por falta de investimentos vem afetando a todos, e qualquer forma de melhorar o desempenho financeiro dos órgãos federais em busca do melhor uso do dinheiro público, se fazem necessários, em um ambiente de crise. Um outro fator importante para ser mencionado e o fato que novos eventos poderem ser adicionados ou excluídos, pois a cada momento surgem novos riscos que antes não se cogitava e outros podem desaparecer.

Com a utilização de uma estrutura para Análise de Riscos baseado na metodologia *bow tie* e fundamentada na norma ABNT ISO/IEC 27005:2019 - Gestão de Riscos de Segurança da Informação, possa garantir através do monitoramento constante, um equilíbrio no consumo de energia elétrica ao mesmo tempo em que possa suportar a necessidade de expansão para atendimento das demandas crescentes nos *campi* e na reitoria do Instituto Federal de Pernambuco, atendendo desta forma as legislações ambientais, impactando de forma reduzida os recursos naturais e trazendo um atendimento eficiente e eficaz a população e assim respondendo a questão principal desta pesquisa.

6.1 PRINCIPAIS CONTRIBUIÇÕES

A metodologia *bow tie* fundamentada na norma ABNT ISO/IEC 27005:2019 - Gestão de Riscos de Segurança da Informação apresenta elementos consistentes que podem ser utilizados para apoiar a equipe na construção de uma gestão de risco para *data centers*. Esta metodologia dentro do processo de gestão de risco de TI para evitar a perda da eficiência energética e uma inovação que pode trazer uma redução no consumo de energia elétrica, bem como práticas sustentáveis dentro do IFPE. Com os levantamentos de informações iniciais obtidas do PUC e DCiE, sobre as causas e consequências de um evento não desejado, facilitará a adoção desta metodologia nas instituições que desejarem utilizar esta prática. A metodologia visual ainda auxilia num rápido entendimento situacional das partes envolvidas facilitando uma tomada de decisão mais assertiva.

6.2 AMEAÇAS E LIMITAÇÕES

- Diante de um novo contexto social e de saúde sanitária vivenciada no ano de 2020, esse estudo teve mais expressivamente algumas limitações tais como as dificuldades de expandir o estudo para outras unidades da IFPE. Não foi possível efetuar o levantamento do PUE e DCiE de todos os *Campi* e Reitoria, pois, o acesso a estas unidades estavam restritos;
- Houve ainda uma demora para a liberação da pesquisa com os servidores ligados à gestão de TI do IFPE devido às novas regras de trabalho decorrentes da pandemia;

- Dificuldades em resolver discussões entre pesquisador e respondentes sobre questões da pesquisa inviabilizando entre outras o pré-teste do questionário de pesquisa devido a pandemia;
- Percebe-se ainda que o grau de maturidade inicial no IFPE quando a matéria é Gestão de Riscos, o que é reforçado pelo fato de que tenha sido aprovado apenas em outubro de 2020 o Plano de Gestão de Riscos e Controles em toda a instituição de ensino;
- Por se tratar uma pesquisa bastante específica, pouco material acadêmico disponível para estudo foi encontrado.

6.3 TRABALHOS FUTUROS

No sentido de ampliar ainda mais os estudos abordados nesta pesquisa, seguem alguns trabalhos futuros que podem ser explorados:

- Aplicar a metodologia desta pesquisa em diversos outros contextos ligados à gestão de risco de TI considerando as visões destes gestores do IFPE;
- Utilizar ferramentas de softwares que possam pôr em prática a metodologia abordada neste estudo;
- Expandir o alcance deste trabalho de maneira adaptável a outras instituições da Administração Pública Federal;
- Comparar a metodologia do trabalho proposto com outras metodologias para a gestão de risco de TI;
- Adaptar a metodologia *bow tie* com regras ou normas técnicas específicas para a gestão de riscos de outras áreas de atuação.

REFERÊNCIAS

- ABDI, Z. et al. **Application of Bow-tie methodology to improve patient safety**. 2016. 425 – 440 p.
- ABNT NBR ISO/IEC 27005. **Tecnologia da Informação — Técnicas de Segurança — Gestão de Riscos de Segurança da Informação**. 3^a. ed. [S.l.: s.n.], 2019. ISBN 978-85-07-08295-8.
- AFEFY, I. H. **Hazard analysis and risk assessments for industrial processes using FMEA and bow-tie methodologies**. 2015. 379 – 391 p.
- ARAÚJO, M. S. de; OLIVEIRA, E. C.; MONTEIRO, S. B. S. 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**, Passo Fundo, v. 9, n. 2, p. 111 – 124, 07 2017. ISSN 176 - 6649. Disponível em: <http://dx.doi.org/10.5335/rbca.v9i2.6099>. Acesso em: 12/01/2021.
- BARROS, C. H. de O. **Modelo Multicritério para Priorização de Ações no Gerenciamento de Riscos de Indisponibilidade de Estoques em Prateleiras com Base na Ferramenta Bow-Tie: Estudo de Caso no Setor Varejista**. 2019. 1 – 72 p.
- CHAHIN, A. et al. **Governo eletrônico: sugestões para o futuro**. São Paulo: Prentice Hall, 2004. ISBN 8587918931.
- CHUEKE, G. V.; LIMA, M. C. Pesquisa Qualitativa: evolução e critérios. **Revista Espaço Acadêmico**, n. 128, Janeiro 2012. ISSN 15196186.
- DELVAZ, B. H.; BOVÉRIO, M. A. **TI Verde - estudo de caso na empresa CSLOG Desenvolvimento de Sistemas Ltda**. São Paulo: [s.n.], 2011. 1 – 22 p. Disponível em: <http://159.203.166.88/index.php/interfacetecnologica/article/view/139>. Acesso em: 24/11/2019.
- FABRO, S. A.; RIVEROS, L. J. M.; WONZOSKI, F. de O. Ti verde – Eficiência Energética de Data Center. p. 1 – 14, 2017. Disponível em: <http://www.revistas.usp.br/revusp/article/view/61684/64573>.
- FREITAS, C. L. de; BORGERT, A.; PFITSCHER, E. D. Agenda Ambiental na Administração Pública: uma análise da aderência de uma IFES as diretrizes propostas pela A3P. In: **XI Colóquio Internacional Sobre Gestão Universitária na América do Sul**. Florianópolis: [s.n.], 2011. p. 1 – 16.
- GIL, A. C. **Como Elaborar Projetos de Pesquisa**. 4. ed. São Paulo: ATLAS S.A, 2002. 176 p. ISBN 85-224-3169-8.
- GOLDHAR, M. P. **Um framework de Métricas de Produtividade e Eficiência Energética em Data Centers**. 2009. Dissertação (Mestrado em Ciência da Computação) — Universidade Federal de Pernambuco. Disponível em: http://repositorio.ufpe.br/bitstream/handle/123456789/2306/arquivo2938_1.pdf?sequence=1&isAllowed=y.
- GUIRARDI, J. M. S.; FEITOZA, E. G. **Boas Práticas em Data Center para Uso de Tecnologia Verde**. 2019. 1 – 22 p.

INSTITUTO FEDERAL DE PERNAMBUCO. **Política de Segurança da Informação e Comunicação do IFPE**. 2017. 1 – 26 p. Disponível em: <https://www.ifpe.edu.br/o-ifpe/conselho-superior/resolucoes/resolucoes-2017-1/resolucao-11-2017-aprova-a-politica-de-seguranca-da-informacao-e-comunicacao-do-ifpe.pdf>. Acesso em: 20/05/2019.

INSTITUTO FEDERAL DE PERNAMBUCO. **Plano de Gestão de Riscos e Controles do Instituto Federal de Pernambuco**. 2020. 1 – 27 p. Disponível em: https://portal.ifpe.edu.br/o-ifpe/governanca-riscos-e-controles/resolucoes/resolucoes-2020/Resolucao_1_2020_1510_1_assinado1.pdf. Acesso em: 30/10/2020.

JACINTO, C.; SILVA, C. **A semi-quantitative assessment of occupational risks using bow-tie representation**. 2009. 973 – 979 p. Disponível em: <http://dx.doi.org/10.1016/j.ssci.2009.08.008>. Acesso em: 02/03/2020.

KHAKZAD, N.; KHAN, F.; AMYOTTE, P. **Dynamic safety analysis of process systems by mapping bow-tie into Bayesian network**. 2013. 46 – 53 p. Disponível em: <http://dx.doi.org/10.1016/j.psep.2012.01.005>.

LOPES, N. da S.; CARRERO, M. A. **Boas Práticas da TI Verde Adotadas Pelas Empresas como Forma de uso Eficiente dos Recursos Energéticos**. 2016. 1 – 16 p.

LUNARDI, G. L.; SIMÕES, R.; FRIO, R. S. **TI Verde - uma análise dos principais benefícios e práticas utilizadas pelas organizações**. 2014. 1 – 30 p.

MARIN, P. S. **Data Centers - Engenharia Infraestrutura Física**. 1ª. ed. São Paulo: PM Books, 2016. 280 p. ISBN 978-85-69397-01-4.

MARTIN, A. S. S. **Adoção da TI Verde em Organizações Públicas Federais no Rio Grande do Sul e o seu Impacto na Sustentabilidade Ambiental**. 2018. 1 – 146 p.

MARTINS, M. S.; SIMÕES JUNIOR, J.; MENEZES, M. S. de. Técnicas de Prevenção e Análise de Acidentes do Trabalho. p. 1 – 14, 2010. Disponível em: <https://safetyergo.files.wordpress.com/2016/06/tc3a9cnicas-de-prevenca3a7c3a3o-e-anc3a1lise-de-acidentes-do-trabalho.pdf>. Acesso em: 19/04/2021.

MELVILLE, N. P. Information Systems Innovation for Environmental Sustainability. **MIS Quarterly**, Michigan, v. 34, n. 1, p. 1 – 21, 03 2010. Acesso em: 12/04/2021.

MORETTI, R. C. V. **Monitorização do consumo de energia em centros de dados**. 2010. 110 p. Dissertação (Engenharia Informática) — Universidade Nova de Lisboa. Acesso em: 20/06/2020.

OLIVEIRA, M. M. de et al. Análise do Gerenciamento de Riscos de um Sistema de Caldeira e Vaso de Pressão - Estudo de Caso. In: **XXXI ENCONTRO NACIONAL DE ENGENHARIA DE PRODUÇÃO**. Belo Horizonte: [s.n.], 2011. p. 1 – 12. Disponível em: http://www.abepro.org.br/biblioteca/enegep2011_TN_STO_138_877_18237.pdf. Acesso em: 19/04/2021.

OLIVEIRA, T. G. V. **Propostas de Eficiência Energética em Infraestrutura para Data Center**. 2017. 1 – 64 p.

PEREIRA, D. M.; SILVA, G. S. As Tecnologias de Informação e Comunicação (TICs) como aliadas para o desenvolvimento. **Cadernos de Ciências Sociais Aplicadas**, Vitória da Conquista, n. 10, p. 151 – 174, 2010.

PLATAFORMA NILO PECANHA. **Plataforma Nilo Peçanha**. 2020. Disponível em: <http://plataformanilopecanha.mec.gov.br/2020.html>. Acesso em: 15/10/2020.

QUEIRÓS, R. C. C. **Proposta de Melhoria para a Adoção das Boas Práticas de TI Verde nas Organizações**. 2019. 102 p. Dissertação (Mestrado Profissional de Sistemas de Gestão) — Universidade Federal Fluminense.

ROTHER, E. T. **Revisão sistemática X revisão narrativa**. 2007. Editora da Acta Paulista de Enfermagem. Disponível em: <https://www.scielo.br/pdf/ape/v20n2/a01v20n2.pdf>. Acesso em: 13/04/2021.

SALLES, A. C. et al. **Adoção de Práticas de TI Verde nas Organizações: Um Estudo Baseado em Mini Casos**. 2013. 1 – 16 p. Disponível em: http://repositorio.furg.br/bitstream/handle/1/5373/2013_EnADI145.pdf?sequence=1.

SILVEIRA, A. D. M. da. **Governança corporativa no Brasil e no mundo: teoria e prática**. Rio de Janeiro: Elsevier, 2010. 397 p. ISBN 9788535236484.

TRIVELATO, B. F.; MENDES, D. P.; DIAS, M. A. A Importância do Gerenciamento de Riscos nas Organizações Contemporâneas. **Revista FATEC Zona Sul**, São Paulo, v. 4, n. 2, p. 1 – 20, 02 2018. ISSN 2359182X.

TRIVINOS, A. N. S. **Introdução à Pesquisa em Ciências Sociais**. São Paulo: ATLAS S.A, 1987. 174 p. ISBN 85-224-0273-6.

UPTIME INSTITUTE. **DCIM Consulting Services**. 2020. Disponível em: <https://pt.uptimeinstitute.com/professional-services/dcim-consulting>. Acesso em: 17/10/2020.

YIN, R. K. **Estudo de Caso : Planejamento e Métodos**. 5. ed. [S.l.]: Bookman, 2014. 320 p. ISBN 978-8582602317.

APÊNDICE A – QUESTIONÁRIO

Pesquisa sobre Cenários do Gerenciamento da Perda da Eficiência Energética nos Data Centers ... https://docs.google.com/forms/d/1cbFyIU7FsvolsfY_wjPNpgVIQA_3dwwoz_V915zDTsQ/printform

Pesquisa sobre Cenários do Gerenciamento da Perda da Eficiência Energética nos Data Centers dos Campi do IFPE

Convidamos o(a) Senhor(a) para participar como voluntário deste trabalho, que está sob a responsabilidade do pesquisador Anderson França Ferreira, estudante do programa de Mestrado Profissional em Gestão da Tecnologia da Informação - 2018 da UFPE, sob a orientação da Prof^a. Dr.^a Patrícia Cabral de Azevedo Restelli Tedesco.

O objetivo desta pesquisa é propor uma Metodologia de Gerenciamento de Riscos, que permita entender melhor, através de uma análise visual, um completo cenário das causas, consequências, barreiras preventivas e protetivas, fatores de escalonamento e barreiras secundárias associados à Perda da Eficiência Energética dos Data Centers dos campi do IFPE.

O público alvo desta pesquisa são gestores da área de Tecnologia da Informação e Comunicação dos Campi do Instituto Federal de Pernambuco.

Todas as informações desta pesquisa serão confidenciais e serão divulgadas apenas em eventos ou publicações científicas, não havendo identificação dos voluntários, a não ser entre os responsáveis pelo estudo, sendo assegurado o sigilo sobre a sua participação. Assim, esta pesquisa atender às determinações éticas das Resoluções nº 196/96 e nº 466/2012 do CNS/MS.

Os dados coletados, por meio deste formulário, ficarão armazenados em computador pessoal, sob a responsabilidade deste pesquisador, pelo período mínimo de 5 anos.

Nada lhe será pago e nem será cobrado para participar desta pesquisa, em que a aceitação deve ser voluntária, ficando garantida a indenização em caso de danos, comprovadamente decorrentes da participação na pesquisa, conforme decisão judicial ou extrajudicial.

Este formulário ficará disponível entre os dias 10/10 a 16/10 de 2020.

Para mais esclarecimentos, contatar:

Patrícia Cabral de Azevedo Restelli Tedesco, Universidade Federal de Pernambuco, Brasil.

Pesquisa sobre Cenários do Gerenciamento da Perda da Eficiência Energética nos Data Centers ... https://docs.google.com/forms/d/1ebFyIU7FsvolsfY_wjPNpgVIQA_3dwwoz_V9l5zDTsQ/printform

(pcart@cin.ufpe.br) ou

Anderson França Ferreira, Universidade Federal de Pernambuco, Brasil.
(aff2@cin.ufpe.br)

Agradeço sua colaboração!
***Obrigatório**

1. Endereço de e-mail *

2. Você concorda em participar como voluntário desta pesquisa? *

Marcar apenas uma oval.

- Sim, concordo em participar desta pesquisa e declaro ter idade maior que dezoito anos.
- Não.

Seção 1 - Dados do Respondente e Unidade de Lotação

Descrição das características gerais do respondente e da unidade de lotação

3. Nome? *

4. Escolaridade? *

Marcar apenas uma oval.

- Ensino Fundamental
- Ensino Médio
- Ensino Superior
- Especialização
- Mestrado
- Doutorado
- Outro

5. Unidade de Lotação? *

Marcar apenas uma oval.

- IFPE - Abreu e Lima
- IFPE - Afogados da Ingazeira
- IFPE - Barreiros
- IFPE - Belo Jardim
- IFPE - Cabo de santo Agostinho
- IFPE - Caruaru
- EAD
- IFPE - Garanhuns
- IFPE - Igarassu
- IFPE - Ipojuca
- IFPE - Jaboatão dos Guararapes
- IFPE - Olinda
- IFPE - Palmares
- IFPE - Paulista
- IFPE - Pesqueira
- IFPE - Recife
- Reitoria
- IFPE - Vitória de Santo Antão

6. Cargo? *

Marcar apenas uma oval.

- Técnico-Administrativo Nível C
- Técnico-Administrativo Nível D
- Técnico-Administrativo Nível E
- Docente

7. Função de Gestão? *

Marcar apenas uma oval.

- Coordenador de TI
- Diretor de TI

8. Tempo nesta Função de Gestão? *

Marcar apenas uma oval.

- 0 a 5 anos
- 5 a 10 anos
- 10 a 15 anos
- 15 a 20 anos
- mais de 20 anos

**Seção 2 -
Questões de
levantamento
das CAUSAS
de Risco para
a Perda de
Eficiência
Energética
do Data
Center**

Nesta seção, buscamos identificar as causas, barreiras preventivas, fatores de escalonamento e barreiras secundárias relacionadas ao risco de perda de eficiência energética do data center na sua unidade de lotação.

Definições:

- . Eficiência Energética do Data Center - Uma forma de medir a Eficiência Energética de um Data Center (PUE=Power Usage Effectiveness) é simplesmente a divisão do consumo energético total do data center (Carga de Infraestrutura) pelo consumo dos sistemas de TI (Carga de TI), para um determinado período, assim temos a fórmula $PUE = \text{Carga de Infraestrutura} / \text{Carga de TI}$, quanto mais próximo de 1 for o resultado, melhor estará a Eficiência Energética do Data Center. Para efeito do estudo, levaremos em conta apenas a carga em KW dos equipamentos em operação na sua unidade de lotação dentro do data center (Carga de Infraestrutura compreendem todos os equipamentos dentro do Rack + Lâmpadas + breaks/geradores + equipamentos de ar-condicionado. Carga de TI compreendem todos os equipamentos dentro do Rack;
- . Evento não Desejado - Risco para a Perda de Eficiência Energética do Data Center na sua unidade de lotação;
- . Causas - Elemento ou Circunstância que PODE LEVAR a um evento não desejado;
- . Barreiras Preventivas - São medidas de detecção/tomada de decisão/ação para EVITAR/REDUZIR que as causas ocorram;
- . Fatores de Escalonamento - Condição que ANULA/REDUZ a eficiência de uma barreira preventiva;
- . Barreiras Secundárias - São medidas adotadas para EVITAR/REDUZIR os fatores de escalonamentos.

9. 1. Com base em sua experiência e a realidade de sua unidade de lotação, gostaríamos que fosse(m) listado(s) a(s) CAUSA(S) que pode(m) levar ao risco de perda de eficiência energética do data center. (Pode registrar mais de uma opção) *

Marque todas que se aplicam.

- Equipamentos Antigos
- Equipamentos de Iluminação funcionando de forma precária
- Temperatura do Sistema de Climatização Oscilando
- A Carga do No Breaks/Geradores próximo ao limite da capacidade
- Equipamentos de Rede próximo ao limite da capacidade (Roteadores, Switchs, Hubs, etc)
- Consumo de Recursos dos Servidores (Constantes picos de I/O) próximo ao limite da capacidade
- Máquinas Físicas ou Virtuais Ociosas

10. 2. Para cada causa listada na pergunta anterior, liste a(s) BARREIRA(S) PREVENTIVA(S) que evite(m) a ocorrência desta(s) causa(s). (Pode registrar mais de uma opção)

Marque todas que se aplicam.

	Equipamentos Antigos	Equipamentos de Iluminação funcionando de forma precária	Temperatura do Sistema de Climatização Oscilando	A Carga do No Breaks/Geradores próximo ao limite da capacidade	Equipamentos de Rede próximo ao limite da capacidade (Roteadores, Switchs, Hubs, etc)	Consumo de Recursos dos Servidores (Constantes picos de I/O) próximo ao limite da capacidade	Máquinas Físicas ou Virtuais Ociosas
Aquisição de Novos Equipamentos	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Manutenção dos Equipamentos	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Configuração dos Equipamentos	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Desativação de Equipamentos	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Redistribuição de	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pesquisa sobre Cenários do Gerenciamento da Perda da Eficiência Energética nos Data Centers ... https://docs.google.com/forms/d/1ebFyIU7FsvolsfY_wjPNpgVIQA_3dwwoz_V9l5zDTsQ/printform

Equipamentos (Dentro do Campus)							
Redistribuição de Equipamentos (Entre Unidades de Lotação)	<input type="checkbox"/>						
Melhoramento de Layout e Distribuição dos Equipamentos	<input type="checkbox"/>						

11. 3. Para cada barreira preventiva na pergunta anterior, liste o(s) FATOR(ES) DE ESCALONAMENTO(S) que pode(m) anular a ação desta(s) barreira(s) preventiva(s). (Pode registrar mais de uma opção)

Marque todas que se aplicam.

	Aquisição de Novos Equipamentos	Manutenção dos Equipamentos	Configuração dos Equipamentos	Desativação de Equipamentos	Redistribuição de Equipamentos (Dentro do Campus)	Redistribuição de Equipamentos (Entre Unidades de Lotação)	Melhoramento de Layout e Distribuição dos Equipamentos
Falta de Recursos Financeiro para Investimentos	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Equipamentos sem Grantias	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Falta de Equipe com Conhecimento Técnico	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Falta de Peças ou Componentes sobressalentes (Dentro do Campus ou nas outras Unidades de Lotação)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pesquisa sobre Cenários do Gerenciamento da Perda da Eficiência Energética nos Data Centers ... https://docs.google.com/forms/d/1ebFyIU7FsvolsfY_wjPNpgVIQA_3dwwoz_V9l5zDTsQ/printform

Falta de Equipamentos (Dentro do Campus ou nas outras Unidades de Lotação)

12. 4. Para cada fator de escalonamento na pergunta anterior, liste a(s) BARREIRA(S) SECUNDÁRIA(S) que evite(m) a ocorrência deste(s) fator(es) de escalonamento(s). (Pode registrar mais de uma opção)

Marque todas que se aplicam.

	Falta de Recursos Financeiro para Investimentos	Equipamentos sem Grantias	Falta de Equipe com Conhecimento Técnico	Falta de Peças ou Componentes sobressalentes (Dentro do Campus ou nas outras Unidades de Lotação)	Falta de Equipamentos (Dentro do Campus ou nas outras Unidades de Lotação)
Capitação de Recursos Financeiros	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Melhoramento no Planejamento de Aquisições e Serviços de TI	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Capacitação Técnica de Servidores	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Seção 3 -

Nesta seção, buscamos identificar as consequências, barreiras protetivas, fatores de escalonamento e barreiras secundárias relacionadas a perda de eficiência energética do data center na sua unidade de lotação.
 Definições:
 . Eficiência Energética do Data Center - Uma forma de medir a Eficiência Energética de um Data Center (PUE- Power Usage Effectiveness) é simplesmente a divisão do consumo energético total do data center (Carga de

Questões de levantamento das CONSEQUÊNCIAS da Perda de Eficiência Energética do Data Center

Infraestrutura) pelo consumo dos sistemas de TI (Carga de TI), para um determinado período, assim temos a fórmula $PUE = \text{Carga de Infraestrutura} / \text{Carga de TI}$, quanto mais próximo de 1 for o resultado, melhor estará a Eficiência Energética do Data Center. Para efeito do estudo, levaremos em conta apenas a carga em KW dos equipamentos em operação na sua unidade de lotação dentro do data center (Carga de Infraestrutura compreendem todos os equipamentos dentro do Rack + Lâmpadas + breaks/geradores + equipamentos de ar-condicionado. Carga de TI compreendem todos os equipamentos dentro do Rack;

- . Evento não Desejado - Perda de Eficiência Energética do Data Center na sua unidade de lotação;
- . Consequências - Possível efeito (indesejado) DECORRENTE do evento não desejado;
- . Barreiras Protetivas - São medidas de detecção/tomada de decisão/ação para EVITAR/REDUZIR as consequências indesejadas;
- . Fatores de Escalonamento - Condição que ANULA/REDUZ A a eficiência de uma barreira protetiva.
- . Barreiras Secundárias - São medidas adotadas para EVITAR/REDUZIR os fatores de escalonamentos.

13. 1. Com base em sua experiência e a realidade de sua unidade de lotação, gostaríamos que fosse(m) listado(s) a(s) CONSEQUÊNCIA(S) quando houver perda de eficiência energética do data center. (Pode registrar mais de uma opção) *

Marque todas que se aplicam.

- Aumento no valor da conta de Energia
- O não cumprimento de normas e legislações em vigor quanto a eficiência e eficácia
- Uso inadequado de recursos públicos

14. 2. Para cada consequência listada na pergunta anterior, liste a(s) BARREIRA(S) PROTETIVA(S) que evite(m) a ocorrência desta(s) consequência(s). (Pode registrar mais de uma opção)

Marque todas que se aplicam.

	Aumento no valor da conta de Energia	O não cumprimento de normas e legislações em vigor quanto a eficiência e eficácia	Uso inadequado de recursos públicos
Avaliação Periódica do Consumo de Energia Elétrica dentro do Data Center	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Planejamento de Redução de Consumo de Energia dentro do Data Center	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Atenção ao cumprimento de normas e legislações vigentes	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Atenção ao uso adequado dos recursos públicos

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
--------------------------	--------------------------	--------------------------

15. 3. Para cada barreira protetiva na pergunta anterior, liste o(s) FATOR(ES) DE ESCALONAMENTO(S) que pode(m) anular a ação desta(s) barreira(s) protetiva(s). (Pode registrar mais de uma opção)

Marque todas que se aplicam.

	Avaliação Periódica do Consumo de Energia Elétrica dentro do Data Center	Planejamento de Redução de Consumo de Energia dentro do Data Center	Atenção ao cumprimento de normas e legislações vigentes	Atenção ao uso adequado dos recursos públicos
Falta de Recursos Humanos	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Falta de Pessoas Comprometidas	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Desconhecimento das normas e legislações vigentes	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

16. 4. Para cada fator de escalonamento na pergunta anterior, liste a(s) BARREIRA(S) SECUNDÁRIA(S) que evite(m) a ocorrência deste(s) fator(es) de escalonamento(s). (Pode registrar mais de uma opção)

Marque todas que se aplicam.

	Falta de Recursos Humanos	Falta de Pessoas Comprometidas	Desconhecimento das normas e legislações vigentes
Realizar Campanhas de Concientização do uso Racional de Energia Elétrica	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Capacitação Técnica de Servidores	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Captação de Recursos Humanos	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Este conteúdo não foi criado nem aprovado pelo Google.

Google Formulários

ANEXO A – DESPACHO DO TERMO DE ANUÊNCIA DA PESQUISA


MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE PERNAMBUCO
REITORIA
PRÓ-REITORIA DE PESQUISA, PÓS-GRADUAÇÃO E INOVAÇÃO
 Avenida Professor Luiz Freire, nº 500 – Cidade Universitária – Recife – CEP: 50.540-740
 (081) 2125-1691 - propesq@reitoria.ifpe.edu.br

Recife, 09 de outubro de 2020

DESPACHO

Ao Magnífico Reitor do IFPE

Assunto: Anuência para realização de pesquisa no IFPE (23294.010706.2020-89).

Trata o presente de solicitação de anuência para realização de pesquisa no IFPE de ANDERSON FRANÇA FERREIRA, servidor do IFPE – Reitoria/DADT, a ser realizada com dados institucionais no âmbito do IFPE, com vistas ao desenvolvimento de trabalho de conclusão Programa de Mestrado Profissional em Ciência da Computação da UFPE.

Constam na solicitação:

1. Requerimento via e-mail;
2. Termo de Anuência do IFPE preenchido;
3. Solicitação, contendo informações do projeto de pesquisa.

A Resolução nº 29/2017/CONSUP/IFPE aprovou o Termo de Anuência para Realização de Pesquisas Descritivas Externas nas Dependências do IFPE. A pesquisa apresentada no presente processo se encaixa nesse perfil e, para ser realizada em nossa instituição, depende de anuência de nosso dirigente máximo.

A pesquisa pretende desenvolver uma metodologia de gerenciamento de riscos, que permita entender melhor, através de uma análise visual, um completo cenário das causas, consequências, barreiras preventivas e protetivas, fatores de escalonamento e barreiras secundárias associados à perda da eficiência energética dos Data Centers dos *campi* do IFPE, avaliar de que forma as políticas de inclusão social voltadas para a diversidade étnico-racial de gênero e sexualidade estão sendo implementadas no IFPE, em articulação com os dispositivos legais concernentes ao tema. Além dos estudos bibliográficos em publicações específicas, será realizado procedimento metodológico de

entrevista com a comunidade por meio de formulário eletrônico da Google. Neste ponto, destacamos a importância na observação dos pontos a seguir.

- 1) A pesquisa deve atender às determinações éticas das Resoluções nº 196/96 e nº 466/2012 do CNS/MS, nos casos de pesquisas envolvendo seres humanos, com o compromisso no resguardo da segurança e bem-estar dos sujeitos de pesquisa nela recrutados;
- 2) Os responsáveis pela pesquisa obrigam-se a prestar todos os esclarecimentos necessários, quando solicitado por qualquer instância do IFPE;
- 3) O IFPE não arcará com nenhuma despesa decorrente das atividades relacionadas à pesquisa desenvolvida.

Entendemos que, em sendo observados os critérios acima, a pesquisa proposta pode ser autorizada e o que o Termo de Anuência possa ser assinado.

Adicionalmente, considerando a importância da temática para a gestão acadêmica do IFPE, sugerimos que seja exigido do solicitante uma cópia da Dissertação de Mestrado, em versão final, assim como, de qualquer eventual publicação do trabalho desenvolvido, para ser(em) anexado(s) ao presente processo, para arquivamento na PROPESQ, com vistas aos trabalhos de autoanálise institucional e planejamentos futuros de melhorias dos processos e regulamentos.



Prof. Dr. Mário Antônio Alves Monteiro
Pró-Reitor de Pesquisa, Pós-graduação e Inovação do IFPE
(Portaria Nº 569/2016-GR, DOU de 3/5/2016, Seção 2, pág. 29)

ANEXO B – TERMO DA ANUÊNCIA DA PESQUISA



MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE PERNAMBUCO
REITORIA
PRÓ-REITORIA DE PESQUISA, PÓS-GRADUAÇÃO E INOVAÇÃO
 Avenida Professor Luiz Freire, n 500 – Cidade Universitária – Recife – CEP: 50.540-740
 (081) 2125-1691- propesq@reitoria.ifpe.edu.br

TERMO DE ANUÊNCIA PARA A REALIZAÇÃO DE PESQUISAS DESCRITIVAS EXTERNAS NAS DEPENDÊNCIAS DO IFPE

(Aprovado pela Resolução CONSUP IFPE Nº 29, de 18, de setembro de 2017)

DADOS DO (A) PESQUISADOR(A)

Nome: Anderson França Ferreira
 Cargo/Instituição: Técnico de Tecnologia da Informação/IFPE
 Telefone(s) com DDD: (81) 99182-9604
 E-mail: anderson.ferreira@reitoria.ifpe.edu.br

DADOS DO PROJETO DE PESQUISA

Programa de Pós-Graduação: Mestrado Profissional em Ciência da Computação
 Curso/Instituição: Gestão da Tecnologia da Informação 2018/UFPE
 Título da Pesquisa: Otimizar a Tomada de Decisão da Alta Gestão quando da Perda de Eficiência Energética no Data Center do IFPE através do Diagrama Bow Tie
 Orientador(a): Prof^o. Dr.^a Patrícia Cabral de Azevedo Restelli Tedesco

O Instituto Federal de Educação, Ciência e Tecnologia de Pernambuco autoriza a realização, em suas dependências, de entrevistas e/ou levantamento de dados e informações inerentes à execução do projeto de pesquisa acima especificado, desde que sejam atendidas as seguintes considerações:

- 1) A pesquisa deve atender às determinações éticas das Resoluções nº 196/96 e nº 466/2012 do CNS/MS, nos casos de pesquisas envolvendo seres humanos, com o compromisso no resguardo da segurança e bem-estar dos sujeitos de pesquisa nela recrutados;
- 2) O(a) responsável pela pesquisa obriga-se a prestar todos os esclarecimentos necessários, quando solicitado por qualquer instância do IFPE;
- 3) O IFPE não arcará com nenhuma despesa decorrente das atividades relacionadas à pesquisa desenvolvida;
- 4) Atendimento aos marcos regulatórios do IFPE.

Recife, 14 de setembro de 2020

Documento assinado digitalmente

 Jose Carlos de Sa Junior
 Data: 10/10/2020 17:05:17-0300
 CPF: 755.456.244-49

Assinatura e carimbo do(a) Reitor(a)

Observação: Para a realização da pesquisa é imprescindível a apresentação do TERMO DE ANUÊNCIA. O TERMO deve estar assinado e carimbado pelo(a) Reitor(a) do IFPE.