UNIVERSIDADE FEDERAL DO TOCANTINS
CAMPUS UNIVERSITÁRIO DE PALMAS
PROGRAMA DE PÓS-GRADUAÇÃO EM MODELAGEM COMPUTACIONAL DE SISTEMAS

DANILLO LUSTOSA WANDERLEY

UM *FRAMEWORK* PARA O GERENCIAMENTO DE RISCOS EM SEGURANÇA DA INFORMAÇÃO NO PODER JUDICIÁRIO DO TOCANTINS

Palmas - TO
2020

DANILLO LUSTOSA WANDERLEY

UM *FRAMEWORK* PARA O GERENCIAMENTO DE RISCOS EM SEGURANÇA DA INFORMAÇÃO NO PODER JUDICIÁRIO DO TOCANTINS

Dissertação apresentada ao Programa de Pós-Graduação em Modelagem Computacional de Sistemas. Foi avaliada para obtenção do título de Mestre em Modelagem Computacional de Sistemas e aprovada em sua forma final pelo orientador e pela Banca Examinadora.

Orientador: Prof. Dr. Gentil Veloso Barbosa

Palmas – TO
2020

FOLHA DE APROVAÇÃO

DANILLO LUSTOSA WANDERLEY

UM *FRAMEWORK* PARA O GERENCIAMENTO DE RISCOS EM SEGURANÇA DA INFORMAÇÃO NO PODER JUDICIÁRIO DO TOCANTINS

Dissertação apresentada ao Programa de Pós-Graduação em Modelagem Computacional de Sistemas. Foi avaliada para obtenção do título de Mestre em Modelagem Computacional de Sistemas e aprovada em sua forma final pelo orientador e pela Banca Examinadora.

Data de aprovação: _____ / _____ / ___

Banca Examinadora

_____

Prof. Dr. Gentil Veloso Barbosa, UFT

_____

Prof. Dr. George Lauro Ribeiro de Brito, UFT

_____

Prof. Dr. Gerson Pesente Focking, IFTO

Palmas – TO
2020

Dedico este trabalho primeiramente a Deus,
que não me deixou fraquejar.
À minha esposa, Tatiana Porto, pelas
orientações e pelo incentivo.
Aos meus filhos, João Pedro e Gabriel, que
também estão trilhando seus caminhos em
busca do conhecimento.
Aos meus pais, Nonato e Jucileide, que sempre
me apoiaram.

AGRADECIMENTOS

Primeiramente ao Prof. Dr. Gentil Veloso Barbosa pela paciência, disponibilidade e orientação.

Ao Tribunal de Justiça do Estado do Tocantins e à Escola Superior da Magistratura Tocantinense - ESMAT pelo apoio institucional e financeiro para realização deste trabalho.

À equipe da Divisão de Administração e Segurança de Redes, João Carlos Batello, Tiago Luz, Ricardo Marx e Marcelo Leal, que me apoiou no desenvolvimento dessa pesquisa e pela troca de experiências na área de segurança da informação.

RESUMO

No cenário atual, em que o Poder Judiciário do Estado do Tocantins depende cada vez mais da informação e de seus sistemas de informática, é imprescindível identificar as ameaças que podem prejudicar o alcance dos objetivos institucionais, bem como avaliar o impacto, a relevância e as consequências que a não conformidade da infraestrutura tecnológica com as normas de segurança podem causar na atividade-fim do Judiciário Tocantinense. Este trabalho teve como objetivo desenvolver um *framework* para o gerenciamento de riscos em segurança da informação, visando aperfeiçoar a governança de tecnologia da informação e comunicação no Poder Judiciário do Tocantins. Para o alcance dos objetivos desta pesquisa foram analisadas as principais normas da Associação Brasileira de Normas Técnicas voltadas a segurança da informação e gestão de riscos. Como ferramentas que compõe o *framework*, foram elaborados artefatos que permitiram identificar, analisar, avaliar e tratar eventos de riscos. Com o intuito de validar o *framework*, efetuou-se uma aplicação prática por meio de um estudo de caso tendo como foco a área de administração e segurança de redes do Tribunal de Justiça. Quanto ao método de gestão de riscos desenvolvido, pode-se afirmar que ele se mostrou eficiente, pois foi possível mapear os principais eventos de riscos, com suas causas e consequências, e assim elaborar um conjunto de medidas mitigatórias.

Palavras-chave: Gestão de riscos. Segurança da informação. *Framework***.**

ABSTRACT

In the current scenario, in which the Judiciary of the State of Tocantins is increasingly dependent on information and its computer systems, it is essential to identify the threats that may harm the achievement of institutional objectives, as well as to assess the impact, relevance and consequences that the non-conformity of the technological infrastructure with the security norms can cause in the main activity of the Tocantinense Judiciary. This work aimed to develop a framework for risk management in information security, aiming to improve the governance of information and communication technology in the Judiciary of Tocantins. To achieve the objectives of this research, the main standards of the Brazilian Association of Technical Standards were analyzed, focused on information security and risk management. As tools that make up the framework, artifacts were created that allowed to identify, analyze, evaluate and treat risk events. In order to validate the framework, a practical application was made through a case study focusing on the area of administration and network security of the Court of Justice. As for the risk management method developed, it can be said that it proved to be efficient, since it was possible to map the main risk events, with their causes and consequences, and thus elaborate a set of mitigation measures.

Keywords: Risk management. Information security. Framework.

LISTA DE ILUSTRAÇÃO

LISTA DE TABELAS

LISTA DE SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
CNJ	Conselho Nacional de Justiça
DTINF	Diretoria de Tecnologia da Informação
ENTIC-JUD	Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário
GPWEB	Sistema de gestão estratégica e gerenciamento de projetos
NBR	Norma Brasileira
PETIC	Plano Estratégico de Tecnologia da Informação e Comunicação
PJTO	Poder Judiciário do Estado do Tocantins
PSI	Política de Segurança da Informação
SEI	Sistema Eletrônico de Informações
TIC	Tecnologia da Informação e Comunicação
TJTO	Tribunal de Justiça do Estado do Tocantins

SUMÁRIO

1 INTRODUÇÃO

Segundo Tauchert; Amaral (2015), o contexto econômico e social da atualidade caracteriza-se pela sua dinâmica e competitividade trazidas com a globalização que, por sua vez, fez com que o mercado se tornasse bastante exigente, influenciando os diversos ramos do conhecimento a buscar inovações. No Judiciário, isso não é diferente, uma vez que ele busca novas tecnologias, como inteligência artificial e a videoconferência, que ajudem na superação de conflitos para tornar a Justiça mais ágil, eficiente e próxima da sociedade.

As inovações tecnológicas apresentam soluções práticas e inteligentes que contribuem para elevar o padrão da qualidade dos serviços prestados pelo Judiciário, um exemplo disso é o Sistema de Processo Judicial Eletrônico (e-Proc).

Com a agilidade e praticidade que as inovações tecnológicas trazem, vem o reconhecimento e a valorização do Judiciário em geral, sendo importante observar que por trás de toda essa informatização de processos existem pessoas que precisam ter conhecimento necessário para lidar com todas essas inovações. Conhecimentos que vão desde noções básicas de informática até noções de segurança da informação.

A informatização e todas as inovações trazidas por ela geram um aumento considerável de investimento em Tecnologia da Informação e Comunicação (TIC) para atender as demandas crescentes do Poder Judiciário do Estado do Tocantins. Cada vez mais, as tecnologias estão em ascensão no cotidiano dos profissionais ligados ao Judiciário, isso permite que eles possam ter acesso às informações de um processo em qualquer lugar, sem a necessidade de ir ao Fórum por exemplo.

Para suportar a demanda crescente dos serviços prestados à sociedade, o Judiciário Tocantinense precisa prover uma infraestrutura de TIC que conte com serviços de telecomunicação, redes físicas e lógicas, equipamentos e sistemas confiáveis e resilientes a falhas.

Essa realidade exige cada vez mais do Judiciário Tocantinense a capacidade de lidar com as incertezas e os riscos inerentes à segurança no âmbito da tecnologia da informação e comunicação. Preservar a confidencialidade, a integridade, a disponibilidade e a autenticidade dos dados é fator primordial para qualquer organização, seja ela pública ou privada. Por isso, gerenciar riscos é de suma importância para proteger a informação.

Segundo Bezerra (2013), risco é a combinação da probabilidade de um evento indesejado ocorrer e de suas consequências para a organização. Ou seja, é a incerteza no alcance dos objetivos. Ainda segundo o autor, em segurança da informação, a incerteza reside nos aspectos

tecnológicos, nos processos executados e, principalmente, nas pessoas que interagem com a tecnologia e se envolvem com os processos.

Em tecnologia da informação, toda atividade realizada envolve riscos. Conforme NBR ISO/IEC 27005, risco em segurança da informação está associado ao potencial de que ameaças possam explorar vulnerabilidades de um ativo ou de um conjunto de ativos de informação e, consequentemente, causar dano a uma organização. Sendo assim, as organizações devem gerenciar os riscos à segurança da informação de modo a mantê-los em níveis aceitáveis e, com isso, concretizar os seus objetivos (ABNT, 2011).

1.1 Problema

Gerenciar um ambiente de TIC e mantê-lo seguro não é tarefa simples. Mesmo com o avanço das ferramentas voltadas para a segurança da informação, as redes corporativas e seus ativos estão sujeitos a ataques diversos, o que pode comprometer computadores, servidores e programas, causando interrupções em serviços essenciais.

No cenário atual, em que o Poder Judiciário do Estado do Tocantins depende cada vez mais da informação e de seus sistemas de informática, é imprescindível identificar as ameaças e os riscos que podem prejudicar o alcance dos objetivos institucionais, bem como avaliar o impacto, a relevância e as consequências que a não conformidade da infraestrutura de TIC com as normas de segurança podem causar na atividade-fim do Judiciário Tocantinense.

Desse modo, tem-se a pergunta norteadora do presente trabalho de pesquisa: como implementar um plano de gerenciamento de riscos em segurança da informação que promova a proteção de informações críticas, minimize falhas no ambiente de tecnologia da informação e contribua para que o Judiciário Tocantinense atinja seus objetivos institucionais?

Para tratar tal questão, este trabalho analisou as principais normas e manuais de boas práticas voltadas à segurança da informação e elaborou um *framework* para o gerenciamento de riscos em TIC aplicável ao Poder Judiciário do Tocantins no ano de 2019.

Acredita-se que o controle e o monitoramento são práticas que necessitam ser estimuladas dentro do Poder Judiciário do Estado do Tocantins para a melhoria contínua do objetivo de negócio, ou seja, a implementação de boas práticas de governança de TIC define uma política organizacional que ajuda na parametrização da segurança da informação.

1.2 Justificativa

Conforme as Diretrizes para a Gestão de Segurança da Informação no âmbito do Poder Judiciário, a adoção de procedimentos que garantam a segurança da informação deve ser

prioridade constante neste Poder, de forma a reduzir falhas e danos que possam comprometer a imagem da Justiça ou trazer prejuízos à sociedade (CNJ, 2012).

Essas diretrizes estabelecem que o modelo de gestão deve contemplar, dentre os vários processos normativos, a gestão de riscos com o objetivo de minimizar o impacto de eventos potencialmente negativos aos ativos e serviços prestados pelo Judiciário, provocando, assim, melhoria contínua na prestação jurisdicional.

Com o intuito de melhorar a infraestrutura e a governança de TIC para que o Poder Judiciário tenha condições de cumprir sua função institucional, o Conselho Nacional de Justiça (CNJ) estabeleceu pela Resolução nº 211, de 2015, a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD) para o período de 2015-2020.

Em suma, a ENTIC-JUD é um instrumento de planejamento para governança de tecnologia da informação e comunicação, pois consiste no estabelecimento de um conjunto de mecanismos com o objetivo de assegurar que o uso de TIC agregue valor à atividade precípua do órgão, com riscos e custos aceitáveis.

Dentre os mecanismos que a ENTIC-JUD estabelece, em seu art. 9º, ela diz que cada órgão deverá elaborar e aplicar política, gestão e processo de segurança da informação a serem desenvolvidos em todos os níveis da instituição, por meio de um Comitê Gestor e em harmonia com as diretrizes nacionais preconizadas pelo Conselho Nacional de Justiça. Dessarte, o Tribunal de Justiça do Estado do Tocantins (TJTO), por meio da Portaria nº 3.433, de 2017, instituiu a Política de Segurança da Informação (PSI) no âmbito do Poder Judiciário Tocantinense.

A Política de Segurança da Informação, dentre as suas finalidades, visa à proteção da informação, e em seu Capítulo VIII-A trata da gestão de riscos de segurança da informação.

> Art. 21-A. O Tribunal deve adotar um conjunto de processos que permitam identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação e equilibrá-los com os custos operacionais e financeiros envolvidos.

Para atender ao que está estabelecido no art. 21-A da Política de Segurança da Informação, torna-se necessário implementar mecanismos para gerenciar os riscos à segurança da informação no Poder Judiciário do Estado do Tocantins.

Além de satisfazer ao que determina a norma, acredita-se que a adoção de uma Política de Gestão de Riscos pode promover a proteção de informações críticas, minimizar falhas no ambiente de TIC e contribuir para que o Judiciário Tocantinense atinja seus objetivos institucionais.

1.3 Objetivo Geral

Desenvolver um *framework* para o gerenciamento de riscos em segurança da informação, visando aperfeiçoar a governança de TIC no Poder Judiciário do Tocantins.

1.3.1 Objetivos Específicos

1. Definir os processos para gerenciar riscos em conformidade com as principais normas e códigos de boas práticas voltadas para o gerenciamento e tratamento de riscos em segurança da informação;
2. Elaborar os artefatos para compor o *framework* de gerenciamento de riscos em segurança da informação;
3. Validar o *framework* de gerenciamento de riscos, considerando a área de infraestrutura de TIC do Poder Judiciário do Estado do Tocantins.

1.4 Metodologia

Foi realizado um estudo com abordagem qualitativa a fim de analisar as principais normas voltadas para o tema de gestão de riscos de segurança da informação e após definidos os processos e elaborados os artefatos para compor o *framework* de gerenciamento de riscos de TIC do Judiciário Tocantinense.

Segundo Gil (2017), esse tipo de pesquisa caracteriza-se pela não utilização de instrumental estatístico na análise dos dados e tem por base conhecimentos teórico-empíricos que permitem atribuir-lhe cientificidade.

Em função do objetivo e das características do projeto, a pesquisa foi de natureza aplicada, pois objetivou gerar conhecimentos para aplicação prática e dirigida à solução de um problema específico de interesse do Poder Judiciário do Tocantins.

Quanto ao objetivo, a pesquisa foi do tipo exploratória. Segundo Gerhardt; Silveira (2009), a pesquisa exploratória envolve levantamento bibliográfico, entrevistas com pessoas que tiveram experiências práticas com o problema pesquisado, entre outros.

Para o desenvolvimento da pesquisa, foi considerada a área de infraestrutura de tecnologia da informação do Tribunal de Justiça do Estado do Tocantins. Para isso, foi construído um mapa de riscos com os serviços mais críticos, utilizando o *framework* desenvolvido para o gerenciamento de riscos em segurança da informação.

Considerando que o ambiente estudado não possui um plano de monitoramento de riscos para sua infraestrutura de TIC, foram abordados pontos relacionados aos princípios de segurança da informação, tornando claros os itens de maior importância a serem gerenciados.

1.4.1 Procedimentos

Para a realização da pesquisa, foram utilizados os métodos de pesquisa bibliográfica, pesquisa documental e estudo de caso, conforme descrito a seguir.

Pesquisa Bibliográfica

Inicialmente, realizou-se um levantamento bibliográfico, visando apresentar um embasamento teórico sobre os temas e conceitos que foram pesquisados e analisados. Os materiais literários foram coletados em periódicos na internet e em bases de pesquisa científica como IEEE, *Google* Acadêmico e foram utilizados os seguintes descritores para a pesquisa: gestão de riscos, segurança da informação, *framework*.

Segundo Gerhardt; Silveira (2009), a pesquisa bibliográfica é feita a partir do levantamento de referências teóricas já analisadas e publicadas por meios escritos e eletrônicos, como livros, artigos científicos e páginas de *web sites*. Qualquer trabalho científico inicia-se com uma pesquisa bibliográfica, que permite ao pesquisador conhecer o que já se estudou sobre o assunto.

Pesquisa Documental

Segundo Gil (2017), a pesquisa documental é semelhante ao estudo bibliográfico e utiliza fontes documentais, isto é, fontes de dados secundários. Ainda segundo o autor, os dados documentais podem ser encontrados junto à empresa como os relatórios e manuais da organização, notas fiscais, relatórios de estoques, de usuários, relatório de entrada e saída de recursos financeiros, entre outros, e externos, como as publicações e resultados de pesquisas já desenvolvidas.

As fontes de pesquisa documental utilizadas no estudo foram os documentos oficiais do Poder Judiciário do Tocantins, como portarias e resoluções que tratam da segurança da informação e da governança de TIC. Além desses documentos, foram utilizadas as principais normas da ABNT[1] voltadas a segurança da informação e gestão de riscos, como: NBR ISO/IEC 27001, NBR ISO/IEC 27002, NBR ISO/IEC 27005, NBR ISO 31000, NBR ISO/IEC 31010 e ISO GUIA 73.

[1] Fundada em 1940, a Associação Brasileira de Normas Técnicas é órgão responsável pela normalização técnica no país. É uma entidade privada e sem fins lucrativos.

Estudo de Caso

Caracteriza-se por ser um estudo exaustivo de um ou poucos objetos de pesquisa, de maneira a permitir o aprofundamento do seu conhecimento. Os estudos de caso têm grande profundidade e pequena amplitude, pois procuram conhecer a realidade de um indivíduo, de um grupo de pessoas, de uma ou mais organizações em profundidade (GIL, 2017).

O estudo de caso foi realizado no Tribunal de Justiça do Estado do Tocantins com abordagem qualiquantitativa do tipo exploratória e descritiva. Esse visou detalhar o cenário atual da infraestrutura e dos principais serviços de Tecnologia da Informação, utilizando o *framework* desenvolvido para o gerenciamento de riscos em segurança da informação.

Levantamento de Dados

O levantamento de dados foi realizado na área de infraestrutura de tecnologia da informação do Tribunal de Justiça do Estado do Tocantins com foco nos objetivos específicos do presente estudo. Sendo esses:

i. Definir os processos para gerenciar riscos em conformidade com as principais normas e códigos de boas práticas voltadas para o gerenciamento e tratamento de riscos em segurança da informação

Este objetivo específico é uma etapa fundamental do trabalho, pois foi por meio dele que se obteve o embasamento teórico que permitiu o alcance dos outros objetivos. Foi exposta uma caracterização descritiva das principais normas de gestão de riscos e uma análise comparativa entre elas a fim de demonstrar a visão geral de cada uma sobre o tema da pesquisa.

Além disso, com esse objetivo específico busca-se descrever o processo necessário para o gerenciamento de riscos em segurança da informação e as atividades necessárias para a execução da gestão.

Cada etapa do processo foi detalhada a fim de permitir a criação de uma metodologia de gestão de riscos de TIC a ser aplicada no Judiciário do Tocantins. Essa metodologia está alinhada ao modelo PDCA de modo a fomentar a sua melhoria contínua e se divide em cinco subprocessos principais interdependentes: estabelecimento do contexto, identificação, análise, avaliação e tratamento de riscos; e duas etapas de suporte: comunicação e consulta e monitoramento e análise crítica.

ii. Elaborar os artefatos para compor o *framework* de gerenciamento de riscos em segurança da informação

Segundo a NBR ISO/IEC 27002, a segurança da informação é obtida através da implementação de controles, processos, políticas e procedimentos, que juntos fortalecem os objetivos de negócio com a minimização dos seus riscos e a promoção da segurança da organização. Garantir a proteção da informação é um princípio base para que qualquer organização forneça um serviço de credibilidade, organizado e controlado (ABNT, 2013b).

Assim, após a definição dos processos e a criação da metodologia para gerenciar riscos de TIC, surgiu um conjunto de conceitos pré-definidos utilizados na resolução do problema proposto no projeto de pesquisa. Esse conjunto de conceitos, técnicas e ferramentas constitui o *framework* para o gerenciamento de riscos em segurança da informação.

O *framework* é baseado nos conceitos preconizados pelas principais normas voltadas para o gerenciamento de riscos em segurança da informação. A intensão é que seja um instrumento de simples compreensão e de fácil utilização, partindo do pressuposto que a usabilidade é um fator decisivo para minimizar a complexidade do processo de gestão de riscos.

Ele visa auxiliar na definição de ações a serem adotadas com objetivo de possibilitar a redução de danos às informações e que contribuam para a tarefa de melhor gerenciar os riscos em TIC.

iii. Validar o *framework* de gerenciamento de riscos considerando a área de infraestrutura de TIC do Poder Judiciário do Estado do Tocantins

O *framework* elaborado foi utilizado para um estudo de caso, onde foi possível verificar sua aplicabilidade em uma situação real. Este objetivo específico é uma etapa fundamental do trabalho, pois é por meio dele que se conseguirá produzir uma lista abrangente de riscos, incluindo fontes e eventos que possam ter algum impacto na consecução dos objetivos da Instituição.

Foram realizadas reuniões com integrantes da área de Tecnologia da Informação do Poder Judiciário do Tocantins para o levantamento preliminar das ameaças às quais a infraestrutura tecnológica está sujeita e para composição do plano de gerenciamento de riscos aplicado à segurança da informação.

1.5 Organização do Trabalho

Este trabalho teve como propósito desenvolver um método para o gerenciamento de riscos em segurança da informação, visando aperfeiçoar a governança de TIC no Poder Judiciário do Tocantins e está estruturado em 6 (seis) capítulos.

O Capítulo 1 descreve o percurso metodológico que foi usado, por esta pesquisa, para atingir os objetivos propostos. Dessa forma, são apresentados: introdução, problema, justificativa, objetivo geral e específico e a metodologia.

O Capítulo 2 tem como objetivo apresentar a temática segurança da informação nas organizações. São abordadas as principais normas de gestão de segurança da informação e de riscos, além de questões relacionadas à governança de TIC.

Já o Capítulo 3 apresenta a estrutura desenvolvida para a gestão de riscos, que envolve a definição de uma política interna e a atribuição de responsabilidades. Traz ainda o desenho do fluxo do processo com o mapeamento de todas as etapas e atividades que compõe a gestão de riscos.

No Capítulo 4 é apresentado o manual desenvolvido para o gerenciamento de riscos em segurança da informação e seus artefatos.

O Capítulo 5 traz o estudo de caso que tem como objetivo validar o *framework* proposto, onde é detalhado o cenário atual da infraestrutura e os principais serviços de Tecnologia da Informação.

No Capítulo 6, são apresentadas as conclusões e recomendações do estudo, indicando quais os possíveis caminhos a serem seguidos a partir deste trabalho.

2 REVISÃO DE LITERATURA

Segundo Sêmola (2014), todas as empresas, independente do seu segmento de mercado, área de negócio e porte, usufruem da informação objetivando melhor produtividade, redução de custos, competitividade e apoio mais eficiente aos processos de tomada de decisão.

Ainda segundo o autor, atualmente um grande volume de informações são geradas, armazenadas, manipuladas e compartilhadas o tempo todo. Para isso, cada vez mais as empresas têm usado recursos de computação em nuvem e processado suas informações em algum lugar que não sabem bem onde é.

Diante desse cenário, é possível perceber o alto grau de dependência das organizações em relação à informação – digitalizada, compartilhada e distribuída - e aos elementos da infraestrutura que a mantém. A informação é vital para a organização e está distribuída por todos os processos de negócio, alimentando-os e circulando por diversos ativos[2], ambientes e tecnologias, cumprindo o importante papel de fornecer instrumentos para a gestão do negócio (SÊMOLA, 2014).

A informação não se encontra confinada a ambientes físicos ou a processos isolados, ela circula por toda a empresa e fora dela também, sendo alvo das mais variadas ameaças[3] e vulnerabilidades[4] que transcendem os aspectos tecnológicos. É fator crítico de sucesso para a gestão da segurança da informação que se identifique os elementos internos e externos geradores de riscos e, com isso, aplicar o tratamento adequado.

2.1 Segurança da Informação

A segurança da informação é uma área do conhecimento dedicada a proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade. Pode ser considerada como a prática de gestão de riscos, incidentes que impliquem o comprometimento dos principais conceitos de segurança: confidencialidade, integridade e disponibilidade da informação (SÊMOLA, 2014).

Como descrito em NBR ISO/IEC 27002, a informação é um ativo relevante para as organizações e necessita ser protegida adequadamente. Proteger a informação das mais variadas

[2] Elemento de valor para um indivíduo ou organização e que, por esse motivo, necessita de proteção adequada. Ou seja, é tudo aquilo que tenha valor para a organização, incluindo equipamentos, aplicações, informações, processos etc.
[3] É todo e qualquer evento que possa explorar vulnerabilidades.
[4] É qualquer fraqueza que possa ser explorada para comprometer a segurança de sistemas ou informações. Fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

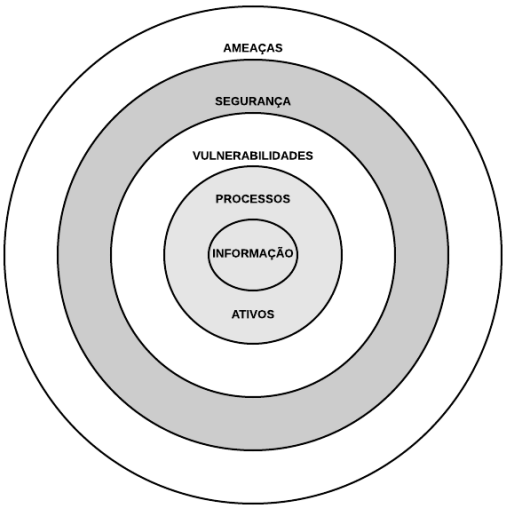
fontes de ameaças é imprescindível para garantir a continuidade, minimizar os danos e maximizar os investimentos e oportunidades do negócio (ABNT, 2013b).

A segurança da informação é obtida pela utilização de controles como políticas, práticas, procedimentos, estruturas organizacionais e infraestrutura de hardware e software. Nesse sentido, ainda segundo NBR ISO/IEC 27002, para que uma organização identifique os requisitos necessários para manter segura a informação, é importante criar processos para identificar ameaças aos ativos, as vulnerabilidades com suas respectivas probabilidades de ocorrências e os impactos ao negócio (ABNT, 2013b). Ou seja, avaliar riscos e gerenciá-los de forma a possibilitar a segurança efetiva dos ativos e sistemas de TIC.

Uma vez que os requisitos de segurança e os riscos tenham sido identificados e as decisões para o tratamento desses tenham sido tomadas, convém que controles apropriados sejam selecionados e implementados para assegurar que os riscos sejam reduzidos a um nível aceitável. Os controles devem ser baseados tanto em requisitos legais como nas melhores práticas de segurança da informação comumente usadas (ABNT, 2013b).

Em segurança da informação, risco é considerado como um evento de impacto negativo motivado pela exploração de uma vulnerabilidade. O processo de identificar, avaliar e administrar eventos que emanam da incapacidade de determinar com precisão a probabilidade de sua ocorrência e os impactos a ele associados é chamado de gestão de riscos (BRASIL, 2016).

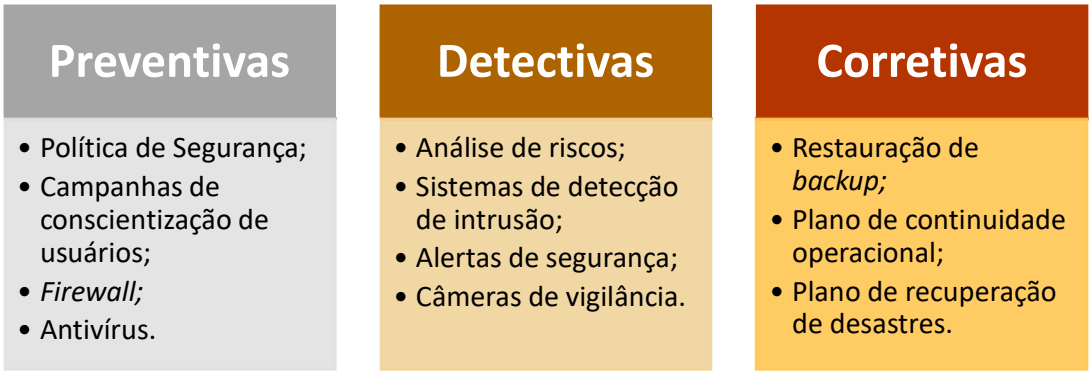
Figura 1 - Perímetros. A informação como alvo (SÊMOLA, 2014, adaptado).



Quando se fala de risco, nem sempre tentar evitá-lo ou reduzi-lo a um nível aceitável é a melhor estratégia a ser adotada. Há casos em que o custo para implementar medidas para evitar ou reduzir o risco é maior do que o valor da informação a ser protegida. Nesse caso, a possibilidade de a organização reter o risco, compartilhá-lo ou terceirizá-lo deve ser avaliada (SÊMOLA, 2014).

De acordo com Sêmola (2014), as medidas de segurança são também referenciadas como controles e podem ser classificadas como: preventivas, detectivas e corretivas.

Figura 2 - Medidas de Segurança. Elaborado pelo autor (2019).



Além das medidas citadas anteriormente, é importante que as organizações adotem diretrizes de governança e conformidade, visando assegurar que as políticas e controles adequados estejam no lugar certo, para diminuir ameaças e potencializar oportunidades.

Assim, ações de GRC – acrônico dos conceitos de governança, risco e conformidade – são importantes para melhorar a gestão da informação, dar maior segurança e eficiência aos processos, passar confiança e estabilidade nas ações estratégicas e garantir o atendimento às normas corporativas e a conformidade com a legislação proporcionando mais credibilidade e respeito à organização (ASSI, 2017).

Segundo Sêmola (2014), o GRC está intimamente ligado à segurança da informação pelos aspectos de controle e garantia de que a organização não seja afetada negativamente por gestão inadequada.

2.2 Governança de TIC

A Governança busca o compartilhamento de decisões dentre os diversos setores de uma organização, com o intuito de uma gestão mais ampla para sustentação e para garantia dos serviços de TIC prestados (OLIVEIRA JÚNIOR, 2015).

Diferentemente da gestão da segurança da informação que visa a melhoria contínua da segurança da informação e representa as várias atividades diárias que são necessárias para um programa de segurança eficaz e ativo; governança de TIC é um sistema pelo qual o uso atual e futuro da tecnologia da informação são dirigidos e controlados. Significa avaliar e direcionar o uso da TIC para dar suporte à organização e monitorar seu uso para realizar planos. Inclui a estratégia e as políticas de uso da tecnologia da informação dentro da organização (ABNT, 2018b).

Figura 3 - Relação entre governança e gestão (BRASIL, 2014)

Segundo Fernandes; Abreu (2014), o principal objetivo da governança de tecnologia da informação é alinhar a TIC aos requisitos do negócio, assim como garantir a continuidade dos serviços e a minimização da exposição do negócio aos riscos de TIC. Além desses objetivos, outros são citados por eles, como: melhoria dos processos, gestão de riscos e *compliance,* alinhamento da arquitetura e das iniciativas de TIC às necessidades do negócio e definição de regras e responsabilidades sobre decisões e ações relativas à TIC no âmbito da organização.

De acordo com Oliveira Júnior (2015), a governança de TIC é, basicamente, uma extensão da governança corporativa. Esta tem foco no direcionamento e monitoramento da gestão da instituição, enquanto aquela foca no direcionamento e monitoramento das práticas de gestão e uso da TIC de uma organização, tendo como guia a alta administração da empresa.

Um exemplo prático de ação da governança de TIC é o estabelecimento de um processo transparente de tomada de decisão sobre a priorização de grandes demandas de tecnologia da informação. Essa é uma medida necessária para garantir que as ações de TIC estejam alinhadas com os objetivos institucionais e para garantir que as demandas que tenham maior impacto nesses objetivos tenham atendimento prioritário (FERNANDES; ABREU, 2014).

Ainda segundo Fernandes; Abreu (2014), a governança de TIC estabelece claramente o processo de tomada de decisões e as diretrizes para o gerenciamento e uso da tecnologia da informação. Isso ocorre de forma alinhada com a visão, missão e metas estratégicas da organização. Para cumprir com esse propósito, a governança de TIC age em cinco frentes distintas:

- **Alinhamento Estratégico:** garante que tanto os processos de negócio como os de tecnologia da informação trabalhem conjuntamente;
- **Entrega de Valor:** benefício importante, pois assegura que o setor de tecnologia da informação seja o mais eficiente e eficaz possível;
- **Gerenciamento de Riscos:** permite que a organização visualize eventuais riscos para o negócio e dá meios de minimizá-los;
- **Gerenciamento de Recursos:** garante que a gestão dos recursos humanos e tecnológicos da organização seja o mais otimizada possível;
- **Mensuração de Desempenho:** utilizando-se de indicadores que vão além dos critérios financeiros, a governança de TIC assegura uma medição e avaliação precisa dos resultados do negócio.

2.2.1 Frameworks de Governança de TIC

Um *framework* de governança de TIC é um modelo de boas práticas que recomenda como devem ser gerenciados os projetos, processos e demais demandas de TIC. São utilizados para guiar o trabalho da TI, estabelecendo padrões e nortes para que a tecnologia da informação seja uma área cada vez mais estratégica dentro da empresa.

Esse modelo de boas práticas pode conter guias, ferramentas, sistemas, técnicas e qualquer outro componente que possa gerenciar a qualidade na prestação de serviço e entrega de produto de tecnologia.

Para auxiliar na implantação da governança de TIC, existem vários *frameworks* de boas práticas de gestão disponíveis para as organizações. Entre os principais, destacam-se:

COBIT (*Control Objectives for Information and related Technology*)

É um *framework* concebido pela ISACA[5] (*Information System Audit and Control*) para ajudar as organizações a desenvolver, organizar e implementar estratégias em torno do gerenciamento de informações e governança.

[5] https://www.isaca.org

Segundo Dourado (2015), o COBIT auxilia as organizações na criação de valor para área de TIC, mantendo o equilíbrio entre a realização de benefícios e a otimização dos níveis de risco e o uso de recursos. Tem como objetivos:

- oferecer um *framework* abrangente que auxilia as organizações a otimizar o valor gerado pela TIC;
- permitir que a TIC seja governada e gerenciada de forma holística para toda a organização;
- criar uma linguagem comum entre TIC e negócios para a governança e gestão de tecnologia da informação corporativa.

O COBIT surgiu, em 1996, como um *framework* para auditoria e controles de TIC. Em 1998, a ISACA lançou a versão 2, que expandiu a metodologia para que pudesse ser aplicada fora da comunidade de auditoria. Mais tarde, nos anos 2000, foi desenvolvida a versão 3, que incluiu as técnicas de gerenciamento de TIC e de controle de informações encontradas no *framework* atual (DOURADO, 2015).

Ainda segundo Dourado (2015), em 2005 o COBIT 4.0 se tornou o *framework* de governança de TIC, com a inclusão de processos de governança e conformidade (compliance). Em 2012, o COBIT 5 foi lançado e, em 2013, a ISACA lançou um complemento a ele, que incluía mais informações para as organizações sobre gerenciamento de riscos e governança de informações.

Em 2018, foi anunciada uma atualização do COBIT, descartando o número da versão, a nomeando de COBIT 2019. Segundo a ISACA, essa versão foi projetada para evoluir constantemente com “atualizações mais frequentes e fluidas”. O objetivo é criar estratégias de governança mais flexíveis, colaborativas e voltadas para tecnologias recentes.

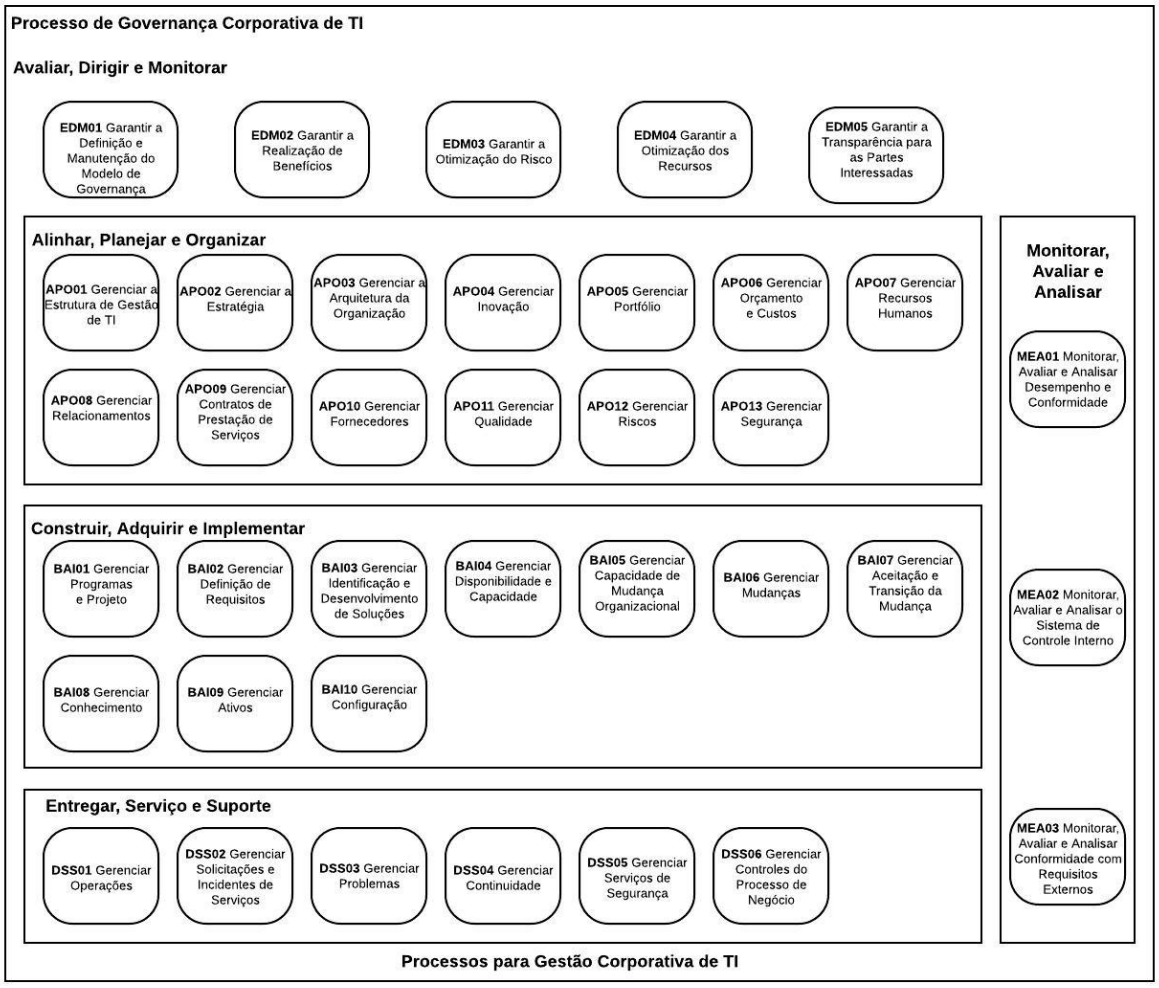
Em se tratando do COBIT 5, pode-se afirmar que ele é focado em governança corporativa de TIC, deixando claro a distinção entre governança e gestão (DOURADO, 2015). A distinção entre esses dois conceitos pode ser percebida no Modelo de Referência de Processos, que subdivide os 37 processos de TIC em duas principais áreas de atividade – governança e gestão – que são divididas em domínios de processos, conforme pode ser visto na Tabela 1.

Tabela 1 - Processos e domínios de governança e gestão (DOURADO, 2015).

Área	Processos	Domínios
Governança	5	Avaliar, Dirigir e Monitorar (*Evaluate, Direct and Monitor - EDM*)
Gestão	32	Alinhar, Planejar e Organizar (*Align, Plan and Organise - APO*)
		Construir, Adquirir e Implementar (*Build, Acquire and Implement - BAI*)
		Entregar, Serviço e Suporte (*Deliver, Service and Support - DSS*)
		Monitorar, Avaliar e Analisar (*Monitor, Evaluate and Assess - MEA*)

Para este trabalho será considerada a visão do processo APO12 – Gerenciar Riscos. A seguir é apresentado na Figura 4 o contexto desse processo.

Figura 4 - Modelo de referência de processos do COBIT 5 (www.isaca.org/cobit, 2019, adaptado).



O processo APO12 faz parte da área de gestão e tem por objetivo identificar, avaliar e reduzir riscos relacionados à TIC de forma contínua, dentro dos níveis de tolerância estabelecidos pela organização. A seguir, será detalhado o que sugere cada subprocesso, segundo COBIT 5.

Tabela 2 - Processo APO12 – Gerenciar Riscos.

Subprocesso	Atividades
APO12.01 – Coletar dados Identificar e coletar dados relevantes para habilitar a efetiva identificação do risco relacionado a TIC, análise e reporte.	Entre as atividades desse subprocesso destaca-se a de estabelecer e manter um método para a coleta, classificação e análise dos dados relacionados ao risco de TIC, acomodando múltiplos tipos de eventos, múltiplas categorias de risco de TIC e fatores de risco. Outra atividade importante é a de registrar dados relevantes sobre o ambiente operacional interno e externo da organização, que possa exercer um papel significativo no gerenciamento do risco.
APO12.02 – Analisar Risco Desenvolver informações úteis para suportar as decisões de risco que levam em conta a relevância dos fatores de risco para o negócio.	Definir o escopo da análise de risco, considerando todos os fatores de risco e a criticidade para o negócio dos ativos. Construir e atualizar regularmente cenários de riscos de TIC, incluindo cenários compostos de tipos de ameaças de modo a desenvolver controles específicos e outras medidas de respostas são atividades importantes a serem desenvolvidas nesse subprocesso.
APO12.03 – Manter o perfil do risco Manter um inventário de risco conhecido e atributos de risco (incluindo frequência esperada, impacto potencial e respostas) e dos recursos relacionados, capacidades e atividades de controle atuais.	Como atividade, devem-se inventariar processos de negócio, incluindo pessoal de suporte, aplicações, infraestrutura, instalações, registros manuais críticos, fornecedores e provedores externos, e documentar a dependência dos processos de gerenciamento de serviços e recurso de infraestrutura de TIC. Além disso, é importante determinar e acordar quais serviços e recursos de infraestrutura de TIC são essenciais para manter a operação dos processos de negócio, analisando dependências e identificando pontos fracos.
APO12.04 – Articular o risco Fornecer informação apropriada para o estado atual de exposições relacionadas a TIC e oportunidades em tempo hábil para todas as partes interessadas.	Deve-se reportar os resultados da análise de risco a todas as partes interessadas afetadas, formatando-os de forma útil para suportar as decisões da organização. Onde for possível, incluir probabilidades e escalas de prejuízo ou ganho ao longo dos níveis de confiança que habilitam a gestão, para balancear o risco sobre o retorno. Cabe ainda fornecer aos tomadores de decisão o perfil de risco atual, incluindo a efetividade do processo de gerenciamento de risco, dos controles, o status de remediação e seus impactos no perfil de risco.
APO12.05 – Definir um portfólio de ações de gerenciamento de risco Gerenciar oportunidades para reduzir o risco em um nível aceitável.	Manter um inventário de atividades de controle que estão estabelecidas para gerenciar o risco, determinando quando cada entidade organizacional monitora o risco e o aceita por estar dentro do seu nível de tolerância.
APO12.06 – Responder ao risco Responder em tempo hábil com medidas efetivas para limitar a magnitude dos prejuízos relacionados a eventos de TIC.	Preparar, manter e testar planos que documentem passos específicos a serem tomados quando um evento de risco puder causar um incidente operacional significativo, com sérios impactos ao negócio. Categorizar incidentes e comparar a exposição atual com os limites de tolerância de risco. Comunicar os impactos de negócio para tomada de decisão como parte de um perfil de risco atualizado e reportado. Aplicar o plano de resposta apropriado para minimizar o impacto quando incidentes ocorrerem.

Fonte: COBIT 5 - Habilitando Processos

ITIL *(Information Technology Infrastructure Library)*

Segundo Cestari Filho (2011), ITIL é uma biblioteca que reúne as melhores práticas para gestão de serviços de tecnologia da informação. É constituído por um conjunto de livros onde estão documentados o que as empresas ao redor do mundo conhecem de melhor sobre a gestão de TIC, após décadas de acúmulo de aprendizado.

A sigla ITIL significa *Information Technology Infrastructure Library*, isso é: Biblioteca de Infraestrutura de Tecnologia da Informação. Entretanto, não é sobre infraestrutura que a ITIL aborda e sim a gestão da tecnologia. É estruturada por processos, funções e outras habilidades requeridas para entregar serviços de TIC e pode ser utilizada por empresas de quaisquer segmentos de negócio.

A ITIL foi criada pelo governo do Reino Unido na década de 1980 e hoje os direitos sob a marca ITIL pertencem a Axelos. Acumula desde então boas práticas para a tecnologia da informação como um todo: como criar a estratégia, planejar, desenvolver novos serviços, oferecer suporte e melhorá-los continuamente (CESTARI FILHO, 2011).

Para a ITIL, gerenciamento de serviço[6] é um conjunto de habilidades especializadas para prover valor aos clientes na forma de serviços. Estas habilidades são essenciais para coordenar de maneira eficiente e eficaz os recursos de forma a atender as necessidades de negócio. Recursos e habilidades são considerados os ativos de serviços.

Conforme Cestari Filho (2011), a estrutura da ITIL é baseada em um ciclo de vida de serviço e é composta por cinco etapas:

a) Estratégia de Serviço (*Service Strategy*)

Provê direcionamento de como projetar, desenvolver e implementar o gerenciamento de serviço, não apenas como uma capacidade organizacional, mas também como um ativo estratégico. Diz respeito a garantir que as organizações estão em posição de lidar com os custos e riscos associados aos seus portfólios de serviços. Os seguintes processos fazem parte da estratégia de serviços:

- Gerenciamento estratégico para serviços de TIC;
- Gerenciamento do portfólio de serviços de TIC;
- Gerenciamento financeiro para Serviços de TIC;
- Gerenciamento da Demanda;

[6] Serviço é um meio de entregar valor para os clientes facilitando os resultados que eles desejam atingir sem que possuam certos custos e riscos específicos.

- Gerenciamento do Relacionamento com o Negócio.

b) Projeto de Serviço (*Service Design*)

Esta é a fase em que o serviço de TIC é desenhado para que cumpra seu objetivo durante todo o ciclo de vida. Tem como principal objetivo garantir uma abordagem holística em todos os aspectos do desenho de serviço: funcional; gerencial e operacional. Os seguintes processos fazem parte do projeto de serviço:

- Gerenciamento de nível de serviços;
- Gerenciamento de catálogo de serviços;
- Gerenciamento de disponibilidade dos serviços de TIC;
- Gerenciamento de capacidade dos serviços de TIC;
- Gerenciamento de fornecedores;
- Gerenciamento de segurança da tecnologia da informação;
- Gerenciamento de continuidade dos serviços de TIC;
- Coordenação do desenho de serviços de TIC.

c) Transição de Serviço (*Service Transition*)

O valor do serviço de TIC é concebido na etapa Estratégia e será percebido e avaliado pelo usuário e cliente na etapa Operação de Serviços, quando os efeitos no negócio finalmente acontecerão de fato. A transição visa garantir que grandes volumes de mudanças possam ser tratados com menor impacto, minimizando os riscos envolvidos com implantação de novos serviços e serviços modificados. Os seguintes processos fazem parte da transição de serviço:

- Gerenciamento de mudanças;
- Gerenciamento de ativos e configuração;
- Gerenciamento de liberação;
- Validação e teste de serviço;
- Avaliação da mudança;
- Gerenciamento do conhecimento;
- Planejamento e suporte à transição.

d) Operação de Serviço (*Service Operation*)

A operação de serviço coordena e desempenha as atividades e os processos requeridos para entregar e gerenciar serviços em níveis acordados para usuários de negócio e clientes. Ou seja, assegura que os serviços estão sendo atendidos baseado no SLA (*Service Level Agreement).* A principal responsabilidade da operação é garantir a estabilidade dos serviços de

TIC para que agreguem valor ao negócio. Os seguintes processos fazem parte da operação de serviço:

- Gerenciamento de incidentes;
- Gerenciamento de problemas;
- Gerenciamento de eventos;
- Cumprimento de requisição;
- Gerenciamento de acesso.

As seguintes funções são desempenhadas no contexto da operação de serviço:

- Central de serviços de TIC (*servicedesk*);
- Gerenciamento técnico;
- Gerenciamento de operações de TIC;
- Gerenciamento de aplicações.

e) Melhoria Contínua de Serviço (*Continual Service Improvement*)

Manter a constante melhoria dos serviços baseando-se no ciclo PDCA (*Plan – Do – Check – Act*). É uma etapa que documenta as melhores práticas requeridas para melhorar a eficácia e a eficiência dos processos e serviços, bem como sua relação custo-benefício.

O processo que faz parte da melhoria contínua é a medição do serviço e o escopo dessa etapa envolve três áreas principais que precisam ser endereçadas:

- A saúde geral do gerenciamento de serviços;
- O alinhamento contínuo do portfólio de serviços com as necessidades atuais e futuras do negócio;
- A maturidade dos processos de sustentação dos serviços.

A Figura 5 apresenta as etapas que compõem um ciclo de vida dos serviços de TIC na estrutura ITIL.

2.3 Normas de Gestão de Segurança e de Riscos

A área de segurança da informação possui um conjunto de normas para serem utilizadas, de modo a permitir a padronização dos requisitos e procedimentos para a implementação de um sistema de gestão de segurança da informação (BEZERRA, 2013). Segundo o autor, essas normas destacam a necessidade de as organizações possuírem uma gestão de riscos estruturada, com processos e requisitos padronizados.

A Tabela 3 apresenta um resumo comparativo entre as normas da ABNT que serão utilizadas como referência no desenvolvimento desse trabalho.

Figura 5 - Relações entre as partes no ciclo de vida de serviço (CESTARI FILHO, 2011, adaptado).

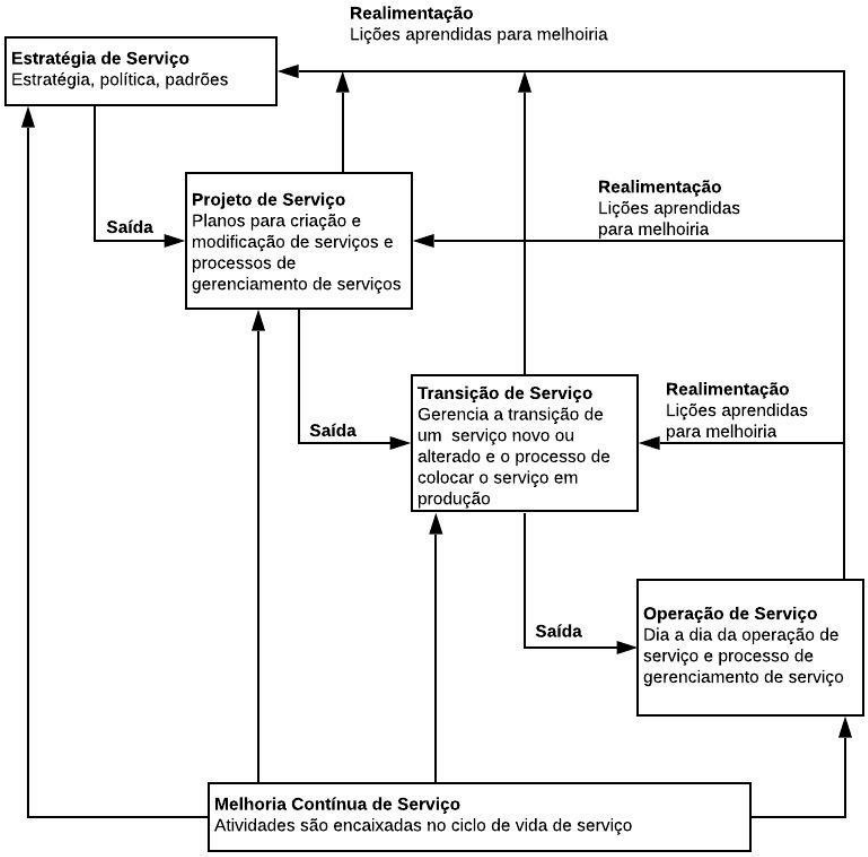


Tabela 3 - Resumo comparativo (BEZERRA, 2013, adaptado).

Norma	Título	Objetivo	Observação
27001	Tecnologia da Informação – Técnicas de segurança – Sistemas de gestão de segurança da informação - Requisitos	Especifica os requisitos para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um SGSI documentado no contexto dos riscos de negócio globais da organização. Especifica requisitos para a implementação de controles de segurança personalizados para as necessidades individuais de organizações ou de suas partes. Cobre todos os tipos de organização.	Trata mais especificamente de diretrizes e princípios para um sistema de gestão de segurança da informação.
27002	Tecnologia da Informação – Técnicas de segurança – Código de prática para a gestão de segurança da informação	Estabelece diretrizes e princípios para iniciar, implementar, manter e melhorar a gestão de segurança da informação. Os objetivos definidos nesta norma proveem diretrizes gerais para as metas e melhores práticas para a gestão da segurança da informação.	Voltada para controles de segurança.
27005	Tecnologia da Informação – Técnicas de segurança – Gestão de riscos de segurança da informação	Apresenta a descrição do processo de gestão de riscos de segurança da informação e das suas atividades.	Esclarece como gerenciar riscos de segurança da informação.

31000	Gestão de riscos – Princípios e diretrizes	Fornece diretrizes para gerenciar riscos enfrentados pelas organizações. A sua aplicação pode ser personalizada para qualquer organização e seu contexto.	Pode ser aplicada a qualquer atividade, incluindo a tomada de decisão em todos os níveis.
31010	Gestão de riscos – Técnicas para o processo de avaliação de riscos	Descreve as diversas técnicas e ferramentas de análise de riscos.	Deve ser trabalhada em apoio à norma 31000.
GUIA 73	Gestão de riscos - Vocabulário	Apresenta as definições de termos genéricos relativos à gestão de riscos.	Destina-se à utilização de terminologia uniforme de gestão de riscos em processos e estruturas para gerenciar riscos.

2.4 Gestão de Riscos de Tecnologia da Informação

Segundo NBR ISO/IEC 27005, a gestão de risco de segurança da informação deve ser um processo contínuo, com contexto interno e externo definido e que avalie e trate os riscos usando um plano de tratamento a fim de implementar as recomendações e decisões. Convém que por meio desse processo sejam analisados os possíveis acontecimentos e suas consequências, antes de decidir o que será feito e quando, a fim de reduzir os riscos a um nível aceitável (ABNT, 2011).

Conforme Bezerra (2013), são princípios da gestão de riscos:

- Criar e proteger valor, pois contribui para melhoria do desempenho referente à segurança, à conformidade legal e regulatória, ao gerenciamento de projetos, à eficiência nas operações, à governança e à reputação;
- Integrar todos os processos organizacionais, incluindo o planejamento estratégico e todos os processos de gestão de projetos e gestão de mudanças;
- Auxiliar na tomada de decisões;
- Tratar as incertezas que residem nos aspectos tecnológicos envolvidos, nos processos executados e, principalmente, nas pessoas que em algum momento interagem com a tecnologia e se envolvem com os processos;
- Considerar fatores humanos e culturais;
- Ser transparente e inclusiva de modo a manter o envolvimento das partes interessadas;
- Ser dinâmica, iterativa e capaz de reagir a mudanças à medida que novos riscos surjam, alguns se modificam e outros desaparecem.

Como descrito na norma 27005, o processo de gestão de riscos envolve a definição do contexto, a identificação, a análise e a avaliação, o tratamento aplicado aos riscos avaliados, a aceitação dos riscos, o monitoramento e análise crítica, e a comunicação sobre riscos com as partes interessadas (ABNT, 2011). A metodologia proposta para este trabalho abrange as etapas citadas e segue a lógica do ciclo PDCA.

O ciclo PDCA é um método gerencial e sistemático de tomada de decisões, sendo utilizado para o controle de processos e solução de problemas. Possui uma vasta área de aplicação, podendo ser útil a diferentes tipos de empreendimentos, pois atua em diversas frentes focando na melhoria contínua.

Pode-se resumir da seguinte forma as principais atividades de gestão de riscos de segurança da informação:

Tabela 4 - Atividades da gestão de riscos sob o enfoque do ciclo PDCA (ABNT, 2011, adaptado).

Ações	Processo de gestão de riscos de segurança da informação
Planejar	Definição do contexto Processo de avaliação de riscos Definição do plano de tratamento do risco Aceitação do risco
Executar	Implementação do plano de tratamento do risco
Verificar	Monitoramento contínuo e análise crítica de riscos
Agir	Manter e melhorar o processo de Gestão de Riscos de Segurança da Informação

Como pode ser observado na Figura 6, o ciclo de vida da gestão de riscos de segurança da informação é iterativo, onde a gestão se desenvolve de maneira incremental, através de sucessão de iterações, e cada iteração libera uma entrega (saída) para a seguinte, minimizando tempo e esforço despendidos na identificação de controles e assegurando que riscos de alto impacto ou de alta probabilidade possam ser adequadamente avaliados (BEZERRA, 2013).

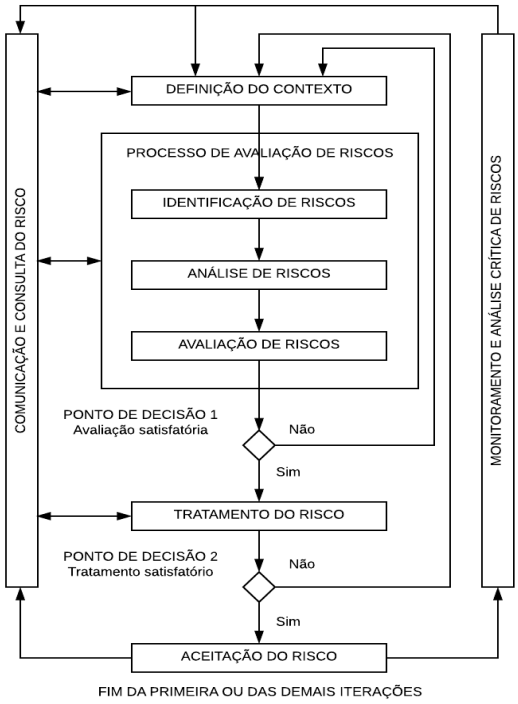
A definição do contexto é a atividade chave da gestão de riscos e essa atividade busca os objetivos da organização, o ambiente, partes interessadas, e demais critérios de risco, os quais revelarão e avaliarão a natureza e a complexidade dos riscos.

Após estabelecido o contexto, a próxima etapa é de análise e avaliação, que permitirá a identificação dos riscos e a determinação das ações necessárias para reduzi-los a um nível aceitável. A partir dos resultados obtidos na análise e avaliação, são definidos os controles necessários para o tratamento dos riscos (ABNT, 2011).

É possível que o tratamento não resulte em um nível de risco residual que seja aceitável. Nesse caso, pode ser necessária outra iteração do processo de avaliação com mudanças nas variáveis do contexto seguida de uma fase adicional de tratamento do risco. A atividade de

aceitação tem de assegurar que os riscos residuais sejam aceitos pelos gestores da organização. Isso é importante em uma situação em que a implementação de controles é adiada, por exemplo, devido aos custos (ABNT, 2011).

Figura 6 - Processo de gestão de riscos de segurança da informação (ABNT, 2011).



É importante que os riscos e a forma como são tratados sejam comunicados para todas as áreas operacionais e seus gestores. Além disso, para melhoria contínua do processo de gestão de riscos, atividades de acompanhamento dos resultados, implementação dos controles e de análise crítica são essenciais (ABNT, 2011).

Como preparação para o desenvolvimento do *framework* proposto nesta pesquisa, foi elaborado um estudo preliminar sobre o mapeamento de riscos de Tecnologia da Informação no Judiciário Tocantinense, fundamentado nas normas NBR ISO/IEC 27005 e NBR ISO 31000, com o intuito de realizar uma análise das ameaças às quais o ambiente de infraestrutura de TIC está sujeito, avaliando os impactos e as consequências que elas podem gerar (WANDERLEY et al., 2019).

Na elaboração do estudo em questão, foi possível observar que o ambiente pesquisado não possuía uma forma sistematizada de lidar com os riscos; e os controles ora implementados não eram processos formalizados, eram apenas de conhecimento de uma equipe específica. A

prática comum, quando se recebia um alerta sobre um evento de risco, era avaliar setorialmente e subjetivamente possíveis consequências, eventualmente implementar controles mitigatórios essenciais e aguardar a evolução da situação.

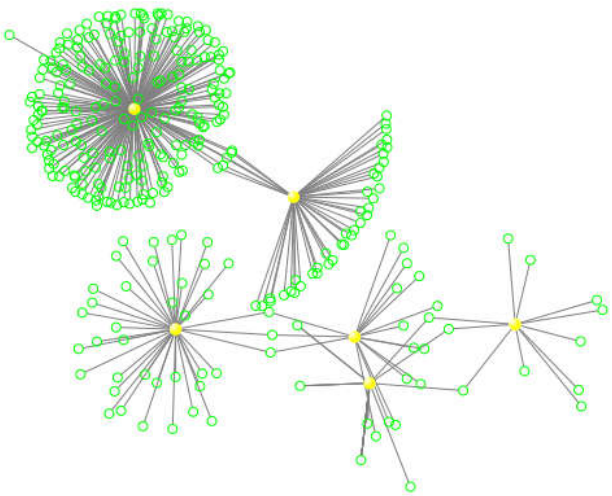
Como resultado do estudo apresentado, foi construído um mapa de respostas aos riscos identificados e foram definidos controles com vista a tratá-los e assim garantir a segurança da informação.

Uma ameaça frequente à segurança da rede do Poder Judiciário do Tocantins são os "vírus" computacionais. Em vista disso, realizou-se um trabalho sobre a epidemia de vírus computacionais no Poder Judiciário do Tocantins onde foi apresentada uma discussão sobre o assunto, apontando as ocorrências, os possíveis danos e as formas de contágio das estações de trabalho (WANDERLEY et al., 2018).

Para isso, foi utilizado o Modelo epidemiológico SIR (Kermack e McKendrick, 1927), no qual cada indivíduo, considerado saudável, no estudo representado por um computador, pode ser suscetível à infecção (S), infectado (I) e assim transmitir a doença a indivíduos saudáveis e removidos (R), que não têm a doença nem podem transmiti-la, pois adquiriram imunidade.

Foram utilizadas duas ferramentas: a solução corporativa de antivírus e o NodeXL, que é uma ferramenta de análise de redes sociais, para expressar graficamente a infecção causada pelos *malwares*. A Figura 7 apresenta uma rede de infecções, onde as estações de trabalho são representadas pelos círculos verdes e os *malwares* pelas esferas amarelas.

Figura 7 - Rede de infecções.



Esse trabalho possibilitou observar que os ataques na maioria das vezes ocorreram por conta de comportamentos inadequados dos próprios usuários, por causa do acesso indevido à Internet e do uso incorreto de dispositivos USB (*Universal Serial Bus*).

Diante desse cenário, onde várias ameaças põem em risco a segurança da informação, torna-se necessário elaborar uma estrutura para a gestão de riscos de TIC no Poder Judiciário do Tocantins, de modo a sistematizar todo o processo. Esse assunto será abordado detalhadamente a partir do capítulo 3.

3 SISTEMA DE GESTÃO DE RISCOS DE TIC DO PJTO

Visando a melhoria da infraestrutura e governança de tecnologia da informação e comunicação, foi instituído no Poder Judiciário do Estado do Tocantins, o Plano Estratégico de Tecnologia da Informação e Comunicação (PETIC) para o período de 2016-2020. O PETIC apresenta nove objetivos estratégicos, são eles:

- Aperfeiçoar as competências gerenciais e técnicas de pessoal;
- Prover infraestrutura de TIC apropriada às atividades judiciais e administrativas;
- Aprimorar a gestão orçamentária e financeira;
- Aperfeiçoar a governança e a gestão;
- Aprimorar as contratações;
- Promover a adoção de padrões tecnológicos;
- Aprimorar e fortalecer a integração e a interoperabilidade de sistemas de informação;
- Aprimorar a segurança da informação;
- Primar pela satisfação dos usuários.

Dentre os objetivos estabelecidos no PETIC, o de aprimorar a segurança da informação trata da implantação do processo de gestão de riscos em todas as divisões da Diretoria de TIC.

Como a informação é um ativo essencial para os negócios de uma organização, ela necessita ser adequadamente protegida. Atualmente, com o aumento da utilização dos sistemas informatizados o número de ameaças e vulnerabilidades tende a ser cada vez maior. Portanto, é essencial que uma organização identifique os seus requisitos de segurança da informação.

Através da análise e avaliação de riscos, é realizada uma estimativa da probabilidade de ocorrência das ameaças e do impacto potencial ao negócio levando-se em conta os objetivos da organização, desta forma antecipando-se a eventuais problemas que possam causar prejuízos à instituição.

Como resultados, espera-se criar uma cultura organizacional de gestão de risco e minimizar perdas e danos à imagem do Tribunal de Justiça do Tocantins, assim como, também atender os requisitos da Resolução 211/2015 do Conselho Nacional de Justiça.

Seguindo as orientações contidas nas normas NBR ISO/IEC 27005 e NBR ISO 31000, o gerenciamento de riscos deve ser precedido da definição de uma estrutura de suporte à gestão de riscos, que envolve basicamente: definição de política interna, atribuição de responsabilidades, desenho do processo de gestão de riscos, alocação de recursos necessários

(pessoas, processos, tecnologia da informação) e estabelecimento de meios de comunicação com partes envolvidas e interessadas e divulgação do conhecimento gerado.

3.1 Política de Gestão de Riscos

Aprovada por meio da Portaria nº 1660 de 12 de agosto de 2019, a Norma-TIC-07 é um ato normativo que atualiza a Política de Segurança da Informação (PSI) instituída pela Portaria nº 3433 de 26 de junho de 2017, e tem por objetivo estabelecer princípios, diretrizes e responsabilidades a serem observadas no processo de gestão de riscos, de forma a possibilitar a identificação, avaliação, tratamento, monitoramento e comunicação de riscos na área de tecnologia da informação e comunicação, incorporando a visão de riscos à tomada de decisão e contribuindo para o aprimoramento da governança de TIC.

A Norma-TIC-07 está estruturada em: definição do objetivo, finalidade, sistematização do processo, partes envolvidas e atribuição de responsabilidades dos componentes do processo de gestão de riscos. O Anexo I apresenta a norma de gestão de risco do Poder Judiciário do Tocantins.

Os integrantes da gestão de riscos e suas responsabilidades estão descritas na Norma-TIC-07. São eles:

- **Diretoria de Tecnologia da Informação (DTINF)**: responsável pelo plano de gestão de riscos de TIC;
- **Comitê Gestor de TIC:** comitê interno da DTINF, responsável pelo estabelecimento da estratégia e da estrutura de gerenciamento de riscos;
- **Gestores de Risco:** responsável pela gestão do processo e acompanhamento da execução das atividades relacionadas à gestão dos riscos de TIC. São gestores de riscos todos os chefes de divisão da DTINF e aqueles servidores delegados por eles;
- **Comitê de Gestão de Riscos do Poder Judiciário do Tocantins (PJTO):** responsável pela avaliação das proposições e documentos produzidos no processo de gestão de risco, subsidiando a tomada de decisão pela Administração.

3.2 Desenho do processo de gestão de riscos

O mapeamento do processo é um recurso indispensável para estabelecer de forma organizada e eficiente as atividades que compõe a gestão de riscos de TIC. O Anexo 2 apresenta

o fluxo do processo, onde foi utilizada a ferramenta de modelagem de processos *Bizagi Process Modeler*[7].

3.2.1 Descrição das Atividades

De acordo com a Figura 8, serão descritas as atividades que compõe o processo de gestão de riscos no PJTO, elencando os atores e suas responsabilidades, as entradas, saídas, e ferramentas utilizadas em cada etapa.

Etapas do processo de gestão de riscos

a) Propor plano de gestão de riscos: compreende a proposição de um plano para identificar, avaliar e tratar riscos relacionados à Tecnologia da Informação e Comunicação que podem impactar na atividade-fim do PJTO.

Responsável: DTINF.

Entradas: Plano Estratégico de TIC (PETIC), Plano Diretor de TIC (PDTI), Processos de Negócio, entre outros.

Saídas: solicitação para os gestores de riscos elaborarem plano de gestão de riscos para determinado processo de negócio ou ativo de informação.

Atividades:

- Formalizar proposta: deverá ser aberto um processo administrativo para solicitação do plano.
- Encaminhar proposta ao gestor de risco: DTINF encaminha solicitação ao gestor.

Ferramentas: Sistema Eletrônico de Informações (SEI).

b) Definir o contexto: compreende a proposição dos objetivos, escopo e limites da avaliação de riscos a ser realizada, com a identificação das partes interessadas.

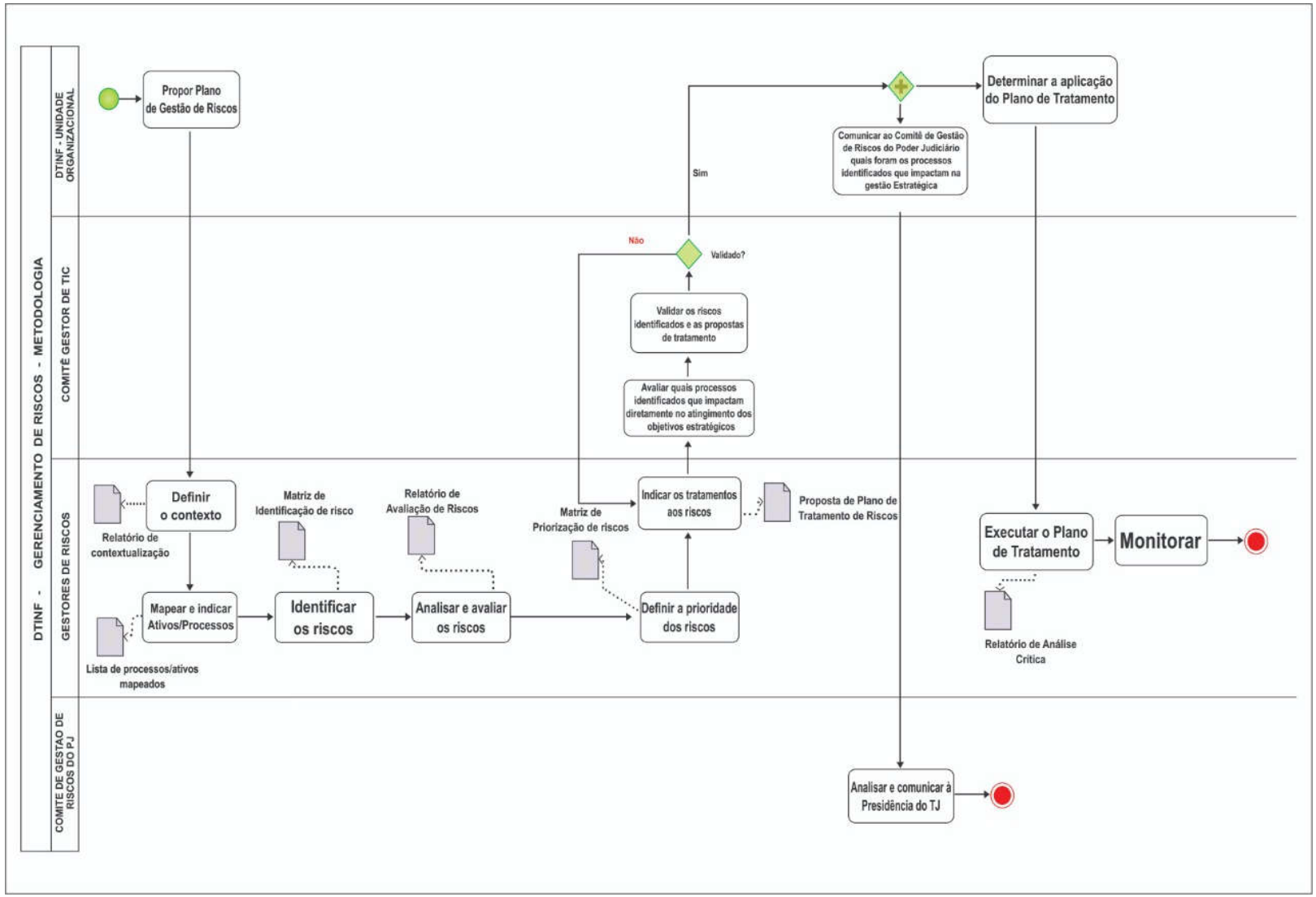
Responsável: gestores de riscos.

Entradas: solicitação para elaboração do plano de gestão de riscos.

Saídas: definição do contexto.

[7] https://www.bizagi.com

Figura 8 - Fluxo do processo de gestão de riscos do PJTO.



Atividades:

- Identificar o propósito da avaliação de riscos.
- Definir o escopo da avaliação de riscos (processos, sistemas, ativos, ambientes).
- Identificar as partes interessadas e envolvidas no processo.
- Elaborar relatório de contextualização.

Ferramentas: SEI e GPWeb (Sistema de gestão estratégica e gerenciamento de projetos).

c) Mapear e indicar ativos/processos: atividade que consiste em elencar os processos/ativos que compõem o escopo, suas características, relacionamentos com sistemas, processos de negócio, responsáveis, tecnologias envolvidas etc.

Responsável: gestores de riscos.

Entradas: escopo da avaliação de riscos, lista de ativos/processos com responsáveis, serviços, sistemas.

Saídas: uma lista de ativos com riscos a serem gerenciados e uma lista dos processos de negócio relacionados aos ativos.

Atividades:

- Identificar os ativos: identificar quais ativos fazem parte do escopo, quem é o responsável, sua localização e função.
- Relacionar ativos com os processos de negócio: relacionar ativos com sistemas e serviços tecnológicos.
- Elaborar relatório: o levantamento de ativos/processos constará no relatório de contextualização.

Ferramentas: SEI e GPWeb.

d) Identificar os riscos: atividade que consiste na identificação de ameaças, vulnerabilidades e dos controles de segurança da informação já implementados, relacionados aos ativos mapeados.

Responsável: gestores de riscos.

Entradas: mapeamento dos ativos.

Saídas: lista de cenários de incidentes com suas consequências associadas aos ativos e processos de negócio.

Atividades:

- Coletar informações: pode ser executada por meio de reuniões (ou outras técnicas recomendadas pela norma NBR ISO/IEC 31010) entre as equipes envolvidas e o objetivo é listar eventos que possam ter algum impacto na consecução dos objetivos identificados na etapa de estabelecimento do contexto.
- Identificar os riscos: produzir uma lista abrangente de riscos, contendo causas e consequências.
- Elaborar matriz de identificação de riscos.

Ferramentas: SEI e GPWeb.

e) Analisar e avaliar os riscos: para essa atividade são informados os valores da probabilidade, severidade e relevância dos ativos, a fim de determinar o nível de risco inerente. Com isso, classificar cada risco analisado.

Responsável: gestores de riscos.

Entradas: identificação de riscos; avaliação da probabilidade, severidade e relevância; escala de níveis de risco.

Saídas: determinação do nível de risco inerente, classificação dos riscos, matriz de análise e avaliação de riscos.

Atividades:

- Definir valores para probabilidade, severidade e relevância: conforme critérios pré-estabelecidos para classificação da probabilidade, severidade e relevância.
- Calcular nível de risco inerente: o nível de risco resulta da multiplicação dos três fatores (Probabilidade, Severidade e Relevância).
- Classificar os riscos: classificação de acordo com a escala de níveis de risco.
- Elaborar relatório: relatório de avaliação de riscos.

Ferramentas: SEI e GPWeb.

f) Definir a prioridade dos riscos: atividade que consiste em apresentar uma lista dos riscos que requerem tratamento, com suas respectivas classificações e prioridades.

Responsável: gestores de riscos.

Entrada: análise dos riscos.

Saídas: lista de riscos priorizada, de acordo com os critérios de avaliação de riscos.

Atividades:

- Avaliar riscos: avaliar os riscos a partir da classificação resultante da análise de riscos e das características dos processos de negócio e ativos envolvidos, bem como escopo definido.
- Definir resposta ao risco: definir os critérios para a proposição de tratamento dos riscos, considerando as restrições organizacionais, estruturais e tecnológicas, os requisitos normativos e/ou legais, os controles de segurança da informação existentes e a análise custo/benefício.
- Elaborar matriz de priorização de riscos.

Ferramentas: SEI e GPWeb.

g) Indicar os tratamentos aos riscos: atividade que compreende a elaboração de plano visando à definição das formas de tratamento dos riscos e de implantação de controles, dos responsáveis por sua implementação e prazos estabelecidos.

Responsável: gestores de riscos.

Entradas: lista de riscos priorizada, de acordo com os critérios de avaliação de riscos.

Saídas: proposta do plano de tratamento de riscos.

Atividades:

- Elaborar plano de tratamento: para cada risco levantado deve ser identificada a estratégia de tratamento (mitigar, evitar, aceitar ou compartilhar); para cada tratamento, deve ser informada a forma de implementação, o responsável e o prazo de execução. No caso de aceitação, deve ser indicada a justificativa.
- Consolidar documentação: o relatório de avaliação de risco e a proposta de tratamento devem ser formalizados (SEI) para que sejam avaliados pela Diretoria de Tecnologia da Informação, que poderá solicitar ajustes ou validá-lo para posterior submissão à consideração superior.

Ferramentas: SEI e GPWeb.

h) Avaliar quais processos identificados que impactam diretamente no atingimento dos objetivos estratégicos: o Comitê de Gestor de TIC avalia a proposta de tratamento de riscos identificando os processos que impactam no atingimento dos objetivos estratégicos. Atividade que compreende a ciência sobre os resultados da análise e avaliação de riscos e a apreciação da proposta do Plano de Tratamento de Riscos.

Responsável: Comitê Gestor de TIC.

Entradas: riscos identificados e proposta de tratamento.

Saídas: manifestação do Comitê Gestor de TIC.

Atividades:

- Avaliar a proposta de tratamento de riscos e tecer observações para auxiliar e/ou subsidiar a DTINF na avaliação do documento.

Ferramentas: SEI e GPWeb.

i) Validar os riscos identificados e as propostas de tratamento: nesta etapa, o Comitê Gestor de TIC valida o plano de tratamento e pode tecer observações para auxiliar e/ou subsidiar a DTINF na avaliação do documento.

Responsável: Comitê Gestor de TIC.

Entradas: plano de tratamento de riscos.

Saídas: decisão aprovando a proposta de plano de tratamento ou determinando correções e ajustes.

Atividades:

- Avaliar a proposição encaminhada: analisar os resultados da análise e avaliação de riscos realizada e o Plano de Tratamento de Riscos proposto, em especial no que diz respeito aos critérios de aceitação de riscos.
- Aprovar a proposta: aprovado o plano de tratamento, encaminha-se para a DTINF determinar a aplicação do plano de tratamento e comunicar ao Comitê Gestor de Riscos do Poder Judiciário do Tocantins (PJTO) quais foram os processos identificados que impactam na gestão estratégica.
- Solicitar ajustes: não aprovado o documento, devolver ao gestor de risco para correções/ajustes.

Ferramentas: SEI e GPWeb.

j) Comunicar ao Comitê de Gestão de Riscos do PJTO sobre quais processos identificados que impactam na gestão estratégica: a DTINF comunica o Comitê de Gestão de Riscos do PJTO quais foram os processos identificados que impactam na gestão estratégica.

Responsável: DTINF.

Entradas: riscos identificados e proposta de tratamento.

Saídas: manifestação da Diretoria de Tecnologia da Informação.

Atividades:

- Comunicar ao Comitê de Gestão de Riscos do PJTO sobre quais processos identificados que impactam na gestão estratégica.

Ferramentas: SEI e GPWeb.

k) Analisar e comunicar à presidência do Tribunal de Justiça (TJ): o Comitê de Gestão de Riscos do PJTO analisa o documento contendo a manifestação do Comitê Gestor de TIC sobre quais processos impactam na gestão estratégica e comunica a Presidência do TJ.

Responsável: Comitê de Gestão de Riscos do PJTO.

Entradas: manifestação da Diretoria de Tecnologia da Informação.

Saídas: manifestação do Comitê de Gestão de Riscos do PJTO.

Atividades:

- Analisar a manifestação da DTINF podendo tecer observações para auxiliar e/ou subsidiar a Presidência na avaliação do documento.
- Manter a Presidência do TJ informada sobre os riscos que podem impactar a gestão estratégica.

Ferramentas: SEI e GPWeb.

l) Determinar a aplicação do plano de tratamento: atividade que autoriza a execução do plano de tratamento.

Responsável: DTINF.

Entradas: riscos identificados e proposta de tratamento.

Saídas: implementação do plano de tratamento.

Atividades:

- Determinar os gestores de riscos a aplicar o plano de tratamento.

Ferramentas: SEI e GPWeb.

m) Executar o plano de tratamento: nesta atividade, as áreas da DTINF implementam os controles para mitigar os riscos elencados, dentro de um prazo definido no plano de tratamento.

Responsável: gestores de riscos.

Entradas: plano de tratamento de riscos.

Saídas: controles implementados.

Atividades:

- Delegar as atividades de implementação dos controles: a implementação dos controles deverá ser delegada de acordo com as responsabilidades estabelecidas no plano de tratamento.
- Gerenciar implementação: cada área deverá planejar a execução das ações, a fim de executá-las no prazo e forma ajustados.
- Registrar a execução das ações: no relatório de monitoramento e análise crítica, deve ser registrada a execução das atividades, o que permitirá o acompanhamento da implementação do plano.

Ferramentas: SEI e GPWeb.

n) Monitorar: esta fase tem por objetivo monitorar a execução do Plano, com a finalidade de assegurar sua implementação dentro dos prazos definidos. Além disso, monitora também os riscos a fim de evitar que eles se concretizem.

Responsável: gestores de riscos.

Entradas: plano de tratamento de riscos e relatório de avaliação de riscos.

Saídas: implementação do plano e relatório de monitoramento e análise crítica.

Atividades:

- Monitorar o plano: o gestor de risco é o responsável por acompanhar o andamento das ações delegadas às equipes técnicas, a fim de aferir sua correspondência com a atividade definida no plano, bem como o cumprimento dos prazos ali estabelecidos.
- Comunicação dos riscos: informar às partes interessadas o nível de risco analisado e avaliado e possíveis alterações.
- Monitorar os riscos: analisar e monitorar os riscos já avaliados para verificar se alguma ocorrência pode ter modificado os níveis de risco, ensejando alguma ação para controlá-los.

Ferramentas: SEI e GPWeb.

3.3 Recursos

Como principal recurso no que tange à estruturação do processo de gestão de riscos de TIC, foi desenvolvido um Manual com o objetivo de padronizar a linguagem de gerenciamento de riscos na instituição e facilitar o levantamento e tratamento de eventos negativos que possam impactar na atividade precípua do Judiciário Tocantinense.

Com as informações contidas no Manual, espera-se que gestores de riscos possam identificar os eventos de risco, suas causas e consequências, avaliar criticamente esses eventos quanto à probabilidade de ocorrência e quanto ao impacto das consequências decorrentes desses, e traçar a estratégia de tratamento visando basicamente mitigar os riscos considerados mais altos e aceitar os mais baixos.

Os artefatos produzidos como resultado do processo de gestão de riscos são:

- **Relatório de Contextualização:** definição da abrangência da análise a ser realizada (quais ativos, serviços e processos serão analisados);
- **Matriz de identificação de riscos:** lista com os riscos identificados contendo causas e consequências;
- **Matriz de análise e avaliação de riscos:** documento que demonstra o nível de risco encontrado na análise e sua classificação;
- **Relatório de avaliação de riscos:** deve conter as informações da etapa de identificação, análise e avaliação dos riscos, levando em consideração os objetivos do levantamento e o resultado da identificação (quantidade de riscos, de causas e de consequências);
- **Matriz de priorização de riscos:** lista de riscos priorizada, de acordo com os critérios de avaliação de riscos;
- **Plano de tratamento de riscos:** definição de medidas para tratamento dos riscos identificados;
- **Relatório de monitoramento e análise crítica:** análise e definição de resposta ao risco;
- **Plano de Comunicação:** estabelece a forma como a equipe envolvida deve se comunicar com as partes interessadas.

O Manual juntamente com os artefatos produzidos constitui a metodologia a ser adotada no PJTO para gerenciar riscos em segurança da informação, ou seja, é um conjunto de conceitos, técnicas e ferramentas elaboradas com o objetivo de solucionar o problema proposto no projeto de pesquisa.

O PJTO não apresenta uma solução informatizada que reúna base de conhecimentos e controles abrangentes para gerenciar riscos em TIC. Como recurso de apoio serão utilizados dois sistemas: o SEI (sistema de processo administrativo) e o GPWeb (sistema de gestão estratégica e gerenciamento de projetos). O SEI será utilizado para registrar as ações realizadas

durante todo o processo e o GPWeb para acompanhar os projetos propostos pela DTINF, no que tange à avaliação e tratamento dos riscos identificados.

Por fim, o engajamento de pessoas na gestão de riscos depende em grande parte dos processos de comunicação que serão utilizados. Todas as etapas desde o levantamento, avaliação e tratamento de riscos devem incluir a constante comunicação com partes interessadas e partes envolvidas, com o objetivo principal de legitimar o conhecimento sobre riscos e dar transparência às ações desenvolvidas.

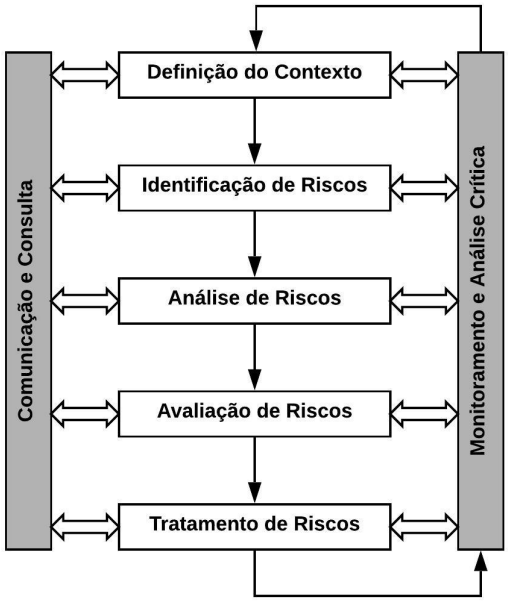
A seguir, será apresentado o Manual de Gestão de Riscos de TIC proposto para ser aplicado no Poder Judiciário do Estado Tocantins. Ele traz a metodologia e os artefatos a serem aplicados no processo.

4 MÉTODO DE GESTÃO DE RISCOS DE TIC DO PJTO

A metodologia proposta para a Gestão de Riscos utiliza como base as seguintes normas: ABNT NBR ISO/IEC 27001, ABNT NBR ISO/IEC 27005, ABNT NBR ISO 31000, ABNT NBR ISO/IEC 31010 e ABNT ISO GUIA 73.

Com base nas regras preconizadas pela norma ABNT NBR ISO/IEC 27005:2011 e nos princípios norteadores de sua gestão de riscos estabelecidos por meio da Portaria nº 1660/2019, está sendo proposto uma metodologia de gerenciamento de riscos de segurança da informação em um processo de melhoria contínua que se organiza em cinco subprocessos principais interdependentes: definição do contexto, identificação, análise, avaliação e tratamento de riscos; e duas etapas de suporte: comunicação e consulta e monitoramento e análise crítica.

Figura 9 - Processo de gestão de riscos em segurança da informação do PJTO (ABNT, 2011, adaptado).



Foram considerados três critérios para a escolha da metodologia:

1. Simplicidade no modelo de gestão;
2. Compatibilidade com a prática de Gestão de Segurança da Informação em uso no Poder Judiciário do Tocantins (PJTO);
3. Flexibilidade. As etapas do ciclo de Gestão de Riscos podem ser adaptadas a outras áreas do PJTO.

Os riscos inerentes às atividades de Tecnologia da Informação e Comunicação (TIC) podem ser identificados e avaliados partindo de estruturas como processos de negócio, ativos de informação, ambientes específicos e pessoas.

Nos processos de negócio, a identificação e avaliação de riscos podem partir da análise de um processo específico das áreas que compõem a Diretoria de Tecnologia da Informação, levando em consideração todos os procedimentos, atividades e tarefas que contribuem para a execução do processo.

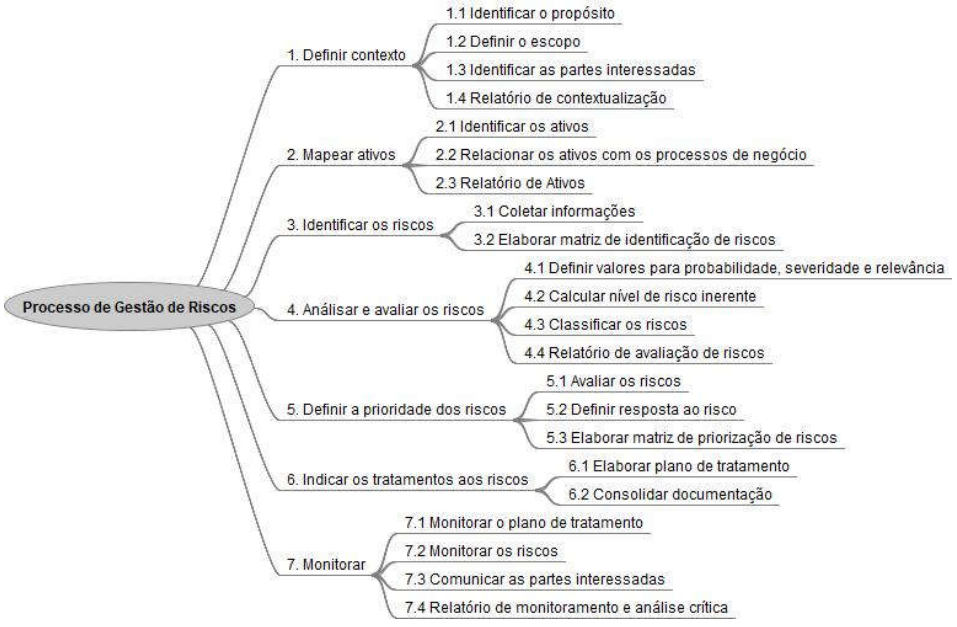
Os riscos podem ser identificados e avaliados também em relação a determinado ativo de informação e/ou um ambiente, sobretudo quando eles são considerados como essenciais ao funcionamento do PJTO. Por exemplo, pode-se levantar riscos em relação a um ambiente específico como o *data center*.

Como um ativo importante, pode-se destacar pessoas que detêm informações ou desempenham atividades relevantes para o negócio. Podem ser servidores, colaboradores terceirizados, estagiários etc.

4.1 Processo de Gestão de Riscos no PJTO

A metodologia de Gestão de Riscos em Segurança da Informação do PJTO adota o ciclo composto pelas etapas apresentadas na Política de Segurança da Informação – Norma-TIC-07. São elas: definição do contexto, identificação, análise, avaliação e tratamento de riscos. Na Figura 10, é demostrado uma estrutura analítica do processo de gestão de riscos de TIC.

Figura 10 - Processo de gestão de riscos em forma de mapa mental.



4.1.1. Definição do contexto

Recebida uma solicitação para que se proceda a gestão de risco de um determinado escopo, a primeira atividade a ser executada é a comunicação das áreas e pessoas envolvidas, a data de início dos trabalhos, os prazos, custos, pessoas envolvidas e resultados esperados.

Nesta fase, ocorre a definição e detalhamento do escopo ou contexto de aplicação da gestão de riscos a fim de delimitar o âmbito de atuação. O escopo pode ser uma estrutura funcional, um processo, sistema, recurso ou determinado ativo. Também devem ser definidos os prazos (cronograma), partes interessadas, pessoas envolvidas e resultados esperados. Estas informações devem ser comunicadas às áreas e pessoas envolvidas já no início dos trabalhos.

O produto a ser gerado nessa etapa será o Relatório de Contextualização, conforme Apêndice C.

4.1.2. Mapeamento de ativos

Esta etapa corresponde ao conjunto de ações necessárias para levantamento, detalhamento e estruturação dos ativos (processos, tecnologias, ambientes e pessoas) que podem impactar os objetivos, missão ou atividades finalísticas do PJTO.

Para que a execução do ciclo de gestão de riscos seja realizada de acordo com os objetivos estratégicos, é necessário que todos os ativos sob o escopo sejam inventariados. Essa atividade pode ser executada por meio de reuniões entre as equipes envolvidas. Como resultado, o produto a ser gerado será uma lista de ativos com riscos a serem gerenciados, e fará parte do relatório de contextualização.

4.1.3. Identificação de riscos

Etapa em que são identificados possíveis riscos para objetivos associados aos processos organizacionais. Essa atividade pode ser executada por meio de reuniões entre as equipes envolvidas e o objetivo é produzir uma lista abrangente de riscos, incluindo fontes e eventos que possam ter algum impacto na consecução dos objetivos identificados na etapa de estabelecimento do contexto.

A norma NBR ISO/IEC 31010 fornece orientações sobre a seleção e a aplicação de técnicas sistemáticas para o processo de avaliação de riscos. Uma das técnicas abordadas pela norma é a de Brainstorming, que consiste em reunir pessoas conhecedoras de certo ativo ou atividade organizacional e incentivar o fluxo livre de conversação entre elas com o objetivo de identificar possíveis perigos, riscos ou controles associados ao objeto analisado (BRASIL, 2018).

Os riscos necessariamente possuem uma ou mais causas conhecidas e podem gerar uma ou mais consequências. As causas podem se originar de ações ou omissões de indivíduos (agentes causadores), de fontes de risco inerente (exemplo, líquido inflamável tem risco de entrar em combustão por natureza; um equipamento elétrico pode parar de funcionar por falta de energia elétrica) ou da combinação de ambos (um agente utilizar uma fonte de risco para causar um dano). A materialização da ocorrência do risco é denominada evento de risco. Ocorrendo o risco, ele irá trazer consequências diretas ou indiretas aos objetivos organizacionais ou ao processo analisado, que podem representar perdas ou danos, ou mesmo ganhos quando se trata de riscos positivos (BRASIL, 2015).

Figura 11 - Elementos do risco (BRASIL, 2015, adaptado).

Visando racionalizar a etapa, foram definidos 5 (cinco) passos básicos para identificação de riscos em qualquer processo, ambiente, projeto ou sistema, conforme citado em Brasil (2015).

Tabela 5 - Passos para identificação de riscos (BRASIL, 2015, adaptado).

1º Passo: Identificar as principais funções ou objetivos do processo, ambiente, ativo ou sistema.
2º Passo: Levantar possíveis eventos que podem impedir ou dificultar a execução ou o atingimento dos objetivos do processo, ambiente, ativo ou sistema.
3º Passo: Levantar as possíveis causas que levam a ocorrência do evento.
4º Passo: Levantar as possíveis consequências da ocorrência do evento (levando em consideração os objetivos organizacionais e conformidade normativa).
5º Passo: Identificar os responsáveis e levantar os controles que atualmente já sejam aplicados na mitigação das causas dos riscos.

O produto a ser gerado nessa etapa será a matriz de identificação de riscos, conforme Apêndice D.

Tabela 6 - Exemplo de identificação de riscos e levantamento de controle (BRASIL, 2015, adaptado).

Ativo	Evento de Risco	Causas	Consequências	Controles Implementados
Data Center	Incêndio no Data Center	1. Curto circuito no Data Center; 2. Curto circuito nas dependências do prédio.	1. Destruição parcial ou total do Data Center.	1. Nenhum.
Estações de Trabalho	Ataques por *software* de código malicioso às	1. Não possuir antivírus instalado;	1. Mau funcionamento das	1. Solução corporativa de antivírus.

	estações de trabalho	2. Antivírus está desatualizado; 3. Acesso indevido a *site* com códigos maliciosos; 4. Mau uso de dispositivos de armazenamento externo.	estações de trabalho; 2. Roubo de dados; 3. Proliferação de programas de código malicioso para outras estações de trabalho.	

4.1.4. Análise de riscos

Com os riscos identificados, com as respectivas causas e consequências relacionadas, e com o levantamento prévio de controles internos, começa a etapa de análise dos riscos com base nos critérios pré-definidos de probabilidade de ocorrência, severidade das consequências e relevância do ativo, processo ou atividade.

Conforme NBR ISO 31000, a análise de riscos é o processo de compreendê-los e determinar seu nível, de modo a subsidiar a avaliação e o tratamento destes. Envolve a apreciação das causas e fontes de risco, suas consequências e a probabilidade de que estas possam ocorrer (ABNT, 2018a).

A multiplicação entre os valores de probabilidade, severidade e relevância define o nível do risco inerente, ou seja, o nível do risco sem considerar quaisquer controles que reduzem ou podem reduzir a probabilidade da sua ocorrência ou do seu impacto.

NRI = P x S x R

Em que:

NRI = nível de risco inerente

P = probabilidade de ocorrência do evento de risco

S = severidade (impacto) do risco

R = relevância do ativo

Para estabelecer um entendimento comum das classificações de probabilidade, severidade e relevância, as Tabelas 7, 8 e 9 apresentam as escalas de valores para cada um desses fatores.

Tabela 7 - Escala de probabilidade de ocorrência de uma ameaça (BRASIL, 2018, adaptado).

PROBABILIDADE	DESCRIÇÃO DA PROBABILIDADE, DESCONSIDERANDO OS CONTROLES	VALOR
Muito baixa	**Improvável.** Em situações excepcionais, o evento poderá até ocorrer, mas nada nas circunstâncias indica essa possibilidade.	**1**
Baixa	**Rara.** De forma inesperada ou casual, o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade.	**2**
Média	**Possível.** De alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade.	**3**
Alta	**Provável.** De forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade.	**4**
Muito alta	**Praticamente certa.** De forma inequívoca, o evento ocorrerá, as circunstâncias indicam claramente essa possibilidade.	**5**

Tabela 8 - Escala de severidade da ocorrência (BRASIL, 2018, adaptado).

SEVERIDADE	CONSEQUÊNCIA PARA O ATIVO, CASO O EVENTO OCORRA	VALOR
Muito baixa	**Mínima,** quase não afeta o ativo.	**1**
Baixa	**Pequena,** afeta pouco o ativo.	**2**
Média	**Moderada,** afeta moderadamente o ativo, porém recuperável.	**3**
Alta	**Significativa,** afeta gravemente o ativo. De difícil reversão.	**4**
Muito alta	**Catastrófica,** afeta o ativo de forma irreversível.	**5**

Tabela 9 - Escala de relevância do ativo (BRASIL, 2015, adaptado).

RELEVÂNCIA	RELEVÂNCIA QUE O PROCESSO OU ATIVO POSSUI PARA A ORGANIZAÇÃO OU PARA O PROCESSO DE NEGÓCIO AVALIADO	VALOR
Muito baixa	São ativos irrelevantes para o alcance do objetivo organizacional ou execução do processo de negócio associado.	**1**
Baixa	São ativos pouco importantes para o alcance do objetivo organizacional ou execução do processo de negócio associado.	**2**
Média	São ativos importantes para o alcance do objetivo organizacional ou execução do processo de negócio associado.	**3**
Alta	São ativos muito importantes para o alcance do objetivo organizacional ou execução do processo de negócio associado.	**4**
Muito alta	São ativos essenciais para o alcance do objetivo organizacional ou execução do processo de negócio associado.	**5**

Os níveis de risco obedecerão ao resultado do produto das variáveis, podendo gerar valores que vão de 1 a 125. A Tabela 10 detalha cada nível de risco:

Tabela 10 - Escala de classificação de risco (BRASIL, 2015, adaptado).

NÍVEL DO RISCO	PSR
Muito baixo	De 1 a 5
Baixo	De 6 a 12
Médio	De 15 a 30
Alto	De 32 a 50
Muito alto	De 60 a 125

O documento base para essa etapa é a Matriz de Análise e Avaliação de Riscos, conforme Apêndice E.

Tabela 11 - Exemplo de Matriz de Análise e Avaliação de Riscos (BRASIL, 2015, adaptado).

Ativo	Evento de Risco	Causas	Consequências	P	S	R	PSR	NRI
Data Center	Incêndio no Data Center	1. Curto circuito no Data Center; 2. Curto circuito nas dependências do prédio.	1. Destruição parcial ou total do Data Center.	2	5	5	50	**ALTO**
Estações de Trabalho	Ataques por *software* de código malicioso às estações de trabalho	1. Não possuir antivírus instalado; 2. Antivírus está desatualizado; 3. Acesso indevido a *site* com códigos maliciosos; 4. Mau uso de dispositivos de armazenamento externo.	1. Mau funcionamento das estações de trabalho; 2. Roubo de dados; 3. Proliferação de programas de código malicioso para outras estações de trabalho.	4	3	4	48	**ALTO**

4.1.5. Avaliação de Riscos

O propósito da avaliação de riscos é apoiar decisões com base nos resultados da análise de riscos, sobre quais riscos necessitam de tratamento e a prioridade para a implementação do tratamento. Caso já existam controles implementados, se eles devem ser modificados, mantidos ou eliminados.

As decisões estratégicas devem considerar o contexto mais amplo do risco, incluindo o exame de quão tolerável são os riscos a serem assumidos. Para isso, com as informações sobre os processos de negócio da organização e os ativos que os suportam, deve-se:

- Priorizar os riscos – os ativos que possuírem os maiores níveis de risco (PSR) serão priorizados em termos de recursos e proteções;
- Ter maior conhecimento sobre os riscos e avaliar as melhores soluções de proteção, considerando seu custo-benefício.

Para o processo de avaliação, foram estabelecidos critérios para priorização e tratamento associados aos níveis de risco conforme exemplificado na Tabela 12. A documentação desta etapa será o Relatório de Avaliação de Riscos (Apêndice F), que consiste em uma lista dos riscos que requerem tratamento, com suas respectivas **classificações e prioridades**.

Tabela 12 - Critérios para priorização e tratamento de riscos (BRASIL, 2015, adaptado).

NÍVEL DE RISCO	CRITÉRIOS PARA PRIORIZAÇÃO E TRATAMENTO DE RISCOS
Muito Alto	São riscos inaceitáveis, e os responsáveis devem ser orientados para que os evitem ou reduzam imediatamente.
Alto	São riscos inaceitáveis, e os responsáveis devem ser orientados para pelo menos reduzi-los e controlá-los.

Médio	São riscos toleráveis, e os responsáveis devem ser orientados a adotar estratégias para mitigar ou compartilhar, porém devem passar por análise de custo-benefício quanto à necessidade de aplicação de controles.
Baixo	São riscos que podem ser aceitáveis, não havendo necessidade de tratamento imediato, devendo apenas ser reconhecidos e monitorados quanto às ocorrências e possíveis consequências.
Muito Baixo	São riscos aceitáveis e devem ser informados aos gestores dos ativos.

4.1.6. Tratamento de Riscos

O tratamento de riscos envolve a seleção de uma ou mais opções para modificar o nível de cada risco e a elaboração de planos de tratamento que, uma vez implementados, implicarão novos controles ou modificação dos existentes. Opções de tratamento de riscos incluem evitar, mitigar, compartilhar e aceitar o risco, devendo-se observar que elas não são mutuamente exclusivas (BRASIL, 2018).

Como risco aceitável, o Poder Judiciário do Tocantins considera os riscos que foram classificados como **Muito Baixo e Baixo**. Portanto, deverão ser tratados os riscos classificados como **Médio, Alto e Muito Alto**, cabendo ao Gestor da área analisar os casos especiais, nos quais a aceitação do risco é justificável. Podem ser entendidos como casos especiais, dentre outros, as atividades temporárias ou de curto prazo, a implantação de controles cujo custo supera o valor da consequência causada pela ocorrência do evento.

Segundo a NBR ISO 31000, a finalidade dos planos de tratamento de riscos é especificar como as opções de tratamento escolhidas serão implementadas de maneira que os arranjos sejam compreendidos pelos envolvidos, e o progresso em relação ao plano possa ser monitorado (ABNT, 2018a).

O plano de tratamento deve ser validado pelo Comitê Gestor de TIC, que definirá ou ajustará as atividades de acordo com as restrições que porventura existam, como orçamento disponível ou priorização de atividades externas à gestão de riscos. Com isso, será atualizado o plano com as devidas justificativas para a não implantação dos controles sugeridos.

Paralelamente, comunicar ao Comitê de Gestão de Riscos do Poder Judiciário quais foram os processos identificados que impactam na Gestão Estratégica e este deverá analisar as medidas de tratamento adotadas e caso necessário, propor adequações. Cabe ainda ao Comitê de Gestão de Riscos comunicar a Presidência do Tribunal de Justiça sobre os riscos que impactam no alcance dos objetivos estratégicos e os planos de ação adotados para o tratamento.

Executar o Plano de Tratamento significa a implantação dos controles selecionados para cada ativo, de acordo com suas particularidades e características.

Dar uma resposta ao risco encontrado envolve decidir se ele vai ser tratado ou não, promovendo a priorização de tratamento dos riscos. Cabe ressaltar que a responsabilidade pela

definição da estratégia de resposta aos riscos e a consequente priorização de tratamentos é atribuída na Política de Segurança da Informação - Norma-TIC-07 aos gestores de riscos. A estratégia de resposta ao risco adotada no PJTO é composta pelas opções evitar, mitigar, compartilhar e aceitar, conforme descrito na Tabela 13.

Tabela 13 - Estratégia de resposta aos riscos (BRASIL, 2015, adaptado).

RESPOSTA AO RISCO	DESCRIÇÃO
Evitar	Inclui basicamente a descontinuação das atividades que geram os riscos. Evitar riscos pode implicar a descontinuação de um software, a alienação de um equipamento ou a extinção de um processo de trabalho.
Mitigar	São adotadas medidas para reduzir a probabilidade ou o impacto dos riscos, ou, até mesmo, ambos. Tipicamente, esse procedimento abrange qualquer uma das centenas de decisões do negócio no dia a dia.
Compartilhar	Redução da probabilidade ou do impacto dos riscos pela transferência ou pelo compartilhamento de uma porção do risco. As técnicas comuns compreendem a aquisição de produtos de seguro, a terceirização de uma atividade e outras.
Aceitar	Quando o nível de risco for baixo ou muito baixo, o risco residual não justifica a implementação de novos controles para mitigá-lo, em uma análise da relação de custo e benefício. Portanto, nenhuma medida é adotada para afetar a probabilidade ou o grau de impacto dos riscos, podendo ser aceitos pelo gestor.

Tabela 14 - Exemplo de matriz de priorização de riscos (BRASIL, 2015, adaptado).

Ativo	Evento de Risco	Causas	Consequências	NRI	Resposta ao Risco
Data Center	Incêndio no Data Center	1. Curto circuito no Data Center; 2. Curto circuito nas dependências do prédio.	1. Destruição parcial ou total do Data Center.	**ALTO**	**Mitigar**
Estações de Trabalho	Ataques por *software* de código malicioso às estações de trabalho	1. Não possuir antivírus instalado; 2. Antivírus está desatualizado; 3. Acesso indevido a *site* com códigos maliciosos; 4. Mau uso de dispositivos de armazenamento externo.	1. Mau funcionamento das estações de trabalho; 2. Roubo de dados; 3. Proliferação de programas de código malicioso para outras estações de trabalho.	**ALTO**	**Mitigar**

4.1.7. Plano de Tratamento de Riscos

Após a avaliação, a definição da estratégia de resposta e a priorização de tratamento dos riscos, faz-se necessário o detalhamento do tratamento dos riscos. Essa etapa será responsável pela seleção e implementação de uma ou mais ações de tratamento para modificar os níveis de riscos.

Antes de elaborar o plano de tratamento de riscos, primeiro é necessário decidir quais controles precisam ser implementados, correlacionando as opções de mitigação e controles com cada risco priorizado. Os controles internos precisam ser reavaliados quanto à eficácia e suficiência, e com base nessa avaliação os gestores de riscos irão definir os controles internos que devem ser aperfeiçoados ou adicionados no tratamento (BRASIL, 2015).

As perguntas que devem ser respondidas na reanálise dos controles internos são basicamente:

- Os controles existentes são capazes de tratar adequadamente o risco, de modo que ele seja controlado a um nível que seja tolerável?
- Na prática, os controles estão operando na forma pretendida e pode ser demonstrado que são eficazes quando requerido?

Conceitualmente, os controles internos podem ser classificados:

a) Pelo impacto na mitigação dos riscos

- Primário: proveem garantia razoável de que os objetivos serão atingidos, por meio da redução do risco de um resultado indesejado a um nível aceitável.
- Secundário: não são totalmente confiáveis do ponto de vista de efetividade, sendo frequentemente associado a controles corretivos ou compensatórios.

b) Por sua natureza de identificação

- Preventivo: projetado com a finalidade de evitar a ocorrência de erros, desperdícios ou irregularidades; atua sobre a probabilidade da ocorrência.
- Detectivo: projetado para detectar erros, desperdícios ou irregularidades, no momento em que eles ocorrem, permitindo a adoção de medidas tempestivas de correção; atua sobre a probabilidade e a severidade da ocorrência do risco.
- Corretivo: projetado para detectar erros, desperdícios ou irregularidades depois que já tenham acontecidos, permitindo a adoção posterior de ações corretivas; atua sobre a severidade da ocorrência do risco.

c) Pelo modo de processamento pode ser automatizado, quando processado por sistema informatizado e, não automatizado, quando processado manualmente.

d) Pela periodicidade ou frequência: anual, trimestral, mensal, diário e eventual.

Reanalisados os controles e definidos quais serão utilizados no tratamento dos riscos priorizados, é necessário elaborar o Plano de Tratamento dos Riscos (Apêndice H). Para elaborar o plano, o mais simples é visualizá-lo como um plano de ação onde são especificados:

quais controles deverão ser aperfeiçoados, desenvolvidos e implementados, quem será o responsável por eles, e quais são os prazos e recursos requeridos.

Tabela 15 - Exemplo de Plano de Tratamento de Riscos (BRASIL, 2015, adaptado).

Evento de Risco	Controles	Descrição	Monitoramento	Responsável	Prazo	Nível de Risco Pretendido
Incêndio no Data Center	Sistema de detecção e combate a incêndio.	O sistema de detecção e combate a incêndio tem como função perceber, captar, sinalizar e evitar a propagação de chamas no data center.	Acompanhar etapas de elaboração e execução do projeto. Registro de ocorrência do evento com periodicidade mensal	Chefe da DASR	120 dias	Atual **Alto** Pretendido **Baixo**
Ataques por *software* de código malicioso às estações de trabalho	Solução corporativa de antivírus.	A solução detecta, impede e atua na remoção de programas de software maliciosos, como vírus e *worms*.	Monitoramento das estações via servidor de administração do antivírus. Registro de ocorrência do evento com periodicidade semanal.	Chefe da DMSU	30 dias	Atual **Alto** Pretendido **Baixo**
	Campanhas de conscientização de segurança.	O treinamento dos usuários para que eles sejam conscientes da segurança os fornecerá as habilidades necessárias para identificar comportamentos suspeitos, como *e-mails* de *phishing*, por exemplo.	Relatório de capacitação de pessoal. Registro de ocorrência do evento com periodicidade mensal	Chefe da DMSU	90 dias	

4.1.8. Comunicação e Consulta

A comunicação e consulta é a etapa responsável pela manutenção de um fluxo regular e constante de informações com as partes interessadas, ocorrendo de forma concomitante durante todas as fases do processo de gestão de riscos. O gerenciamento das comunicações inclui os processos necessários para assegurar que as informações sejam geradas, coletadas,

distribuídas, armazenadas, recuperadas e organizadas de maneira oportuna e apropriada (BRASIL, 2015).

Durante a execução do processo de avaliação e tratamento de riscos, todas as etapas e atividades deverão ser devidamente comunicadas, seja às partes interessadas bem como às partes envolvidas. Tipos de informação que pode ser gerada no processo: relatórios, quadros, tabelas, inventários, matrizes de análise e avaliação, planos, planilhas de registro, ofícios e outros comunicados internos e externos, boletins de informação (notícias), convites em agenda eletrônica, formulários físicos e eletrônicos etc.

A comunicação poderá ser realizada por meio de ferramentas de apoio como correio eletrônico e comunicação instantânea, divulgação de informações no portal do Tribunal, por informações e despachos em processos administrativos, ferramenta de gerenciamento de projetos, reuniões etc.

O Apêndice I contém um modelo de Formulário para Comunicação e Consulta.

Tabela 16 - Exemplo de Comunicação e Consulta (BRASIL, 2015, adaptado).

Partes	Comunicador	Propósito	Conteúdo	Meio de Comunicação	Data	Frequência
Gestores de Risco	Diretor de Tecnologia da Informação	Promover a análise dos riscos identificados	Convocar os gestores de riscos para a etapa de análise dos riscos identificados, visando apurar o nível de risco	Sistema SEI	15/10/19	Única

4.1.9. Monitoramento e Análise Crítica

O processo de gestão de riscos deverá ser constantemente controlado e avaliado. Depois de planejada e executada a avaliação e tratamento dos riscos, durante sua execução deverá haver controle e ao final de cada ciclo de gestão de riscos deverá haver uma avaliação sobre o que deu certo e o que deu errado, visando adoção de medidas que corrijam os desvios em um próximo ciclo de gestão de riscos.

Devem ser analisados os artefatos do projeto (relatórios) em todas as fases do processo de gestão de riscos, de forma a mantê-los alinhados às diretrizes gerais estabelecidas. Os riscos devem ser monitorados e analisados criticamente, a fim de verificar regularmente, no mínimo, as seguintes mudanças:

a) Nos critérios de avaliação e aceitação dos riscos;

b) No ambiente;
c) Nos ativos de informação;
d) Nas ações de Segurança da Informação;
e) Nos fatores do risco (ameaça, vulnerabilidade, probabilidade e severidade).

Conforme à evolução dos processos internos de gestão de riscos, podem ser necessárias atualizações nas diretrizes e normas aplicáveis, isso implica em possíveis revisões da Política e no Manual de Gestão de Riscos. Revisar diretrizes e normas também é parte da análise crítica do processo de gestão de riscos, e visa garantir que as regras aplicáveis ao gerenciamento de riscos estejam sempre atuais e condizentes com a realidade organizacional.

O documento base para essa etapa é o Relatório de Monitoramento e Análise Crítica, conforme Apêndice J.

5 ESTUDO DE CASO

Para validar o *framework* proposto, foi realizada uma aplicação prática, por meio de um estudo de caso. Para o desenvolvimento da análise, foi considerada a área de infraestrutura de Tecnologia da Informação do Tribunal de Justiça do Estado do Tocantins.

O estudo visa identificar as ameaças às quais a infraestrutura tecnológica está sujeita e os riscos que elas impõem sobre a atividade-fim do Judiciário. Com isso, elaborar um mapa de respostas aos riscos com os controles necessários para mitigá-los e garantir os princípios da segurança da informação, quais sejam: confidencialidade, integridade, disponibilidade e autenticidade.

A análise e a avaliação de riscos levaram em conta o cenário atual da infraestrutura e os principais serviços de Tecnologia da Informação. Foram realizadas reuniões com integrantes da Divisão de Administração e Segurança de Redes, com o intuito de levantar os dados necessários.

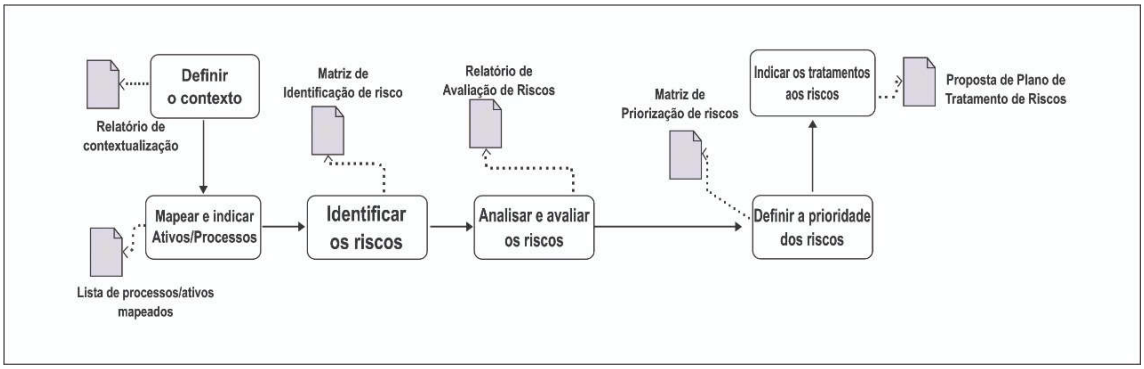
Durante as reuniões, utilizou-se de técnicas como *Brainstorming*, que consiste em reunir pessoas conhecedoras de certo ativo ou atividade organizacional e incentivar o fluxo livre de conversação entre elas com o objetivo de identificar possíveis perigos, riscos ou controles associados ao objeto analisado, e também a de Análise Preliminar de Perigos (APP), que é semelhante à anterior. Nessa técnica, as pessoas que detenham informações sobre o objeto da análise são reunidas em grupo. Os participantes consideram as informações existentes, como atividades, recursos, ambiente, e produzem, de comum acordo, uma lista de situações perigosas ou de riscos (BRASIL, 2018).

As técnicas citadas foram utilizadas conforme orientações da norma NBR ISO/IEC 31010, que é um complemento da norma NBR ISO 31000. A norma 31010 fornece orientações sobre a seleção e a aplicação de técnicas sistemáticas para o processo de avaliação de riscos.

5.1 Etapas do estudo de caso

De acordo com a metodologia elaborada, o processo de gerenciamento de riscos de TIC do Poder Judiciário do Tocantins é composto pelas etapas apresentadas na Política de Segurança da Informação – Norma-TIC-07 (Portaria nº 1660/2019). São elas: definição do contexto, identificação, análise, avaliação e tratamento de riscos.

Figura 12 – Atividades do processo de gestão de riscos.



Cada etapa foi descrita seguindo as atividades que compõe o processo de gestão de riscos do PJTO e foram utilizados os artefatos desenvolvidos durante a pesquisa. Com isso, foi possível identificar os eventos de risco, suas causas e consequências, avaliar esses eventos quanto à probabilidade de ocorrência e quanto ao impacto das consequências, e assim, elaborar o plano de tratamento visando mitigar os riscos considerados mais altos.

5.2 Resultados

5.2.1 Definição do contexto

Nesta etapa, ocorre a definição da abrangência da análise a ser realizada. O escopo pode ser uma estrutura funcional, um processo, sistema, recurso ou determinado ativo. O foco do estudo foi o *Data Center* que é um ambiente projetado para abrigar a infraestrutura tecnológica, onde ocorre todo o processamento e armazenamento das informações.

O *Data Center* possui arquitetura modular e tem como missão proteger, com fonte de energia ininterrupta e climatização, todos os equipamentos de TIC e sistemas computacionais do Poder Judiciário do Tocantins. Para garantir eficiência e alta disponibilidade, foram instalados dois *sites*, sendo um principal localizado no prédio do Tribunal de Justiça, e um de *backup* no Fórum de Palmas.

Durante essa etapa, foi realizado o inventário dos ativos com o objetivo de gerar uma lista contendo detalhes como a função, sua localização e o setor responsável. A Tabela 17 apresenta os ativos que compõem o escopo.

Tabela 17 - Descrição dos ativos.

Ativo	Descrição	Responsável
Servidores	Equipamento utilizado para armazenamento e processamento de dados.	Divisão de Administração e Segurança de Redes.
Switches Core	Equipamento central da rede com grande capacidade de comutação de pacotes e com portas de alta velocidade (1 Gbps, 10 Gbps ou mais).	Divisão de Administração e Segurança de Redes.
Firewall	Solução de segurança baseada em *hardware / software* que, a partir de um conjunto de regras ou instruções, analisa o tráfego de rede para determinar quais operações de transmissão ou recepção de dados podem ser executadas.	Divisão de Administração e Segurança de Redes.
Solução de Virtualização	Solução que permite criar vários ambientes simulados ou recursos dedicados a partir de um único sistema de *hardware* físico. O software chamado *hypervisor* conecta-se diretamente ao *hardware* e possibilita a divisão de um único sistema em ambientes distintos, separados e seguros, conhecidos como máquinas virtuais.	Divisão de Administração e Segurança de Redes.
Enlace de Internet Principal	Provedor de Serviço de Internet Principal (500 MB).	Divisão de Administração e Segurança de Redes.
Enlace de Internet Redundante	Provedor de Serviço de Internet Redundante (100 MB)	Divisão de Administração e Segurança de Redes.
Meios de transmissão	Cabeamento estruturado e fibra óptica.	Divisão de Administração e Segurança de Redes.
Sistema Elétrico	Fornecimento e monitoramento de energia elétrica.	Divisão de Administração e Segurança de Redes.
Sistema de Climatização	Ares-condicionados de precisão, condensadoras, sensores de temperatura e umidade.	Divisão de Administração e Segurança de Redes.

Como a maior parte das operações do Judiciário Tocantinense é digital, o ambiente computacional apresenta uma relevância muita alta para a realização da atividade precípua do órgão em questão. A indisponibilidade dos recursos de TIC afeta sobremaneira o funcionamento do Judiciário, pois causa atrasos e interrompe atividades que são realizadas rotineiramente.

Os dados levantados pelos servidores da Divisão de Redes do Tribunal de Justiça foram reunidos no documento “Relatório de Contextualização Validado” e a compilação dessas informações resultou no conteúdo apresentado no Apêndice K.

5.2.2 Identificação de riscos

Segundo Brasil (2018), a identificação de riscos é o processo de busca, reconhecimento e descrição dos riscos, tendo por base o contexto estabelecido. O objetivo é produzir uma lista abrangente de riscos, incluindo fontes e eventos que possam ter algum impacto no alcance dos objetivos institucionais.

Para realização dessa etapa, foram seguidos os passos propostos no manual de gestão de riscos elaborado durante o desenvolvimento da pesquisa. São eles:

1. Identificar as principais funções ou objetivos do processo, ambiente, ativo ou sistema;
2. Levantar possíveis eventos que podem impedir ou dificultar a execução ou o atingimento dos objetivos do processo, ambiente, ativo ou sistema;
3. Levantar as possíveis causas que levam a ocorrência do evento;
4. Levantar as possíveis consequências da ocorrência do evento (levando em consideração os objetivos organizacionais e conformidade normativa);
5. Identificar os responsáveis e levantar os controles que atualmente já sejam aplicados na mitigação das causas dos riscos.

A Tabela 18 apresenta os riscos identificados pelos servidores que ocupam funções estratégicas na segurança da rede do Poder Judiciário. Foram elencados aqueles de maior relevância e que podem impactar de maneira negativa na prestação jurisdicional.

Tabela 18 - Riscos identificados conforme contexto estabelecido.

id	Riscos Identificados
1.	Acesso não autorizado ao *Data Center;*
2.	Inundação no *Data Center;*
3.	Incêndio no *Data Center;*
4.	Falha nos ares-condicionados de precisão;
5.	Interrupção no fornecimento de energia elétrica;
6.	Falha no gerador;
7.	Falha nos nobreaks do *Data Center*;
8.	Falha ou dano permanente no *Firewall;*
9.	Falha ou dano permanente no s*witch core;*
10.	Falha ou dano permanente na solução de virtualização*;*
11.	Indisponibilidade de acesso à Internet Principal;
12.	Indisponibilidade de acesso à Internet Redundante;
13.	Falha ou indisponibilidade do servidor de arquivos;
14.	Acesso não autorizado às pastas e arquivos departamentais;
15.	Indisponibilidade do sistema de processo judicial eletrônico – e-Proc;
16.	Indisponibilidade do sistema eletrônico de informações – SEI

O produto gerado nessa etapa foi a Matriz de Identificação de Riscos, presente no "Relatório de Avaliação de Riscos Validado" (Apêndice L), contendo causas, consequências e os controles já implementados visando mitigar as causas dos riscos.

5.2.3 Análise de riscos

Após a identificação dos riscos, com suas causas e consequências relacionadas, e com o levantamento prévio de controles já implementados, começa a etapa de análise dos riscos com base nos critérios pré-definidos de probabilidade de ocorrência, severidade das consequências e relevância do ativo.

Para cada um dos 16 (dezesseis) eventos de riscos identificados, foi calculado o **NRI** (nível de risco inerente) por meio da multiplicação entre os valores de probabilidade, severidade e relevância conforme escalas de valores estabelecidas no manual de gestão de riscos.

Com o NRI calculado, os riscos foram classificados conforme escala de classificação de riscos presente no manual. Os resultados obtidos subsidiaram as etapas de análise e tratamentos dos riscos, pois permitiram criar uma lista de riscos priorizada, de acordo com os critérios de avaliação.

A etapa de análise apresenta como produto a Matriz de Análise e Avaliação de Riscos, presente no "Relatório de Avaliação de Riscos Validado" (Apêndice L), e é um documento que demonstra o nível de risco encontrado na análise e sua classificação.

5.2.4 Avaliação de riscos

A documentação desta etapa geralmente consiste em uma lista dos riscos que requerem tratamento, com suas respectivas classificações e prioridades. A Tabela 19 apresenta uma lista dos riscos identificados por ativo e se eles possuem ou não algum controle implementado.

Tabela 19 - Lista de riscos que requerem tratamento.

id	Ativo	Risco Identificado	Nível de Risco	Controle
1	*Data Center*	Incêndio.	Muito Alto	NÃO
2	*Firewall*	Falha ou dano permanente no *Firewall.*	Alto	SIM
3	*Switch*	Falha ou dano permanente no s*witch core.*	Alto	SIM
4	Solução de Virtualização	Falha ou dano permanente na solução de virtualização.	Alto	SIM
5	e-Proc	Indisponibilidade do sistema de processo judicial eletrônico.	Alto	SIM
6	SEI	Indisponibilidade do sistema eletrônico de informações.	Alto	SIM
7	*Data Center*	Falha nos ares-condicionados de precisão.	Alto	SIM
8	*Data Center*	Interrupção no fornecimento de energia elétrica.	Alto	SIM

9	Enlace de Internet Principal	Indisponibilidade de acesso à Internet Principal.	Alto	SIM
10	*Data Center*	Acesso não autorizado ao *Data Center*.	Alto	SIM
11	*Data Center*	Falha no gerador.	Médio	SIM
12	*Data Center*	Inundação.	Médio	NÃO
13	Servidor de Rede	Acesso não autorizado às pastas e arquivos departamentais.	Médio	SIM
14	*Data Center*	Falha nos *nobreaks*.	Médio	SIM
15	Servidor de Rede	Falha ou indisponibilidade do servidor de arquivos.	Médio	SIM
16	Enlace de Internet Redundante	Indisponibilidade de acesso à Internet Redundante.	Médio	SIM

Como apresentado na Tabela 20, 6,25% das ameaças são de risco muito alto, 56,25% de alto risco e 37,5% de médio risco. Com os dados apresentados, é possível observar que das 16 (dezesseis) ameaças identificadas somente 2 (duas) não possuem algum controle de tratamento implementado.

Tabela 20 - Quantidade de riscos por nível.

Nível	Quantidade de Riscos	Percentual
Muito Alto	**1**	**6,25 %**
Alto	**9**	**56,25 %**
Médio	**6**	**37,5 %**
Baixo	**0**	**0 %**
Muito Baixo	**0**	**0 %**
TOTAL	**16**	

Figura 13 - Percentual de ameaças classificadas pelo nível de risco.

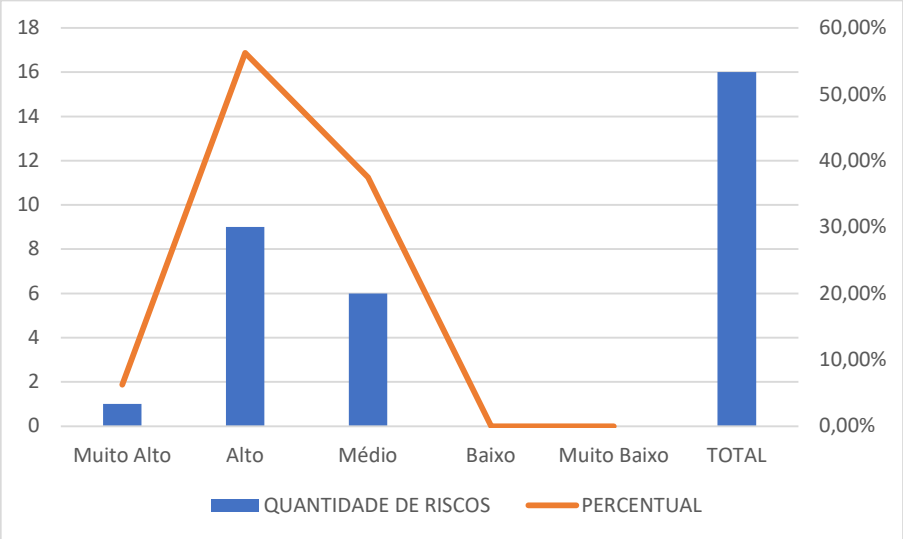
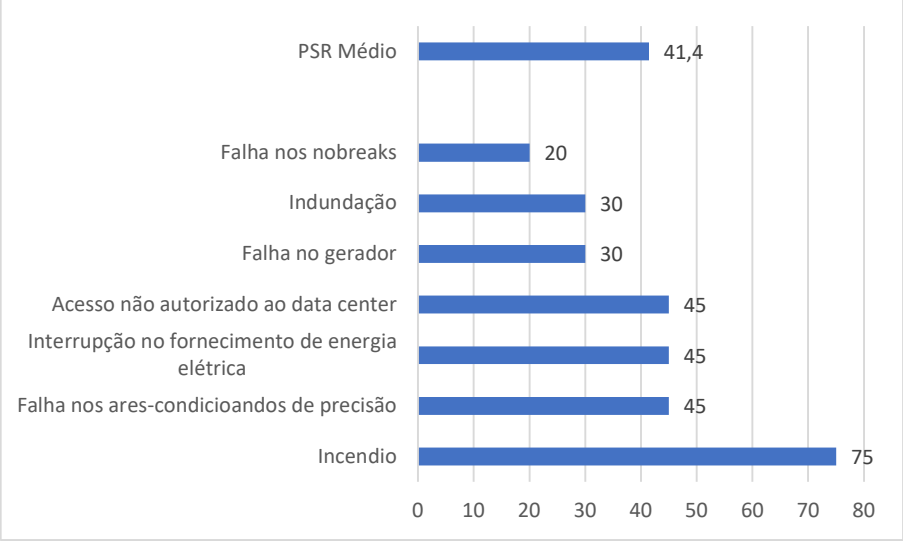


Tabela 21 – Riscos relacionados ao *Data Center*.

Evento de Risco	NRI	PSR
Incêndio	Muito Alto	75
Falha nos ares-condicionados de precisão	Alto	45
Interrupção no fornecimento de energia elétrica	Alto	45
Acesso não autorizado ao data center	Alto	45
Falha no gerador	Médio	30
Inundação	Médio	30
Falha nos nobreaks	Médio	20
PSR Médio		41,4

Figura 14 – PSR dos riscos relacionados ao *Data Center* e PSR médio.



A Tabela 21 traz os 7 (sete) riscos relacionados diretamente ao *Data Center*. Ao calcular o PSR médio de todos os eventos, encontra-se um valor de 41,4 que é considerado alto conforme escala de classificação de risco apresentada no capítulo anterior. Isso demonstra o grau de sensibilidade do ambiente estudado e quanto é importante ter um processo de monitoramento de riscos estruturado.

5.2.5 Tratamento dos riscos

O tratamento de riscos envolve a seleção de uma ou mais opções para modificar o nível de cada risco e a elaboração de planos de tratamento que, uma vez implementados, implicarão novos controles ou modificação dos existentes (BRASIL, 2018).

Ainda segundo o autor, opções de tratamento de riscos incluem evitar, mitigar, compartilhar e aceitar o risco, devendo-se observar que elas não são mutuamente exclusivas.

Segundo a NBR ISO 31000, a finalidade dos planos de tratamento de riscos é especificar como as opções de tratamento escolhidas serão implementadas de maneira que os arranjos sejam compreendidos pelos envolvidos, e o progresso em relação ao plano possa ser monitorado (ABNT, 2018a).

O levantamento de riscos relacionados ao *Data Center* e aos sistemas de processo judicial e administrativo teve como objetivo mapear as principais fontes de riscos, eventos, causas e consequências que possam impactar na atividade principal do Judiciário Tocantinense.

Ao todo, foram identificados 16 (dezesseis) eventos de riscos, 40 (quarenta) causas e 36 (trinta e seis) consequências. Desses dezesseis eventos identificados, somente dois não possuem algum controle de tratamento implementado.

Com o intuito de apresentar um plano de ação e propor soluções aos riscos identificados e analisados, o Apêndice M apresenta o Plano de Tratamento de Riscos onde foi utilizado o artefato desenvolvido nessa pesquisa. Foram identificados os eventos de riscos, suas causas e consequências, os controles já existentes, o nível de risco avaliado pelo método proposto e o plano de ações, com as medidas a serem tomadas, os recursos necessários e o monitoramento exigido para manter o tratamento de riscos eficaz.

Segundo a análise de riscos realizada no estudo, apenas 6,25% das ameaças apresentam risco muito alto ao negócio da Instituição e ainda não foi implementado nenhum controle para tratá-las adequadamente. Neste caso, a Instituição aceita o risco pela incapacidade momentânea de tomar qualquer medida sobre o risco.

Como identificado no Apêndice M, a ação necessária para tratar o risco identificado como muito alto (Incêndio no *Data Center*), seria a implantação de um sistema de prevenção e combate a incêndio. Conforme discutido em reunião com a equipe da Divisão de Redes do TJTO, o processo para contratação da solução está em fase de estudos preliminares e elaboração do termo de referência. Após essa etapa, será aberto o procedimento licitatório para aquisição.

No plano de tratamento elaborado, a opção escolhida como resposta aos riscos identificados foi tratá-los, com o objetivo de reduzir o nível de cada um por meio dos controles existentes e das ações que foram propostas. Para todos eles, o gestor de risco definiu um prazo de 120 dias para implementação das ações e ao final avaliar o que deu certo e o que deu errado, visando adoção de medidas para corrigir os desvios em um próximo ciclo de gestão de riscos.

A etapa de tratamento dos riscos apresenta como produto a Matriz de Priorização de Riscos, presente no "Plano de Tratamento de Riscos Validado" (Apêndice M), e é um documento que define as medidas para tratamento dos riscos identificados.

O plano de tratamento proposto visa manter os controles existentes, mantendo o monitoramento das ameaças, bem assim propõe novos controles para tratá-las. Mesmo implementando-se várias ações para tratar as ameaças identificadas, ainda vai existir o risco residual, o qual ainda permanece depois de considerado o efeito das respostas adotadas pela gestão para reduzir a probabilidade e o impacto dos riscos, incluindo controles internos e outras ações.

5.3 Análises preliminares

De acordo com o estudo realizado, foi possível observar a forte dependência da atividade precípua do Judiciário Tocantinense com a infraestrutura de Tecnologia da Informação, sendo que a maioria das operações é digital, incluindo o sistema de processo judicial, e a indisponibilidade dos recursos de TIC afeta sobremaneira o funcionamento do Judiciário.

Nesse sentido, pode-se afirmar que as atividades do Judiciário apresentam significativo grau de dependência em relação à área de Tecnologia da Informação, uma vez que esta dá sustentação para que o Judiciário Tocantinense atinja seus objetivos.

Os dados coletados no estudo referem-se à análise realizada na área de infraestrutura do TJTO. Foram mapeados os eventos mais críticos do órgão e apontados nos documentos que compõe o *framework* de gestão de riscos de TIC proposto nessa pesquisa.

Foi possível observar ainda que o ambiente estudado não possuía uma forma sistematizada de lidar com os riscos; e os controles ora implementados não eram processos formalizados, eram apenas de conhecimento de uma equipe específica. A prática comum, quando se recebia um alerta sobre um evento de risco, era avaliar setorialmente e subjetivamente possíveis consequências, eventualmente implementar controles mitigatórios essenciais e aguardar a evolução da situação.

No que diz respeito ao modelo de gestão de riscos proposto, pode-se afirmar que o mesmo se mostrou eficiente, evidenciando que a área de infraestrutura de TIC possui controles de segurança implementados, mas que ainda precisa avançar em relação a gestão de riscos de modo que se possa construir um plano de monitoramento de riscos de TIC estruturado e documentado.

Com o modelo, foi possível mapear os principais eventos de riscos, com suas causas e consequências, e assim elaborar um conjunto de medidas mitigatórias. Mesmo com a adoção dessas medidas, ainda vai existir o risco residual, o qual ainda permanece depois de considerado o efeito das respostas adotadas para reduzir a probabilidade e o impacto dos riscos.

Como forma de analisar o risco residual, na etapa de monitoramento e análise crítica, faz-se uma avaliação sobre o que deu certo e o que deu errado, visando adoção de medidas que corrijam os desvios em um próximo ciclo de gestão de riscos.

O produto a ser gerado é o Relatório de Monitoramento e Análise Crítica, que nesse estudo não foi elaborado, pois algumas das ações propostas no plano de tratamento ainda não foram executadas e estabeleceu-se um prazo de 120 dias para isso, só após será possível avaliar o processo. Sendo assim, não foi possível detectar falhas nos resultados obtidos.

Portanto, o monitoramento das medidas adotadas para tratar os riscos identificados deverá continuar, de modo a verificar possíveis mudanças nos fatores de risco como novas ameaças ou vulnerabilidades e assim propor as melhorias necessárias.

6 CONCLUSÃO

Tendo como meta promover a melhoria da governança, da gestão e da infraestrutura tecnológica no âmbito do Poder Judiciário, o Conselho Nacional de Justiça estabeleceu por meio da Resolução 211 de 15/12/2015 a ENTIC-JUD para o período de 2015 a 2020. Ela é um instrumento de planejamento para governança de TIC, pois visa assegurar que o uso de Tecnologia da Informação e Comunicação agregue valor à atividade principal do órgão, com riscos e custos aceitáveis.

A resolução estabelece ainda que cada órgão deverá elaborar e manter o Plano Estratégico de Tecnologia da Informação e Comunicação (PETIC), visando melhorar a infraestrutura e governança de TIC.

Para atender ao que determina a resolução, foi instituído no âmbito do Poder Judiciário Tocantinense o PETIC. Dentre os seus objetivos, o de aprimorar a segurança da informação e aperfeiçoar a gestão e a governança tratam da implantação do processo de gestão de riscos em todas as divisões da Diretoria de Tecnologia da Informação.

No cenário atual, em que o Poder Judiciário do Estado do Tocantins depende cada vez mais da informação e de seus sistemas de informática, a indisponibilidade, quebra de confidencialidade, e perda de integridade dessas informações podem acarretar prejuízos enormes à sociedade. Assim, torna-se necessário uma gestão eficaz da segurança da informação para identificar as ameaças e os riscos que podem prejudicar o alcance dos objetivos institucionais.

Com base nesses fundamentos e metas a serem cumpridas, é que esta pesquisa se desenvolveu. O objetivo principal foi construir um *framework* para o gerenciamento de riscos em segurança da informação que permitisse estruturar e documentar todos os procedimentos. A realização do presente estudo possibilitou criar um modelo a ser seguido, com as ferramentas e regras gerais para gerenciar os riscos de TIC.

O primeiro artefato produzido foi a política interna, instituída por meio da Portaria nº 1660 de 12 de agosto de 2019, que tem por objetivo estabelecer princípios, diretrizes e responsabilidades a serem observadas no processo de gestão de riscos. A política elaborada permitiu sistematizar o processo, definindo as etapas que deveriam ser seguidas.

Para completar essa primeira parte da pesquisa foi desenhado, em conjunto com o escritório de projetos, o fluxo do processo de gestão de riscos, onde foram mapeadas as atividades que comporiam cada uma das etapas definidas na política. Isso contribuiu para

definir os atores do processo e suas responsabilidades, as entradas necessárias, os produtos gerados e os recursos que deveriam ser utilizados.

No que tange à estruturação do processo de gestão de riscos de TIC, faltava definir um conjunto de conceitos e regras que permitissem aos atores envolvidos realizar o levantamento e o tratamento de eventos negativos que pudessem impactar na prestação jurisdicional. Então, para suprir essa necessidade, foi desenvolvido um manual contendo a metodologia a ser adotada. Sendo assim, o manual tornou-se o principal artefato produzido, pois ele tem a função de padronizar a linguagem de gerenciamento de riscos na instituição.

Até esse ponto da pesquisa, foi possível cumprir com os seguintes objetivos: definir os processos para gerenciar riscos em conformidade com as principais normas e códigos de boas práticas voltadas para o gerenciamento e tratamento de riscos em segurança da informação e elaborar os artefatos para compor o *framework*. Para o alcance do último objetivo, foi realizado um estudo de caso na área de administração e segurança de redes do TJTO.

Com as orientações presentes nesse manual e com a utilização dos artefatos elaborados, foi possível identificar os eventos de risco, suas causas e consequências, avaliar criticamente esses eventos quanto à probabilidade de ocorrência e quanto ao impacto das consequências decorrentes destes, e traçar a estratégia de tratamento visando basicamente mitigar os riscos considerados mais altos e aceitar os mais baixos.

O estudo de caso revelou que o ambiente estudado não possuía uma forma sistematizada de lidar com os riscos; e os controles ora implementados não eram processos formalizados, eram apenas de conhecimento de uma equipe específica. A aplicação do modelo proposto possibilitou documentar as ações necessárias para o tratamento dos eventos de riscos identificados. Foi possível ainda, levantar as causas e as consequências decorrentes do evento negativo caso ele se concretizasse.

Quanto à viabilidade, a metodologia elaborada se mostrou capaz de solucionar o problema pesquisado, pois permitiu elaborar um planejamento de ações com o objetivo de proteger as informações críticas e minimizar as falhas no ambiente de Tecnologia da Informação.

O modelo desenvolvido precisa ainda ser apreciado e validado pelo Comitê Gestor de TIC, que é o comitê interno da Diretoria de Tecnologia da Informação, para depois ser apresentado aos futuros gestores de riscos que conduzirão a maior parte das atividades do processo.

Adotar procedimentos que garantam a segurança da informação será sempre uma prioridade no Judiciário Tocantinense. Nesse sentido, com a implantação da gestão de riscos de

TIC, será possível estimar a probabilidade de ocorrência de ameaças e o impacto ao negócio caso elas se concretizem, dessa forma se antecipar a eventuais problemas que possam causar prejuízos a Instituição.

Não obstante os objetivos deste trabalho terem alcançado êxito, é notório a necessidade de envolver os profissionais de TIC a fim de implantar o modelo em todas as divisões da Diretoria de Tecnologia da Informação, bem como mantê-lo e aprimorá-lo de modo a possibilitar uma gestão eficaz da segurança da informação.

É importante salientar que o modelo elaborado pode ser modificado e adaptado a outras áreas do Poder Judiciário, em razão da sua abrangência e por poder utilizar diversas fontes de conhecimento. Além disso, o modelo teve como uma das fontes bibliográficas a norma ABNT NBR 31000, que fornece diretrizes para gerenciar riscos enfrentados pelas organizações. A sua aplicação pode ser personalizada para qualquer organização e seu contexto.

Por fim, vale destacar que o *framework* proposto no trabalho pode não ser a solução para todos os problemas de gerenciamento de riscos, mas é suficientemente estruturado para apoiar os gestores na análise, avaliação e tratamento dos riscos, tendo sido concebido da compilação de boas práticas no domínio.

Dentre as contribuições primárias do trabalho, é possível destacar: 1) a elaboração da política de gestão de riscos em segurança da informação; 2) o manual de gestão de riscos de TIC; 3) os artefatos para identificação, análise, avaliação e tratamento dos riscos; 4) o desenho do fluxo do processo de gestão de riscos, 5) o mapeamento das atividades do processo com a definição dos recursos que deveriam ser utilizados.

As ações desenvolvidas na pesquisa, além de contribuírem para o aprimoramento da gestão da segurança da informação, ajudaram na melhoria e composição da pontuação do iGovTIC-JUD, que é um índice de Governança de Tecnologia da Informação e Comunicação desenvolvido com o propósito de o CNJ identificar, avaliar e acompanhar a situação da Governança, Gestão e Infraestrutura de TIC dos órgãos do Poder Judiciário.

Como trabalhos futuros, sugere-se algumas ações para aprimorar o processo de gestão de riscos no Poder Judiciário do Tocantins. São elas:

- Campanhas de conscientização e treinamentos a serem desenvolvidos com os profissionais de TIC sobre o tema da pesquisa;
- Automatizar a maneira de se gerenciar os riscos de TIC, por meio do desenvolvimento de um sistema tendo como base os artefatos produzidos;

- Reavaliação anual do *framework,* em função de mudanças ocorridas nos ambientes e sistemas de TIC, surgimento de novas ameaças e/ou vulnerabilidades;
- Propor a criação do Núcleo de Segurança da Informação (NSI), responsável pela gestão do processo e acompanhamento da execução das atividades relacionadas à gestão dos riscos de TIC.

REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ISO GUIA 73:2009. **Gestão de Riscos - Vocabulário.** Rio de Janeiro, 2009.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27001:2013. **Tecnologia da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação - Requisitos.** Rio de Janeiro, 2013a.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27002:2013. **Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação.** Rio de Janeiro, 2013b.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27005:2011. **Tecnologia da Informação - Técnicas de Segurança - Gestão de Riscos de Segurança da Informação.** Rio de Janeiro, 2011.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO 31000:2018. **Gestão de Riscos - Diretrizes.** Rio de Janeiro, 2018a.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 31010:2012. **Gestão de Riscos - Técnicas para o processo de avaliação de riscos.** Rio de Janeiro, 2012.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 38500:2018. **Tecnologia da informação - Governança da TI para a organização.** Rio de Janeiro, 2018b.

ALENCAR, Gliner Dias; QUEIROZ, Anderson A.L.; DE QUEIROZ, R. J. G. B**. Insiders:** Um Fator Ativo na Segurança da Informação**.** IX Simpósio Brasileiro de Sistemas de Informação (SBSI 2013), p. 61-72, 2013.

ASSI, Marcos. **Governança, Riscos e Compliance: Mudando a Conduta nos Negócios.** 1 ed. São Paulo: Editora Saint Paul, 2017. 168 p.

AZEVEDO, Rúben Manuel da Rocha. **Propagação de Vírus Informáticos Baseada em Modelos Biológicos.** Dissertação (Mestrado) – Instituto Superior de Engenharia do Porto, 2013. Disponível em: < http://recipp.ipp.pt/handle/10400.22/6519>. Acesso em: 28 jun. 2018.

BERMEJO, Paulo Henrique de Souza et al. **ForRisco: gerenciamento de riscos em instituições públicas na prática.** 2 ed. Brasília: Editora Evobiz, 2019. Disponível em: <http://forrisco.org/livro.php>. Acesso em: 29 ago. 2019.

BEZERRA, Edson Kowask. **Gestão de Riscos de TI: NBR 27005.** Rio de Janeiro: RNP/ESR, 2013. 138 p.

BRASIL. Conselho Nacional de Justiça. Segurança da Informação - **Diretrizes para a gestão de segurança da informação no âmbito do Poder Judiciário.** Brasília, 2012**.** Disponível em: <http://www.cnj.jus.br/images/dti/Comite_Gestao_TIC/Diretrizes_Gestao_SI_PJ.pdf>. Acesso em: 13 out. 2018.

BRASIL. Conselho Nacional de Justiça. **Resolução n. 211, de 15 de dez. de 2015.** Dispõe sobre a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário. Brasília, 2015. Disponível em:

<http://www.cnj.jus.br///images/atos_normativos/resolucao/resolucao_211_15122015_18122015173345.pdf>. Acesso em: 13 out. 2018.

BRASIL. Superior Tribunal de Justiça. **Gestão de riscos**. Superior Tribunal de Justiça. Ed. rev. e atual. em janeiro/2016. - Brasília: STJ, 2016. 35 p.: il. Disponível em: http://www.stj.jus.br/static_files/STJ/Institucional/Gestão%20estratégica/6_gestao_riscos_21jun.pdf. Acesso em: 13 de junho de 2018.

BRASIL. Tribunal de Contas da União. **Referencial básico de gestão de riscos** / Tribunal de Contas da União. Brasília: TCU, Secretaria Geral de Controle Externo (Segecex), 2018. 154 p. Disponível em: <https://portal.tcu.gov.br/biblioteca-digital/referencial-basico-de-gestao-de-riscos.htm>. Acesso em: 5 out. 2018.

BRASIL. Tribunal de Justiça do Tocantins. **Portaria n. 3433, de 26 de jun. de 2017**. Dispõe sobre a Política de Segurança da Informação (PSI). Palmas, 2017. Disponível em: <http://www.tjto.jus.br/tic/index.php/governanca-de-tic/documentos-normativos/send/98-normativas/1147-politica-de-seguranca-da-informacao>. Acesso em: 15 nov. 2018.

BRASIL. Tribunal de Justiça do Tocantins. **Portaria n. 1660, de 12 de agosto de 2019**. Promove atualizações em seu conteúdo e inclui normas de gestão de risco de segurança da informação e de gestão dos processos de backup, alterando a Portaria nº 3.433, de 26 de junho de 2017. Palmas, 2019. Disponível em: < http://wwa.tjto.jus.br/elegis/Home/Imprimir/1970>. Acesso em: 8 out. 2019.

BRASIL. Tribunal de Justiça do Tocantins. **Resolução n. 10, de 19 de maio de 2016**. Dispõe sobre o Plano Estratégico de Tecnologia da Informação e Comunicação (PETIC). Palmas, 2016. Disponível em: < http://wwa.tjto.jus.br/elegis/Home/Imprimir/1100>. Acesso em: 4 out. 2019.

BRASIL. Tribunal Regional do Trabalho da 8ª Região. **Manual de Gestão de Riscos**. Coleção Manuais de Gestão. Volume III. Manual Vermelho: Gestão de Riscos. Belém, 2015. 69 p. Disponível em: <https://www.trt8.jus.br/governanca/gestao-de-riscos>. Acesso em: 23 ago. 2019

CECCONELLO, Moisés S.; PEREIRA, Chryslaine M.; BASSANEZI, Rodney C. **Análise Qualitativa da Solução Fuzzy do Modelo Epidemiológico SIR.** Biomatemática, v. 22, p. 77-92, 2012.

CESTARI FILHO, Felício. **ITIL V3 Fundamentos**. Rio de Janeiro: RNP/ESR, 2011. 172 p.

DO NASCIMENTO, Janilson Pereira. **Segurança em Redes de Computadores:** Uma Abordagem sobre o Comprometimento Individual em Benefício da Corporação". Tecnologias em Projeção, v. 6, n. 1, p. 01-06, 2015.

DOURADO, Luzia. **Apostila COBIT 5 Framework de Governança e Gestão Corporativa de TI.** Disponível em: <https://lmdourado.wordpress.com/category/governanca-de-ti/cobit/>. Acesso em: 2 set. 2019.

FERNANDES, A. A; ABREU, V. F. **Implantando a Governança de TI: da estratégia à gestão dos processos e serviços.** 4 ed. Rio de Janeiro: Brasport, 2014.

FIGUEIREDO, Daniel R. **Introdução a redes complexas**. Atualizações em Informática, pg. 303-358, 2011.

FIGUEIREDO, Daniel R. **Redes Complexas Aula 15.** Disponível em: <http://www.land.ufrj.br/~daniel/rc/slides/aula_15_modelando_epidemia.pdf>. Acesso em: 11 jun. 2018.

GERHARDT, Tatiana E. **Métodos de pesquisa.** / [organizado por] Tatiana Engel Gerhardt e Denise Tolfo Silveira; coordenado pela Universidade Aberta do Brasil - UAB/UFRGS e pelo Curso de Graduação Tecnológica - Planejamento e Gestão para o Desenvolvimento Rural da SEAD/UFRGS. - Porto Alegre: Editora da UFRGS, 2009. 120 p.; 17,5x25cm. (Série Educação à Distância).

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa.** 6 ed. São Paulo: Atlas, 2017.

GRIFFIN, Dan; **Network Security:** The Four Pillars of Endpoint Security. Disponível em: <https://technet.microsoft.com/en-us/library/gg213837.aspx>. Acesso em: 28 jun. 2018.

KERMACK, W. O. y MCKENDRICK, A.G. (1927). **Contributions to the Mathematical Theory of Epidemics THE ROYAL SOCIETY. Proceedings of the Royal Society of London A**: mathematical, physical and engineering sciences. [S.l.], 1927. v. 115, n. 772, p. 700–721.

LUIZ, Mônica Helena Ribeiro. **Modelos Matemáticos em Epidemiologia**. Dissertação (mestrado) - Universidade Estadual Paulista, Instituto de Geociências e Ciências Exatas. Rio Claro, 2012.

ISACA. **Cobit 5: Habilitando processos.** Disponível em: <http://www.isaca.org/COBIT/Pages/COBIT-5-portuguese.aspx>. Acesso em: 6 set. 2019.

OLIVEIRA JÚNIOR, Nilson Cândido. **Uma proposta de implantação de governança de TIC em instituições federais de ensino.** 2015. 192 f. Dissertação (Mestrado) - Universidade Federal de Pernambuco. CIN, Ciência da Computação, 2015.

SÊMOLA, Marcos. **Gestão da segurança da informação: uma visão executiva.** 2 ed. Rio de Janeiro: Elsevier, 2014.

SILVA, Edna Lúcia da. **Metodologia da pesquisa e elaboração de dissertação**. Edna Lúcia da Silva, Estera Muszkat Menezes. - 4. ed. rev. atual. – Florianópolis: UFSC, 2005. 138p. Disponível em: <https://projetos.inf.ufsc.br/arquivos/Metodologia_de_pesquisa_e_elaboracao_de_teses_e_dissertacoes_4ed.pdf>. Acesso em: 13 jun. 2018.

TAUCHERT, Maicon Rodrigo; AMARAL, Suely Galvão. **O avanço tecnológico do judiciário como facilitador do acesso à justiça.** Jus Navigandi, 2015. Disponível em: <https://jus.com.br/artigos/44341/o-avanco-tecnologico-do-judiciario-como-facilitador-do-acesso-a-justica>. Acesso em: 18 jul. 2019.

VIEIRA, Gustavo Borges. **Teoria Qualitativa e Estabilidade de Lyapunov para Sistemas de Equações de Ordem Fracionária e uma Aplicação em um Modelo SIR-SI para a Dengue.** UFAL, Alfenas, 2017.

WANDERLEY, Danillo Lustosa; BATELLO, João Carlos Vilela; PRATA, David Nadler; BARBOSA, Gentil Veloso. **Um Estudo Sobre a Epidemia de Vírus Computacionais no Poder Judiciário do Tocantins**. Revista Cereus, v. 10, n. 4, p. 182-197, 2018. Disponível

em: < http://www.ojs.unirg.edu.br/index.php/1/article/view/2392/740>. Acesso em: 18 out. 2019.

WANDERLEY, Danillo Lustosa; BATELLO, João Carlos Vilela; BARRETO, Marcelo Leal de Araújo; BARBOSA, Gentil Veloso. **Mapping of information technology risks in the Judiciary Tocantinense.** International Journal of Development Research, Vol. 09, Issue 09, pp. 29633-29639, September 2019. Disponível em: < http://www.journalijdr.com/sites/default/files/issue-pdf/16815.pdf>. Acesso em: 18 out. 2019.

APÊNDICES

APÊNDICE A – Um Estudo Sobre a Epidemia de Vírus Computacionais no Poder Judiciário do Tocantins

A Study on the Computer Virus Epidemic in the Judicial Power of Tocantins

Danillo Lustosa Wanderley, João Carlos Vilela Batello, David Nadler Prata, Gentil Veloso Barbosa

http://ojs.unirg.edu.br/index.php/1/article/view/2392
DOI: 10.18605/2175-7275/cereus.v10n4p182-197

RESUMO

A segurança da informação não é processo acabado e pronto. Pelo contrário, é um processo que está sempre em evolução. Mesmo implementando-se mecanismos como *firewall* e antivírus, não significa que o ambiente computacional esteja totalmente seguro. É de fundamental importância proteger os pontos de extremidade da rede, de modo que esta continue a funcionar mesmo estando sob ataque. Assim, este estudo apresentará uma discussão acerca das principais ameaças à segurança da rede do Poder Judiciário do Tocantins, identificando suas ocorrências, os possíveis danos e as formas de contágio das estações de trabalho. Para tanto, foi utilizado o modelo epidemiológico SIR, desenvolvido por Kermack e McKendrick (1927). Após a realização do estudo, evidenciou-se que uma das principais ameaças é o uso inadequado do recurso computacional por parte dos usuários.

Palavras-Chave: Modelagem de Epidemias. Código Malicioso. Segurança da Informação.

ABSTRACT

The security of information is not process finished and Ready. On the contrary, it is a process that is always evolving. Even if you implement mechanisms such as firewall and antivirus, it does not mean that the computational environment is completely secure. It is of paramount importance to protect the network endpoints so that it continues to function even though it is under Attack. Thus, this study will present a discussion about the main threats to the security of the Judiciary network of Tocantins, identifying its occurrences, the possible damage and the forms of contagion of the Workstations. For this purpose, the SIR epidemiological model was used, developed by Kermack and McKendrick (1927). After the study was carried out, we showed that one of the main threats is the inadequate use of the computational resource on the part of the users.

Keywords: Epidemic Modeling. Malicious Code. Information Security.

1. INTRODUÇÃO

As redes corporativas e seus ativos sofrem constantes ataques de invasores, o que pode comprometer computadores, servidores e programas, causando interrupções em serviços essenciais das empresas.

Com ciberataques cada vez mais sofisticados, as empresas devem estar atentas para a adoção de soluções de segurança de modo a prevenir os perigos vindos da Internet e, com isso, proteger os pontos de extremidade da rede. Entende-se por pontos de extremidade todos os

dispositivos nos quais o trabalho é realizado, ou seja, servidores, estações de trabalho e dispositivos móveis (GRIFFIN, 2018).

Para proteção dos pontos de extremidade, é necessário garantir que eles estejam utilizando as mais recentes tecnologias de defesas contra ameaças. Um exemplo de contramedida a ameaças digitais são os softwares antivírus.

Segundo Nascimento (2015), os vírus e outras ferramentas de sabotagem digitais estão sempre alguns passos à frente das medidas de defesa, burlando as regras de *firewall* e os mecanismos de detecção dos antivírus, tornando frequentes as invasões às redes corporativas.

A segurança da informação não é processo acabado e pronto. Pelo contrário, é um processo que está sempre em evolução. Mesmo implementando-se mecanismos como firewall e antivírus, não significa que o ambiente computacional esteja totalmente seguro. Assim, é preciso desenvolver políticas de segurança empregando todos os mecanismos de proteção disponíveis, e o comprometimento do usuário a essa política é de fundamental importância.

A vulnerabilidade de uma rede é inversamente proporcional ao grau de comprometimento de cada um de seus usuários (NASCIMENTO, 2015). Quanto mais o usuário estiver integrado aos processos de segurança, mais segura será a navegação na rede interna e na Internet.

O órgão do Poder Judiciário onde o estudo foi realizado conta com aproximadamente 2.500 estações de trabalho que estão divididas entre o Tribunal e as Comarcas. A principal justificativa para realização deste estudo é que a existência de ataques provocados por objetos de código malicioso pode causar riscos às informações, como perda de arquivos importantes, exploração de informações sigilosas e atraso na execução de tarefas, devido a problemas na rede, como lentidão e parada de sistemas.

Nesse sentido, este trabalho propõe apresentar as principais ameaças à rede do Poder Judiciário do Tocantins, identificando suas ocorrências, os possíveis danos e as formas de contágio das estações de trabalho.

Para tanto, foi utilizado o modelo epidemiológico SIR, desenvolvido por Kermack e McKendrick (1927), no qual cada indivíduo, considerado saudável, neste trabalho representado por um computador, pode ser suscetível à infecção (S), infectado (I) e assim transmitir a doença a indivíduos saudáveis e removidos (R), que não têm a doença nem podem transmiti-la, pois adquiriram imunidade.

Dessarte, além de apresentar as ameaças e ataques ocorridos na rede, este trabalho tem o objetivo de identificar suas causas e as formas de como conter tais ameaças à segurança da informação.

2. REFERÊNCIAL TEÓRICO

Segundo Azevedo (2013), os vírus de computador são preparados para ter um comportamento igual aos vírus biológicos, porque são desenvolvidos para enviar cópias de si mesmos, na tentativa de se espalharem para outros computadores.

O autor ainda afirma, em termos mais populares, que os vírus informáticos são comparados aos vírus biológicos, fazendo analogia entre os computadores e o corpo humano, atribuindo assim uma visão humanizada ao computador como se tratasse de um corpo vulnerável a doenças virais.

O uso de modelos matemáticos no controle de doenças tornou a teoria mais próxima da prática; dessa maneira, vários modelos foram criados buscando o entendimento do comportamento da dinâmica epidemiológica (LUIZ, 2012). Tais modelos são ferramentas matemáticas desenvolvidas para estudar e entender os diversos tipos de comportamentos, podendo ser aplicados a qualquer tipo de sistema físico ou biológico para investigação da modelagem de doenças infecciosas (VIEIRA, 2017).

Os modelos epidemiológicos têm-se mostrado uma importante ferramenta para compreender e analisar o comportamento das epidemias. O modelo SIR, proposto por Kermack e Mckendrick em 1927, é um dos modelos mais utilizados para representação de doenças infecciosas. Nesse modelo os indivíduos são divididos em três classes:

- Suscetíveis (S): indivíduos que estão sujeitos a contrair a doença quando em contato com os infecciosos;
- Infectados (I): indivíduos portadores e com capacidade de transmitir a doença para os suscetíveis;
- Removidos (R): indivíduos que após contraírem a doença adquirem imunidade e perdem a capacidade de transmissão da doença.

O modelo clássico SIR descreve a propagação de uma doença infecciosa ao longo do tempo e considera que a distribuição de indivíduos é espacial e temporalmente homogênea. A forma de contágio nesse modelo é probabilística e ocorre por meio de arestas com os vizinhos (FIGUEIREDO, 2011).

Segundo Cecconello et al. (2012), nesse modelo, são analisadas, ao longo do tempo, as quantidades de indivíduos nas três categorias, levando-se em consideração que alguns dos suscetíveis adquirem a doença ao entrar em contato com indivíduos infectados da população. Além disso, com o passar do tempo, os infectados adquirem imunidade, deixando assim de contribuir para a propagação da doença.

Ainda segundo este mesmo autor, desde o modelo proposto por Kermack e McKendrick, diversos outros modelos têm sido propostos para descrever a propagação de uma epidemia em uma população.

> No modelo compartimental do tipo SI, a população é dividida em suscetíveis e infecciosos e este modelo é adequado quando são consideradas doenças transmissíveis de caráter crônico, para as quais os indivíduos infecciosos não voltam a ser suscetíveis nem se recuperam da infecção. Nos modelos do tipo SIS, os infecciosos se recuperam da infecção tornando-se suscetíveis à doença novamente. Já no modelo do tipo SIRS os infecciosos adquirem imunidade temporária, tornando-se suscetíveis com a evolução no tempo (CECCONELLO et al., 2012, p. 79).

A Figura 1 mostra uma população de tamanho constante, N > 0, subdividida nas três classes citadas no modelo: suscetíveis, infectados e removidos. Pode-se observar que, no primeiro momento, todos os indivíduos da rede estão sujeitos (S – suscetíveis) a contrair a doença quando em contato com os infectados. Após o contato com os infectados, que são aqueles portadores e com capacidade de transmitir a doença, mais indivíduos da rede contraem-na. Com o passar do tempo e com a adoção de contramedidas para barrar a infecção, os indivíduos que contraíram a doença adquirem imunidade, perdem a capacidade de transmissão e passam a formar a classe dos removidos.

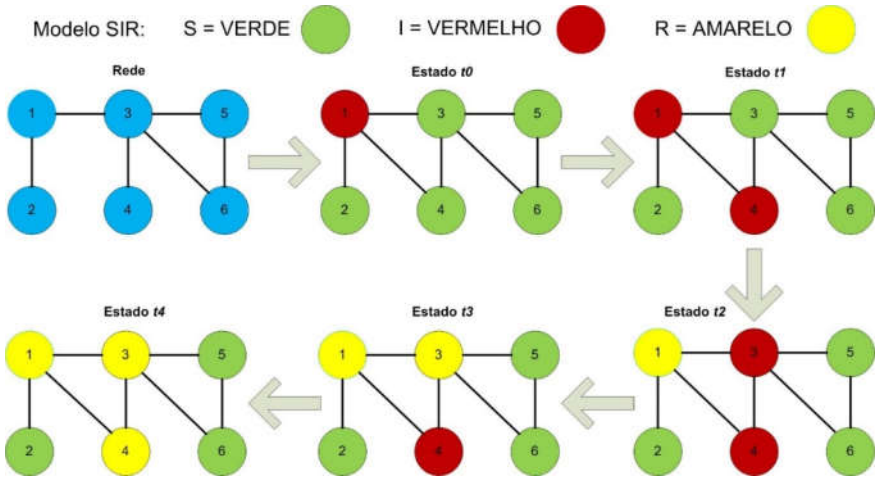


Figura 1. Representação conceitual do modelo SIR. Adaptado de Figueiredo (2018).

3. MATERIAIS E MÉTODOS

Este trabalho de pesquisa foi realizado no Poder Judiciário do Tocantins com abordagem qualiquantitativa do tipo exploratória e descritiva. Segundo Silva; Menezes (2005), a pesquisa exploratória envolve levantamento bibliográfico, entrevistas com pessoas que tiveram experiências práticas com o problema pesquisado, entre outros. Já a pesquisa descritiva visa descrever as características de determinada população ou fenômeno e envolve o uso de técnicas padronizadas de coleta de dados: questionários, planilhas, entrevistas ou observações.

Para o estudo em questão, fez-se uma revisão bibliográfica com vista a apresentar um embasamento teórico sobre o assunto tratado, dando mais ênfase ao modelo epidemiológico que foi utilizado para descrever as formas de contágio das estações de trabalho.

Os dados foram levantados por meio de pesquisa documental, sendo os relatórios gerados pela solução corporativa de antivírus a principal fonte de pesquisa utilizada, nos meses de junho a julho de 2018. A análise dos dados se deu à luz da literatura pertinente e foram realizadas discussões acerca das particularidades.

Os materiais literários foram coletados por buscas em bases ACM, IEEE e *google* acadêmico, durante o mês de junho de 2018, e utilizados os seguintes descritores para a pesquisa: modelagem de epidemias, código malicioso, segurança da informação.

Foram considerados como critérios de seleção dos materiais literários do estudo: a) sem delimitação do tempo de publicação; b) conteúdo relacionado à modelagem de epidemias, código malicioso e segurança da informação; c) idiomas português e inglês.

Durante a análise dos relatórios apresentados pela solução de antivírus, percebeu-se uma forte relação entre computadores infectados e dispositivos de armazenamento externo, ou seja, a dinâmica da infecção em sua maior parte era derivada dessa relação. Atualmente esses dispositivos representam uma das principais fontes de propagação de vírus de computador.

Uma única estação de trabalho apresentou 69 arquivos infectados pelo *malware Trojan.WinLNK.Agent.qg*. Na análise do relatório de ameaças, verificou-se que a infecção foi originada pelo uso de um dispositivo USB infectado. Nesse caso, após a utilização de medidas de precaução de imunização em tempo real, todos os arquivos foram recuperados.

Para a estação de trabalho citada anteriormente, pode-se representar o caminho de transição de estado da seguinte forma:

Figura 2. Transição de um indivíduo da rede para o estado removido.

Uma situação detectada foi a de estações de trabalho as quais se encontravam em estado crítico em virtude de o aplicativo de segurança estar desatualizado há bastante tempo. Isso acontecia principalmente por problemas de comunicação com o servidor de administração ou com o acesso ao servidor de rede que é utilizado como repositório dos arquivos de atualização do banco de dados do aplicativo.

Nessas estações de trabalho, detectou-se a presença de um *malware* denominado *Trojan.JS.Miner.m* que foi baixado da Internet por meio do acesso a páginas *web* que continham *exploits*. Como o aplicativo de segurança estava com mau funcionamento, este *malware* não foi neutralizado. Então, o caminho de transição de estado é representado da seguinte maneira:

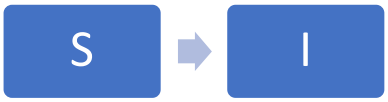


Figura 3. Transição de indivíduos da rede para o estado infectado.

Para sanar o problema, o aplicativo de segurança dessas estações foi reinstalado, e sua base de dados, atualizada. Após a realização da tarefa de verificação completa, o programa de código malicioso foi removido. Dessa maneira, representa-se o caminho de transição de estado, conforme figura abaixo:

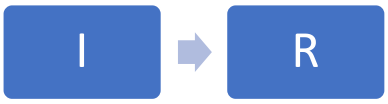


Figura 4. Transição de indivíduos da rede do estado infectado para removido.

4. RESULTADOS e DISCUSSÃO

Esta seção faz uma discussão dos resultados obtidos pelos relatórios da solução corporativa de antivírus utilizados pelo órgão do Poder Judiciário, sendo possível identificar as principais ameaças e ataques sofridos pelas estações de trabalho.

A Figura 5 apresenta os *malwares* mais representativos em termos percentuais detectados pela solução corporativa de antivírus. Por questão de simplicidade, são apresentados apenas os mais expressivos.

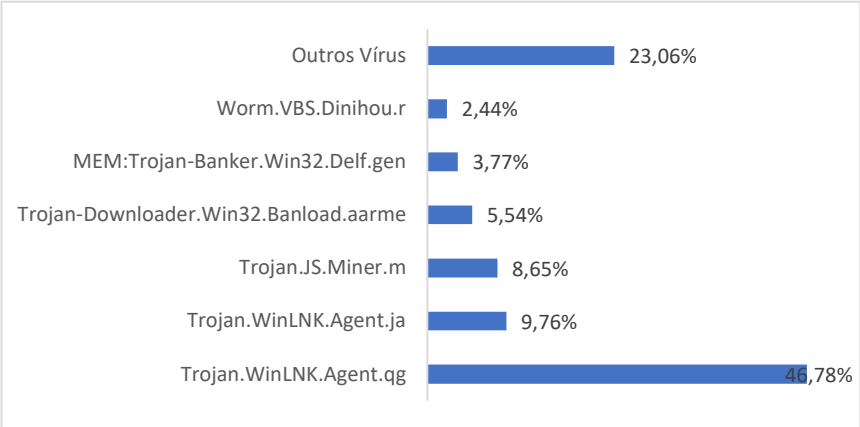


Figura 5. Ameaças com maior número de ocorrências.

Pode-se observar na Figura 5 que o *Trojan.WinLNK.Agent.qg* representa 46,78% da infecção. O *Trojan.WinLNK.Agent.ja* aparece como o segundo *malware* que mais infectou as estações de trabalho, com 9,76%. Esses *malwares* baixam arquivos maliciosos ou contêm um arquivo executável mal-intencionado, projetado para destruir, bloquear, modificar ou copiar dados, interferindo assim na operação de computadores ou redes de computadores.

O *Trojan.JS.Miner.m* foi responsável por 8,65% das infecções. Ele pode incluir nas estações de trabalho programas maliciosos com *scripts* JS usados para mineração de moeda criptografada sem o conhecimento do usuário.

O *Trojan-Downloader.Win32.Banload.aarme*, com 5,54% das infecções, tem como característica se instalar nas estações por meio do acesso a *sites* da Internet que contêm *exploits*. Outro *malware* que também causou problemas foi o *MEM:Trojan-Banker.Win32.Delf.gen*. Esse *malware* rouba os dados bancários do usuário pela instalação de programas *spyware* que são ativados quando *sites* de Internet *Banking* são acessados. Os dados são então transmitidos ao usuário mal-intencionado que controla o *trojan*. E-mail, FTP, a *web* ou outros métodos podem ser usados para transitar os dados roubados.

Já o *Worm.VBS.Dinihou.r* é classificado como vírus que pesquisa redes de computadores remotas e copia a si mesmo para diretórios que são acessíveis para leitura/gravação. Ademais, esses *worms* usam funções integradas do sistema operacional para procurar diretórios de rede acessíveis e/ou pesquisam aleatoriamente computadores na Internet,

conectam-se a eles e tentam obter acesso total aos discos destes. Esse *malware* foi responsável por 2,44% das infecções.

Além dos *malwares* citados, foram detectados mais 45 outros diferentes que, devido ao pequeno número de ocorrências, não foram relacionados na discussão. Entretanto, ao somar todas as ocorrências desses *malwares,* chegou-se a um total de 23,06% das infecções. Podem-se destacar alguns pela relevância do dano que podem causar. São eles:

- *Exploit*: programas que contêm dados ou códigos executáveis que tiram proveito de uma ou mais vulnerabilidade em *softwares* executados num computador local ou remoto para propósitos claramente maliciosos. Os *exploits* são comumente usados por *Net-Worms* para *hackear* um computador da vítima sem que seja necessária alguma ação do usuário;
- *Trojan-Ransom*: esse tipo de cavalo de troia modifica os dados no computador da vítima para que não possa mais usá-los ou impede que o computador seja executado corretamente. Depois que os dados são "tomados como reféns" (bloqueados ou criptografados), o usuário receberá uma solicitação de resgate;
- *Rootkit*: esse tipo de programa malicioso é projetado para ocultar certos objetos ou atividades no sistema. É usado para impedir que programas mal-intencionados sejam detectados;
- *Backdoor*: são projetados para permitir que usuários mal-intencionados controlem remotamente o computador infectado. Esses tipos de programas mal-intencionados possibilitam fazer qualquer coisa que o autor queira no computador infectado: enviar e receber arquivos, iniciar arquivos ou excluí-los, exibir mensagens, excluir dados, reinicializar o computador etc. São frequentemente usados para unir um grupo de computadores de vítimas e formar uma rede de *botnets* ou zumbis. Isso dá aos usuários mal-intencionados controle centralizado sobre um exército de computadores infectados que podem ser usados para fins criminosos.

A Figura 6 representa uma epidemia em rede, em que as estações de trabalho simbolizadas pelos círculos verdes foram infectadas pelos *malwares* definidos por esferas amarelas. Pode-se observar uma concentração de ataques do *Trojan.WinLNK.Agent.qg* no canto superior esquerdo da Figura 6. Esses ataques, como apresentado na Figura 5, representaram 46,78% das ocorrências.

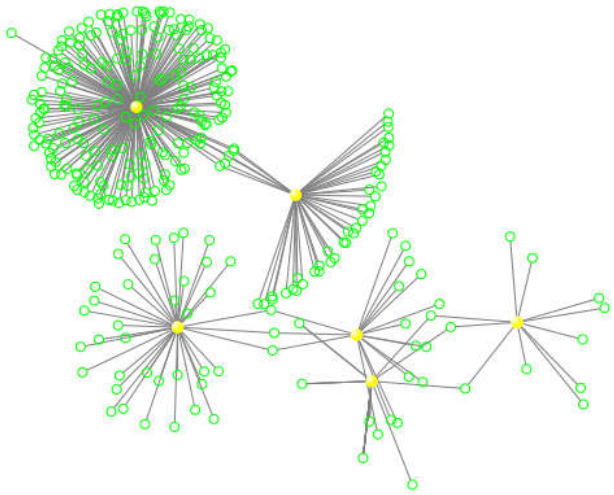


Figura 6. Rede de infecções causadas pelos *malwares* apresentados na figura 5. As estações de trabalho estão representadas pelos círculos verdes e os *malwares* pelas esferas amarelas.

Pode-se entender o *malware Trojan.WinLNK.Agent.qg* como uma ameaça *offline*, pois utilizam os dispositivos USB (*pendrives*, HDs externos), CDs e DVDs contaminados para disseminar programas de códigos maliciosos. Os *trojans* "WinLNK" são ícones de falsos arquivos do Sistema Operacional Windows potencialmente maliciosos que infectam após a efetivação de um duplo clique no arquivo.

Ao se analisar os relatórios da solução de segurança, um fato que chamou a atenção foi o número de infecções causadas pela utilização de “cracks” para a ativação de *softwares*. Vale ressaltar que um “crack” pode apresentar código malicioso que agirá silenciosamente no dispositivo infectado e pode causar dano não somente a este, mas a toda a rede.

Ainda na Figura 6, é possível observar que muitas estações de trabalho sofreram a infecção de dois ou mais *malwares* diferentes, como no caso do *MEM:Trojan-Banker.Win32.Delf.gen*, ilustrado na Figura 8, e do *Trojan.JS.Miner.m*, na figura 10, os quais se utilizam de *Java Script* para realizar seus ataques. Para aplicar os golpes, *hackers* modificam páginas na *web* e incluem um código em *Java Script* a ser executado no navegador. Esse tipo de ataque é transparente para o usuário que acaba não percebendo que o dispositivo está sendo infectado.

Nas Figuras de 7 a 12 serão apresentados, de forma visual, os ataques dos 6 tipos de ameaças com maior número de ocorrências. Os ataques de cada um dos *malwares* estão destacados na cor vermelha.

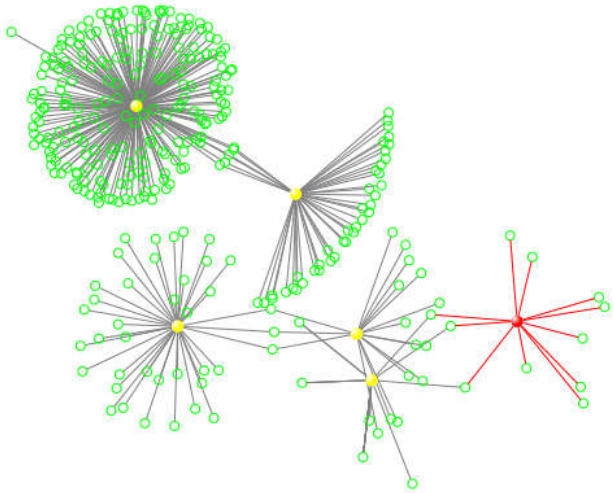


Figura 7. Rede de infecção causada pelo *malware Worm.VBS.Dinihou.r*.

Conforme relatórios analisados, percebeu-se que a infecção representada pelo *malware Worm.VBS.Dinihou.r* (Figura 7) foi resultado da cópia de uma série de arquivos infectados de um dispositivo USB para uma pasta compartilhada na rede e teve como origem um único usuário. Ao terem sido acessados, esses arquivos ocasionaram a infecção de outras máquinas.

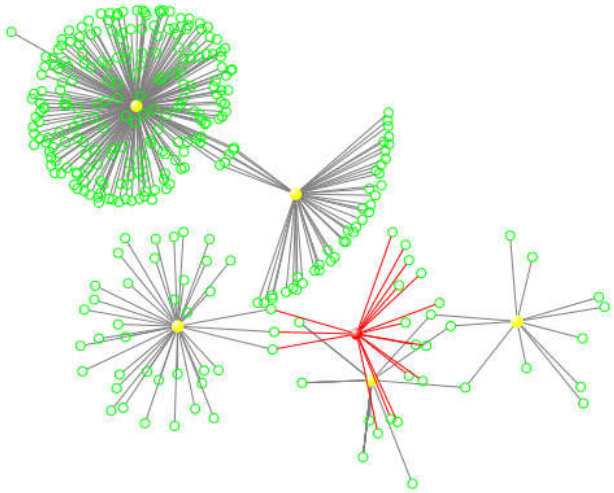


Figura 8. Rede de infecção causada pelo *malware MEM:Trojan-Banker.Win32.Delf.gen*.

A infecção destacada em vermelho na Figura 8 é resultado de acessos a *sites* que contêm programas de código malicioso e devido a *downloads* com arquivos infectados. A solução de antivírus, na maioria dos casos, conseguiu bloquear e/ou excluir essa ameaça. Em dois computadores nos quais os bancos de dados do aplicativo de segurança se encontravam desatualizados, essa ameaça não foi neutralizada. Somente após a atualização do banco de dados do aplicativo é que a ameaça foi removida dos computadores.

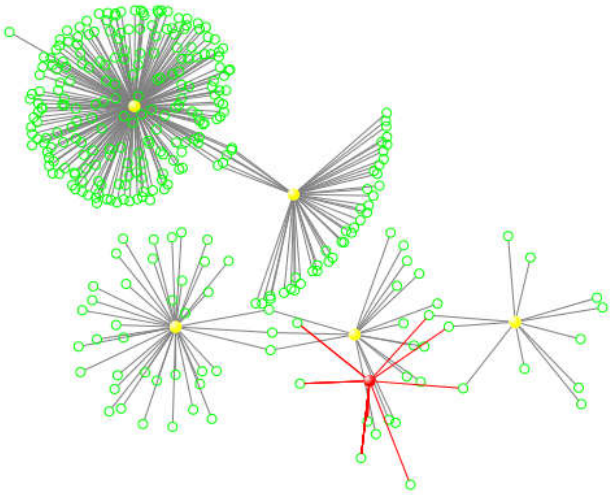


Figura 9. Rede de infecção causada pelo *malware Trojan-Downloader.Win32.Banload.aarme*.

O acesso a páginas *web* maliciosas e o *download* de arquivos obtidos nessas páginas foram a causa da infecção destacada na Figura 9.

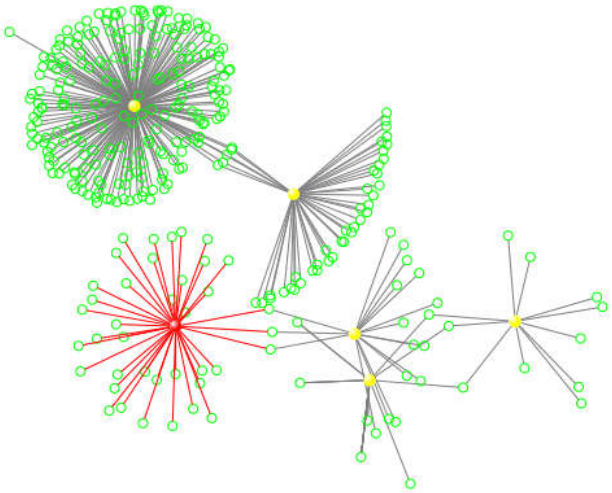


Figura 10. Rede de infecção causada pelo *malware Trojan.JS.Miner.m*.

Ao analisar o comportamento do *malware Trojan.JS.Miner.m*, em vermelho no canto inferior esquerdo da Figura 10, observou-se que a infecção também ocorreu de maneira semelhante à causada pelo *Trojan-Banker.Win32.Delf.gen*. Ambas aconteceram por meio de acessos a páginas *web* que continham programas de código malicioso. Cabe salientar que a solução de segurança não conseguiu neutralizar a ameaça em 59,4% das ocorrências, pois as estações de trabalho infectadas apresentavam estado crítico devido à ausência de comunicação com o servidor de administração da solução. Essa limitação de comunicação ocasionou o mau funcionamento do aplicativo de segurança em razão de o banco de dados estar desatualizado.

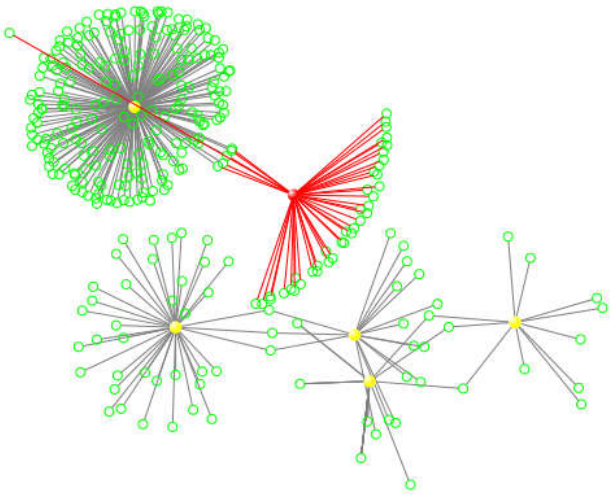


Figura 11. Rede de infecção causada pelo *malware Trojan.WinLNK.Agent.ja*.

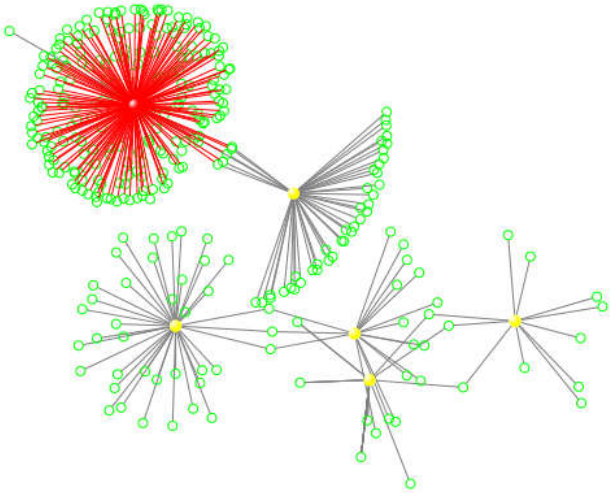


Figura 12. Rede de infecção causada pelo *malware Trojan.WinLNK.Agent.qg*.

Os *trojans* apresentados em vermelho nas Figuras 11 e 12 foram os responsáveis por 56% de toda infecção da rede. Em 96,5% dessas ocorrências, a solução de antivírus excluiu os arquivos infectados, e em 3,5%, os arquivos foram colocados em quarentena. Observou-se que nas máquinas em que os arquivos foram colocados em quarentena, o aplicativo de segurança estava com o banco de dados desatualizado.

Mediante o estudo realizado, foi possível identificar as principais ameaças e ataques sofridos pelas estações de trabalho do Poder Judiciário do Tocantins. Na maioria das vezes, os ataques ocorreram por uso indevido do recurso computacional por parte dos usuários e por vulnerabilidades do Sistema Operacional Windows.

Com a análise dos relatórios da solução de antivírus, observou-se que vários arquivos infectados que continham fotos e músicas foram executados por uma mídia removível e houve acessos a páginas da Internet com conteúdo inadequado. Em geral, essas ações foram neutralizadas pelo aplicativo de segurança instalado nos computadores.

Nesse cenário, destaca-se a necessidade de manter as estações de trabalho com o sistema operacional atualizado, de modo a corrigir possíveis vulnerabilidades. Além disso, existem problemas no manuseio de dispositivos USB, sendo necessária a adoção de uma política de uso, de modo que os usuários possam fazer uma gestão mais cuidadosa dos meios de armazenamento externo.

5. CONSIDERAÇÕES FINAIS

Como a maior parte das operações do órgão do Poder Judiciário em questão são digitais, tornou-se mais do que necessário proteger toda a rede, de modo a reduzir a exposição dos ativos a ameaças e ataques cibernéticos.

A solução de antivírus utilizada pelo órgão ajuda a fortalecer as estações de trabalho para torná-las resilientes aos ataques de *malwares* sem prejudicar o seu desempenho e a produtividade dos usuários. Ademais, simplifica o gerenciamento e aplicação das políticas de segurança a todas as estações, o que facilita as tarefas diárias dos administradores da rede.

Pela revisão bibliográfica realizada para dar embasamento teórico sobre o assunto tratado e pela pesquisa documental para levantamento dos dados, foi possível demonstrar no presente estudo os ataques de *malwares* nos ativos que integram a rede do Judiciário Tocantinense.

Foi possível concluir que os ataques na maioria das vezes ocorreram por conta de comportamentos inadequados dos próprios usuários, por causa do acesso indevido à Internet e do uso incorreto de dispositivos USB.

Segundo Alencar et al. (2013), as pessoas podem se tornar uma ameaça interna à segurança da informação por diversos motivos. Existem as que facilitam a ocorrência de um ataque à rede sem mesmo saber que estão cometendo algo errado, como também existem as que agem propositadamente e com finalidades específicas. Geralmente estas têm conhecimento dos processos internos da instituição, são chamadas de *insiders*.

Nesse sentido, é importante ressaltar o quanto a variável pessoa pode ser prejudicial para a Instituição, uma vez que a maioria dos incidentes, direta ou indiretamente, envolve a participação humana, gerando assim muitos prejuízos (ALENCAR et al., 2013).

Assim, a segurança da rede só será possível por meio da colaboração dos próprios usuários que devem fazer uso racional dos ativos. É extremamente importante que aqueles atuem de forma proativa, zelando pela segurança da informação.

Por fim, acredita-se que o fato de o usuário que tenha um melhor entendimento das ameaças e ataques de redes possa colaborar para uma mudança positiva em relação à segurança da informação. Isso modificaria o ambiente corporativo como um todo, pois criaria dificuldades para exploração de vulnerabilidades, diminuiria os riscos e aumentaria a segurança do ambiente.

REFERÊNCIAS

ALENCAR, Gliner Dias; QUEIROZ, Anderson A.L.; DE QUEIROZ, R. J. G. B**. Insiders:** Um Fator Ativo na Segurança da Informação**.** IX Simpósio Brasileiro de Sistemas de Informação (SBSI 2013), p. 61-72, 2013.

AZEVEDO, Rúben Manuel da Rocha. **Propagação de Vírus Informáticos Baseada em Modelos Biológicos.** Dissertação (Mestrado) – Instituto Superior de Engenharia do Porto, 2013. Disponível em: < http://recipp.ipp.pt/handle/10400.22/6519>. Acesso em: 28 jun. 2018.

CECCONELLO, Moisés S.; PEREIRA, Chryslaine M.; BASSANEZI, Rodney C. **Análise Qualitativa da Solução Fuzzy do Modelo Epidemiológico SIR.** Biomatemática, v. 22, p. 77-92, 2012.

DO NASCIMENTO, Janilson Pereira. **Segurança em Redes de Computadores:** Uma Abordagem sobre o Comprometimento Individual em Benefício da Corporação". Tecnologias em Projeção, v. 6, n. 1, p. 01-06, 2015.

FIGUEIREDO, Daniel R. **Introdução a redes complexas**. Atualizações em Informática, pg. 303-358, 2011.

FIGUEIREDO, Daniel R. **Redes Complexas Aula 15.** Disponível em: < http://www.land.ufrj.br/~daniel/rc/slides/aula_15_modelando_epidemia.pdf>. Acesso em: 11 jun. 2018.

GRIFFIN, Dan; **Network Security:** The Four Pillars of Endpoint Security. Disponível em: <https://technet.microsoft.com/en-us/library/gg213837.aspx>. Acesso em: 28 jun. 2018.

KERMACK, W. O. y MCKENDRICK, A.G. (1927). **Contributions to the Mathematical Theory of Epidemics THE ROYAL SOCIETY. Proceedings of the Royal Society of London A**: mathematical, physical and engineering sciences. [S.l.], 1927. v. 115, n. 772, p. 700–721.

LUIZ, M.H.R**. Modelos Matemáticos em Epidemiologia**, IGCE/UNESP, Rio Claro, 2012.

SILVA,E.L.DA; MENEZES. E.M. **Metodologia da Pesquisa e Elaboração de Dissertação.** UFSC, 4. ed. Ver. Atual. Florianópolis 2005.

VIEIRA, Gustavo Borges. **Teoria Qualitativa e Estabilidade de Lyapunov para Sistemas de Equações de Ordem Fracionária e uma Aplicação em um Modelo SIR-SI para a Dengue.** UFAL, Alfenas, 2017.

APÊNDICE B – Mapping of Information Technology Risks in the Judiciary Tocantinense

[1,2]Danillo Lustosa Wanderley, [1,2]João Carlos Vilela Batello, [1,2]Marcelo Leal de Araújo Barreto and [1]Gentil Veloso Barbosa
[1]UFT – Universidade Federal do Tocantins, Brazil
[2]TJTO – Tribunal de Justiça do Estado do Tocantins, Brazil

https://www.journalijdr.com/mapping-information-technology-risks-judiciary-tocantinense
Vol. 09, Issue, 09, pp. 29633-29639, September, 2019

ABSTRACT

Managing an Information Technology (IT) environment and keeping it secure is not a simple task. Corporate networks and their assets are subject to various attacks, which can compromise computers, servers, and programs, causing disruption to critical services. This reality increasingly requires organizations to cope with the uncertainties and risks inherent to security in the field of information technology. Thus, this study will present a discussion about the risks related to the IT infrastructure of the judiciary of the state of Tocantins, in which critical events are punctuated with a chance of occurrence and impact before the institution's objective. After the study, it was possible to observe the strong dependence of the primary activity of the Judiciary Tocantinense with the IT infrastructure, since most of the operations are digital, including the judicial process system.

Keywords: Risk Management. IT Infrastructure. Threats. Information Security.

INTRODUCTION

Managing an Information Technology (IT) environment and keeping it secure is not a simple task for organizations. Even with the advancement of information security tools, corporate networks and their assets are subject to various attacks, which can compromise computers, servers, and programs, causing disruption to essential services.

This reality increasingly requires organizations to cope with the uncertainties and risks inherent to security in the field of information technology. Preserving the confidentiality, integrity, availability and authenticity of data is a key factor for any organization, whether public or private. Therefore, managing risks is of paramount importance to protect information.

According to Bezerra (2013), risk is the combination of the probability of an unwanted event occurring and its consequences for the organization. That is, it is uncertainty in achieving the objectives. According to the author, in information security, uncertainty lies in the technological aspects, in the processes performed and, mainly, in the people who interact with the technology and engage with the processes.

In conformity with ABNT (2011), risk of information security is associated with the potential that threats can exploit vulnerabilities of an asset or a set of information assets and, consequently, cause damage to an organization. Thus, organizations should manage the risks to information security in order to keep them at acceptable levels and thus achieve their goals.

According to the guidelines for the management of information security within the judiciary, the adoption of procedures that ensure the security of information must be a constant priority in this power, in order to reduce failures and damages that may compromise the image of justice or to bring harm to society (CNJ, 2012).

These guidelines establish that the management model should contemplate, among the various normative processes, the risk management in order to minimize the impact of potentially negative events on the assets and services provided by the judiciary, provoking, continuous improvement in judicial provision.

In order to improve the infrastructure and governance of information and communication technology (ICT) so that the judiciary can be able to fulfill its institutional function, the National Council of Justice (CNJ) established by resolution No. 211, of 2015 , the National Strategy for Information Technology and Communication of the Judiciary (ENTIC-JUD) for the period of 2015-2020.

In short, ENTIC-JUD is a planning tool for governance of information technology and communication, because it consists in the establishment of a set of mechanisms in order to ensure that the use of this technology adds value to the main activity of the organ, with acceptable risks and costs.

Among the mechanisms that ENTIC-JUD establishes in its art. 9, it says that each organ should elaborate and apply policy, management and process of information security to be developed at all levels of the institution, through a steering committee and in harmony with the national guidelines advocated by the Council National justice. Thereby, the Court of Justice of the State of Tocantins, through Ordinance No. 3,433, of 2017, instituted the Information Security Policy (PSI) in the context of the Judiciary Tocantinense.

The information security policy, among its purposes, aims at the protection of information, and in its chapter VIII-A deals with the management of information security risks. Art. 21-A says that the "court should adopt a set of procedures to identify and implement the protective measures necessary to minimize or eliminate the risks to which their information assets are subject and to balance them with the operational costs and financial resources involved".

Thus, to meet what is established in art. 21-A of the information security policy it is necessary to implement mechanisms to manage the risks to the security of information in the judiciary of the state of Tocantins.

Thereby, this work proposes to study the risks related to the information technology infrastructure of the judiciary of the state of Tocantins, where critical events will be punctuated with a chance of occurrence and impact on the business. For this, a case study was carried out, concentrating on evaluating the study environment and relating the results found to the objective of the work.

The research in question did not take into consideration the external context as recommended by the standard, because the objective is to evaluate the internal controls and procedures. Therefore, the objective of this paper is to identify the threats to which the Information Technology infrastructure is subjected and the risks they impose on the final activity of the judiciary, as well as the construction of a risk response map related in this study with the implementation of controls to mitigate risks and ensure the principles of information security, such as confidentiality, integrity, availability and authenticity.

METHODOLOGY

This case study was carried out at the Court of Justice of the state of Tocantins with a qualitative and quantitative approach of the exploratory and descriptive type. For the study in question, a bibliographic review was performed with a view to presenting a theoretical basis on the subject treated. The literary materials were collected by searches in ACM, IEEE and Google academic bases, during the month of October 2018, and used the following descriptors for the research: IT risk Management, IT infrastructure, threats, information security.

The selection criteria of the literary materials of the study were considered: a) without delimitation of the time of publication; b) Content related to risk management, IT infrastructure, threats and information security; c) Languages in Portuguese and English.

For the development of this analysis, the area of information technology infrastructure of the explored environment was considered. For this, a risk map was built based on the most critical services, where risk identification and monitoring are relevant.

Considering that the environment studied does not have a risk monitoring plan for its information technology infrastructure, points related to the principles of information security were addressed, making clear the most important items to be managed.

INFORMATION TECHNOLOGY RISK MAPPING

This section discusses the results obtained by the study of the infrastructure environment of information technology and the risks imposed by it in the activities of the judiciary of the state of Tocantins. For the research in question, a risk management methodology was used based on the ABNT NBR ISO/IEC 27005 and ABNT NBR ISO/IEC 31000 standards.

The study aims to detail the current scenario of the information technology infrastructure of the Court of Justice of the State of Tocantins in order to conduct an analysis of the threats to which the environment is subject, assessing the impacts and consequences that they can generate.

Initially, the current scenario of the information technology infrastructure and its relationship with the main activity of the judiciary of Tocantins will be detailed.

The information technology infrastructure existing in the judiciary is comprised of servers, switches, firewall, virtualization solution, data storage system, structured cabling, main and redundant Internet linkage, electricity supply, data center, among others. The central point of this structure is the data center, where all the processing and storage of information occurs, in order to meet all the demands of the judiciary of the state of Tocantins.

The network of Judicial Power Tocantinense, called TELEJURIS, is formed by a virtual private network (VPN) and several subnets as shown in Figure 1.

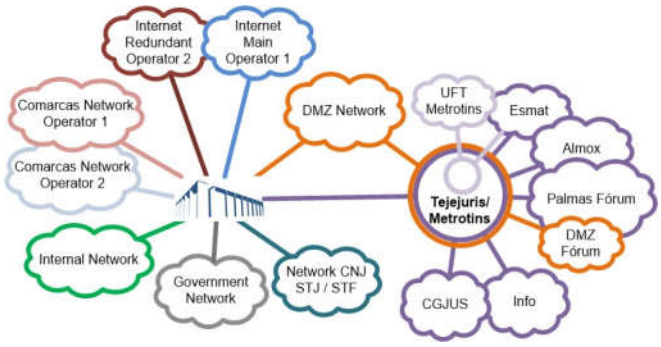


Figure 1. Network Telejuris

The Intranet subnet provides data communication between the Comarcas and annexes with the Court of Justice, through a long-distance virtual private network with Multiprotocol Label Switching (MPLS) technology. The Intranet consists of the subnets Comarcas operator 1, Comarcas operator 2, internal and Metrotins.

The DMZ network is perimeter, all systems and services of the judiciary that have external access, such as HTTP servers, electronic mail, among others, are maintained.

The Government and CNJ/STJ/STF subnets interconnect the State Court of Tocantins to the network of the state executive branch and to the network of the National Council of Justice and Superior Courts, respectively.

The METROTINS subnet offers a pair of dedicated fiber optics with a speed of 1G, whose purpose is to make the interconnection of the Court of Justice of the State of Tocantins with the forum of Palmas, CGJUS, Tocantinense Magistracy School (ESMAT) and other annexes in the capital.

The access of all judicial units to the Internet occurs by the Court of Justice, where are the Internet links main operator 1, with speed of 300 MB, and Internet redundant operator 2, 100 MB.

The risk management model defined by the ABNT NBR ISO/IEC 27005 standard is basically divided into three stages: the definition of the context, the risk assessment process and the risk treatment. The methodology proposed for this study covers the steps cited and is based on the norm.

As illustrated in Figure 2, the internal context of the Court of Justice of the State of Tocantins is composed of the people who develop the judicial activities and the computational environment with the assets that contribute to the judiciary Tocantinense fulfill its mission, namely, "guaranteeing citizenship through the distribution of swift, safe and effective justice".

As most of the operations of the Court of Justice of the State of Tocantins are digital, including the judicial process system, called E-Proc/TJTO, the computational environment has a very high relevance for the realization of the main activity of the organ in question. The unavailability of information and communication technology resources greatly affects the functioning of the judiciary, because it causes delays and interrupts activities routinely performed. Thus, the analysis and risk assessment were carried out considering the computer network and the set of assets that compose it.

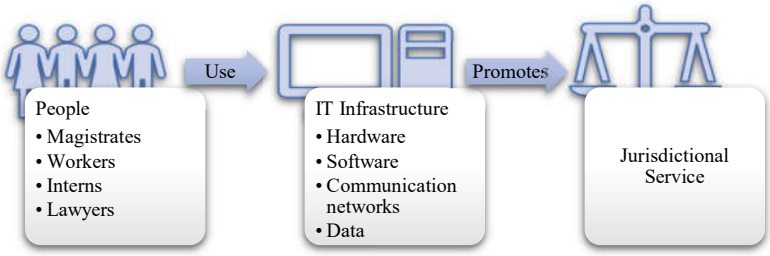


Figure 2. Internal context of the Court of Justice of the State of Tocantins.

As described in ABNT (2011), the risk management process involves defining the context, identification, analysis and evaluation, selection and implementation of responses to the risks assessed, monitoring and controls, and communication on risks with the stakeholders.

Figure 3 contextualizes the flow of the risk management process adopted for this study. As previously mentioned, the proposed methodology is based on the ABNT NBR ISO/IEC 27005 standard.

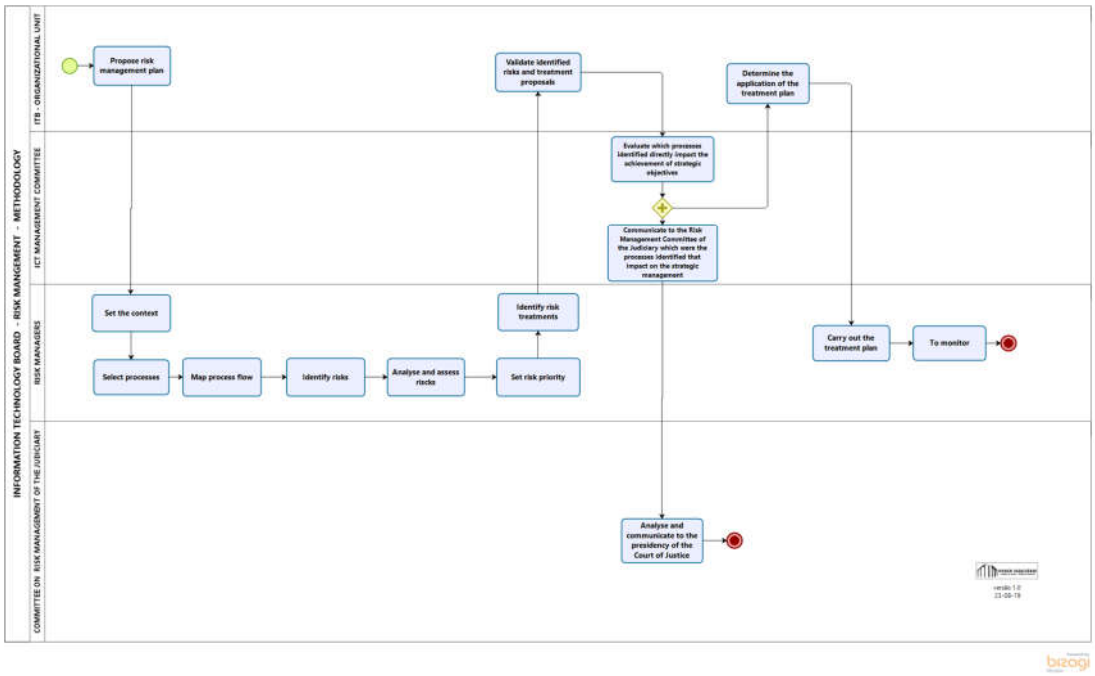


Figure 3. Risk management process flow.

To identify risks, we used the techniques of brainstorming and the preliminary hazard analysis, which is like the previous one. The techniques cited were used according to the norm ABNT NBR ISO/IEC 31010, which is an addition to the standard ABNT NBR ISO/IEC 31000. According to Bermejo et al. (2019), the tools and techniques adopted in the study are strongly applied for the identification of risks and allow to raise relevant information that assists in decision making and the establishment of prioritization for the treatment of risks.

Table 1 presents the risks identified by the five servers that occupy strategic functions in the security of the judiciary network, including the authors of this study. The most relevant ones that could negatively impact the jurisdictional service were listed.

Table 1. Risks identified using the techniques of brainstorming and preliminary hazard analysis, according to ISO 31010.

ID	IDENTIFIED RISKS
1.	Fire in the Data Center
2.	Unavailability of the main Internet access
3.	Unavailability of the electronic process system – e-Proc/TJTO
4.	Malicious code software attacks on workstations

The identified risks are analyzed by determining the consequences and their probability. The result of the analysis process will be to assign to each risk a classification, both for the probability and for the impact of the event, the combination of which will determine the level of risk (BRASIL, 2018).

At this stage of the study, risks were analyzed using a semi-quantitative method that uses previously agreed numerical scales to measure the consequence and its likelihood of occurrence, which are combined using a formula to produce the risk level.

Considering the simplicity that is intended in the application of this method, absolute real values of probability and consequences will not be employed, but their degrees:

- Degree of probability of occurrence (P);
- Degree of expected consequences (C).

In this way, the risk level (R) will be calculated by the formula:

$$\boldsymbol{R = P \, x \, C}$$

To establish a common understanding of the ratings of probabilities and consequences, the analysis in question used the semiquantitative method based on the scales exemplified below.

Table 2. Probability scale of occurrence of a threat (BRASIL, 2018, adapted)

PROBABILITY	DESCRIPTION OF THE PROBABILITY, DISREGARDING THE CONTROLS	VALUE
Very low	**Unlikely.** In exceptional situations, the event may even occur, but nothing in the circumstances indicates this possibility.	0.1
Low	**Rare.** Unexpectedly or casually, the event may occur, because the circumstances do not indicate this possibility.	0.2
Average	**Possible.** In some way, the event may occur, because the circumstances indicate moderately that possibility.	0.5
High	**Likely.** Until expected, the event may occur, because the circumstances strongly indicate this possibility.	0.8
Very high	**Practically certain.** Unambiguously, the event will occur, the circumstances clearly indicate this possibility.	1.0

Table 3. Scale of consequences resulting in the case of materialization of a threat (BRASIL, 2018, adapted).

CONSEQUENCE	DESCRIPTION OF THE IMPACT ON STRATEGIC AND OPERATIONAL OBJECTIVES IF THE EVENT OCCURS	VALUE
Very low	**Minimum** impact on objectives.	1
Low	**Small** impact on objectives.	2
Average	**Moderate** impact on objectives, but recoverable.	5
High	**Significant** impact on objectives, difficult to revert.	8
Very high	**Catastrophic** impact on objectives, irreversibly.	10

The level of risk that will be calculated in this section is the one before the adoption of control and treatment measures, which is called the inherent risk level. The results of the combinations of probability and consequence, classified according to the scale of risk levels presented in Table 4, can be expressed in an array, as exemplified in Table 5 (BRASIL, 2018).

Table 4. Risk Rating Scale (BRASIL, 2018, adapted).

LR (Low Risk)	MR (Medium Risk)	HR (High Risk)	ER (Extreme Risk)
0 – 0.9	1.0 – 3.9	4.0 – 7.9	8.0 – 10.0

Table 5. Risk Matrix (BRASIL, 2018, adapted).

CONSEQUENCE						
	Very High 10	1.0 MR	2.0 MR	5.0 HR	8.0 ER	10.0 ER
	High 8	8 LR	1.6 MR	4.0 HR	6.4 HR	8.0 ER
	Average 5	0.5 LR	1.0 MR	2.5 RM	4.0 HR	5.0 HR
	Low 2	0.2 LR	0.4 LR	1.0 MR	1.6 MR	2.0 MR
	Very Low 1	0.1 LR	0.2 LR	0.5 LR	0.8 LR	1.0 MR
		Very Low 0.1	Low 0.2	Average 0.5	High 0.8	Very High 1.0
		PROBABILITY				

For each risk presented in the study, the probability criteria were applied, which is the possibility of the threat being realized, and consequence, that are the losses that the threat can offer to the final activity of the judiciary, according to Tables 2 and 3. Then, the inherent risk was calculated using the aforementioned formula and classified according to the risk matrix (Table 5).

The result of the classification, according to the methodology adopted, is presented in Table 6. To estimate the probability and consequences, an analysis of the occurrences records

of the events listed in Table 1 was performed. In addition, the existing controls and the efficiency with which reduce the risks of each of the listed events were evaluated.

Table 6. Classification of identified risks (BRASIL, 2018, adapted).

ID	IDENTIFIED RISKS	PROBABILITY	CONSEQUENCE	INHERENT RISK LEVEL
1.	Fire in the Data Center	A (0.5)	VH (10)	HR (5.0)
2.	Unavailability of the main Internet access	L (0.2)	A (5)	MR (1.0)
3.	Unavailability of the electronic process system – e-Proc/TJTO	A (0.5)	A (5)	MR (2.5)
4.	Malicious code software attacks on workstations	A (0.5)	L (2)	MR (1.0)

As shown in Table 6, the event unavailability of the main Internet access was classified with a low probability, due to having occurred only twice in the period from 2012 to 2018. The consequence of this event, according to the criteria set out in Table 3, was classified as mean, since one of the impacts will be the unavailability of access to the judicial process system (e-Proc) by the external public. Although the e-Proc is one of the main systems of the Judiciary Tocantinense and its unavailability generate delays in the process progress, in general the risk of the unavailability of the main Internet link was considered medium because it is not of difficult recovery.

Another example of the event listed in Table 6 is fire in the Data Center. Its probability of occurrence was classified as mean because there are no efficient and effective controls to mitigate this threat. Although it has never occurred before, it is not impossible that at some point this will occur, since the recent history of fires in the building of the Court of Justice of the State of Tocantins brings an incident that occurred in August 2018. Its consequences were classified as high, because they generate a significant impact on the objectives of the Judiciary Tocantinense. Thus, by applying the established criteria, the risk is considered high and impacts in an important way in the jurisdictional services.

For the evaluation process, criteria were established for prioritization and treatment associated with risk levels as exemplified in Table 7. The documentation of this step usually consists of a list of the risks that require treatment, with their respective classifications and priorities.

Table 7. Criteria for prioritization and risk treatment (BRASIL, 2018, adapted).

RISK LEVEL	CRITERIA FOR PRIORITIZATION AND RISK TREATMENT
ER	Risk level far beyond risk appetite. Any risk at this level should be communicated to the Governance Committee and the General Board and have an immediate response.

HR	Risk level beyond risk appetite. Any risk at this level must be communicated to the General Board and have an action taken in a given period.
MR	Risk level within the risk appetite. Usually no special measures are required, but it requires monitoring the controls adopted to keep the risk at this level or reduce it at no additional cost.
LR	Risk level within the risk appetite. No special measures are required. Requires monitoring of the controls adopted to maintain the level of risk.

For each risk classified in the analysis stage, the criteria contained in Table 7 were applied. They were prioritized according to the level of risk and their probability of occurrence, in that order. Thus, a list was generated (Table 8) in which the first were placed those that could cause more damage to the judicial provision.

Table 8. List of risks requiring treatment.

ID	IDENTIFIED RISKS	RISK LEVEL	CONTROL
1.	Fire in the Data Center	HR	NO
2.	Unavailability of the electronic process system – e-Proc/TJTO	MR	YES
3.	Malicious code software attacks on workstations	MR	YES
4.	Unavailability of access to the main Internet	MR	YES

Table 8 presents four threats from the area of information technology that are correlated to the final activity of the judiciary. Of these, 75% are medium-risk and 25% high-risk threats. It can also be observed that three threats already have some control implemented treatment, corresponding to 75% of the total.

In this same table, a single high-risk threat was listed, and it has no treatment or control implemented. According to the criteria set out in table 7, high-risk threats must have an action taken in a given period and be communicated to the General Board of the Court of Justice of the State of Tocantins.

After the analysis and assessment of the risks that the infrastructure imposes on the judicial provision, it is possible to establish whether or not to treat threats based on their level of risk. Risk treatment involves the selection of one or more options to modify the level of each risk and the elaboration of treatment plans that, once implemented, will imply new controls or modification of existing ones (BRASIL, 2018).

Table 9 presents an analysis and risk assessment matrix, and the events related to these, their consequences, the existing controls and the level of risk assessed by the proposed method were identified. Table 10 presents an action plan and proposes solutions to the risks identified and analyzed, enumerating the measures to be taken, the necessary resources and the monitoring required to maintain effective risk management.

According to the risk analysis carried out in the study, 25% of the threats present a high risk to the institution's business and no control has yet been implemented to treat them

adequately. In this case, the institution accepts the risk for the momentary inability to take any measure on the risk.

As identified in Table 10, the action needed to treat the risk identified as high (fire in the Data Center) would be the implementation of a fire prevention and combat system, which requires financial resources, resources that the institution does not currently available.

The proposed action plan aims to maintain the existing controls, while maintaining the monitoring of threats, as well as proposing new controls to treat them. Even if several actions are implemented to address the identified threats, there will still be residual risk, which still remains after considering the effect of the responses adopted by the management to reduce the probability and impact of risks, including Internal controls and other actions.

Table 9. Analysis and risk Assessment matrix

IDENTIFIED RISK	CAUSES	CONSEQUENCES	IDENTIFIED CONTROLS	RISK LEVEL
Fire in the Data Center	1. Short circuit in the Data Center; 2. Short circuit on the premises of the building.	1. Partial or total destruction of the Data Center.	1. None	High Risk (5.0)
Unavailability of the electronic process system – e-Proc/TJTO	1. Human error (programming and configuration); 2. Failure to communicate with the database; 3. Failures in the services running on the application server.	1. Suspension of procedural deadlines; 2. User dissatisfaction; 3. Hearings reschedules.	1. Monitoring of system and infrastructure parameters by management software.	Medium risk (2.5)
Malicious code software attacks on workstations	1. Do not have antivirus installed; 2. Antivirus is out of date; 3. Improper access to malicious website; 4. Misuse of external storage devices.	1. Malfunction of the workstations; 2. Data theft; 3. Proliferation of malicious code programs for other workstations.	1. Enterprise Antivirus solution.	Medium Risk (1.0)
Unavailability of the main Internet access	1. Fiber optic disruption; 2. Failure, burning or stopping of network assets; 3. Cables disconnected accidentally; 4. Traffic overhead in the logical network.	1. Total unavailability of access to external services and systems; 2. Unavailability of external users in accessing the services and systems provided by the TJTO.	1. Monitoring of network assets via management software; 2. Service level Agreement (SLA) with the telecommunication operator.	Medium Risk (1.0)

Table 10. Action plan.

ACTION PLAN			
IDENTIFIED RISK	**PROPOSED ACTIONS**	**REQUIRED RESOURCES**	**MONITORING**
Fire in the Data Center	1. Implement fire prevention and combat system.	1. Financial availability; 2. Bidding process.	1. Monitoring by means of smoke sensors. 2. Reports of periodic preventive maintenance of all devices.
Unavailability of the electronic process system – e-Proc/TJTO	1. Analyze the failure presented and apply the necessary corrections; 2. Provide redundancy of service hosting; 3. Maintain network assets reserve.	1. Training of the human resources of the intervening areas regarding the unavailability of the service; 2. Allocate spare network assets.	1. System and infrastructure management via monitoring software.
Malicious code software attacks on workstations	1. Make users aware of information security; 2. Adopt policy of using external devices in the TJTO network.	1. Users ' awareness of the topic of information security; 2. Maintenance of the safety solution.	1. Monitoring of stations via antivirus administration server; 2. Device usage policy in the TJTO network.
Unavailability of the main Internet access	1. Enable redundant Internet binding and apply traffic controls; 2. Provide external access to the services and systems of the TJTO via redundant Internet linkage; 3. Configure the DNS service with the addresses of the redundant Internet operator; 4. Get autonomous system number (ASN).	1. Training of procedures regarding the unavailability of the service; 2. Technical consultancy; 3. Financial resources.	1. Monitoring via software of communication linkage availability and bandwidth utilization; 2. Pro-active monitoring of the carrier; 3. Service level Agreement (SLA).

CONCLUSION

According to the study, it was possible to verify the strong dependence of the primary activity of the Judiciary Tocantinense with the infrastructure of information technology, and most of the operations are digital, including the judicial process system, and the unavailability of information and communication technology resources greatly affects the functioning of the judiciary.

In this sense, it is possible to affirm that the activities of the judiciary have a significant degree of dependence in relation to the area of information technology, since this provides support for the judiciary to achieve its objectives.

The data collected in the study refer to the analysis carried out in the infrastructure area of the Court of Justice of the State of Tocantins. The most critical events of the organ were

mapped and identified in the analysis and risk assessment matrix (table 9). A plan of actions was proposed (table 10) with the measures to be taken, the necessary resources and the monitoring required to maintain effective risk management.

Considering that the studied environment has implemented security controls, but does not yet have a risk management policy or a risk monitoring plan for its structured and documented information technology infrastructure, it is believed that this study can help in making important decisions that help to treat risks identified during the realization of this research and that may affect the functioning of the judiciary.

Finally, it is understood that the management of information security risks should be implemented at the Court of Justice of the State of Tocantins in search of the protection of assets and to ensure the confidentiality, integrity, availability and authenticity of Information, your most valuable asset. Thus, the adoption of procedures that ensure the security of information must be a constant priority in the judiciary, in order to reduce failures and damages that may compromise the image of justice or bring harm to society.

ACKNOWLEDGEMENTS

We would like to thank the Court of Justice of the State of Tocantins for the institutional and financial support to accomplish this work. We also thank the Information Technology Board and the Coordination of Strategic Management for technical support in mapping the process of risk management and diagramation.

REFERENCES

ABNT. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 27005:2011: Tecnologia da Informação - Técnicas de Segurança - Gestão de Riscos de Segurança da Informação. Rio de Janeiro, 2011. 87 p.

ABNT. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 31000:2018: Gestão de Riscos - Diretrizes. Rio de Janeiro, 2018. 17 p.

ABNT. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 31010:2012: Gestão de Riscos - Técnicas para o processo de avaliação de riscos. Rio de Janeiro, 2012. 96 p.

BERMEJO, P. H. de S. et al. (2019) ForRisco: gerenciamento de riscos em instituições públicas na prática, 2 ed., Editora Evobiz, Brasília, Brasil. Disponível em: <http://forrisco.org/livro.php>. Acesso em: 29 ago. 2019.

BEZERRA, E. K. Gestão de Riscos de TI: NBR 27005. Rio de Janeiro: RNP/ESR, 2013. 138 p.; 28 cm.

BRASIL. TRIBUNAL DE CONTAS DA UNIÃO. Referencial básico de gestão de riscos / Tribunal de Contas da União. Brasília: TCU, Secretaria Geral de Controle Externo (Segecex), 2018. 154 p. Disponível em: <https://portal.tcu.gov.br/biblioteca-digital/referencial-basico-de-gestao-de-riscos.htm>. Acesso em: 5 out. 2018.

CNJ. CONSELHO NACIONAL DE JUSTIÇA. Segurança da Informação – Diretrizes para a gestão de segurança da informação no âmbito do Poder Judiciário. Brasília, 2012. Disponível em: <http://www.cnj.jus.br/images/dti/Comite_Gestao_TIC/Diretrizes_Gestao_SI_PJ.pdf>. Acesso em: 13 out. 2018.

CNJ. CONSELHO NACIONAL DE JUSTIÇA. Resolução n. 211, de 15 de dez. de 2015. Dispõe sobre a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário. Brasília, 2015. Disponível em: <http://www.cnj.jus.br///images/atos_normativos/resolucao/resolucao_211_15122015_18122015173345.pdf>. Acesso em: 13 out. 2018.

GERHARDT, T. E. Métodos de pesquisa. / [organizado por] Tatiana Engel Gerhardt e Denise Tolfo Silveira; coordenado pela Universidade Aberta do Brasil – UAB/UFRGS e pelo Curso de Graduação Tecnológica – Planejamento e Gestão para o Desenvolvimento Rural da SEAD/UFRGS. – Porto Alegre: Editora da UFRGS, 2009. 120 p.; 17,5x25cm. (Série Educação à Distância).

SÊMOLA, M. Gestão da segurança da informação: uma visão executiva. 2 ed. Rio de Janeiro: Elsevier, 2014.

SILVA, E. L. DA. Metodologia da pesquisa e elaboração de dissertação. Edna Lúcia da Silva, Estera Muszkat Menezes. – 4. ed. rev. atual. – Florianópolis: UFSC, 2005. 138p. Disponível em: <https://projetos.inf.ufsc.br/arquivos/Metodologia_de_pesquisa_e_elaboracao_de_teses_e_dissertacoes_4ed.pdf>. Acesso em: 13 jun. 2018.

TJTO. TRIBUNAL DE JUSTIÇA DO TOCANTINS. Portaria n. 3433, de 26 de jun. de 2017. Dispõe sobre a Política de Segurança da Informação (PSI). Palmas, 2017. Disponível em: <http://www.tjto.jus.br/tic/index.php/governanca-de-tic/documentos-normativos/send/98-normativas/1147-politica-de-seguranca-da-informacao>. Acesso em: 15 nov. 2018.

APÊNDICE C - Modelo de Relatório de Contextualização

PODER JUDICIÁRIO ESTADO DO TOCANTINS	**Unidade Organizacional:** Diretoria de Tecnologia da Informação – DTINF
GESTÃO DE RISCOS DE TIC	
RELATÓRIO DE CONTEXTUALIZAÇÃO	**DATA:**
Área: *<< Informar da divisão responsável pela avaliação dos riscos. >>*	
Gestor de Risco:	

1. Definição do escopo da avaliação de riscos

<< Descrever o escopo da avaliação de riscos (quais processos, subprocessos, atividades, tarefas, projetos, sistemas, ambientes, ativos terão os riscos avaliados e tratados). >>

2. Relevância do(s) processo(s)/ativo(s) na estratégia institucional

<< Identificar de que forma o processo/ativo que está sendo analisado quanto aos riscos contribui para o alcance dos objetivos organizacionais definidos no plano estratégico institucional. >>

3. Descrição do(s) processo(s)/ativo(s)

<< Descrever o processo que está sendo avaliado quanto aos riscos, além de levantar todos os ativos envolvidos. Se necessário avaliar as interações do processo com os demais processos da organização. Solicitar apoio do escritório de projetos para mapear fluxo do processo. >>

Processo/Ativo	Descrição	Responsável
<< Listar processo/ativo >>	*<< Descrever processo/ativo >>*	*<< Área responsável pelo processo/ativo.*

4. Partes interessadas e envolvidas no(s) processo(s)/ativo(s)

<< Identificar que são as partes interessadas, tanto interna quanto externamente, e as partes envolvidas no processo/ativo, no intuito de equilibrar os interesses das partes na execução da atividade e no processo de gerenciamento de riscos. >>

Partes Interessadas	
Internas	**Externas**
<< Listar as partes interessadas internas >>	*<< Listar as partes interessadas internas >>*
Partes Envolvidas	
<< Listar as partes envolvidas internamente >>	

APÊNDICE D - Modelo de Matriz de Identificação de Riscos de TIC

PODER JUDICIÁRIO ESTADO DO TOCANTINS	**Unidade Organizacional:** Diretoria de Tecnologia da Informação - DTINF	**Data:**
Gestor de Risco:		**Área:**

Matriz de Identificação de Riscos de TIC					
ID	**Ativo**	**Evento de Risco**	**Causa**	**Consequência**	**Controles Implementados**

APÊNDICE E - Modelo de Matriz de Análise e Avaliação de Riscos de TIC

PODER JUDICIÁRIO ESTADO DO TOCANTINS	**Unidade Organizacional:** Diretoria de Tecnologia da Informação - DTINF	**Data:**
Gestor de Risco:	**Área:**	

Matriz de Análise e Avaliação de Riscos de TIC									
ID	**Ativo**	**Evento de Risco**	**Causa**	**Consequência**	**P**	**S**	**R**	**P.S.R.**	**Nível de Risco**

APÊNDICE F - Modelo de Relatório de Avaliação de Riscos de TIC

PODER JUDICIÁRIO ESTADO DO TOCANTINS	**Unidade Organizacional:** Diretoria de Tecnologia da Informação – DTINF
GESTÃO DE RISCOS DE TIC	
RELATÓRIO DE AVALIAÇÃO DE RISCOS	**Data:**
Área: *<< Informar da divisão responsável pela avaliação dos riscos. >>*	
Gestor de Risco:	

1. Resumo da Avaliação de Riscos

<< Nesta Seção deverão ser resumidas as informações da etapa de identificação dos riscos, análise e avaliação dos riscos, levando em consideração os objetivos do levantamento, as bases de conhecimento utilizadas e o resultado da identificação (quantidade de riscos, de causas e de consequências). >>

Exemplo: O levantamento de riscos do processo/ativo XYZ teve como objetivo mapear as principais fontes de riscos, eventos, causas e consequências que podem vir a comprometer o alcance dos objetivos organizacionais. O mapa de riscos foi baseado nos serviços XYZ, em que são relevantes a identificação e o monitoramento dos riscos. Para tanto, foram levantadas informações em documentos gerados no processo, bem como o conhecimento e experiência de pessoas-chave no processo. Com isso, ao todo foram identificados 20 (vinte) eventos de riscos, 35 (trinta e cinco) causas e 30 (trinta) consequências.

<< Deverá constar como anexo a esse documento a Matriz de Identificação de Riscos. >>

2. Metodologia Adotada

<< Neste campo deverá ser explicada a metodologia adotada para a identificação, análise e avaliação dos riscos. É importante pontuar quais as técnicas utilizadas para a identificação dos riscos, bem como a abrangência do estudo inicial. A forma de cálculo dos parâmetros da análise de riscos e do nível de risco referente à avaliação deve ser citada, porém sem detalhamentos, haja vista se encontrar no Manual de Gestão de Riscos de TIC. >>

Exemplo: Na etapa de identificação dos riscos foram utilizadas as técnicas de brainstorming e de análise de fluxograma para mapear as fontes de risco e chegar aos possíveis eventos, bem como suas causas e consequências. Para tanto, a equipe do projeto se reuniu com pessoas-chave no processo analisado, tendo previamente desenhado junto com a COGES o fluxograma básico do processo. Com os riscos identificados, foram aplicados os critérios definidos no Manual de Gestão de Riscos do TJTO para classificar a relevância do processo, a probabilidade de ocorrência dos eventos e a severidade do impacto das consequências para os objetivos organizacionais. Com os parâmetros aplicados, foi realizado o cálculo do nível de risco, conforme a metodologia adotada (produto entre os parâmetros e aplicação na faixa de nível de risco).

<< Deverá constar como anexo a esse documento a Matriz de Avaliação de Riscos. >>

3. Conclusões

3.1. Riscos identificados por ativo

<< Neste campo, deve ser apresentada uma lista dos riscos identificados por ativo com sua classificação e se eles possuem ou não algum controle implementado. >>

ATIVO	RISCO IDENTIFICADO	CONTROLE

<< Comentário sobre as informações prestadas. >>

3.2. Quantidade de riscos por nível

<< Nesse campo, devem ser apresentados a quantidade e o percentual de risco por nível, além de um breve comentário sobre as informações apresentadas. >>

NÍVEL	QUANTIDADE DE RISCOS	PERCENTUAL
Muito Alto		
Alto		
Médio		
Baixo		
Muito Baixo		
TOTAL		

PODER JUDICIÁRIO ESTADO DO TOCANTINS	**Unidade Organizacional:** Diretoria de Tecnologia da Informação - DTINF	**Data:**
Gestor de Risco:		**Área:**

Matriz de Identificação de Riscos de TIC					
ID	**Ativo**	**Evento de Risco**	**Causa**	**Consequência**	**Controles Implementados**

PODER JUDICIÁRIO ESTADO DO TOCANTINS	**Unidade Organizacional:** Diretoria de Tecnologia da Informação - DTINF	**Data:**
Gestor de Risco:	**Área:**	

Matriz de Análise e Avaliação de Riscos de TIC									
ID	**Ativo**	**Evento de Risco**	**Causa**	**Consequência**	**P**	**S**	**R**	**P.S.R.**	**Nível de Risco**

APÊNDICE G - Modelo de Matriz de Priorização dos Riscos de TIC

PODER JUDICIÁRIO ESTADO DO TOCANTINS	**Unidade Organizacional:** Diretoria de Tecnologia da Informação - DTINF	**Data:**
Gestor de Risco:	**Área:**	

Matriz de Priorização de Riscos de TIC						
ID	**Ativo**	**Evento de Risco**	**Causa**	**Consequência**	**NRI**	**Resposta ao Risco**

NRI (Nível de Risco Inerente): 1 – Muito Baixo, 2 – Baixo, 3 – Médio, 4 – Alto, 5 – Muito Alto
Resposta ao Risco: 1 – Evitar, 2 – Mitigar, 3 – Compartilhar, 4 - Aceitar

APÊNDICE H - Modelo de Plano de Tratamento de Riscos de TIC

PODER JUDICIÁRIO ESTADO DO TOCANTINS	**Unidade Organizacional:** Diretoria de Tecnologia da Informação – DTINF
GESTÃO DE RISCOS DE TIC	
PLANO DE TRATAMENTO DE RISCOS	**Data:**
Área: *<< Informar da divisão responsável pela avaliação dos riscos. >>*	
Gestor de Risco:	

1. Apresentação

<< Apresentar de forma resumida o resultado da avaliação de riscos e demonstrar a importância do tratamento dos riscos priorizados >>

2. Priorização dos Riscos

<< Apresentar a matriz de priorização de riscos >>

Matriz de Priorização de Riscos de TIC						
ID	**Ativo**	**Evento de Risco**	**Causa**	**Consequência**	**NRI**	**Resposta ao Risco**

NRI (Nível de Risco Inerente): 1 – Muito Baixo, 2 – Baixo, 3 – Médio, 4 – Alto, 5 – Muito Alto
Resposta ao Risco: 1 – Evitar, 2 – Mitigar, 3 – Compartilhar, 4 – Aceitar

3. Tratamento dos Riscos

<< Apresentar o plano de tratamento de riscos >>

Matriz de Tratamento de Riscos de TIC						
Evento de Risco	**Controles**	**Descrição**	**Monitoramento**	**Responsável**	**Prazo**	**Nível de Risco Pretendido**
						Atual Pretendido
						Atual Pretendido

Explicação sobre cada campo do plano de tratamento.	
Evento de Risco	Risco priorizado conforme tabela de priorização de riscos para tratamento.
Controles	Controles propostos para o risco em tratamento.
Descrição	Descrição detalhada dos tratamentos, incluindo os custos.
Monitoramento	Detalhes de como se dará o monitoramento e análise crítica do risco e seu tratamento após sua implementação.
Responsável	Servidor responsável pela implementação do tratamento.
Prazo	Prazo para a implementação dos controles.
Nível de Risco Pretendido	Informar se o tratamento atacou a probabilidade e/ou a consequência do risco, informando os novos valores do cálculo do risco e seu novo nível de risco.

APÊNDICE I - Modelo de Formulário de Comunicação e Consulta

PODER JUDICIÁRIO ESTADO DO TOCANTINS	**Unidade Organizacional:** Diretoria de Tecnologia da Informação – DTINF
GESTÃO DE RISCOS DE TIC	
FORMULÁRIO DE COMUNICAÇÃO E CONSULTA	**Data:**

5. Atividades

<< Todas as atividades de comunicação e consulta durante o processo de avaliação e tratamento dos riscos devem ser descritas na matriz abaixo. >>

Partes Interessadas e Envolvidas	Comunicador	Propósito	Conteúdo	Meio de Comunicação	Data	Frequência

APÊNDICE J - Modelo de Relatório de Monitoramento e Análise Crítica

PODER JUDICIÁRIO ESTADO DO TOCANTINS	**Unidade Organizacional:** Diretoria de Tecnologia da Informação – DTINF
GESTÃO DE RISCOS DE TIC	
MONITORAMENTO E ANÁLISE CRÍTICA	**DATA:**
Área: *<< Informar da divisão responsável pela etapa de monitoramento e análise crítica. >>*	
Gestor de Risco:	

Descrição do Risco					
ID	**Causas**		**Evento**		**Consequências**
Análise e Avaliação do Risco (Probabilidade, Severidade e Relevância)					
Ano	**P**	**S**	**R**	**P.S.R.**	**Nível de Risco Inerente**

Observações sobre a análise e avaliação do risco:
<< Explicar sobre a avaliação da probabilidade, severidade e relevância. >>

Resposta ao risco:
<< Definir uma resposta ao risco (evitar, mitigar, compartilhar ou aceitar) e justificar. >>

Controle existente:

Controle Novo:
<< Novo controle sugerido após a definição da resposta ao risco. >>

Execução e Monitoramento do Controle Novo:
<< Breve descrição do novo controle implementado, o andamento da implementação e o responsável. >>

Apuração do Risco Residual		
Risco Inerente	**Risco de Controle**	**Risco Residual**

Observação:
<< A atividade de Monitoramento e Análise Crítica pode gerar recomendações de melhorias para o tratamento do risco. >>

Avaliação dos controles	Risco de Controle
Controles inexistentes.	Muito Alto 1,0
Controle fraco, tendem a ser aplicados caso a caso e a responsabilidade é individual, dependendo das pessoas envolvidas.	Alto 0,8
Controles implementados mitigam alguns aspectos do risco, mas não contemplam todos os aspectos relevantes do risco devido a deficiências no desenho ou nas ferramentas utilizadas.	Médio 0,6
Controles implementados e sustentados por ferramentas adequadas e, embora passíveis de aperfeiçoamento, mitigam o risco satisfatoriamente.	Baixo 0,4
Controles implementados podem ser considerados a “melhor prática”, mitigando todos os aspectos relevantes do risco	Muito Baixo 0,2

APÊNDICE K – Relatório de Contextualização Validado

PODER JUDICIÁRIO ESTADO DO TOCANTINS	**Unidade Organizacional:** Diretoria de Tecnologia da Informação – DTINF
GESTÃO DE RISCOS DE TIC	
RELATÓRIO DE CONTEXTUALIZAÇÃO	**DATA: 03/12/2019**
Área: Divisão de Administração e Segurança de Redes - DASR	
Gestor de Risco: Danillo Lustosa Wanderley	

1. Definição do escopo da avaliação de riscos

O objetivo é elaborar um plano para avaliação e tratamento de riscos relacionados ao *Data Center* do Poder Judiciário do Estado do Tocantins e seus ativos. A ideia é que o processo de avaliação de riscos forneça um mapeamento sobre as vulnerabilidades existentes e as ameaças às quais esse ambiente está sujeito e, com isso, propor as medidas necessárias para o tratamento dos riscos identificados.

2. Relevância do(s) processo(s)/ativo(s) na estratégia institucional

O *Data Center* é um ambiente projetado para abrigar a infraestrutura tecnológica, onde ocorre todo o processamento e armazenamento das informações, de modo a atender as demandas do Poder Judiciário do Estado Tocantins.

Como a maior parte das operações do Poder Judiciário do Estado do Tocantins é digital, o ambiente computacional apresenta uma relevância muita alta para a realização da atividade precípua do órgão em questão. A indisponibilidade dos recursos de TIC afeta sobremaneira o funcionamento do Judiciário, pois causa atrasos e interrompe atividades que são realizadas rotineiramente.

3. Descrição do(s) processo(s)/ativo(s)

O *Data Center* possui arquitetura modular e tem como missão proteger, com fonte de energia ininterrupta e climatização, todos os equipamentos de TIC e sistemas computacionais do Poder Judiciário do Tocantins. Possui racks de TIC, réguas de distribuição de energia (PDU), painéis e quadros elétricos, sistema de gerenciamento e monitoramento ambiental por meio de dispositivos visuais e sensoriais (câmeras e sensores de temperatura, humidade, ponto de orvalho e de fumaça).

Para garantir eficiência e alta disponibilidade, foram instalados dois *sites*, sendo um principal localizado no prédio do Tribunal de Justiça, e um de *backup* no Fórum de Palmas. Ambos os *sites* possuem leitor biométrico nas portas corta-fogo e câmeras de

monitoramento. Por meio do software de gerência os dois ambientes são monitorados e são obtidas informações de cada componente existente.

Ativo	Descrição	Responsável
Servidores	Equipamento utilizado para armazenamento e processamento de dados.	Divisão de Administração e Segurança de Redes.
Switches Core	Equipamento central da rede com grande capacidade de comutação de pacotes e com portas de alta velocidade (1 Gbps, 10 Gbps ou mais).	Divisão de Administração e Segurança de Redes.
Firewall	Solução de segurança baseada em *hardware / software* que, a partir de um conjunto de regras ou instruções, analisa o tráfego de rede para determinar quais operações de transmissão ou recepção de dados podem ser executadas.	Divisão de Administração e Segurança de Redes.
Solução de Virtualização	Solução que permite criar vários ambientes simulados ou recursos dedicados a partir de um único sistema de *hardware* físico. O *software* chamado *hypervisor* conecta-se diretamente ao hardware e possibilita a divisão de um único sistema em ambientes distintos, separados e seguros, conhecidos como máquinas virtuais.	Divisão de Administração e Segurança de Redes.
Enlace de Internet Principal	Provedor de Serviço de Internet Principal (500 MB).	Divisão de Administração e Segurança de Redes.
Enlace de Internet Redundante	Provedor de Serviço de Internet Redundante (100 MB)	Divisão de Administração e Segurança de Redes.
Meios de transmissão	Cabeamento estruturado e fibra óptica.	Divisão de Administração e Segurança de Redes.
Sistema Elétrico	Fornecimento e monitoramento de energia elétrica.	Divisão de Administração e Segurança de Redes.
Sistema de Climatização	Ares-condicionados de precisão, condensadoras, sensores de temperatura e umidade.	Divisão de Administração e Segurança de Redes.

4. Partes interessadas e envolvidas no(s) processo(s)/ativo(s)

Partes Interessadas	
Internas	**Externas**
Presidência do Tribunal. Comitê Gestor de Segurança da Informação. Diretoria Geral.	Profissionais ligados ao Judiciário.

Partes Envolvidas
Diretoria de Tecnologia da Informação. Comitê Gestor de TIC. Divisão de Administração e Segurança de Redes. Divisão de Banco de Dados. Divisão de Sistemas. Divisão de Manutenção e Suporte ao Usuário. Serviço de Telecomunicação.

APÊNDICE L – Relatório de Avaliação de Riscos Validado

PODER JUDICIÁRIO ESTADO DO TOCANTINS	**Unidade Organizacional:** Diretoria de Tecnologia da Informação – DTINF
GESTÃO DE RISCOS DE TIC	
RELATÓRIO DE AVALIAÇÃO DE RISCOS	**Data: 04/12/2019**
Área: Divisão de Administração e Segurança de Redes	
Gestor de Risco: Danillo Lustosa Wanderley	

1. Resumo da Avaliação de Riscos

O levantamento de riscos relacionados ao *Data Center* e aos sistemas de processo judicial e administrativo teve como objetivo mapear as principais fontes de riscos, eventos, causas e consequências que possam impactar na atividade principal do Judiciário Tocantinense. O mapa de riscos foi baseado na infraestrutura de TIC, em que são relevantes a identificação e o monitoramento dos riscos. Para tanto, foram realizadas reuniões com integrantes da área de segurança de redes com o intuito de levantar as ameaças às quais a infraestrutura tecnológica está sujeita e com isso elaborar o plano de tratamento de riscos. Ao todo foram identificados 16 (dezesseis) eventos de riscos, 40 (quarenta) causas e 36 (trinta e seis) consequências.

2. Metodologia Adotada

Para o desenvolvimento dessa análise, foram utilizados os conceitos propostos pelo Manual de Gestão de Riscos em Segurança da Informação do Poder Judiciário do Tocantins.

Na etapa de identificação dos riscos, foram realizadas reuniões com integrantes da área de segurança de redes e utilizadas a técnica de *Brainstorming*, que consiste em reunir pessoas conhecedoras de certo ativo ou atividade organizacional e incentivar o fluxo livre de conversação entre elas com o objetivo de identificar possíveis perigos, riscos ou controles associados ao objeto analisado, e também a de Análise Preliminar de Perigos (APP), que é semelhante a anterior. Nessa técnica, as pessoas que detenham informações sobre o objeto da análise são reunidas em grupo. Os participantes consideram as informações existentes, tais como atividades, recursos, ambiente, interfaces entre os diversos elementos e os objetivos a alcançar e produzem, de comum acordo, uma lista de situações perigosas ou de riscos.

Com os riscos identificados, foram aplicados os critérios definidos no Manual de Gestão de Riscos para classificar a relevância do processo, a probabilidade de ocorrência dos

eventos e a severidade do impacto das consequências para os objetivos organizacionais. Com os parâmetros aplicados, foi realizado o cálculo do nível de risco, conforme a metodologia adotada (produto entre os parâmetros e aplicação na faixa de nível de risco).

3. Conclusões

3.1. Riscos identificados por ativo

Aqui é apresentada uma lista dos riscos identificados por ativo e se eles possuem ou não algum controle implementado.

ATIVO	RISCO IDENTIFICADO	CONTROLE
Data Center	Acesso não autorizado ao *Data Center.*	SIM
Data Center	Inundação.	NÃO
Data Center	Incêndio.	NÃO
Data Center	Falha nos ares-condicionados de precisão.	SIM
Data Center	Interrupção no fornecimento de energia elétrica.	SIM
Data Center	Falha no gerador.	SIM
Data Center	Falha nos *nobreaks.*	SIM
Firewall	Falha ou dano permanente no *Firewall.*	SIM
Switch	Falha ou dano permanente no s*witch core.*	SIM
Solução de Virtualização	Falha ou dano permanente na solução de virtualização.	SIM
Enlace de Internet Principal	Indisponibilidade de acesso à Internet Principal.	SIM
Enlace de Internet Redundante	Indisponibilidade de acesso à Internet Redundante.	SIM
Servidor de Rede	Falha ou indisponibilidade do servidor de arquivos.	SIM
Servidor de Rede	Acesso não autorizado às pastas e arquivos departamentais.	SIM
e-Proc	Indisponibilidade do sistema de processo judicial eletrônico.	SIM
SEI	Indisponibilidade do sistema eletrônico de informações.	SIM

Constam neste relatório a matriz de identificação de riscos, que é uma lista com os riscos identificados contendo causas e consequências; e a matriz de análise e avaliação, que é um documento que demonstra o nível de risco encontrado na análise e sua classificação.

3.2. Quantidade de riscos por nível

NÍVEL	QUANTIDADE DE RISCOS	PERCENTUAL
Muito Alto	**1**	**6,25 %**
Alto	**9**	**56,25 %**
Médio	**6**	**37,5 %**
Baixo	**0**	**0 %**
Muito Baixo	**0**	**0 %**
TOTAL	**16**	

Como apresentado na tabela do item 3.2, 6,25% das ameaças são de risco muito alto, 56,25% de alto risco e 37,5% de médio risco. Com os dados apresentados no item 3.1, é possível observar que das 16 (dezesseis) ameaças identificadas somente 2 (duas) não possuem algum controle de tratamento implementado.

Após a análise e avaliação dos riscos que a infraestrutura impõe sobre a prestação jurisdicional, pode-se estabelecer a possibilidade ou não de tratamento das ameaças com base no seu nível de risco.

PODER JUDICIÁRIO ESTADO DO TOCANTINS	**Unidade Organizacional:** Diretoria de Tecnologia da Informação - DTINF	**Data: 04/12/2019**
Gestor de Risco: Danillo Lustosa Wanderley	**Área: Divisão de Administração e Segurança de Redes**	

Matriz de Identificação de Riscos de TIC					
ID	**Ativo**	**Evento de Risco**	**Causa**	**Consequência**	**Controles Implementados**
1	*Data Center*	Acesso não autorizado ao *Data Center.*	1. Falha no controle de acesso físico.	1. Poderá haver danos a infraestrutura e serviços de TIC; 2. Roubo de informações; 3. Desconfigurarão de dispositivos.	1. Leitor com biometria; 2. Câmeras de monitoramento.
2	*Data Center*	Inundação.	Alagamento causado por: 1. Excesso de chuva; 2. Rompimento de tubulação.	1. Destruição parcial ou total dos equipamentos do *Data Center*; 2. Indisponibilidade parcial ou total dos serviços e sistemas.	1. Nenhum.
3	*Data Center*	Incêndio.	1. Curto circuito no *Data Center*; 2. Curto circuito nas dependências do prédio.	1. Destruição parcial ou total do *Data Center;* 2. Interrupção parcial ou total dos serviços e sistemas.	1. Nenhum.
4	*Data Center*	Falha nos ares-condicionados de precisão.	1. Defeito ou queima de componentes.	1. Parada total dos ares-condicionados; 2. Aumento da temperatura ambiente; 3. Sobreaquecimento dos equipamentos de TIC.	1. Dois ares-condicionados como *backup.*
5	*Data Center*	Interrupção no fornecimento de energia elétrica.	1. Falha por parte da concessionaria; 2. Falha na subestação do prédio; 3. Parada programada no fornecimento de energia.	1. Desligamento dos ativos de rede; 2. Possível indisponibilidade de serviços e sistemas.	1. *Nobreak*; 2. Grupo gerador.
6	*Data Center*	Falha no gerador.	1. Falta de combustível; 2. Bateria descarregada; 3. Vida útil das peças comprometida;	1. Descarga completa das baterias dos nobreaks; 2. Interrupção no fornecimento de energia para o Data Center;	1. Manutenção preditiva, preventiva e corretiva mensal.

			4. Falha em algum componente; 5. Falta de manutenção preventiva.	3. Desligamento de todos os equipamentos; 4. Indisponibilidade dos serviços e sistemas providos pelo TJTO.	
7	*Data Center*	Falha nos *nobreaks.*	1. Curto-circuito nos *nobreaks*; 2. Módulos ou baterias danificadas.	1. Desligamento inesperado de todos os equipamentos de TIC. 2. Indisponibilidade de todos os serviços e sistemas.	1. Redundância nos módulos de potência do *nobreak*; 2. Bancos de bateria de alta autonomia; 3. Manutenção preditiva, preventiva e corretiva mensal.
8	*Firewall*	Falha ou dano permanente no *Firewall.*	1. Falha ou parada do equipamento; 2. Erro humano (configuração).	1. Indisponibilidade total dos acessos a rede, serviços e sistemas para usuários internos e externos.	1. Backup da configuração; 2. Dois equipamentos ligados em HA (*High-Availability*); 3. Suporte e garantia dos equipamentos com processo de autorização de troca (RMA - *Return Merchandise Authorization*).
9	*Switch*	Falha ou dano permanente no s*witch core.*	1. Falha, queima ou parada do equipamento.	1. Indisponibilidade total de acesso a serviços e sistemas internos e externos.	1. Monitoramento do ativo de rede via software de gerenciamento; 2. Equipamento reserva.
10	Solução de Virtualização	Falha ou dano permanente na solução de virtualização.	1. Falha ou parada dos servidores; 2. Erro humano (configuração);	1. Indisponibilidades das máquinas virtuais; 2. Indisponibilidade de acesso aos serviços e sistemas.	1. Redundância de equipamentos no *site backup*; 2. Suporte e garantia dos equipamentos com processo de autorização de troca (*RMA - Return Merchandise Authorization*).
11	Enlace de Internet Principal	Indisponibilidade de acesso à Internet Principal.	1. Rompimento de fibra óptica; 2. Falha, queima ou parada dos ativos de rede; 3. Cabos desconectados acidentalmente; 4. Sobrecarga de tráfego na rede lógica.	1. Indisponibilidade total dos acessos a serviços e sistemas externos; 2. Indisponibilidades dos usuários externos em acessar os serviços e sistemas providos pelo TJTO.	1. Monitoramento dos ativos de rede via software de gerenciamento; 2. Acordo de níveis de serviços (ANS) junto a operadora de telecomunicação;

					3. Enlace de Internet Redundante.
12	Enlace de Internet Redundante	Indisponibilidade de acesso à Internet Redundante.	1. Rompimento de fibra óptica; 2. Falha, queima ou parada dos ativos de rede; 3. Cabos desconectados acidentalmente; 4. Sobrecarga de tráfego na rede lógica.	1. Indisponibilidade do acesso à Internet via enlace de dados redundante.	1. Monitoramento dos ativos de rede via software de gerenciamento; 2. Acordo de níveis de serviços (ANS) junto a operadora de telecomunicação.
13	Servidor de Rede	Falha ou indisponibilidade do servidor de arquivos.	1. Erro humano (configuração); 2. Falha, queima ou parada do equipamento; 3. Falha, queima ou parada do switch de rede.	1. Indisponibilidade dos serviços de rede (acesso a pastas e arquivos, autenticação de usuários, acessos a serviços e sistemas internos e externos); 2. Falha no serviço de DHCP.	1. Monitoramento do ativo de rede via software de gerenciamento; 2. Gerenciamento via iLO do servidor para analisar a falha; 3. Equipamento reserva.
14	Servidor de Rede	Acesso não autorizado às pastas e arquivos departamentais.	1. Erro humano (Configuração de permissões de acesso); 2. Engenharia social.	1. Acesso indevido a informações importantes; 2. Cópia ou destruição de dados sigilosos ou restritos.	1. Política de controle de acesso; 2. Auditoria; 3. Registro (logs) dos acessos dos usuários.
15	e-Proc	Indisponibilidade do sistema de processo judicial eletrônico.	1. Erro humano (programação e configuração); 2. Falha de comunicação com o banco de dados; 3. Falhas nos serviços que são executados no servidor de aplicação.	1. O sistema fica indisponível aos usuários internos e externos; 2. Suspensão de prazos processuais; 3. Insatisfação dos usuários; 4. Reagendamentos de audiências.	1. Monitoramento de parâmetros do sistema e de infraestrutura através de software de gerenciamento.
16	SEI	Indisponibilidade do sistema eletrônico de informações.	1. Erro humano (programação e configuração); 2. Falha de comunicação com o banco de dados; 3. Falhas nos serviços que são executados no servidor de aplicação.	1. O sistema fica indisponível aos usuários internos e externos; 2. Insatisfação dos usuários; 3. Atraso no andamento dos processos administrativos do TJTO.	1. Monitoramento de parâmetros do sistema e de infraestrutura através de software de gerenciamento.

PODER JUDICIÁRIO ESTADO DO TOCANTINS	**Unidade Organizacional:** Diretoria de Tecnologia da Informação - DTINF	**Data: 04/12/2019**
Gestor de Risco: Danillo Lustosa Wanderley	**Área: Divisão de Administração e Segurança de Redes**	

Matriz de Análise e Avaliação de Riscos de TIC									
ID	**Ativo**	**Evento de Risco**	**Causa**	**Consequência**	**P**	**S**	**R**	**P.S.R.**	**Nível de Risco**
1	*Data Center*	Acesso não autorizado ao *Data Center.*	1. Falha no controle de acesso físico.	1. Poderá haver danos a infraestrutura e serviços de TIC; 2. Roubo de informações; 3. Desconfigurarão de dispositivos.	3	3	5	45	**Alto**
2	*Data Center*	Inundação.	Alagamento causado por: 1. Excesso de chuva; 2. Rompimento de tubulação.	1. Destruição parcial ou total dos equipamentos do *Data Center*; 2. Indisponibilidade parcial ou total dos serviços e sistemas.	2	3	5	30	**Médio**
3	*Data Center*	Incêndio.	1. Curto circuito no *Data Center*; 2. Curto circuito nas dependências do prédio.	1. Destruição parcial ou total do *Data Center;* 2. Interrupção parcial ou total dos serviços e sistemas.	3	5	5	75	**Muito Alto**
4	*Data Center*	Falha nos ares-condicionados de precisão.	1. Defeito ou queima de componentes.	1. Parada total dos ares-condicionados; 2. Aumento da temperatura ambiente; 3. Sobreaquecimento dos equipamentos de TIC.	3	3	5	45	**Alto**
5	*Data Center*	Interrupção no fornecimento de energia elétrica.	1. Falha por parte da concessionaria; 2. Falha na subestação do prédio; 3. Parada programada no fornecimento de energia.	1. Desligamento dos ativos de rede; 2. Possível indisponibilidade de serviços e sistemas.	3	3	5	45	**Alto**

6	*Data Center*	Falha no gerador.	1. Falta de combustível; 2. Bateria descarregada; 3. Vida útil das peças comprometida; 4. Falha em algum componente; 5. Falta de manutenção preventiva.	1. Descarga completa das baterias dos nobreaks; 2. Interrupção no fornecimento de energia para o Data Center; 3. Desligamento de todos os equipamentos; 4. Indisponibilidade dos serviços e sistemas providos pelo TJTO.	3	2	5	30	**Médio**
7	*Data Center*	Falha nos *nobreaks.*	1. Curto-circuito nos *nobreaks*; 2. Módulos ou baterias danificadas.	1. Desligamento inesperado de todos os equipamentos de TIC. 2. Indisponibilidade de todos os serviços e sistemas.	2	2	5	20	**Médio**
8	*Firewall*	Falha ou dano permanente no *Firewall.*	1. Falha ou parada do equipamento; 2. Erro humano (configuração).	1. Indisponibilidade total dos acessos a rede, serviços e sistemas para usuários internos e externos.	2	5	5	50	**Alto**
9	*Switch*	Falha ou dano permanente no s*witch core.*	1. Falha, queima ou parada do equipamento.	1. Indisponibilidade total de acesso a serviços e sistemas internos e externos.	2	5	5	50	**Alto**
10	Solução de Virtualização	Falha ou dano permanente na solução de virtualização.	1. Falha ou parada dos servidores; 2. Erro humano (configuração);	1. Indisponibilidades das máquinas virtuais; 2. Indisponibilidade de acesso aos serviços e sistemas.	2	5	5	50	**Alto**
11	Enlace de Internet Principal	Indisponibilidade de acesso à Internet Principal.	1. Rompimento de fibra óptica; 2. Falha, queima ou parada dos ativos de rede; 3. Cabos desconectados acidentalmente; 4. Sobrecarga de tráfego na rede lógica.	1. Indisponibilidade total dos acessos a serviços e sistemas externos; 2. Indisponibilidades dos usuários externos em acessar os serviços e sistemas providos pelo TJTO.	3	3	5	45	**Alto**

12	Enlace de Internet Redundante	Indisponibilidade de acesso à Internet Redundante.	1. Rompimento de fibra óptica; 2. Falha, queima ou parada dos ativos de rede; 3. Cabos desconectados acidentalmente; 4. Sobrecarga de tráfego na rede lógica.	1. Indisponibilidade do acesso à Internet via enlace de dados redundante.	3	3	2	18	**Médio**
13	Servidor de Rede	Falha ou indisponibilidade do servidor de arquivos.	1. Erro humano (configuração); 2. Falha, queima ou parada do equipamento; 3. Falha, queima ou parada do switch de rede.	1. Indisponibilidade dos serviços de rede (acesso a pastas e arquivos, autenticação de usuários, acessos a serviços e sistemas internos e externos); 2. Falha no serviço de DHCP.	2	3	3	18	**Médio**
14	Servidor de Rede	Acesso não autorizado às pastas e arquivos departamentais.	1. Erro humano (Configuração de permissões de acesso); 2. Engenharia social.	1. Acesso indevido a informações importantes; 2. Cópia ou destruição de dados sigilosos ou restritos.	3	3	3	27	**Médio**
15	e-Proc	Indisponibilidade do sistema de processo judicial eletrônico.	1. Erro humano (programação e configuração); 2. Falha de comunicação com o banco de dados; 3. Falha nos serviços que são executados no servidor de aplicação.	1. O sistema fica indisponível aos usuários internos e externos; 2. Suspensão de prazos processuais; 3. Insatisfação dos usuários; 4. Reagendamentos de audiências.	3	3	5	45	**Alto**
16	SEI	Indisponibilidade do sistema eletrônico de informações.	1. Erro humano (programação e configuração); 2. Falha de comunicação com o banco de dados; 3. Falha nos serviços que são executados no servidor de aplicação.	1. O sistema fica indisponível aos usuários internos e externos; 2. Insatisfação dos usuários; 3. Atraso no andamento dos processos administrativos do TJTO.	3	3	5	45	**Alto**

APÊNDICE M – Plano de Tratamento de Riscos Validado

PODER JUDICIÁRIO ESTADO DO TOCANTINS	**Unidade Organizacional:** Diretoria de Tecnologia da Informação – DTINF
GESTÃO DE RISCOS DE TIC	
PLANO DE TRATAMENTO DE RISCOS	**Data: 05/12/2019**
Área: Divisão de Administração e Segurança de Redes	
Gestor de Risco: Danillo Lustosa Wanderley	

1. Apresentação

O levantamento de riscos relacionados ao *Data Center* e aos sistemas de processo judicial e administrativo teve como objetivo mapear as principais fontes de riscos, eventos, causas e consequências que possam impactar na atividade principal do Judiciário Tocantinense.

O mapa de riscos foi baseado na infraestrutura de TIC, em que são relevantes a identificação e o monitoramento dos riscos. Para tanto, foram realizadas reuniões com integrantes da área de segurança de redes com o intuito de levantar as ameaças às quais a infraestrutura tecnológica está sujeita e com isso elaborar o plano de tratamento de riscos.

Ao todo foram identificados 16 (dezesseis) eventos de riscos, 40 (quarenta) causas e 36 (trinta e seis) consequências. Desses dezesseis eventos identificados, somente dois não possuem algum controle de tratamento implementado.

Tabela 1. Quantidade de riscos por nível

NÍVEL	QUANTIDADE DE RISCOS	PERCENTUAL
Muito Alto	**1**	**6,25 %**
Alto	**9**	**56,25 %**
Médio	**6**	**37,5 %**
Baixo	**0**	**0 %**
Muito Baixo	**0**	**0 %**
Total	**16**	

2. Priorização dos Riscos

Matriz de Priorização de Riscos de TIC						
ID	**Ativo**	**Evento de Risco**	**Causa**	**Consequência**	**NRI**	**Resposta ao Risco**
1	*Data Center*	Incêndio.	1. Curto circuito no *Data Center*; 2. Curto circuito nas dependências do prédio.	1. Destruição parcial ou total do *Data Center;* 2. Interrupção parcial ou total dos serviços e sistemas.	**Muito Alto (PSR 75)**	**Mitigar**
2	*Firewall*	Falha ou dano permanente no *Firewall.*	1. Falha ou parada do equipamento; 2. Erro humano (configuração).	1. Indisponibilidade total dos acessos a rede, serviços e sistemas para usuários internos e externos.	**Alto (PSR 50)**	**Mitigar**
3	*Switch*	Falha ou dano permanente no s*witch core.*	1. Falha, queima ou parada do equipamento.	1. Indisponibilidade total de acesso a serviços e sistemas internos e externos.	**Alto (PSR 50)**	**Mitigar**
4	Solução de Virtualização	Falha ou dano permanente na solução de virtualização.	1. Falha ou parada dos servidores; 2. Erro humano (configuração);	1. Indisponibilidades das máquinas virtuais; 2. Indisponibilidade de acesso aos serviços e sistemas.	**Alto (PSR 50)**	**Mitigar**
5	e-Proc	Indisponibilidade do sistema de processo judicial eletrônico.	1. Erro humano (programação e configuração); 2. Falha de comunicação com o banco de dados; 3. Falhas nos serviços que são executados no servidor de aplicação.	1. O sistema fica indisponível aos usuários internos e externos; 2. Suspensão de prazos processuais; 3. Insatisfação dos usuários; 4. Reagendamentos de audiências.	**Alto (PSR 45)**	**Mitigar**
6	SEI	Indisponibilidade do sistema eletrônico de informações.	1. Erro humano (programação e configuração); 2. Falha de comunicação com o banco de dados; 3. Falhas nos serviços que são executados no servidor de aplicação.	. O sistema fica indisponível aos usuários internos e externos; 2. Insatisfação dos usuários; 3. Atraso no andamento dos processos administrativos do TJTO.	**Alto (PSR 45)**	**Mitigar**

7	*Data Center*	Falha nos ares-condicionados de precisão.	1. Defeito ou queima de componentes.	1. Parada total dos ares-condicionados; 2. Aumento da temperatura ambiente; 3. Sobreaquecimento dos equipamentos de TIC.	**Alto (PSR 45)**	**Mitigar**
8	*Data Center*	Interrupção no fornecimento de energia elétrica.	1. Falha por parte da concessionaria; 2. Falha na subestação do prédio; 3. Parada programada no fornecimento de energia.	1. Desligamento dos ativos de rede; 2. Possível indisponibilidade de serviços e sistemas.	**Alto (PSR 45)**	**Mitigar**
9	Enlace de Internet Principal	Indisponibilidade de acesso à Internet Principal.	1. Rompimento de fibra óptica; 2. Falha, queima ou parada dos ativos de rede; 3. Cabos desconectados acidentalmente; 4. Sobrecarga de tráfego na rede lógica.	1. Indisponibilidade total dos acessos a serviços e sistemas externos; 2. Indisponibilidades dos usuários externos em acessar os serviços e sistemas providos pelo TJTO.	**Alto (PSR 45)**	**Mitigar**
10	*Data Center*	Acesso não autorizado ao *Data Center.*	1. Falha no controle de acesso físico.	1. Poderá haver danos a infraestrutura e serviços de TIC; 2. Roubo de informações; 3. Desconfigurarão de dispositivos.	**Alto (PSR 45)**	**Mitigar**
11	*Data Center*	Falha no gerador.	1. Falta de combustível; 2. Bateria descarregada; 3. Vida útil das peças comprometida; 4. Falha em algum componente; 5. Falta de manutenção preventiva.	1. Descarga completa das baterias dos nobreaks; 2. Interrupção no fornecimento de energia para o Data Center; 3. Desligamento de todos os equipamentos; 4. Indisponibilidade dos serviços e sistemas providos pelo TJTO.	**Médio (PSR 30)**	**Mitigar**

12	*Data Center*	Inundação.	Alagamento causado por: 1. Excesso de chuva; 2. Rompimento de tubulação.	1. Destruição parcial ou total dos equipamentos do *Data Center*; 2. Indisponibilidade parcial ou total dos serviços e sistemas.	**Médio (PSR 30)**	**Mitigar**
13	Servidor de Rede	Acesso não autorizado às pastas e arquivos departamentais.	1. Erro humano (Configuração de permissões de acesso); 2. Engenharia social.	1. Acesso indevido a informações importantes; 2. Cópia ou destruição de dados sigilosos ou restritos.	**Médio (PSR 27)**	**Mitigar**
14	*Data Center*	Falha nos *nobreaks.*	1. Curto-circuito nos *nobreaks*; 2. Módulos ou baterias danificadas.	1. Desligamento inesperado de todos os equipamentos de TIC. 2. Indisponibilidade de todos os serviços e sistemas.	**Médio (PSR 20)**	**Mitigar**
15	Servidor de Rede	Falha ou indisponibilidade do servidor de arquivos.	1. Erro humano (configuração); 2. Falha, queima ou parada do equipamento; 3. Falha, queima ou parada do switch de rede.	1. Indisponibilidade dos serviços de rede (acesso a pastas e arquivos, autenticação de usuários, acessos a serviços e sistemas internos e externos); 2. Falha no serviço de DHCP.	**Médio (PSR 18)**	**Mitigar**
16	Enlace de Internet Redundante	Indisponibilidade de acesso à Internet Redundante.	1. Rompimento de fibra óptica; 2. Falha, queima ou parada dos ativos de rede; 3. Cabos desconectados acidentalmente; 4. Sobrecarga de tráfego na rede lógica.	1. Indisponibilidade do acesso à Internet via enlace de dados redundante.	**Médio (PSR 18)**	**Mitigar**

NRI (Nível de Risco Inerente): 1 – Muito Baixo, 2 – Baixo, 3 – Médio, 4 – Alto, 5 – Muito Alto

Resposta ao Risco: 1 – Evitar, 2 – Mitigar, 3 – Compartilhar, 4 – Aceitar

3. Tratamento dos Riscos

Matriz de Tratamento de Riscos de TIC						
Evento de Risco	**Controles**	**Descrição**	**Monitoramento**	**Responsável**	**Prazo**	**Nível de Risco Pretendido**
Incêndio.	Sistema de detecção e combate a incêndio.	O sistema de detecção e combate a incêndio tem como função perceber, captar, sinalizar e evitar a propagação de chamas no *data center*. Recursos necessários: disponibilidade financeira e processo licitatório.	Acompanhar etapas de elaboração e execução do projeto. Registrar ocorrência do evento com periodicidade mensal. Analisar laudos da manutenção preventiva periódica de todos os dispositivos.	Chefe da DASR	120 dias	Atual **Muito Alto** Pretendido **Baixo**
Falha ou dano permanente no *Firewall.*	*Backup* da configuração; Dois equipamentos ligados em HA (*High-Availability*); Suporte e garantia dos equipamentos com processo de autorização de troca (RMA - *Return Merchandise Authorization*). Atualização do *firmware* do equipamento.	Realizar diariamente *backup* das configurações. Verificar mensamente a necessidade de atualização do *firmware* do equipamento. Manter a equipe atualizada quanto aos procedimentos para restauração das configurações do equipamento. Renovar o suporte e garantia dos equipamentos. Recursos necessários: disponibilidade financeira e processo licitatório.	Manter documentação para restauração do sistema e atualização do equipamento. Inspecionar semanalmente o equipamento. Fazer a gestão do contrato (dar atenção às datas de vencimento de licenças e suporte/garantia).	Chefe da DASR	120 dias	Atual **Alto** Pretendido **Baixo**

Falha ou dano permanente no s*witch core.*	Equipamento reserva. *Backup* da configuração do equipamento. Aquisição de novos equipamentos.	Manter o *backup* das configurações do equipamento e equipamento de reserva para uma eventual substituição. A aquisição de novos equipamentos se faz necessária para substituição dos atuais que se encontram com mais de 5 (cinco) anos de uso. Recursos necessários: disponibilidade financeira e processo licitatório.	Monitorar o ativo de rede via *software* de gerenciamento. Fazer a gestão do contrato dos novos equipamentos adquiridos (dar atenção aos requisitos de suporte e garantia). Disponibilizar equipamento reserva.	Chefe da DASR	120 dias	Atual **Alto** Pretendido **Baixo**
Falha ou dano permanente na solução de virtualização.	Redundância de equipamentos. Suporte e garantia dos equipamentos com processo de autorização de troca. Backup das VMs. Atualização tecnológica da solução.	Prover redundância de equipamentos no *site backup*. Realizar *backup* das máquinas virtuais diariamente. Capacitar a equipe para o gerenciamento da solução.	Gerenciar recursos da solução. Fazer a gestão do contrato (dar atenção às datas de vencimento de licenças e suporte/garantia). Celebrar contrato de manutenção.	Chefe da DASR	120 dias	Atual **Alto** Pretendido **Baixo**
Indisponibilidade do sistema de processo judicial eletrônico.	Monitoramento de parâmetros do sistema e de infraestrutura pelo software de gerenciamento. Redundância da hospedagem de serviços.	Analisar a falha apresentada e aplicar as correções necessárias. Prover a redundância do serviço no *site backup*.	Gerenciar o sistema e a infraestrutura via software de monitoramento.	Chefe da DASR	120 dias	Atual **Alto** Pretendido **Baixo**

	Ativos de rede reserva. Capacitação dos recursos humanos das áreas intervenientes quanto à indisponibilidade do serviço.					
Indisponibilidade do sistema eletrônico de informações.	Monitoramento de parâmetros do sistema e de infraestrutura pelo software de gerenciamento. Redundância da hospedagem de serviços. Ativos de rede reserva. Capacitação dos recursos humanos das áreas intervenientes quanto à indisponibilidade do serviço.	Analisar a falha apresentada e aplicar as correções necessárias. Prover a redundância do serviço no *site backup*.	Gerenciar o sistema e a infraestrutura via software de monitoramento.	Chefe da DASR	120 dias	Atual **Alto** Pretendido **Baixo**
Falha nos ares-condicionados de precisão.	Dois ares-condicionados em backup, configurados para fazer rodízio dentre os seis existentes (se um apresentar problema, o que está em backup assume automaticamente).	Analisar a falha e se possível aplicar correções necessárias. Manter manutenções mensais. Substituir peças com defeito.	Realizar manutenção preditiva, preventiva e corretiva mensal. Emitir relatórios descritivos de cada manutenção e os status do equipamento.	Chefe da DASR	120 dias	Atual **Alto** Pretendido **Baixo**

		Recursos necessários: aquisição de peças e disponibilidade financeira.				
Interrupção no fornecimento de energia elétrica.	Manutenção preventiva periódica de todos os dispositivos e infraestrutura elétrica da subestação. Monitoramento do gerador enquanto ele estiver fornecendo energia. Abastecimento periódico do gerador.	Nobreak assume a carga de energia dos racks de TI até que o gerador é acionado e estabilizado (em torno de 20 segundos). Recursos necessários: combustível para o gerador, investimento em materiais elétricos e disponibilidade financeira.	Monitorar o *Data Center* via *software* de gerenciamento. Emitir laudos da manutenção preventiva periódica de todos os dispositivos e infraestrutura elétrica da subestação.	Chefe da DASR	120 dias	Atual **Alto** Pretendido **Baixo**
Indisponibilidade de acesso à Internet Principal.	Monitoramento dos ativos de rede via software de gerenciamento. Acordo de níveis de serviços (ANS) junto a operadora de telecomunicação. Enlace de Internet Redundante.	Ativar o enlace de Internet redundante e aplicar controles de tráfego. Prover acesso externo aos serviços e sistemas do TJTO via enlace de Internet redundante. Configurar o serviço de DNS com os endereços da operadora de Internet redundante. Obter ASN (Número de Sistema Autônomo). Monitorar chamado e o cumprimento do ANS.	Monitorar via software a disponibilidade do enlace de comunicação e da utilização de banda. Monitoramento pró ativo da operadora. Acordo de Níveis de Serviços – ANS.	Chefe da DASR	120 dias	Atual **Alto** Pretendido **Baixo**

		Recursos necessários: treinamento dos procedimentos quanto a indisponibilidade do serviço, consultoria técnica e disponibilidade financeira.				
Acesso não autorizado ao *Data Center.*	Leitor com biometria na porta do datacenter. Câmeras de monitoramento.	Aperfeiçoar a segurança física do ambiente. Adotar política de controle de acesso físico.	Administrar o acesso ao local por meio de procedimentos e equipamentos que tenham o objetivo de proteger o ambiente.	Chefe da DASR	120 dias	Atual **Alto** Pretendido **Baixo**
Falha no gerador.	Manutenção mensal.	Analisar a falha e se possível aplicar correções necessárias. Manter manutenções mensais. Monitorar tanques de combustível semanalmente. Recursos necessários: contrato de manutenção, aquisição de peças e disponibilidade financeira.	Realizar manutenção preditiva, preventiva e corretiva mensal. Emitir relatórios descritivos de cada manutenção e os status do equipamento.	Chefe da DASR	120 dias	Atual **Médio** Pretendido **Baixo**
Inundação.	Plano de desastres. Redundância de equipamentos. Redundância de hospedagem de serviços.	Elaborar plano de desastres, que deverá prever como o TJTO buscará manter suas atividades e recuperar seus dados. Instalar dispositivo detector de alagamento.	Monitorar o ambiente via software de gerenciamento do dispositivo de detecção de alagamento.	Chefe da DASR	120 dias	Atual **Médio** Pretendido **Baixo**

	Dispositivo detector de alagamento.	Projetar novo *data center* em edificação de uso dedicado isolado do prédio do TJTO. Recursos necessários: disponibilidade financeira.				
Acesso não autorizado às pastas e arquivos departamentais.	Política de controle de acesso. Auditoria. Registro (logs) dos acessos dos usuários.	Manter registros de logs. Manter solução de backup. Adotar política de senhas.	Definir uma política de senhas. Conscientizar os usuários para o tema da segurança da informação. Levar ao conhecimento dos servidores, por meio de campanhas de conscientização, a PSI e suas normas.	Chefe da DASR	120 dias	Atual **Médio** Pretendido **Baixo**
Falha nos *nobreaks*.	Redundância nos módulos de potência do nobreak. Bancos de bateria de alta autonomia (3h). Manutenção mensal.	Analisar a falha e se possível aplicar correções necessárias. Manter manutenções mensais. Monitorar a carga das baterias. Recursos necessários: contrato de manutenção, aquisição de peças e disponibilidade financeira.	Realizar manutenção preditiva, preventiva e corretiva mensal. Emitir relatórios descritivos de cada manutenção e os status do equipamento.	Chefe da DASR	120 dias	Atual **Médio** Pretendido **Baixo**
Falha ou indisponibilidade do servidor de arquivos.	Monitoramento do ativo de rede via software de gerenciamento.	Manter equipamento sobressalente.	Monitorar o ativo via *software* de gerenciamento.	Chefe da DASR	120 dias	Atual **Médio**

	Gerenciamento via iLO do servidor para analisar a falha. Equipamento reserva. Suporte e garantia.	Manter backup atualizado dos dados. Habilitar o serviço de DHCP no firewall. Recursos necessários: servidores reservas, aquisição de componentes, disponibilidade financeira.	Fazer a gestão do contrato de suporte e garantia.			Pretendido **Baixo**
Indisponibilidade de acesso à Internet Redundante.	Monitoramento dos ativos de rede via software de gerenciamento. Acordo de níveis de serviços (ANS) junto a operadora de telecomunicação.	Monitorar chamado e o cumprimento do ANS. Treinar a equipe para realização dos procedimentos quanto a indisponibilidade do serviço.	Monitorar via software a disponibilidade do enlace de comunicação e da utilização de banda. Monitoramento pró ativo da operadora. Acordo de Níveis de Serviços – ANS.	Chefe da DASR	120 dias	Atual **Médio** Pretendido **Baixo**

Explicação sobre cada campo do plano de tratamento.	
Evento de Risco	Risco priorizado conforme tabela de priorização de riscos para tratamento.
Controles	Controles propostos para o risco em tratamento.
Descrição	Descrição detalhada dos tratamentos, incluindo os custos.
Monitoramento	Detalhes de como se dará o monitoramento e análise crítica do risco e seu tratamento após sua implementação.
Responsável	Servidor responsável pela implementação do tratamento.
Prazo	Prazo para a implementação dos controles.
Nível de Risco Pretendido	Informar se o tratamento atacou a probabilidade e/ou a consequência do risco, informando os novos valores do cálculo do risco e seu novo nível de risco.

ANEXOS

ANEXO 1 – Portaria nº 1660/2019

PODER JUDICIÁRIO
ESTADO DO TOCANTINS

Portaria Nº 1660, de 12 de agosto de 2019

O PRESIDENTE DO TRIBUNAL DE JUSTIÇA DO ESTADO DO TOCANTINS, no uso de suas atribuições legais e regimentais,

CONSIDERANDO os termos da Portaria nº 3.433, de 26 de junho de 2017, que institui a política de segurança da informação no âmbito do Poder Judiciário do Estado do Tocantins;

CONSIDERANDO a necessidade de promover atualizações em seu conteúdo e incluir normas de gestão de risco de segurança da informação e de gestão dos processos de *backup*;

CONSIDERANDO o contido nos autos SEI nº 16.0.000005260-8,

RESOLVE:

Art. 1º A Portaria nº 3.433, de 26 de junho de 2017, passa a vigorar acrescida do Capítulo VIII-A e correspondente art. 21-A, com a seguinte redação:

"**Capítulo VIII-A**

GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

Art. 21-A. O Tribunal deve adotar um conjunto de processos que permitam identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação e equilibrá-los com os custos operacionais e financeiros envolvidos."

Art. 2º O Anexo I da Portaria nº 3.433, de 26 de junho de 2017, passa a vigorar acrescido dos seguintes itens:

".....

61. Risco: efeito da incerteza nos objetivos. Um efeito é um desvio em relação ao esperado – positivo e/ou negativo. Risco de segurança da informação é a possibilidade de uma determinada ameaça explorar vulnerabilidades de um ativo ou de um conjunto de ativos, desta maneira prejudicando a organização. É medido em função da combinação da probabilidade de um evento e de sua consequência;

62. Controle: medida que está modificando o risco;

63. Nível de Risco: magnitude de um risco, expressa em termos da combinação das consequências e de suas probabilidades

64. Risco Residual: risco remanescente após tratamento do risco;

65. Análise de Riscos: processo de compreender a natureza do risco e determinar o nível do risco;

66. Processo de Avaliação de Riscos: processo global de identificação de riscos, análise de riscos e avaliação de riscos;

67. Comunicação e Consulta: processos contínuos e iterativos que uma organização conduz para fornecer, compartilhar ou obter informações e se envolver no diálogo com as partes interessadas, com relação a gerenciar riscos;

68. Avaliação de Riscos: processo de comparar os resultados da análise de riscos com os critérios de risco para determinar se o risco e/ou sua magnitude é aceitável ou tolerável;

69. Identificação de Riscos: processo de busca, reconhecimento e descrição de riscos;

70. Parte Interessada: pessoa ou organização que pode afetar, ser afetada, ou perceber–se afetada por uma decisão ou atividade;

71. Gestor de risco: pessoa responsável por acompanhar as ações de mapeamento, avaliação e mitigação de riscos inerentes aos processos de trabalho;

72. *Backup*: cópia de segurança gerada para possibilitar o acesso ou recuperação futura de dados;

73. Janela de *backup:* período de tempo requerido para a geração do *backup* (total, diferencial ou incremental);

74. Mídia de *backup:* suporte magnético, óptico ou eletrônico utilizado para armazenamento de dados. Dentre as mídias de *backup* destacam-se os discos rígidos, fitas e cartuchos magnéticos, discos ópticos, *pen-drives* e discos de estado sólido;

75. *Restore:* cópia eventual de dados armazenados em *backup* para um disco ou outra mídia através da qual podem ser acessados pelos usuários ou aplicações;

76. *Virtual Tape Library* (VTL): equipamento que simula uma *tape library* através da utilização de discos rígidos em lugar de mídias de *backup* convencionais, possibilitando otimização dos processos de *backup* e *restore*;

77. *Software de backup*: conjunto de programas especializados no planejamento, identificação do *backup*, processamento e controle do *backup* de servidores, *storage* e demais dispositivos que armazenam dados.

78. Período de Retenção: tempo que o dado estará disponível até ser expirado, sobregravado ou apagado.” (NR)

Art. 3º O Anexo II da Portaria nº 3.433, de 26 de junho de 2017, passa a vigorar acrescido dos seguintes itens:

“.....

7. Norma-TIC-07: Gestão de Riscos de Segurança da Informação (GRSI);

8. Norma-TIC-08: processos de *backup*.

.....

7. **Norma-TIC-07**: Gestão de Riscos de Segurança da Informação (GRSI): regras de segurança para minimizar ou eliminar os riscos a que estão sujeitos os ativos de informação do Poder Judiciário do Tocantins.

7.1. Disposições iniciais

7.1.1. A Gestão de Riscos de Segurança da Informação (GRSI) tem como objetivo minimizar ou eliminar os riscos a que estão sujeitos os ativos de informação do Poder Judiciário do Tocantins.

7.1.2. A Gestão de Riscos de Segurança da Informação (GRSI) deve ser implementada no âmbito do Poder Judiciário do Tocantins, visando identificar, analisar e tratar riscos à segurança da informação.

7.1.3. As áreas da Diretoria de Tecnologia da Informação responsáveis por ativos de informação deverão identificar seus ativos relevantes para que seja implementado o processo de gestão de riscos.

7.1.4. A Gestão de Riscos de Segurança da Informação (GRSI) deve ser atualizada periodicamente, no mínimo 1 (uma) vez por ano ou oportunamente, em função de inventários de ativos, mudanças, ameaças ou vulnerabilidades.

7.2. Sistematização da gestão de riscos

7.2.1. A Gestão de Riscos de Segurança da Informação (GRSI) será estruturada nas seguintes etapas:

7.2.1.1. Entendimento do contexto: etapa em que são identificados os objetivos relacionados ao processo organizacional e definidos os contextos externo e interno a serem levados em consideração ao gerenciar riscos;

7.2.1.2. Identificação de riscos: etapa em que são identificados possíveis riscos para objetivos associados aos processos organizacionais;

7.2.1.3. Análise/avaliação de riscos: etapa em que são identificadas as possíveis causas e consequências do risco. Uma vez identificados, os níveis de riscos são estimados;

7.2.1.4. Priorização de riscos: etapa em que são definidos quais riscos terão suas respostas priorizadas, levando em consideração os níveis calculados na etapa anterior;

7.2.1.5. Definição de respostas aos riscos: etapa em que são definidas as respostas aos riscos, de forma a adequar seus níveis ao apetite estabelecido para os processos organizacionais, além da escolha das medidas de controle associadas a essas respostas;

7.2.1.6. Comunicação e monitoramento: etapa que ocorre durante todo o processo de gerenciamento de riscos e é responsável pela integração de todas as instâncias envolvidas, bem como pelo monitoramento contínuo da própria gestão de riscos, com vistas a sua melhoria.

7.3. Responsabilidades

7.3.1. Integram a estrutura da gestão de riscos de segurança da informação do Poder Judiciário do Tocantins:

7.3.1.1. Comitê Gestor de Segurança da Informação;

7.3.1.2. Gestores de riscos.

7.3.2. O Comitê Gestor de Segurança da Informação é o responsável pelo estabelecimento da estratégia e da estrutura de gerenciamento de riscos.

7.3.3. Cada risco mapeado e avaliado deve estar associado a um gestor responsável formalmente identificado.

7.3.3.1. O gestor de riscos deve orientar e acompanhar as ações de mapeamento, avaliação e mitigação do risco.

7.3.3.2. São responsabilidades do gestor de risco:

7.3.3.2.1. Assegurar que o risco seja gerenciado de acordo com a política de gestão de riscos do Poder Judiciário do Tocantins;

7.3.3.2.2. Monitorar o risco ao longo do tempo, de modo a garantir que as respostas adotadas resultem na manutenção do risco em níveis adequados, de acordo com a política de gestão de riscos; e

7.3.3.2.3. Garantir que as informações adequadas sobre o risco estejam disponíveis em todos os níveis do Poder Judiciário do Tocantins.

8. **Norma-TIC-08**: processos de *backup*: norma da segurança da informação que trata da gestão dos processos de *backup* (cópias de segurança) das informações eletrônicas, para proteção, acesso e recuperação futura dos dados sensíveis a continuidade dos serviços.

8.1. Disposições iniciais

8.1.1. A norma de segurança da informação que trata da gestão dos processos de *backup* aborda os conceitos, processos de *backup* e tem como objetivo o acesso e/ou recuperação futura de dados existentes nos sistemas de *backup* do PJTO.

8.2. Diretrizes da gestão dos processos de *backup*

8.2.1. Utilizar recursos adequados para a geração de cópias de segurança para garantir que as informações e sistemas essenciais possam ser recuperados após a perda de dados devido a desastres, erros, falhas de mídias ou outros fatores;

8.2.2. Registrar informações das cópias de segurança em documentação apropriada e sistematizada;

8.2.3. Todas as aplicações institucionais e/ou departamentais devem armazenar os dados nos servidores de arquivos, servidores de bancos de dados e servidores de aplicação para os quais será assegurada a execução de rotina de *backup*, de acordo com esta política;

8.2.4. Esta norma não se aplica aos *backups* de dados locais, cabendo essa responsabilidade ao usuário de TIC;

8.2.5. A Diretoria de Tecnologia da Informação (DTINF) é responsável por assegurar a execução das rotinas de *backup* no âmbito do PJTO.

8.3. Processo de *backup*

8.3.1. Tem por objetivo estabelecer uma política de *backup* de dados estruturados e não estruturados a fim de evitar que os arquivos sejam perdidos ou danificados em caso de algum incidente;

8.3.2. Os arquivos de *backup* evitam ou minimizam as perdas de dados casos algum incidente/acidente aconteça.

8.3.3. A rotina de *backup* deve ser aplicável a dados estruturados e não estruturados:

8.3.3.1. *backup* diário: processado diariamente, com período de retenção dos últimos 6 (seis) dias ou conforme necessidade.

8.3.3.2. *backup* semanal: processado semanalmente em um dia específico da semana, com retenção das 4 (quatro) últimas semanas.

8.3.3.3. *backup* mensal: processado na última sexta-feira do mês, com retenção dos últimos 12 (doze) meses.

8.3.3.4. *backup* anual: processado na última sexta feira do ano, com retenção dos últimos 5 (cinco) anos ou conforme necessidade.

8.4. Sistema de *backup*

8.4.1. O *backup* deve ser processado em equipamento específico: Mídias de *backup*, *storages*, servidores de *backup*, servidores *NAS*, *backup* via computação em nuvem, data center local ou remoto ou outros dispositivos de armazenamento sob controle do software de *backup* homologado pela DTINF.

8.4.2. Qualquer solicitação de serviços que envolva outros equipamentos, software de *backup*, local de armazenamento de mídias, alteração na frequência de geração ou no tempo de retenção

do *backup* deverá ser analisada previamente pela DTINF, quanto à sua viabilidade, em prazo negociado entre as partes.

8.4.3. O *backup* deverá ser processado, preferencialmente, durante a noite, em horário que gere menor impacto nas demais rotinas e serviços do Data Center primário e secundário do PJTO.

8.4.4. O *backup* de *logs* de bancos de dados serão realizados ao longo do dia a cada uma hora.

8.5. Responsabilidades

8.5.1 Cabe às chefias de divisões da Diretoria de Tecnologia da Informação eleger um ou mais administradores de *backup* para fazer a gestão dos processo de cópia de segurança, ficando responsável pela política e procedimentos relativos aos serviços de *backup* e *restore*, bem como guardar as mídias de *Backup*." (NR)

Art. 4º Esta Portaria entra em vigor na data de sua publicação.

Publique-se. Cumpra-se.

Desembargador HELVÉCIO DE BRITO MAIA NETO

Presidente

Este texto não substitui o publicado no DJe nº 4560 de 14/08/2019 Última atualização: 14/08/2019

ANEXO 2 – Fluxo do Processo de Gestão de Riscos TIC