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

MARCELO LEAL DE ARAÚJO BARRÊTO

ESTUDO SOBRE A GESTÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO NO PODER JUDICIÁRIO DO ESTADO DO TOCANTINS

Palmas - TO
2021

MARCELO LEAL DE ARAÚJO BARRÊTO

ESTUDO SOBRE A GESTÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO NO PODER JUDICIÁRIO DO ESTADO 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
2021

Dados Internacionais de Catalogação na Publicação (CIP)
Sistema de Bibliotecas da Universidade Federal do Tocantins

B273e Barrêto, Marcelo Leal de Araújo .

Estudo sobre a Gestão da Política de Segurança da Informação no Poder Judiciário do Estado do Tocantins. / Marcelo Leal de Araújo Barrêto. – Palmas, TO, 2021.

90 f.

Dissertação (Mestrado Acadêmico) - Universidade Federal do Tocantins – Câmpus Universitário de Palmas - Curso de Pós-Graduação (Mestrado) em Modelagem Computacional de Sistemas, 2021.

Orientador: Gentil Veloso Barbosa

1. Segurança da Informação. 2. Política de Segurança da Informação. 3. Fluxos dos Processos. 4. Teste de Conformidade. I. Título

CDD 004

Elaborado pelo sistema de geração automática de ficha catalográfica da UFT com os dados fornecidos pelo(a) autor(a).

FOLHA DE APROVAÇÃO

MARCELO LEAL DE ARAÚJO BARRÊTO

ESTUDO SOBRE A GESTÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO NO PODER JUDICIÁRIO DO ESTADO 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: 19 / 01 / 2021

Banca Examinadora

_____

Professor Doutor Gentil Veloso Barbosa, UFT

_____

Professor Doutor Gerson Pesente Focking, IFTO

_____

Professor Doutor George Lauro Ribeiro de Brito, UFT

_____

Professor Doutor David Nadler Prata, UFT

Palmas – TO
2021

Agradeço a Deus que me protegem e me mantém de pé diante dos desafios. Este trabalho é dedicado aos meus pais David de Araújo Barrêto, Hortência Leal de Araújo Barreto, e minha querida irmã Marciley Leal de Araújo Barreto que formam a pedra angular da minha vida.

AGRADECIMENTOS

Ao Professor Doutor Gentil Veloso Barbosa pela paciência e s ensinamentos sobre resiliência.

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.

A equipe da Divisão de Administração e Segurança de Redes (DASR): Danillo Lustosa, João Carlos, Ricardo Marx e Tiago Luz, formação esta, que a mais de uma década zela pela excelência na gestão da rede do Poder Judiciário Tocantinense.

A minha irmã, Marciley Leal (Analista Judiciária do PJTO), pelos ensinamentos sobre a organização do Poder Judiciário Tocantinense.

A minha namorada, Professora Simone Cavalcante (APAE de Palmas), pelo incentivo.

E aos que direta ou indiretamente, deram sustentação para conclusão dessa etapa.

Minha imensa gratidão!

RESUMO

O presente trabalho de pesquisa versa sobre o estudo da Gestão da Política de Segurança da Informação no Poder Judiciário do Estado do Tocantins. Para tal foi utilizado, como procedimento metodológico, a pesquisa documental em Leis, Resoluções, Portarias, Instruções normativas do Poder Judiciário do Estado do Tocantins (PJTO) e do Conselho Nacional de Justiça (CNJ). Os objetivos do projeto de pesquisa assentam-se em apresentar como ocorreu a implantação dos processos de segurança abordando a criação do Comitê Gestor de Segurança e, também, a Política de Segurança da Informação no âmbito do PJTO através da Portaria nº 3433, de 26 de junho de 2017. No ano de 2019 foram publicadas duas portarias contendo novas normas de conformidade, quais sejam: a Portaria nº 1660, de 12 de agosto de 2019, que trata de: a) gestão de riscos e b) processos de *backup*, que formam os artefatos oriundo da pesquisa do mestrado aplicado ao Poder Judiciário tocantinense, e a Portaria nº 2361/2019, de 08 de novembro de 2019, que cria um Grupo de Trabalho para apoio ao Comitê Gestor de Segurança da Informação do PJTO, cumprindo assim com requisitos da Resolução 211/2015 do CNJ. Ademais, realizou-se pesquisa bibliográfica e estudo do *framework* da ABNT 27002 como um instrumento de avaliação do grau de maturidade em segurança da informação, formado por 59 questões de controle e envolvendo 14 domínios presentes na ABNT 27002. O instrumento foi aplicado nas áreas estratégicas, táticas e operacionais do Tribunal de Justiça do Estado do Tocantins. Tais artefatos objetivam subsidiar o Comitê Gestor da Segurança da Informação na tomada de decisões em busca do aprimoramento da gestão da segurança da informação, no âmbito do Poder Judiciário do Estado do Tocantins.

Palavras-chave: Segurança da Informação, Política de Segurança da Informação, Fluxos dos Processos, Teste de Conformidade.

ABSTRACT

This research paper is about the study of Information Security Policy Management in the Judiciary of the State of Tocantins. For this purpose, documentary research on Laws, Resolutions, Ordinances, Normative Instructions of the Judiciary of the State of Tocantins (PJTO) and the National Council of Justice (CNJ) was used as a methodological procedure. The objectives of the research project are based on presenting how the implementation of the security processes took place, addressing the creation of the Security Management Committee and also the Information Security Policy in the scope of the PJTO through Ordinance nº 3433 of June 26, 2017. In the year 2019 two ordinances were published containing new norms of conformity, which are: the Ordinance nº 1660, of August 12, 2019, which deals with: a) risk management and b) backup processes, which form the artifacts from the research of the Master applied to the Tocantinense Judiciary, and the Ordinance nº 2361/2019, of November 8, 2019, which creates a Working Group to support the Information Security Management Committee of the PJTO, thus fulfilling the requirements of Resolution 211/2015 of the CNJ. Furthermore, bibliographic research and study of the ABNT 27002 framework as an instrument to evaluate the degree of maturity in information security, formed by 59 control questions and involving 14 domains present in ABNT 27002. The instrument was applied in the strategic, tactical and operational areas of the Tocantins State Court of Justice. These artifacts are intended to subsidize the Information Security Management Committee in its decision making efforts to improve the management of information security, within the scope of the Judiciary Branch of the State of Tocantins.

Keywords: Information Security, Information Security Policy, Process Flows, Compliance Testing.

LISTA DE ILUSTRAÇÃO

Figura 1 - Representação da REDE TELEJURIS..... 22
Figura 2 - Tríade da Segurança da Informação 34
Figura 3 - Conceito da organização do *framework* da ABNT 27002 39
Figura 4 - Processo de melhoria contínua de um SGSI 41
Figura 5 - Fluxo do Processo de Monitoramento da PSI do PJTO..... 58

LISTA DE GRÁFICOS

Gráfico 1 - iGovTIC-JUD da TIC do PJTO 60
Gráfico 2 - Resultado da frequência das respostas na visão Estratégica 66
Gráfico 3 - Resultado da frequência das respostas na visão Tática 68
Gráfico 4 - Resultado da frequência das respostas na visão Operacional 69
Gráfico 5 - Resultado da frequência: Estratégica, Tática e Operacional 70

LISTA DE TABELAS

Tabela 1 - Representação dos domínios, descrição, quantidade de controles e sigla 65
Tabela 2 - Representação da frequência das respostas na visão Estratégica..... 66
Tabela 3 - Representação da frequência das respostas na visão Tática 67
Tabela 4 - Representação da frequência das respostas na visão Operacional..... 68
Tabela 5 - Consolidação das frequências de todas as respostas 69
Tabela 6 – Pontuação de todas as respostas 70

LISTA DE QUADROS

Quadro 1 - Metodologia Científica Aplicada à Pesquisa 26
Quadro 2 - Classificação de Ativos 32
Quadro 3 - Tipo de proteção de ativos 32
Quadro 4 - Fatores a serem observados na Segurança da Informação 35
Quadro 5 - Categoria de problemas na Segurança da Informação 35
Quadro 6 - Sistema de pontuação das respostas do *framework* da ABNT 27002 43
Quadro 7 - Análise de cenário da aplicação do *framework* da ABNT 27002 44
Quadro 8 - Análise das Normas 46
Quadro 9 - Exemplo da declaração de uma Diretriz na PSI do PJTO 49
Quadro 10 - Exemplo da declaração do manual de organização e conceitos da PSI 49
Quadro 11 - Exemplo da Norma nº 08 na PSI do PJTO 50
Quadro 12 - Achados da Auditoria de Conformidade. 55
Quadro 13 - Papéis e responsabilidades no processo de monitoramento da PSI do PJTO. 59
Quadro 14 – Pontuação do *framework* da ABNT 27002 conforme as áreas 71
Quadro 15 - Oportunidade de Aprimoramento da Segurança da Informação do PJTO 72

LISTA DE SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
AQUIDEVSISTEMAS	Aquisição, Desenvolvimento e Manutenção de Sistemas - Domínio 10 da ABNT 27002
CADSUPRIMENTOS	Relacionamento na Cadeia de Suprimentos - Domínio 11 da ABNT 27002
CGSI	Comitê Gestor de Segurança da Informação Multidisciplinar
CGTIC	Comitê de Gestão de Tecnologia da Informação e Comunicação
COGES	Coordenadoria de Gestão Estratégica, Estatística e Projetos
CONFORMIDADE	Conformidade - Domínio 14 da ABNT 27002
CONTRACESSO	Controle de Acesso - Domínio 05 da ABNT 27002
CNJ	Conselho Nacional de Justiça
CRIPTOGRAFIA	Criptografia - Domínio 06 da ABNT 27002
CSCPJ	Comitê de Segurança Cibernética do Poder Judiciário
DTINF	Diretoria de Tecnologia da Informação e Comunicação
DIGER	Diretoria Geral
ENTIC-JUD	Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário
GESTATIVOS	Gestão de Ativos- Domínio 04 da ABNT 27002
GESTINCIDENTE	Gestão de Incidentes de Segurança da Informação- Domínio 12 da ABNT 27002
GDPR	*General Data Protection Regulation*
GRSI	Gestão de Riscos de Segurança da Informação
GT-CGSI	Grupo de Trabalho de Apoio ao Comitê Gestor de Segurança da Informação Multidisciplinar (CGSI)
LGDP	Lei Geral de Proteção a Dados
NBR	Norma Brasileira
PAA	Plano Anual de Auditoria
PALP	Plano de Auditoria de Longo Prazo
PEI	Planejamento Estratégico Institucional
PETIC	Planejamento Estratégico de TIC
PDTI	Plano Diretor de TIC

PJTO	Poder Judiciário do Estado do Tocantins
PPICiber/PJ	Protocolo de Prevenção a Incidentes Cibernéticos do Poder Judiciário
PSI	Política de Segurança da Informação
SEI	Sistema Eletrônico de Informações
SI	Segurança da Informação
TCU	Tribunal de Contas da União
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicação
TJTO	Tribunal de Justiça do Estado do Tocantins
TRF-4	Tribunal Regional Federal da 4ª Região
ORGSEGINFORMACAO	Organização da Segurança da Informação- Domínio 02 da ABNT 27002
POLSEGINFORMACAO	Política de Segurança da Informação- Domínio 01 da ABNT 27002
SEGCONTNEGOCIO	Aspectos da Segurança da Informação na Gestão da Continuidade do Negócio - Domínio 13 da ABNT 27002
SEGCOMUNICACOES	Segurança nas Comunicações - Domínio 09 da ABNT 27002
SEGFIAMBIENTE	Segurança Física do Ambiente - Domínio 07 da ABNT 27002
SEGOPERACOES	Segurança nas Operações - Domínio 08 da ABNT 27002
SEGRECHUMANOS	Segurança em Recursos Humanos - Domínio 03 da ABNT 27002
SGSI	Sistema de Gestão da Segurança da Informação

SUMÁRIO

1. INTRODUÇÃO 18

1.1. Problema 21

1.2. Justificativa 23

1.3. Objetivo Geral 24

1.3.1. Objetivos Específicos 25

1.4. Metodologia 25

1.4.1. Quanto à Natureza 26

1.4.2. Quanto aos Objetivos 26

1.4.3. Quanto à Abordagem 27

1.4.4. Quanto aos Procedimentos 27

1.5. Estudos Técnicos Preliminares 28

1.5.1. Atuação na Área Administrativa 28

1.5.2. Atuação na Área Acadêmica 29

1.6. Estruturação do Trabalho 30

2. REVISÃO DE LITERATURA 31

2.1. Segurança 31

2.2. Ativos 32

2.3. Segurança da Informação 33

2.3.1. Fatores a serem observados na Segurança da Informação 35

2.3.2. As categorias mais comuns de problemas na Segurança da Informação 35

2.4. Normas da ABNT 36

2.5. A Política de Segurança da Informação 36

2.6. A Conformidade com a ABNT 27002 38

2.6.1. O *Framework* e os Controles de Segurança 39

2.6.2. O Sistema de Gestão da Segurança da Informação 40

2.6.3. O teste de conformidade do *framework* da ABNT 27002 42

2.6.4. A metodologia de pontuação da aplicação do *framework* de conformidade com a ABNT 27002 42

2.6.5. O índice da situação da organização segundo o *framework* de conformidade com a ABNT 27002 43

3. ANÁLISE DAS PRINCIPAIS RESOLUÇÕES E NORMAS DE CONFORMIDADE APLICADAS À SEGURANÇA DA INFORMAÇÃO NO ÂMBITO DO PJTO 45

3.1. A Segurança da Informação no Poder Judiciário Tocantinense 46

3.2. O Comitê Gestor de Segurança da Informação 48

3.3. A Política de Segurança da Informação (PSI) aplicada à Tecnologia da Informação 48

3.4. A metodologia para elaboração da minuta da Política de Segurança da Informação 49

3.5. Os domínios e controles da primeira PSI 51

4. A IDENTIFICAÇÃO DA IMPORTÂNCIA DE UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO NO ÂMBITO DO PJTO 53

4.1. Aspectos Técnicos 53

4.2. Conformidade 53

4.2.1. Resolução CNJ 211/2015 54

4.2.2. Auditoria de Conformidade da Controladoria Interna 54

4.3. Mapeamento dos fluxos de processos para a Gestão da Política de Segurança da Informação 57

4.4. O iGovTIC-JUD 59

5. AVALIAÇÃO DO GRAU DE MATURIDADE DA SEGURANÇA DE INFORMAÇÃO NO ÂMBITO DO PJTO 62

5.1. Estudo de Caso 63

5.1.1. A formalização do Instrumento de Pesquisa 64

5.1.2. O Questionário de Pesquisa 64

5.1.3. O Resultado do Instrumento de Pesquisa 64

5.1.3.1. O Resultado na visão Estratégica 65

5.1.3.2. O Resultado na visão Tática 67

5.1.3.3. O Resultado na visão Operacional 68

5.1.3.4. Consolidação dos Resultados 69

5.1.4. Análise do sistema de pontuação do *framework* da ABNT 27002 70

5.2. Considerações sobre o resultado do teste de *framework* da ABNT 27002 72

6. CONSIDERAÇÕES FINAIS 74

7. REFERÊNCIAS BIBLIOGRÁFICAS 78

APÊNDICES 81

APÊNDICE A – Artigos Publicados 82

APÊNDICE B – Fluxo do Processo de Monitoramento da PSI do PJTO.....83
APÊNDICE C – Questionário 84

1. INTRODUÇÃO

Os adventos da Internet, as tecnologias digitais, o mundo globalizado e suas influências no campo socioeconômico transformaram, de modo considerável, a realidade da vida das pessoas e também dos setores público e privado. As relações econômicas e o acesso às informações foram alterados de forma significativa.

A democratização do acesso ao conteúdo *web*, comércio eletrônico, redes e mídias sociais trazem grandes benefícios à vida moderna. Contudo, trazem também problemas de segurança oriundos do mundo virtual, que podem afetar desde os aspectos econômicos até o comportamento das pessoas.

Os crimes praticados de forma eletrônica provocam polêmicas em torno da interpretação ou falta de legislação. Aliado a isso, cabe destacar questões envolvendo vulnerabilidades, vírus, ataques cibernéticos e fraudes. O mau uso dos recursos computacionais são exemplos de exposição. Este cenário de risco pode afetar economicamente e/ou impedir o alcance dos objetivos das organizações, seja dos setores público ou privado.

Segundo RAMOS (2008), a segurança busca proteção contra situações indesejadas, não previstas, que possam causar prejuízos. E, no mundo eletrônico, a Segurança da Informação lida com um tipo específico de ativo chamado de “ativo de informação, isto é, ativos que geram, processam, manipulam, transmitem e armazenam informações”.

Ainda em RAMOS (2008), como também na ABNT 17799/2005 a Segurança da Informação está balizada em três princípios: **Confidencialidade, Integridade e Disponibilidade**.

Visando garantir a segurança da informação, tem-se então a necessidade de adoção de normas, leis, documentos e políticas que descrevam as regras de negócios das instituições.

Segundo RAMOS (2008), a Política de Segurança da Informação de uma organização é dita como um conjunto de documentos que descreve os objetivos e as regras de negócios. Para os órgãos públicos, a Política de Segurança da Informação (PSI) visa garantir a segurança institucional e deve estar alinhada com a missão, visão e valores institucionais.

Na ABNT 27002 a Política de Segurança da Informação faz parte do Sistema de Gestão da Segurança da Informação - SGSI.

Para compreensão do escopo e atuação deste trabalho de pesquisa é importante conhecer a estrutura organizacional e legislação vigente do Poder Judiciário do Estado do Tocantins

(PJTO), que possui sua estrutura instituída através da Lei Complementar nº 10[1], de 11 de janeiro de 1996, a qual prevê em seu art. 2º que o Tribunal de Justiça, o Conselho da Magistratura, a Corregedoria-Geral da Justiça e a Justiça Militar têm jurisdição em todo o território do Estado.

A referida Lei Complementar também versa sobre a Divisão Judiciária, contemplando as Comarcas e os Distritos Judiciários, onde uma Comarca pode ser constituída de um ou mais municípios contíguos, formando uma Unidade Judiciária, na qual a sede da Comarca é do município que lhe dá o nome (Capítulo 2º).

Trata ainda a Lei Complementar nº 10 da criação, classificação, instalação, elevação, rebaixamento e extinção das Comarcas, sendo que as Comarcas são classificadas em 03 (três) entrâncias, a saber: a) **3ª Entrância** (as com maior volume processual); b) **2ª Entrância** (com volume processual inferior às de 3ª entrância) e c) **1ª Entrância** (Comarcas de menor volume processual).

O art. 13, *caput*, da Lei em comento, nos apresenta quais são os órgãos do Poder Judiciário estadual, a saber: a) **Tribunal de Justiça**; b) **Juízes de direito e juízes substitutos**; c) **Juizados Especiais**; d) **Justiça de Paz**; e) **Tribunais do Júri**; e f) **Conselhos da Justiça Militar**.

O escopo das estruturas organizacionais que são atendidas neste trabalho pode ser resumido da seguinte forma: a) O Tribunal de Justiça do Estado do Tocantins (TJTO), formado pelos Gabinetes dos Desembargadores, Diretorias e suas Unidades Setoriais); b) o Conselho da Magistratura; c) a Corregedoria-Geral de Justiça (CGJUS) e d) Comarcas e Distritos Judiciários do Estado do Tocantins.

Visando prover mecanismos que garantam a confidencialidade das informações, a integridade dos dados e a disponibilidade dos sistemas é que se fez necessário a imersão na segurança da informação aplicado ao Poder Judiciário do Estado do Tocantins (PJTO).

Deste modo, o PJTO editou a primeira versão da Política de Segurança da Informação (PSI), contendo diretrizes, conceitos e normas para uso dos recursos computacionais no âmbito do Poder Judiciário tocantinense, por meio da Portaria nº 3433[2], de 26 de junho de 2017.

Quando da sua criação, a PSI possuía as seguintes normas complementares: a) Norma-TIC-01: Responsabilidades do Usuário; b) Norma-TIC-02: Troca de informações com partes externas; c) Norma-TIC-03: Responsabilidade dos Ativos; d) Norma-TIC-04: Controle de Acesso do Usuário; e) Norma-TIC-05: Manuseio de Mídias; e f) Norma-TIC-06: Controle de Acesso ao Conteúdo *Web*.

---

[1] http://www.tjto.jus.br/joomlatools-files/docman-files/arquivos/legislacao_interna/leis/lei_complementar_10_96.pdf
[2] http://wwa.tjto.jus.br/elegis/Home/Imprimir/1199

No ano de 2019, através das ações relacionadas ao aprimoramento da PSI, ocorreu uma atualização nas diretrizes, nos conceitos e em especial no acréscimo de normas. Assim, com a publicação da Portaria nº 1660[3], de 12 de agosto de 2019, a PSI aplicada ao PJTO passou a contar com duas novas normas complementares, conforme segue: a) Norma-TIC-07: Gestão de Riscos de Segurança da Informação (GRSI) e b) Norma-TIC-08: Gestão de Processos de *Backup*.

Vale ressaltar que a PSI do Poder Judiciário tocantinense foi elaborada por uma equipe técnica e revisada e aprovada pelo Comitê Gestor de Segurança da Informação Multidisciplinar[4] (CGSI) o qual é composto por um Desembargador; um Juiz Auxiliar da Corregedoria-Geral da Justiça; um Juiz de Direito; pelo Diretor-Geral, pelos Diretores Judiciário, Administrativo, de Gestão de Pessoas e de Tecnologia da Informação; e pelo Assessor Militar da Presidência.

Com esta ação, o PJTO cumpre com itens de conformidade previstos na Resolução nº 211[5], de 15 de dezembro de 2015, do Conselho Nacional de Justiça (CNJ), que institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD).

As normas da PSI do PJTO visam garantir a segurança dos ativos[6] da organização, quer sejam os ativos físicos, computacionais e humanos. A PSI pretende garantir o uso eficaz e eficiente dos recursos públicos e cumprir com requisitos de conformidade e de negócios, com foco na segurança dos ativos da instituição.

No cenário da segurança da informação e comunicação, a PSI consiste no regramento da proteção, dos controles, orientando a tomada de decisão com relação aos investimentos em infraestrutura computacional do Poder Judiciário tocantinense.

O presente trabalho de pesquisa objetiva apresentar o estudo sobre a gestão da segurança da informação com a análise das principais normas de conformidade, a identificação da importância da política de segurança da informação, bem como a realização da primeira avaliação do grau de maturidade da segurança da informação, tudo no âmbito do Poder Judiciário do Estado do Tocantins.

[3] http://wwa.tjto.jus.br/elegis/Home/Imprimir/1970
[4] http://wwa.tjto.jus.br/elegis/Home/Imprimir/899
[5] https://atos.cnj.jus.br/atos/detalhar/atos-normativos?documento=2227
[6] Na ABNT NBR ISO/IEC 17799:2005, um ativo pode ser físico, lógico, um recurso humano. Um ativo é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegido.

1.1. Problema

Os recursos computacionais promoveram uma melhoria considerável na prestação jurisdicional, contribuindo para o alcance da missão institucional do Tribunal de Justiça do Estado do Tocantins que é **garantir a cidadania através da distribuição de uma justiça célere, segura e eficaz**.

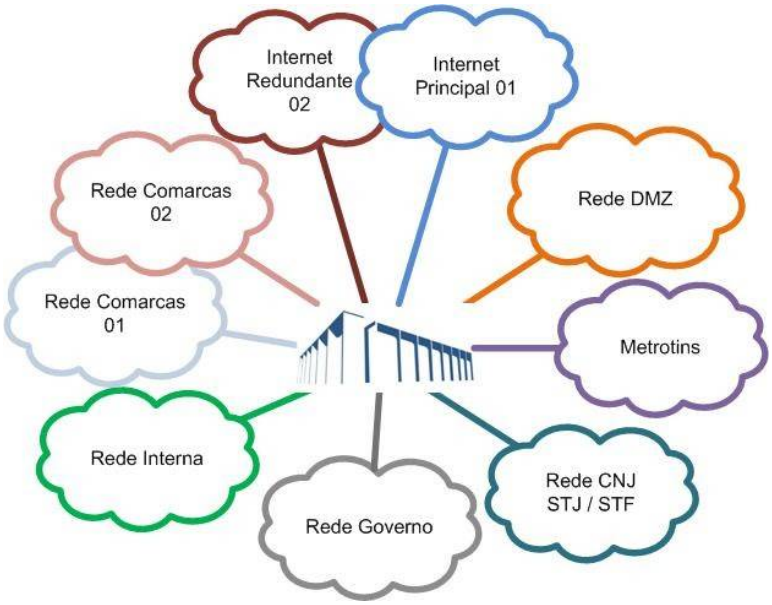
O ambiente computacional do PJTO é formado por aproximadamente 2.500 computadores. Um parque tecnológico desta magnitude requer cuidados que vão além dos recursos tecnológicos, mas sobretudo o regramento destes recursos, em especial, o zelo com a informação que é armazenada ou trafega na rede. Assim, temos um complexo sistema formado por usuários, computadores, sistemas, redes e, no centro, a preocupação com a segurança da informação.

Denominada de REDE TELEJURIS, inaugurada no ano de 2004, a rede de dados do PJTO passou por vários processos de evolução e hoje é formada por várias subredes, dentro de um contexto de gestão, controle e conexão de vários órgãos.

A REDE TELEJURIS é formada por: a) rede da sede do TJTO; b) rede de Serviços (DMZ[7]); c) redes das Comarcas (*Intranet*) composta por dois segmentos/prestadoras de serviço; d) rede de acesso à rede do governo; e) rede de acesso as redes do CNJ, SFT e STJ; f) rede de acesso à rede Metrotins/RNP; e g) as redes de acesso à *Internet* (principal e secundária). A figura 1 possui uma representação gráfica das nove (09) subredes que formam a grande REDE TELEJURIS.

[7] Rede DMZ ou *demilitarized zone*, formada pela rede de serviços para os públicos internos e externo.

Figura 1 - Representação REDE TELEJURIS



O parque tecnológico presente na REDE TELEJURIS pode ser descrito, de forma resumida, da seguinte maneira: a) 02 *Data Centers*; b) 03 Grupos Geradores; c) 03 *Nobreaks* de grande porte; d) 09 Aparelhos de Ar Condicionado de precisão; e) 09 Segmentos de Redes; f) 08 Servidores Hiperconvergentes; f) 03 Servidores *NAS*; g) 02 *Appliances* de *Backup*; h) 90 Servidores Virtuais; i) 11 Servidores Físicos; j) 50 *Firewalls*; l) 50 Servidores de Redes; m) 50 Circuitos de Dados; n) 150 *Access Points*; o) 180 *Switches*; p) 08 Servidores CAS; q) 08 Servidores de Bancos de Dados; r) 09 Servidores de Videoconferência; e s) aproximadamente 2.500 computadores.

Em uma estrutura organizacional composta por recursos humanos, recursos tecnológicos e processos é necessário identificar ameaças e vulnerabilidades, e ainda, mitigar os riscos e impactos que possam comprometer a missão da instituição.

Segundo Sêmola (2014), existem alguns equívocos no processo de implantação da segurança da informação. Assim, destacam-se para o âmbito do PJTO eventuais obstáculos que podem ocorrer, quais sejam:

- Atribuir exclusivamente à área de tecnologia a segurança da informação;
- Posicionar hierarquicamente a equipe de segurança da informação abaixo da diretoria de TI;
- Definir investimentos subestimados e limitados à abrangência dessa diretoria;
- Adotar ferramentas pontuais como medidas paliativas;
- Não cultivar corporativamente a cultura da gestão de riscos;

- Tratar a segurança da informação como projeto e não como processo contínuo.

Diante do exposto, visando implantar a segurança da informação no âmbito do Poder Judiciário Tocantinense, tem-se como destaque a PSI, formada por diretrizes e normas, controles e sobretudo com a ação efetiva de um CGSI.

Desse modo, surge o questionamento acerca de **quais processos foram adotados na gestão da Política de Segurança da Informação bem como qual o grau de maturidade em segurança da informação no Poder Judiciário do Estado do Tocantins?**

Assim sendo, com vistas a responder o referido questionamento, este trabalho analisará normas, resoluções, portarias e práticas adotadas para a implantação da PSI como parte do processo de segurança da informação. E, para avaliar o grau de maturidade da segurança da informação, será aplicado um *framework* da ABNT 27002 as áreas estratégicas, táticas e operacionais do PJTO.

1.2. Justificativa

O PJTO, no ano de 2020, está finalizando o seu segundo ciclo do Planejamento Estratégico, compreendendo o período de 2015 a 2020[8]. Assim, se faz necessário contextualizar as ações motivadoras que provocaram a melhoria da infraestrutura, segurança e governança na área de Tecnologia da Informação e Comunicação (TIC), tendo como base os seguintes eventos:

- No ano de 2011, ocorreu mudança de paradigma do processo físico para o eletrônico com a adoção do Sistema e-Proc[9] (área fim) e SEI[10] (área meio), oriundos do Tribunal Regional Federal da 4ª Região (TRF-4).
- No ano de 2014, foi criado o Comitê Gestor de Segurança da Informação (CGSI) [11], que possui competência para deliberação, tomada de decisões e regulamentação das tecnologias aplicáveis à segurança da informação.
- No ano de 2016 foi criado o Comitê de Governança de Tecnologia da Informação e Comunicação (CGTIC)[12], para atender a conformidade com a Resolução do CNJ

[8] http://www.tjto.jus.br/coges/index.php/planejamento-estrategico/ciclo-2015-2020/plano-estrategico-2015-2020/send/25-plano-estrategico-2015-2020/1111-pe-caderno-final-capa-resol-anexo
[9] http://wwa.tjto.jus.br/elegis/Home/Imprimir/365
[10] http://wwa.tjto.jus.br/elegis/Home/Imprimir/425
[11] http://wwa.tjto.jus.br/elegis/Home/Imprimir/899
[12] http://wwa.tjto.jus.br/elegis/Home/Imprimir/1101

de nº 211/15, no tocante a elaboração e aplicação de processos para a gestão da segurança da informação.

- No ano de 2017, foi publicada a primeira PSI do PJTO através da Portaria nº 3433[13], contendo Diretrizes, Manual de Organização de Conceitos e Normas Complementares.
- E, no ano de 2019, foram realizadas ações visando aprimorar a segurança da informação, tais como: atualização da PSI, mapeamento de fluxos de processos e publicação das Portarias de nº 1660[14] e nº 2361[15].

Cabe destacar que a função do CGSI é orientar a gestão da instituição, visando evitar a interrupção dos serviços e sistemas, assegurando a confidencialidade, a integridade e a disponibilidade das informações. Surge então, a necessidade de aprimorar e avaliar os procedimentos adotados na gestão da segurança da informação no âmbito do PJTO.

Neste contexto, este trabalho justifica-se pela importância dos processos aplicados na PSI, como também em estabelecer mecanismos para realizar a avaliação do grau de maturidade da segurança da informação no âmbito do PJTO, em conformidade com a Resolução do CNJ e norma da ABNT 27002.

A melhoria contínua da segurança da informação atende objetivos da governança judiciária bem como, da melhoria da infraestrutura e governança de TIC, contribuindo assim, com objetivos relacionados ao cumprimento da missão do PJTO que, no ciclo do planejamento estratégico 2015-2020, busca "**garantir a cidadania através de distribuição de uma justiça célere, segura e eficaz**".

1.3. Objetivo Geral

Identificar e analisar os processos adotados na Política de Segurança da Informação (PSI), com base em normas da ABNT, bem como avaliar o grau de maturidade em segurança da informação, visando aperfeiçoamento da mesma no âmbito do Poder Judiciário do Estado do Tocantins (PJTO).

[13] http://wwa.tjto.jus.br/elegis/Home/Imprimir/1199
[14] http://wwa.tjto.jus.br/elegis/Home/Imprimir/1970
[15] http://wwa.tjto.jus.br/elegis/Home/Imprimir/2020

1.3.1. Objetivos Específicos

1. Analisar as principais normas e resoluções de conformidade aplicadas à segurança da informação no âmbito PJTO;
2. Identificar a importância de política de segurança da informação no âmbito PJTO;
3. Avaliar o grau de maturidade da segurança da informação no âmbito PJTO.

1.4. Metodologia

Para este trabalho realizou-se ações, que vão desde a análise da atual PSI, sua construção e viabilidade técnica e operacional, pesquisas em documentos, normas, leis, resoluções e portarias com ênfase na identificação da importância de uma PSI para o PJTO. Realizou-se, também, uma avaliação do grau de maturidade, com base no *framework* da ABNT 27002, na gestão da segurança da informação no PJTO.

Para analisar as principais normas, com foco na conformidade, aplicadas à segurança da informação e identificação da importância de uma PSI no ambiente corporativo, foram realizados estudos em normas, livros, teses, artigos e dados oriundos de fontes indexadas.

Assim, na revisão da literatura, foram analisados trabalhos científicos e normas relevantes para o tema como: RAMOS (2008), NOCÊRA (2009), SEMOLA (2014), ABNT 17799:2005, ABNT 27001:2013 e ABNT 27002:2013.

Durante a pesquisa documental foram realizados estudos de documentos oficiais, como: leis, portarias, resoluções, normas e decretos relacionados ao TJTO, CNJ e outros.

Com relação ao processo de avaliação do grau de maturidade da segurança da informação no PJTO, foi confeccionado um formulário, com base no *framework* de conformidade com a ABNT 27002 e submetido às áreas estratégica, tática e operacional com foco na gestão do TJTO. Desta forma, tem-se como fruto deste trabalho, o resultado da primeira avaliação dos processos de segurança da informação, da percepção e avaliação do grau de maturidade em segurança da informação do PJTO.

A seleção dos materiais literários usados neste estudo ocorreu a partir dos seguintes critérios: a) conceitos de gestão da segurança da informação, com foco na política de segurança da informação; b) ausência de delimitação do tempo de publicação; c) idiomas em português e inglês.

Baseado em *Waslawick* (2014), a metodologia de pesquisa tem como objetivo subsidiar os caminhos para o alcance dos objetivos. Assim, a execução e desdobramentos se tornam fatores críticos de sucesso para a busca de resultados satisfatórios. A metodologia utilizada pode resumida no Quadro 1.

Quadro 1 - Metodologia Científica Aplicada à Pesquisa (Elaborado pelo Autor).

Metodologia	**Especificações**
Natureza	Aplicada
Objetivo	Exploratório
Abordagem	Qualitativa
Procedimentos	Estudo de leis, resoluções, portarias, processos administrativos, normas e referencial bibliográfico
Perspectivas	Aprimoramento da gestão segurança da informação, com foco na política de segurança da informação e avaliação do grau de maturidade na segurança da informação do PJTO

Ainda segundo *Waslawick* (2014), Silva e Menezes (2005), uma pesquisa pode ser classificada conforme os seguintes aspectos: quanto à natureza; aos objetivos; à abordagem e aos procedimentos. Então, a presente pesquisa foi classificada conforme segue abaixo.

1.4.1. Quanto à Natureza

A pesquisa será de natureza aplicada, pois objetiva obter conhecimentos e padrões que foram aplicados na construção da PSI do âmbito do PJTO.

O desenvolvimento de procedimentos necessários para a gestão da PSI, contemplando o processo de atualização, alteração e/ou confecção de novas normas, aliado ao resultado da avaliação do grau de maturidade da gestão da segurança da informação no PJTO, resultante da aplicação do *framework* de conformidade com ABNT NBR 27002, servirão de subsídios para que o CGTIC, bem com o CGSI, possam priorizar ações relacionadas aos planos de contratações, capacitações, deliberações e tomada de decisões para o aprimoramento da segurança da informação.

1.4.2. Quanto aos Objetivos

Os objetivos desta pesquisa serão exploratórios, pois pretende-se analisar um conjunto de documentos, leis, portarias, resoluções, levantamento bibliográfico e documentos de referência adotados no PJTO.

1.4.3. Quanto à Abordagem

A pesquisa realizada teve abordagem qualitativa, pois realizou a análise desde a criação do CGSI e da PSI, dos procedimentos adotados para atualizações e da criação de novas normas. Em seguida, avaliou-se o grau de maturidade da gestão da segurança da informação no PJTO, através da aplicação de um *framework* de conformidade previsto na ABNT 27002.

1.4.4. Quanto aos Procedimentos

Nos procedimentos metodológicos foram usados: pesquisa em material bibliográfico, análise de documentos, normativas e resoluções pertinentes ao PJTO e realização de um estudo de caso, conforme descritos a seguir:

Pesquisa Bibliográfica

Quanto aos procedimentos bibliográficos, foram necessários pesquisa em material bibliográfico, tais como estudos de artigos, teses, livros, normas, publicações usualmente disponibilizadas por fontes indexadas. Neste trabalho, utilizou-se desde revisão da literatura como trabalhos científicos e conformidade com normas relevantes para o tema pesquisado. Para isto, foram realizadas pesquisas em materiais de autores como: RAMOS (2008), NOCÊRA (2009), SEMOLA (2014), FONTES (2017), ABNT 17799:2005, ABNT 27001:2013 e ABNT 27002:2013.

Pesquisa Documental

A pesquisa documental foi iniciada com análise da Resolução TJTO Nº 22, de 16 de outubro de 2014, que instituiu o CGSI no âmbito do PJTO. No artigo 5º da Resolução do TJTO de nº 22/2014, diz:

> "Compete à Diretoria de Tecnologia da Informação prover o apoio necessário à implementação e compreensão da Política de Segurança da Informação - PSI deste Poder Judiciário".

Apesar da Resolução do TJTO de nº 22, ter sido publicada no ano de 2014, somente no ano de 2015 foi designado grupo de trabalho para elaboração da Minuta da PSI. Assim, foi realizada uma pesquisa documental, tendo como referência a Resolução de nº 211 de 15 de dezembro de 2015 do CNJ, que Institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD).

O artigo 9º da Resolução CNJ 211/2015, diz:

> "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 de Segurança da Informação, e em harmonia com as diretrizes nacionais preconizadas pelo Conselho Nacional de Justiça".

Visando atender a Resolução do CNJ de nº 211/2015, foram realizados os mapeamentos de processos da gestão da política de segurança da informação, edição de novas normas, que foram submetidas e aprovadas pelo CGSI, gerando a publicação de novas portarias.

Estudo de Caso

Para compreensão situacional da segurança da informação foi realizado um estudo de caso com a aplicação de um questionário, com base no *framework* de conformidade com a ABNT 27002, tendo como objetivo conhecer o grau de maturidade da segurança da informação do PJTO.

Assim, a partir do resultado desse questionário, será possível analisar a efetividade e resultados alcançados através dos procedimentos, resoluções, portarias e demais atos praticados pelo TJTO no cumprimento de normas e resoluções do CNJ bem como, normas da ABNT.

1.5. Estudos Técnicos Preliminares

Os estudos técnicos preliminares deste trabalho acadêmico possui como premissa o aprimoramento da segurança da informação aplicada ao PJTO. Desta maneira, foi necessário fazer uma imersão nos documentos oficiais do Poder Judiciário, como leis, portarias, resoluções, normas, decretos e leis do TJTO e do CNJ. Além disso, foi realizada a análise de conformidade e cumprimento de itens de da Resolução do CNJ de nº 211/2015. Desta forma os estudos técnicos preliminares oportunizaram o desenvolvimento e aplicabilidade dentro de contextos de gestão, na área administrativa e de publicação de artigos na área acadêmica.

1.5.1. Atuação na Área Administrativa

A atuação no campo administrativo do PJTO compreende a participação efetiva deste Mestrando junto aos Comitês de segurança (CGSI) e de governança (CGTIC), no desenvolvimento, na apresentação de minutas de portarias, justificando a relevância dos temas no CGSI, atuação na deliberação e remessa para publicação junto a Presidência do TJTO.

Com relação a publicações no âmbito do PJTO que contribuíram para o aprimoramento da segurança da informação no PJTO, destacam-se as seguintes ações:

- A revisão e atualização da Portaria TJTO nº 3433/2017[16], que institui a PSI, no âmbito do PJTO;
- A publicação da Portaria TJTO nº 1660/2019[17], que altera a Portaria Nº 3433 de 2017 em seu conteúdo e inclui normas de gestão de risco de segurança da informação e de gestão dos processos de *backup*;
- A publicação da Portaria TJTO nº 2361/2019[18], que designa membros para o CGSI e cria um Grupo de Trabalho de Apoio ao Comitê Gestor de Segurança da Informação Multidisciplinar (GT-CGSI).

1.5.2. Atuação na Área Acadêmica

No campo acadêmico destacam-se as pesquisas na busca por um instrumento de avaliação do grau de maturidade da segurança da informação em conformidade com norma da ABNT 27002 e sobretudo na publicação de artigos com temas que pudessem contribuir com o aprimoramento da segurança da informação e serem aplicadas no âmbito do PJTO.

As publicações científicas, na forma de artigos, com temas relacionados ao aprimoramento da segurança da informação, versam sobre as áreas de gestão de riscos, automação e gestão de ativos de TIC:

- *Mapping Of Information Technology Risks In The Judiciary Tocantinense* [19] (Mapeamento de Riscos no Poder Judiciário do Tocantins): Que trata de um estudo e desenvolvimento de metodologia para gestão de riscos baseada nas Normas ABNT NBR ISO/IEC 27005, contemplando a definição do contexto, o processo de avaliação de riscos e tratamento dos mesmos. A Norma ABNT NBR ISO/IEC 31000 descreve seleção e aplicação de técnicas sistemáticas para o processo de avaliação de riscos.
- Gerenciamento Remoto de Recursos de *Softwares* no Tribunal de Justiça do Tocantins [20]: que descreve a evolução dos procedimentos e ferramentas usadas na automação de tarefas usadas para padronizar os aplicativos para o usuário final,

[16] http://wwa.tjto.jus.br/elegis/Home/Imprimir/1199
[17] http://wwa.tjto.jus.br/elegis/Home/Imprimir/1970
[18] http://wwa.tjto.jus.br/elegis/Home/Imprimir/2020
[19] https://www.journalijdr.com/mapping-information-technology-risks-judiciary-tocantinense
[20] https://revista.unitins.br/index.php/humanidadeseinovacao/article/view/2525/1679

bem como os sistemas operacionais usados nos computadores das sedes das Comarcas, Anexos e do Tribunal de Justiça, sobretudo na implantação do *FOG Project* como um serviço oficial para a gestão e manutenção dos Sistemas Operacionais.

1.6. Estruturação do Trabalho

Este documento está organizado em seis (06) capítulos, iniciando com este capítulo de introdução, seguido pelo referencial teórico, com principal foco na Política de Segurança da Informação no Poder Judiciário do Estado do Tocantins e demais capítulos descritos a seguir:

O Capítulo 1 descreve o caminho metodológico utilizado para atingir os objetivos propostos, contendo Introdução, Problema, Justificativa, Objetivo Geral e Específicos, Metodologia e o resumo dos estudos técnicos preliminares.

O Capítulo 2 apresenta a revisão de literatura acerca dos temas afetos à Política de Segurança da Informação aplicado ao Poder Judiciário do Estado do Tocantins, tendo como base a ABNT 27002. No Capítulo 3 é realizada uma análise das principais normas de conformidade aplicadas à segurança da informação no âmbito do PJTO.

Já no Capítulo 4 é descrita a importância da gestão da política de segurança da informação no âmbito do PJTO e no Capítulo 5 é realizada uma avaliação do grau de maturidade da segurança da informação no âmbito do PJTO, conforme teste de *framework* da ABNT 27002.

No Capítulo 6 são apresentadas as considerações finais do trabalho, bem como são indicados os pontos a serem aplicados ao PJTO.

2. REVISÃO DE LITERATURA

Neste capítulo serão abordados os conceitos da segurança da informação relacionados à segurança, aos ativos, à segurança da informação, as normas da ABNT, os conceitos da política de segurança da informação e a conformidade com a ABNT 27002.

2.1. Segurança

O termo segurança possui origem do latim, significa “sem preocupações” e possui inúmeras aplicações e inúmeros contextos. No presente trabalho, o termo segurança será compreendido como a capacidade de resolução de preocupações, ou seja, de problemas.

Assim, considerando a realidade, algumas preocupações estão presentes no âmbito das relações públicas e privadas. Em RAMOS (2008), temos como exemplo um recorte com uma lista de eventuais problemas:

- Terrorismo;
- Criminalidade;
- Crimes eletrônicos;
- Aprimoramento do direito internacional;
- Discordância de legislação (direitos e patentes);
- Aumento dos *softwares* maliciosos;
- Fraudes financeiras;
- Pirataria;
- Espionagem;
- Guerra cibernética.
- Outros

Tais exemplos de problemas trazem prejuízos financeiros e afetam a imagem nas relações de negócios dos segmentos públicos e privados. Um único problema pode impedir o alcance dos objetivos de uma organização, gerando inúmeras preocupações. Então, um problema, ou um conjunto deles, no contexto deste trabalho, é considerado um problema de segurança.

Conforme RAMOS (2008), nas organizações, a segurança é vista como uma capacidade de tratar problemas e incertezas, podendo ser aplicada naquilo que afeta sua missão e seus valores. Assim, aquilo que possui valor para uma organização e necessita de proteção, é denominado de ativo, ressaltando que os ativos presentes neste trabalho são os intangíveis, os lógicos, os físicos e os humanos.

2.2. Ativos

O termo ativo é usado em várias áreas e/ou profissões. No geral, um ativo é tudo aquilo que possui valor. Contudo, em RAMOS (2008) temos uma classificação de ativo, que será usada neste trabalho. Assim, os ativos podem ser classificados ou agrupados de acordo com suas características ou conceitos.

Segundo RAMOS (2008, pág. 17) os ativos podem ser classificados da seguinte forma:

Quadro 2 - Classificação de Ativos

Categoria de Ativos	**Exemplo**
Tangíveis	Informações (impressas ou digitais) Impressoras Móveis de escritório
Intangíveis	Imagem da empresa Confiabilidade de um órgão (PJTO) Marca ou produto
Lógicos	Dados armazenados sem Servidor Rede lógica (configuração de uma rede VoIP)
Físicos	Estação de trabalho Rede física (Equipamentos de rede física como switches)
Humanos	Servidores Prestadores de Serviços

Observamos que a classificação de ativos e suas características e as proteções para garantir a segurança dos ativos, também possuem suas particularidades. No Quadro abaixo temos uma visão das proteções de acordo com tipo de ativo:

Quadro 3 - Tipo de proteção de Ativos

Tipo de Proteção	**Exemplo**
Lógicos	Permissão em servidor de arquivos Regras de *Firewalls* Perfis de acessos dos usuários e aplicações
Físicos	Portas Fechaduras Guardas
Administrativos	Políticas Normas Procedimentos

Com base nos conceitos de segurança e ativos, temos então que pensar em segurança do ativo intangível, de grande relevância na atualidade, que é a informação. Assim, temos que a proteção do ativo de informação, em especial os que geram, processam, manipulam, armazenam e transmitem informações é visto como um ativo de Segurança da Informação.

Na ABNT 27002, os conceitos de valor, ativos e do tipo informação, reforçam a importância da segurança da informação:

> "O valor da informação vai além das palavras escritas, números e imagens: conhecimento, conceitos, ideias e marcas são exemplos de formas intangíveis da informação. Em um mundo interconectado, a informação e os processos relacionados, sistemas, redes e pessoas envolvidas nas suas operações são informações que, como outros ativos importantes, têm valor para o negócio da organização e, consequentemente, requerem proteção contra vários riscos".
> (...)
> "Ativos são objeto de ameaças, tanto acidentais como deliberadas, enquanto que os processos, sistemas, redes e pessoas têm vulnerabilidades inerentes. Mudanças nos processos e sistemas do negócio ou outras mudanças externas (como novas leis e regulamentações), podem criar novos riscos de segurança da informação. Desta forma, em função das várias maneiras nas quais as ameaças podem se aproveitar das vulnerabilidades para causar dano à organização, os riscos de segurança da informação estão sempre presentes. Uma segurança da informação eficaz reduz estes riscos, protegendo a organização das ameaças e vulnerabilidades e, assim, reduzindo o impacto aos seus ativos".
> (...)
> "A segurança da informação é alcançada pela implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, quando necessário, para assegurar que os objetivos do negócio e a segurança da informação da organização sejam atendidos. Um sistema de gestão da segurança da informação (SGSI), a exemplo do especificado na ABNT NBR ISO/IEC 27001".

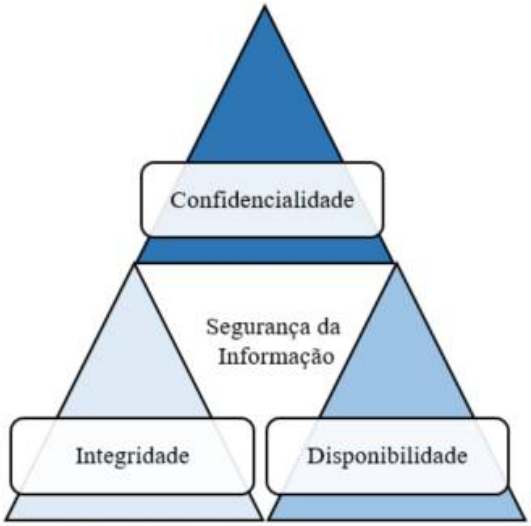
2.3. Segurança da Informação

A Segurança da Informação pode ser compreendida como um conjunto de ações visando a proteção de ativos do tipo informação. Assim, a Segurança da Informação está balizada em três princípios básicos, conforme ABNT 17799:

- Confidencialidade;
- Integridade;
- Disponibilidade.

Conforme RAMOS (2008), a pirâmide ou tríade da Segurança da Informação pode ser representada da seguinte forma (figura 2):

Figura 2 - Tríade da Segurança da Informação – (adaptação do Autor)



A Confidencialidade está relacionada ao sigilo, em garantir que a informação possa ser acessada para quem de fato deve ter o direito ao acesso. A Integridade envolve a proteção da informação no seu estado original, ou seja, garantia de que a informação não foi alterada e a Disponibilidade trata da garantia do acesso à informação para quem necessita da informação.

A tríade da Segurança da Informação traz um conceito clássico e consiste na base para a segurança da informação. Contudo, para FONTES (2017), quando se trata da proteção da informação, além da Confidencialidade, Integridade e Disponibilidade podem ser inseridos:

- Legalidade: em que o uso da informação deve estar de acordo com a legislação pertinente, os contratos e as licenças, seguindo os princípios éticos desejados pela sociedade;
- Auditabilidade: em que o acesso e o uso da informação devem ser registrados, possibilitando a identificação de quem fez o acesso e o que foi feito com a informação;
- Não repúdio de autoria: onde o usuário que gerou ou alterou a informação não pode negar o fato, pois existem mecanismos que garantem sua autoria, ou seja, a garantia da autenticidade.

Desta feita, temos em RAMOS (2008) os conceitos clássicos da segurança da informação e em FONTES (2017) o acréscimo de importantes elementos, como a necessidade de se ter em mãos os registros das atividades, a capacidade de identificação, a comprovação da autenticidade e as questões correlatas à legalidade do acesso às informações.

2.3.1. Fatores a serem observados na Segurança da Informação

Para o alcance da Segurança da Informação, faz-se necessário observar alguns fatores como: Valor, Ameaça, Vulnerabilidade, Impacto e Risco. Para tal, baseado em RAMOS (2008) temos seguintes fatores:

Quadro 4 - Fatores a serem observados na Segurança da Informação

Fator	Descrição
Valor	A importância do ativo para a organização, podendo ser avaliado em propriedade mensurável como o lucro provido, ou propriedade abstrata como a imagem de uma organização
Ameaça	Um dado evento com capacidade de comprometer os objetivos da organização ou trazer danos aos ativos físicos, lógicos e humanos
Vulnerabilidade	Uma ausência de controle que possa favorecer o sucesso das ameaças.
Impacto	Um prejuízo causado pela ocorrência de falhas ou falta de controles, assim, o impacto e o dano causado, depende do tipo de ameaça que se concretizou.
Risco	É uma métrica, um indicador da probabilidade de que uma determinada ameaça se concretize. Quanto maior a probabilidade de uma ameaça ocorrer, e o impacto que ela trata, maior será o risco deste incidente.

2.3.2. As categorias mais comuns de problemas na Segurança da Informação

Os problemas mais comuns de segurança podem ser categorizados da seguinte forma: Natural, Acidental e Intencional. Assim, baseado em RAMOS (2008), apresentamos, a seguir, os exemplos comuns de origem dos problemas de segurança:

Quadro 5 - Categoria de problemas na Segurança da Informação

Origem do Evento	Exemplo
Natural	Chuvas e queimadas
Acidental	Erro de usuário Falhas dos sistemas Falha de energia elétrica
Intencional	Invasões físicas e/ou lógicas Sequestro de dados Espionagem e vazamento de informações

2.4. Normas da ABNT

As normas ABNT 27001:2013 e ABNT 17799:2005, tratam sobre a tecnologia da informação, técnicas de segurança, sistema de gestão de segurança da informação e código de prática para a gestão da segurança da informação e ambas se dividem em várias áreas de controles. A política de segurança é uma dessas áreas de controle e, em consequência, é imprescindível criar uma PSI, que segundo Beal (2005, pág. 43) é:

> "O documento que registra os princípios e as diretrizes de seguranças adotados pela organização, a serem observados por todos os seus integrantes e colaboradores e aplicados a todos os sistemas de informação e processos corporativos".

De acordo com Fontes (2012, pág. 12), existe a necessidade da implantação da PSI:

> "É estrutural que a organização tenha uma política de segurança da informação para que o processo de proteção da informação possa ser elaborado, implementado e mantido. Essa política (ou conjunto de políticas) definirá as diretrizes, os limites e o direcionamento que a organização deseja para os controles que serão implantados na proteção da sua informação."

A PSI, segundo Araújo e Ferreira (2008, pág. 37) deve:

> "Ser criada antes da ocorrência de problemas com a segurança, ou depois, para evitar reincidências. Ela é uma ferramenta tanto para prevenir problemas legais como para documentar a aderência ao processo de controle de qualidade".

2.5. A Política de Segurança da Informação

A ABNT 27001:2013 recomenda que pessoas que estejam sob o comando da organização devem estar cientes da Política de Segurança da Informação (PSI) e, também, devem colaborar com a sua melhoria, reportando implicações de não conformidade com a gestão da segurança da informação.

Segundo RAMOS (2008, pág. 96), a elaboração de uma Política de Segurança da Informação é de responsabilidade do *Security Officer* e/ou Gestor da Segurança do departamento.

Uma equipe de desenvolvimento deve ser formada por:

- Principais
    - Comitê Executivo de Segurança da Informação;
    - Profissionais de Segurança da Informação;
    - Profissionais de Tecnologia.
- Opcionais

- Jurídico;
- Recursos Humanos;
- Segurança Física e Patrimonial;
- Auditoria;
- Usuários.

Conforme RAMOS (2008, pág. 99), a estruturação de uma política, pode ser dividida em três grupos:

- Diretrizes: Regras de nível estratégico;
- Normas: Regras de nível Tático;
- Instruções e Procedimentos: Regras de nível operacional.

A manutenção da PSI é necessária em virtude das constantes mudanças da organização, conforme RAMOS (2008, pág. 100), que afirma:

> "Por conta das constantes mudanças às quais as organizações se submetem, as políticas devem ser constantemente atualizadas para refletirem tais mudanças".

Para que um sistema de segurança seja efetivo é necessário que todos colaborem com as medidas adotadas. A participação universal é fator crucial de sucesso da política. O monitoramento de incidentes deve ser constante para avaliar a eficácia das políticas. Segundo RAMOS (2008, pág. 102), um canal de comunicação e colaboração deve existir para que seja possível:

- Permitir que o processo de monitoramento alcance um escopo maior que aquele que a equipe de segurança consegue e é capaz de controlar, aumentando a capacidade de resposta da instituição;
- Servir para coleta de informações estatísticas utilizadas para o abastecimento das métricas de eficácia da segurança;
- Permitir o desenvolvimento de sinergia entre os colaboradores e a área de segurança, fazendo com que eles vejam a utilidade de sua colaboração e sintam o reconhecimento devido.

Sabemos que o mundo ao nosso redor vive passando por mudanças e com as organizações ocorre o mesmo, sendo necessário o aprimoramento constante. Partindo dessa premissa, é vital que a PSI também esteja em constante evolução. Caso contrário, será um conjunto de documentos que deixarão de fazer sentido e serão abandonados. RAMOS (2008, pág. 103) diz

que: “quanto mais tempo levarmos para atualizar as políticas, maior será a probabilidade de que elas se tornem inadequadas”.

Em Nocêra (2009), planejar, executar, checar e agir, também conhecido como PDCA (*plan – do – check – act*), está presente nas metodologias da gestão de projetos. O ciclo evolutivo presente no PDCA também pode ser aplicado à gestão da segurança da informação, uma vez que a política de segurança da informação tende a evoluir de acordo com as necessidades da organização, neste caso, no PJTO.

Com base em Sêmola (2004), a segurança da informação é a área do conhecimento que trata da proteção de ativos do tipo informação, objetivando garantir a confiabilidade, integridade e disponibilidade das informações, validando assim o conceito da tríade da segurança da informação. Portanto, é notória a importância de uma Política de Segurança da Informação nas organizações público e privada.

2.6. A Conformidade com a ABNT 27002

Para assegurar a qualidade e o reconhecimento dos produtos e serviços, seja no meio público ou privado é necessária a adoção de boas práticas. A busca pela conformidade tem sido fundamental ao alcance deste objetivo. Por isso, no que diz respeito à PSI no PJTO, a busca pela atualização e gestão deve passar por uma avaliação. Assim, temos como norte o *framework* de conformidade com a norma 27002 da ABNT Associação Brasileira de Normas Técnicas - ABNT.

Em Sêmola (2014, pág. 139), temos que as normas servem para sugerir parâmetros comuns a um determinado assunto.

> “As normas surgiram para sugerir bases comuns, cada qual com sua especificidade, como vemos na ISO 9001 (Qualidade) e na ISO 14000 (Meio Ambiente). São exemplos de critérios, padrões e instrumentos de controles aplicáveis parcial ou totalmente em função de natureza de cada negócio, que acabaram formando cultura e recebendo o reconhecimento mundial de segmentos específicos. ”

Assim, para área da Segurança da Informação, foi criada a norma 27002:2013, publicada pela ABNT.

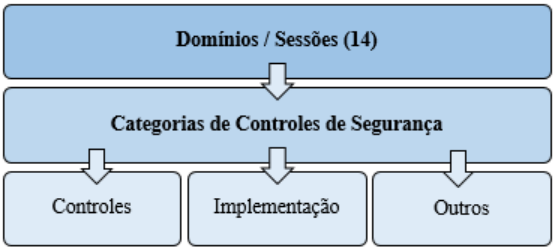
É importante ressaltar que a ABNT 27002:2013 possui sua base conceitual na ABNT 17799:2000, que por sua vez possui base na Norma Britânica BS 7799. A partir da ABNT 17799, foram criadas as normas ABNT 27001:2013 e ABNT 27002:20103.

A importância da ABNT 27002:2013 é notória por tratar de uma série de práticas de gestão da segurança da informação **abordando 14 temas ou domínios, organizados em 35 grupos, contendo, ao total, 114 controles** aplicados à Segurança da Informação.

2.6.1. O *Framework* e os Controles de Segurança

A estrutura do *framework* da ABNT 27002:2013 é formada por quatorze (14) domínios de controle de segurança, onde cada um contém várias categorias de controle de segurança. Assim, dentro de cada categoria de controle de segurança, a ABNT 27002 estabelece controles suportados e orientações para a sua implementação. A figura 3 ilustra a arquitetura do *framework* da ABNT 27002.

Figura 3 - Conceito da organização do *framework* da ABNT 27002



Observa-se, portanto, que estruturas de controles de segurança possuem caráter descritivo e não prescritivo. Desta forma, podem ser adaptadas e referenciadas por todas as organizações, independentemente do tamanho ou da natureza, se públicas ou privadas.

A aplicação de um *framework* de controles de segurança, definido pela ABNT 27002:2013, dentro do sistema de gestão da segurança da informação é o caminho para a obtenção da Certificação ABNT 27002 que confere valor ao alcance dos objetivos estratégicos e às diretrizes das empresas e/ou órgãos públicos.

Contudo, segundo Sêmola (2014, pág. 141), o caminho que conduz à efetividade da conformidade é longo, requer coordenação, planejamento e seleção dos controles aplicáveis. Então, os trabalhos são iniciados tendo como referência as seguintes ações:

- Definição das diretrizes da Política de Segurança da Informação;
- Definição do Sistema de Gestão da Segurança da Informação;
- Execução de uma análise de riscos;
- Definição de uma estrutura para o gerenciamento de riscos;
- Seleção dos objetos de controles e os controles aplicáveis;
- Preparação da declaração de aplicabilidade dos controles;

- Implementação dos controles.

As ações acima descritas fornecem um caminho para a conformidade com a ABNT 27002:2013. Contudo, é importante conhecer o teor de cada um dos quatorze (14) domínios presentes no Sistema de Gestão da Segurança da Informação.

2.6.2. O Sistema de Gestão da Segurança da Informação

O Sistema de Gestão da Segurança da Informação (SGSI) sugerido na ABNT 27002:2013, aplicada a uma organização, descreve a eventual atuação em quatorze (14) domínios de controles de segurança, sendo que o **primeiro domínio** trata das Políticas de Segurança da Informação, onde é verificada a existência do documento com o teor da Política de Segurança da Informação na organização.

Já o **segundo domínio** versa sobre a organização da segurança da informação. Este domínio possui controles que verificam a existência de responsável, definições de papéis, atribuições, acordos de cooperação, gerenciamento de projetos e políticas para dispositivos móveis.

No **terceiro domínio,** o tema é afeto à segurança dos recursos humanos e possui controles em que são tratados os critérios de seleção, contratação, capacitação, processos administrativos disciplinares e encerramento de contratos de recursos humanos.

A gestão de ativos é abordada no **quarto domínio** onde são verificados controles que tratam dos inventários dos ativos físicos, tecnológicos e humanos. Ainda são analisados a classificação da informação, gestão e descarte de mídias.

O **quinto domínio,** que versa sobre os controles de acesso, possui controles que atuam nas regras de negócios para controle de acesso dos usuários às redes, aos sistemas e aplicações. Então, chegamos no **sexto domínio** que trata das políticas e gestão dos recursos afetos ao uso de criptografia.

A segurança física do ambiente está presente no **sétimo domínio** onde são tratados os controles de definições de perímetro, manutenção de equipamentos, infraestrutura elétrica, cabeamento e gestão de equipamentos.

No **oitavo domínio** são tratadas questões relacionadas à segurança das operações. Nesse domínio são avaliados os controles de responsabilidades, a definição dos procedimentos operacionais, gestão de mudança e capacidade. Nota-se o nível de exigência e complexidade neste domínio, uma vez que cuida da segregação dos ambientes, proteções, procedimentos de cópia, registros de *logs*, atualização e auditoria nos sistemas.

A segurança das comunicações está presente no **nono domínio**, no qual encontram-se os aspectos como o gerenciamento e segregação de redes, políticas para transferência e proteção de mensagens e, por fim, os acordos de confidencialidade.

No **décimo domínio** são observados os procedimentos para aquisição, desenvolvimento e manutenção de sistemas. Neste domínio, são analisados controles para requisitos, garantia, desenvolvimento, documentação, aceitação e testes nos sistemas.

O relacionamento da cadeia de suprimento, em que são verificados requisitos de entregas dos produtos e serviços junto aos fornecedores, faz parte do **décimo primeiro domínio**.

O **décimo segundo domínio** diz respeito aos requisitos da gestão de incidentes de segurança da informação. As questões que tratam da disponibilidade e redundância estão presentes no **décimo terceiro domínio,** denominado como os aspectos da segurança da informação na gestão da continuidade do negócio.

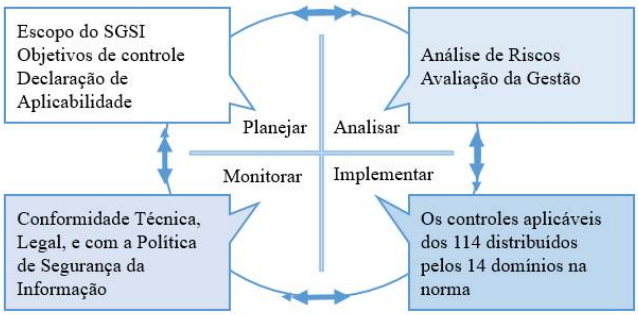
E por fim, tem-se o **décimo quarto domínio**, que versa sobre a conformidade. Neste domínio são analisados os requisitos legais, contratuais, documentação, implementações, controles para a privacidade, etc.

O **décimo quarto domínio**, que trata da conformidade, tem sido fator decisivo crítico de sucesso para que as organizações promovam as adequações necessárias para a adesão e conformidade com o Sistema de Gestão da Segurança da Informação (SGSI), definido na NBR ISO/IEC 27002:2013, bem como as regulamentações institucionais pertinentes à organização.

Como trata-se de um universo amplo, é necessário que as organizações façam a auto avaliação através de um teste de conformidade, previsto no *framework* de conformidade da ABNT 27002:2013. Assim, será possível verificar em que situação a organização se apresenta, além de servir de subsídio para auxiliar na tomada de decisão na busca pela gestão da segurança da informação.

Considerando a ABNT 27002:2013 e baseado em Sêmola (2014), o processo de melhoria contínua do SGSI é representado da seguinte forma:

Figura 4 – Processo de melhoria contínua de um SGSI (Adaptação do Autor)



Na figura 4 pode-se notar que na fase de planejamento é construído o escopo do sistema de gestão da segurança da informação através da declaração e definição dos domínios e respectivos controles que serão aplicados. Na análise, são realizadas as análises de riscos e avaliação da gestão. Já na fase de implementação são aplicados os controles de acordo com os domínios. E na fase de monitoramento é verificada a conformidade com a política de segurança da informação.

No sistema de gestão da segurança da informação, a política de segurança da informação se apresenta como um importante instrumento de normatização, pois define as regras de negócio para o uso adequado dos recursos e ativos de uma organização. Portanto, a PSI deve ser aprimorada de forma contínua, sistematizada e atualizada de acordo com a própria evolução da organização.

2.6.3. O teste de conformidade do *framework* da ABNT 27002

Sêmola (2014) desenvolveu um instrumento de auxílio para a percepção do grau de aderência das organizações públicas e/ou privadas, em relação às recomendações de segurança da informação da ABNT 27002.

Em Sêmola (2014, pág. 143), temos que o próprio autor considera o teste como superficial. Contudo, trata-se de uma forma simples e rápida de se fazer um diagnóstico. Formado por perguntas objetivas com pontuação associada, o teste mostrará a percepção em relação ao grau de aderência da organização aos controles sugeridos pela norma da ABNT 27002.

O teste elaborado por Sêmola (2014) é formado por **59 questões, abordando questões afetas aos 14 domínios de controles de segurança**. Todas as questões possuem três opções para pontuação.

O Apêndice C contém o teor do formulário do questionário baseado no *framework* de conformidade com a ABNT 27002 adaptado para a realidade do PJTO.

2.6.4. A metodologia de pontuação da aplicação do *framework* de conformidade com a ABNT 27002

Em Sêmola (2014), as respostas e pontuações são aplicadas da seguinte forma. A resposta “A” = “SIM”, valem 2 pontos, já a resposta “B” = “SIM, porém desatualizada”, vale 1 ponto e por fim, a opção “C” = “NÃO” onde não é somado nem subtraído ponto algum. Conforme descrito na Quadro 6:

Quadro 6 - Sistema de pontuação das respostas do *framework* da ABNT 27002

Pontuação do *framework* de conformidade com a ABNT 27002 proposto por Sêmola (2014)	
Resposta	**Pontuação**
SIM	Soma-se 2 pontos
SIM, porém desatualizados	Some-se 1 ponto
Não	Não soma e nem subtrai pontos

Após o preenchimento do questionário, baseado no *framework* de conformidade com a ABNT 27002, adaptado para a realidade do PJTO, é necessário fazer a somatória dos pontos, conforme pontuação, apresentado no Quadro 6 para se obter o índice de maturidade, conforme *framework* proposto por Sêmola (2014).

2.6.5. O índice da situação da organização segundo o *framework* de conformidade com a ABNT 27002

Conforme Sêmola (2014, pág. 150), com a análise do resultado da pontuação, obtida através da pontuação do teste de conformidade do *framework* da ABNT 27002, é possível fazer a análise de riscos bem como verificar em que situação a organização está aderente ou não com relação às referências nacionais e internacionais no tocante a segurança da informação.

Considerando que são 14 domínios, que as organizações possuem realidades estruturais e econômicas diferentes, então é necessário relativizar o fato dos resultados serem alcançados em um determinado domínio e em outros não.

Vale destacar que o resultado do teste de conformidade do *framework* da ABNT 27002, apesar ser relativamente superficial, já traz um norte, um indicador do caminho para se fazer o levantamento de ameaças, impactos, vulnerabilidades físicas, tecnológicas e humanas.

Isto posto, com base em Sêmola (2014), foi adaptado e confeccionado um modelo conceitual, para a interpretação e análise de cenário após a aplicação do *framework* da ABNT 27002, formado por três classificações, contendo a pontuação e suas características. O Quadro 7 apresenta o resumo desta análise, da seguinte forma:

Quadro 7 - Análise de cenário da aplicação do *framework* da ABNT 27002 (adaptação do Autor)

Pontuação	Situação conforme teste do *framework* da ABNT 27002
De 0 a 38	A situação não é confortável para a organizações público e/ou privado; A Segurança não está sendo tratada como prioridade; Ausência ou ineficiência dos controles recomendado pela norma; Desconhecimento dos riscos pela alta gestão; A segurança não é considerada pelos clientes como fator crítico de sucesso; Ações isoladas e não coordenadas não geram o impacto e resultado esperado.
De 39 a 77	A organização mostra bom nível de consciência, mas também deficiência na estrutura, gestão ou falta de recursos financeiros para a continuidade; A organização pode ter adotado quase a totalidade dos controles, mas os requisitos podem estar desatualizados ou inativos; Alerta para a necessidade de priorização organizacional e financeira visando a evolução dos controles, caso contrário pode ocorrer estagnação do processo.
De 78 a 118	A organização entende que a segurança da informação, aplicação dos controles, impacta diretamente no sucesso da área de negócio; Apesar de não ocorrer uniformização em 11 domínios, a organização está consciente da importância para a imagem e saúde do negócio; O processo de maturidade contínua será alcançado com a análise de riscos e gestão por um *Security Officer*.

Segundo Sêmola (2014), é importante ter a compreensão de que, ao obter os resultados, os mesmos retratam uma situação de momento da organização. Portanto, a organização pode usar este questionário para avaliar periodicamente o índice de aderência aos controles presentes no *framework* da ABNT 27002. Desta forma, a organização terá a análise de cenário, podendo observar se o momento é de estagnação e/ou evolução da segurança da informação.

Assim, visando assegurar a missão e diretrizes da organização, este instrumento se mostra como uma excelente ferramenta de auxílio na tomada de decisões em busca da melhoria contínua, da segurança da informação, gestão de riscos e continuidade do negócio.

O capítulo de revisão de literatura apresentou os principais conceitos afetos à segurança da informação. Dessa forma, foi necessário contextualizar segurança, ativos, confidencialidade, integridade e disponibilidade, que são aspectos presentes na segurança da informação. Observa-se ainda, a importância dos conceitos acerca dos valores, ameaças, vulnerabilidades, impactos e riscos.

Vimos que um sistema de gestão de segurança da informação possui 14 domínios abordando os controles a serem observados na organização, e para fazer uma avaliação do grau de maturidade, foi apresentado um teste de conformidade via o *framework* da ABNT 27002.

3. ANÁLISE DAS PRINCIPAIS RESOLUÇÕES E NORMAS DE CONFORMIDADE APLICADAS À SEGURANÇA DA INFORMAÇÃO NO ÂMBITO DO PJTO

Os processos aplicados à segurança de rede e à necessidade de sistematização dos procedimentos tiveram início com a publicação da Resolução nº 017/2009[21], que dispõe sobre a organização e funcionamento das unidades integrantes dos Serviços Auxiliares do TJTO.

Constam do Art. 111 da Resolução nº 017/2009, no tocante à segurança de rede, de forma resumida, as seguintes atribuições:

I. Monitorar, rastrear acessos indevidos, invasões, ataques à rede do judiciário;
II. Implementar rotinas de segurança, prevenção, contingenciamento, mitigando os efeitos de ataques;
III. Implementar controle para evitar uso indevido de sistemas operacionais e aplicativos, suspender a transmissão, para evitar ataques ou fraude.

Desta forma, a Resolução nº 017/2009, consiste no primeiro documento de conformidade com a segurança da informação, no âmbito do PJTO.

A implementação dos controles de segurança de redes de computadores, no âmbito do PJTO, teve como referência a norma BS7799, *British Standard* 7799, que foi um padrão publicado originalmente pelo *BSI Group* (BSI) em 1995, e escrita pelo Departamento de Indústria e Comércio do Governo do Reino Unido.

A BS7799 serviu de base para a ABNT NBR ISO/IEC 17799, e seu processo de evolução passou pelas ABNT NBR ISO/IEC 27001:2013, ABNT NBR ISO/IEC 27002:2013, que, conjuntamente, formam a base teórica e prática da segurança da informação para a Diretoria de Tecnologia da Informação (DTINF) do TJTO.

Neste contexto, até o ano de 2010, artigos e livros baseados na BS7799, foram os materiais de referência usados pela Divisão de Administração e Segurança de Redes (DASR), vinculada à DTINF, que é a unidade organizacional responsável pela aplicação dos controles de segurança em servidores de redes e sistemas operacionais.

A edição de resoluções do CNJ acerca da gestão da segurança da informação impactou na evolução da referida gestão no âmbito do PJTO, por meio de publicação de portarias, normas e resoluções buscando a conformidade com as determinações do Conselho.

Para compreensão dos itens de conformidade que serão abordados neste capítulo, no Quadro 8, temos um demonstrativo de normas, que é uma adaptação de Bezerra (2013),

[21] http://wwa.tjto.jus.br/elegis/Home/Imprimir/339

adicionadas às normas, resoluções, portarias e demais artefatos aplicados à segurança computacional pelo PJTO.

Quadro 8 – Análise das Normas

Conformidade	Título	Objetivo
BS 7799	*British Standard* 7799	Norma Britânica para gerenciamento de segurança da informação (serviu de base para a ABNT 17799 e ABNT 27001 e 27002)
ABNT 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 negócios 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.
ABNT 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 almeja prover diretrizes gerais para as metas e melhores práticas para a gestão da segurança da informação.
Resolução TJTO nº 17/2009	Tribunal de Justiça do Tocantins. Resolução nº 017/2009.	Dispõe sobre a organização e funcionamento das unidades integrantes dos Serviços Auxiliares do Tribunal de Justiça do Estado do Tocantins e dá outras providências.
Resolução TJTO nº 22/2014	Tribunal de Justiça do Tocantins. Resolução nº 22/2014.	Institui Comitê Gestor de Segurança da Informação Multidisciplinar no âmbito do Poder Judiciário do Estado do Tocantins, e adota outras providências.
Resolução CNJ nº 211/2015	Conselho Nacional de Justiça. Resolução nº 211/ 2015	Institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário.
Resolução TJTO nº 11/2016	Tribunal de Justiça do Tocantins. Resolução nº 11/2016	Institui o Comitê de Governança de Tecnologia da Informação e Comunicação (CGTIC) no âmbito do Poder Judiciário do Estado do Tocantins e dá outras providências.
Portaria TJTO nº 3433/2017	Tribunal de Justiça do Tocantins. Portaria nº 3433/2017	Institui a Política de Segurança da Informação (PSI), no âmbito do Poder Judiciário do Estado do Tocantins e dá outras providências.
Portaria TJTO nº 1660/2019	Tribunal de Justiça do Tocantins. Portaria nº 1660/2019	Altera a Portaria nº 3433 de 2017 em seu conteúdo e inclui normas de gestão de risco de segurança da informação e de gestão dos processos de *backup*.
Portaria TJTO nº 2361/2019	Tribunal de Justiça do Tocantins. Portaria nº 2361/2019	Designa membros para o Comitê Gestor de Segurança da Informação Multidisciplinar (CGSI) e cria o Grupo de Trabalho de Apoio ao Comitê Gestor de Segurança da Informação Multidisciplinar (GT-CGSI).

3.1. A Segurança da Informação no Poder Judiciário Tocantinense

No ano de 2010, o CNJ promoveu um curso de Segurança da Informação ministrado em Brasília – DF pela empresa *Módulo Security Solutions* S/A. Assim, a segurança da informação passou a ser tema do planejamento da DTINF, onde foram iniciados os estudos para a aplicação de gerenciamento de riscos, bem como sugerir a criação de uma PSI aplicada ao PJTO.

O fruto dessa capacitação resultou em recomendações voltadas à segurança da informação abrangendo desde aspectos físicos de infraestrutura, gestão de ativos, recursos

humanos e tecnológicos, bem como um modelo baseado na ABNT 27002 para futura confecção das políticas de segurança da informação.

O ano de 2010 foi marcado por vários avanços no tocante à governança no PJTO com o início do primeiro ciclo do planejamento estratégico, compreendendo o período de 2010 a 2014. Neste contexto, a Coordenadoria de Gestão Estratégica, Estatística e Projetos (COGES), responsável pelo escritório de projetos do PJTO, gerenciou vários projetos estratégicos e foi aqui que a segurança passou a ser vista como estratégica.

No Mapa Estratégico do Poder Judiciário do Tocantins (ciclo 2010 a 2014), no que diz respeito aos recursos de Infraestrutura e Tecnologia, foram contemplados como objetivos: a) garantir infraestrutura apropriada às atividades administrativas e judiciais; e b) garantir a disponibilidade de sistemas essenciais de TI.

Em virtude disso, a DTINF, por meio da DASR, elaborou três projetos estratégicos:

- **Projeto de Sala Segura**: denominado de ambiente de alta disponibilidade – AAD, refere-se à aquisição de dois datacenters, sendo um principal localizado na sede do Tribunal de Justiça (AAD - TJTO), e um secundário localizado na sede da Comarca de Palmas (AAD - Fórum de Palmas). Estes ambientes estão interligados fia fibra ótica e comportam a infraestrutura de conectividade de rede, armazenamento e processamento para todos os sistemas do Poder Judiciário do Estado do Tocantins.
- **Projeto de Segurança de Redes**: refere-se à aquisição de equipamentos de proteção lógica, do tipo *firewalls*, para a sede do Tribunal de Justiça, bem como todas as sedes de Comarcas e Anexos interligados na REDE TELEJURIS.
- **Projeto de Consolidação do ambiente de TIC**: iniciado com as recomendações e apoio técnico do CNJ, através do uso de infraestrutura aplicada à virtualização de todos os servidores físicos. Assim, o Tribunal de Justiça deu continuidade, evoluindo a infraestrutura inicial e, atualmente, contando com o uso de solução de hiperconvergência de servidores ocorrendo, periodicamente, a sincronização de dados do Tribunal de Justiça para o Fórum de Palmas.

As ações decorrentes dos projetos listados versam sobre a preocupação com segurança da informação, balizadas na necessidade de prover a confidencialidade, a integridade e a disponibilidade das informações. Foi necessário, então, aprimorar a gestão de usuários, computadores e da REDE TELEJURIS.

Desta feita, no campo da segurança da informação, a DASR, vinculada à DTINF, com apoio da COGES, implantou projetos do ciclo do planejamento estratégico (2010-2014)[22], tendo como pendência a criação da PSI aplicada ao PJTO.

3.2. O Comitê Gestor de Segurança da Informação

A criação do Comitê Gestor de Segurança da Informação (CGSI) se deu por meio da Resolução nº 22, de 16 de outubro de 2014, motivada pela mudança de paradigma do processo físico para o processo eletrônico, uma vez que no ano de 2011, o PJTO adotou os sistemas e-Proc e SEI, oriundos do TRF-4 e, posteriormente, adaptados à realidade da justiça estadual, para seus processos Judiciais e Administrativos, respectivamente.

A implantação do Processo Eletrônico Judicial (Sistema e-Proc) se deu pela Resolução nº 1[23], de 15 de fevereiro de 2011, e a implantação do Processo Eletrônico Administrativo (Sistema SEI), pela Instrução Normativa nº 08[24], de 07 de dezembro de 2011.

3.3. A Política de Segurança da Informação (PSI) aplicada à Tecnologia da Informação

Após a conclusão dos projetos de sala segura (*data centers*), segurança de redes (*firewalls*) e consolidação de servidores (virtualização), o advento da Resolução nº 211/2015 do CNJ, que institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD) prevendo no seu art. 9º que cada órgão deverá elaborar e aplicar política, gestão e processo de segurança da informação, funcionou como pedra angular que norteou os processos de governança de TIC no âmbito do PJTO.

Em 2016, foi instituído grupo de trabalho formado por integrantes das áreas da DTINF, cuja missão seria a criação da primeira PSI. Tal grupo de trabalho se debruçou sobre o tema, tendo como referências a ABNT 27001:2013 e a ABNT 27002:2013 para iniciar a confecção da PSI aplciada ao Poder Judiciário tocantinense.

Em seguida, foi elaborada a minuta da Política de Segurança da Informação contendo diretrizes, conceitos e normas que serão abordadas na seção seguinte, mas antes de sua publicação, um importante fato histórico ocorreu, que foi a aprovação da Resolução TJTO nº 11/2016, que versa sobre o Comitê de Governança de Tecnologia da Informação e

[22] http://www.tjto.jus.br/coges/index.php/planejamento-estrategico/ciclo-2010-2014/plano-estrategico-2010-2014/send/20-plano-estrategico/1073-formulacao-estrategicatj-to-res-21-09-12-09-final-pdf
[23] http://wwa.tjto.jus.br/elegis/Home/Imprimir/365
[24] http://wwa.tjto.jus.br/elegis/Home/Imprimir/425

Comunicação (CGTIC)[25]. Assim, o CGSI e o CGTIC passaram a atuar em prol das ações da Tecnologia da Informação no Poder Judiciário tocantinense.

3.4. A metodologia para elaboração da minuta da Política de Segurança da Informação

Tendo como base as normas da ABNT 27001 e 27002, as recomendações contidas no Curso *Security Officer* ofertado pelo CNJ, foi construída a minuta da PSI contemplando os seguintes documentos: a) Diretrizes; b) Manual de Organização e Conceitos; e c) Normas Complementares. Desta maneira, esta estrutura organizacional de documentos serviu de base para o desenvolvimento de um padrão na forma de portaria interna, que foi a forma escolhida pelo Poder Judiciário tocantinense.

As Diretrizes são organizadas por capítulos, contendo o tema dentro da segurança da informação e seus artigos correlatos. Assim, na Portaria nº 3433, de 26 de junho de 2017, foram definidas as seguintes diretrizes de segurança: Segurança organizacional; Propriedade da informação; Gestão de ativos; Segurança em pessoas; Segurança física e do ambiente; Gestão de operações e comunicações; Controle de acesso; Gestão de incidentes e segurança da informação; Gestão de continuidade; Monitoramento; Conformidade; Avaliação e revisão e Penalidades. Para materialização do conteúdo o Quadro 9 possui um exemplo da declaração de uma Diretriz:

Quadro 9 - Exemplo da declaração de uma diretriz na PSI

(...) DIRETRIZES DE SEGURANÇA Capítulo I SEGURANÇA ORGANIZACIONAL Art. 4º A presidência do Tribunal de Justiça deve estabelecer, na sua estrutura organizacional, área responsável pela gestão da segurança da informação. (...)

O Manual de Organização de Conceitos contém os termos e definições utilizados nas Diretrizes e Normas Complementares, presentes na Política de Segurança da Informação. Para exemplificar temos um recorte, contendo conceitos, conforme quadro 10:

Quadro 10 - Exemplo da declaração do manual de organização e conceitos da PSI

(...) MANUAL DE ORGANIZAÇÃO DE CONCEITOS Este manual apresenta os termos e definições utilizados na documentação da Política de Segurança da Informação do Poder Judiciário do Tocantins.

[25] http://wwa.tjto.jus.br/elegis/Home/Imprimir/1101

1. Diretoria de Tecnologia da Informação: área responsável por desenvolver e manter os recursos computacionais e de telecomunicações do Poder Judiciário do Tocantins (Resolução TJTO nº 17/2009), competindo-lhe:
(...)
2. Divisão de Sistema da Informação: responsável pelo desenvolvimento de sistemas e programas computacionais relativos às atividades-fim e meio do Poder Judiciário, bem como à manutenção e à assistência técnica daqueles em funcionamento. (Resolução TJTO nº 17/2009);
3. Divisão de Administração e Segurança de Rede: compete gerenciar redes com formatos em diferentes ambientes de dados, como interfaceamento de sistemas de plataformas e com redes abertas e redes virtuais. (Resolução TJTO nº 17/2009);
4. Divisão de Administração de Banco de Dados: compete a participação em projetos de modelagem de dados, manutenção em objetos de banco de dados, monitoramento e administração das bases de dados corporativas do Poder Judiciário, assim como controle de acesso, instalação lógica e física, implementação de rotinas de segurança, backup e recuperação de dados. (Resolução TJTO nº 17/2009);
5. Divisão de Manutenção e Suporte: compete dar suporte aos usuários e manutenção dos computadores e periféricos, no Poder Judiciário do Tocantins. (Resolução TJTO nº 17/2009);
6. Arquivo público: conjuntos de documentos produzidos e recebidos, no exercício de suas atividades, por órgãos públicos de âmbito federal, estadual, do Distrito Federal e municipal em decorrência de suas funções administrativas, legislativas e judiciárias (Lei Federal nº 8.159/91).
7. Acesso: possibilidade de consulta e/ou reprodução aos documentos de arquivo.
8. Alta direção: diretoria executiva e conselho de administração.
9. Ativo: qualquer coisa que tenha valor para a organização.
10. Áreas de segurança: locais onde estão armazenadas ou são manipuladas informações classificadas como confidenciais.
11. Backup: cópia de segurança dos arquivos de computador.
12. Classificação: atribuição, pelo classificador, de grau de segurança a dado, informação, documento ou material (Decreto Federal nº 7.845/12).
(...)
15. Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados.
(...)
21. Ambiente de Alta Disponibilidade (AAD): compreende as salas seguras, sendo uma principal na sede do Tribunal de Justiça (AAD-TJTO) e uma secundária no
Fórum de Palmas (AAD-FORUM).
22. NOC: significa *Network Operations* Center (centro de operação de rede);
(...)

Nas Normas Complementares são descritas as regras de negócio de acordo com o domínio ou controle de que trata a respectiva norma. A estrutura de uma norma complementar é formada por uma identificação numérica, com o código "Norma-TIC", as disposições iniciais, diretrizes da norma, contendo o teor das regras, e por fim as responsabilidades. O Quadro 11, contém a Norma-TIC-08, que trata dos processos de *backup*, presente na PSI:

Quadro 11 - Exemplo da nº 08 na PSI do PJTO

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. Os *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 processos de cópia de segurança, ficando responsável pela política e procedimentos relativos aos serviços de *backup* e *restore*, bem como guardar as mídias de *backup*.

Tendo como premissa a definição de diretrizes, apresentação dos conceitos através do manual de organização de conceitos, construção de normas complementares, definição dos controles é criada a minuta da PSI a qual foi submetida ao CGSI que deliberou, aprovou e a remeteu para a Presidência do órgão para devida publicação.

3.5. Os domínios e controles da primeira PSI

A PSI do Poder Judiciário tocantinense adotou, inicialmente, a criação de normas complementares que fossem viáveis e exequíveis tendo como premissas: a estratégica, a tática e operacionalização das normas. Assim, foram escritas seis (06) Normas Complementares, composta pelos seguintes controles:

1. Norma-TIC-01: Responsabilidades do Usuário;
2. Norma-TIC-02: Troca de informações com partes externas;

3. Norma-TIC-03: Responsabilidade dos Ativos;

4. Norma-TIC-04: Controle de Acesso do Usuário;

5. Norma-TIC-05: Manuseio de Mídias;

6. Norma-TIC-06: Controle de Acesso ao Conteúdo *Web*.

Desta forma, no ano de 2016, foi confeccionada a primeira minuta da PSI e sua publicação se deu no ano de 2017, através da Portaria Nº 3433 de PSI 26 de junho de 2017.

Neste capítulo pudemos observar a caminhada do PJTO na construção de uma Política de Segurança da Informação. Os avanços tecnológicos do Planejamento Estratégico dos ciclos 2010 a 2014 e 2015 a 2020 provocaram mudanças significativas. Assim, constam a criação do CGSI em 2014 e a metodologia para elaboração da minuta e publicação da Portaria nº 3433/2017, de 26 de junho de 2017 contendo a primeira PSI do PJTO.

Atualmente a PSI aplicada à área de tecnologia possui oito (08) normas complementares, podendo ser analisadas através das Portarias de nº 3433/2017 e 1660/2019, que contemplam a publicação da PSI na íntegra, atualizada, contendo as Diretrizes, Manual de Organização de Conceitos e Normas Complementares.

4. A IDENTIFICAÇÃO DA IMPORTÂNCIA DE UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO NO ÂMBITO DO PJTO

No Planejamento Estratégico do ciclo 2015 a 2020[26] é notória a importância da busca pela instituição da **governança judiciária** e da **melhoria da infraestrutura e governança de TIC**, para fins de auxiliar o PJTO no cumprimento da sua missão de **garantir a cidadania através de distribuição de uma justiça célere, segura e eficaz**.

Neste contexto, assegurar a confidencialidade da informação através do sigilo, garantir a integridade e proteção da informação e permitir que as informações estejam disponíveis ao público alvo são os desafios do cotidiano do PJTO, onde, nos termos da ABNT NBR ISO/IEC 27002:2013, é notável que a PSI é um dos instrumentos que orientam na tomada de decisões para apoiar a gestão, conforme os requisitos do negócio e das leis e regulamentações pertinentes.

4.1. Aspectos Técnicos

A importância da PSI, no campo técnico, diz respeito aos controles formados pelo conjunto de diretrizes e normas de segurança da informação, aplicados ao órgão. Então, com base na ABNT NBR ISO/IEC 27002:2013, uma PSI deve ser aprovada pela direção, publicada e comunicada a todos os funcionários e partes externas relevantes.

Uma PSI deve estar em conformidade com os objetivos estratégicos, táticos e operacionais do órgão. Assim, na ABNT NBR ISO/IEC 27002:2013, temos que a PSI deve possuir controles, abrangendo os seguintes temas: a) organização da segurança da informação; b) segurança em recursos humanos; c) gestão de ativos; d) controle de acesso; e) criptografia; f) segurança física do ambiente; g) segurança nas operações; h) segurança nas comunicações; i) aquisição de bens e serviços; j) desenvolvimento e manutenção de sistemas; l) relacionamento na cadeia de suprimentos; m) gestão de incidentes de segurança da informação; n) aspectos da segurança da informação na gestão da continuidade do negócio e o) conformidade.

4.2. Conformidade

Atualmente, a busca pela conformidade tem sido um dos itens mais tratados na área da governança e, neste contexto, são observadas as instruções normativas internas do PJTO, as

[26] http://www.tjto.jus.br/coges/index.php/planejamento-estrategico/ciclo-2015-2020/plano-estrategico-2015-2020/send/25-plano-estrategico-2015-2020/1111-pe-caderno-final-capa-resol-anexo

externas do Tribunal de Contas da União (TCU), Tribunal de Contas do Estado do Tocantins (TCE) e resoluções do CNJ.

Portanto, é importante conhecer os principais instrumentos normativos de conformidade que se vinculam à governança e a segurança da informação. Por tratar-se de tema de grande amplitude, pretende-se aqui apresentar os itens de conformidade aplicados à PSI no âmbito da TIC do Poder Judiciário tocantinense.

4.2.1. Resolução CNJ 211/2015

A Resolução nº 211, de 15 de dezembro de 2015, trata da Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTICJUD) e traz como objetivo estratégico para a área segurança da informação, através dos processos internos, o aprimoramento da segurança da informação. O art. 9º, da referida Resolução prevê 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 de Segurança da Informação, e em harmonia com as diretrizes nacionais preconizadas pelo Conselho Nacional de Justiça".

Já o art. 12 sugere que os órgãos deverão constituir e manter estruturas organizacionais adequadas e compatíveis com a relevância e demanda de TIC, considerando no mínimo, os seguintes macroprocessos de segurança informação: a) de continuidade de serviços essenciais; b) de incidentes de segurança e c) de riscos. Desta forma, a Resolução do CNJ nº 211/2015, promove e exige dos tribunais o desenvolvimento de boas práticas para gestão da segurança da informação.

4.2.2. Auditoria de Conformidade da Controladoria Interna

Por meio da Portaria nº 6519/2017, publicada no DJ nº 4167/2017[27], a Presidência do TJTO, em atenção às determinações contidas na Resolução nº 171/2013 do CNJ, que dispõe sobre as normas técnicas de auditoria, inspeção administrativa e fiscalização nas unidades jurisdicionais vinculadas ao mesmo, aprovou o Plano de Auditoria de Longo Prazo - PALP 2018/2021, visando, no tocante à área de Tecnologia da Informação:

> "Avaliar a gestão de TI quanto à estrutura de governança, estratégia para mitigar riscos relacionados às atividades, planejamento de contratações (PETI, PDTI), além de

[27] http://wwa.tjto.jus.br/diario/diariopublicado/3006.pdf

> verificar o cumprimento das metas institucionalmente delimitadas para a integração dos sistemas informatizados, administrativos e judiciais. ”

Na mesma data, por meio da Portaria nº 6520/2017, foi aprovado o Plano Anual de Auditoria (PAA), **exercício 2018**, contemplando a auditoria interna na área de Tecnologia da Informação do PJTO, no referido ano, onde procedeu-se à avaliação dos conteúdos estabelecidos para a governança e gestão de TIC, considerando projetos, processos, riscos e resultados de TIC em comparação com padrões internacionalmente aceitos, como COBIT, PMBOK, ITIL, CMMI, ISO 17799, ISO 27001, as Resoluções CNJ nº 91/2009, nº 182/2013, nº198/2014 e nº 211/2015 e o perfil de governança de TI desenhado pelo TCU.

Assim, nos conteúdos estabelecidos para Governança e Gestão de TIC, foram examinados o planejamento em nível estratégico e tático, bem como a elaboração, execução e o monitoramento do alcance dos objetivos e resultados estabelecidos nos planos:

- Estratégico (PETIC[28]), cujo período é de 2016 a 2020;
- Diretor de TIC (PDTIC[29]), cujo período é de 2017 a 2018.

O resultado da referida auditoria de conformidade relatou 29 (vinte e nove) achados em diversas áreas de TIC. Assim, no campo da segurança da informação, foram encontrados 06 (seis) achados que foram tratados direto e indiretamente durante a elaboração desta dissertação de mestrado, os quais podem ser verificados no Quadro 12 que apresenta os números dos achados, a descrição, quais os critérios de análise, a situação no ano de 2018 e as providências tomadas em 2019, com vistas a resolver a questão.

Quadro 12 – Achados da auditoria de conformidade

Achado: 03	**Critério: ISSO 31000**	
Descrição	Situação em 2018	Providência tomada em 2019
Ausência de política de gestão de riscos de TI	Não foram constatadas políticas formais para gestão de riscos de TI.	Criação da Norma-TIC-07: Gestão de Riscos de Segurança da Informação, através da publicação da Portaria nº 1660/2019[30]
Achado: 06	**Critério: ISO 27002**	
Descrição	Situação em 2018	Providência tomada em 2019

[28] PETIC – Planejamento Estratégico de Tecnologia da Informação e Comunicação, disponível em http://www.tjto.jus.br/tic/index.php/component/jdownloads/category/56-petic-2016-2020?Itemid=404
[29] PDTIC – Plano Diretor de Tecnologia da Informação e Comunicação, disponível em http://www.tjto.jus.br/tic/index.php/component/jdownloads/category/68-plano-diretor-de-tic-pdti?Itemid=404
[30] http://wwa.tjto.jus.br/elegis/Home/Imprimir/1970

Ausência de política formal para cópia de segurança.	Não ficaram evidenciadas políticas formais para cópia de segurança (*backup*)	Criação da Norma-TIC-08: Gestão dos Processos de *Backup*, através da publicação da Portaria nº 1660/2019.
Achado: 17	**Critério: Resolução CNJ nº 211/15**	
Descrição	Situação em 2018	Providência tomada em 2019
Ausência de processo de gestão de riscos de TI	Não foi constatado o processo de gestão de riscos de TI formalmente instituído.	Além da publicação da Portaria nº 1660/2019, foi realizado o mapeamento e criação do fluxo de processos aplicado à gestão de riscos
Achado: 18	**Critério: Resolução nº 22 de 16 de outubro de 2014[31]**	
Descrição	Situação em 2018	Providência tomada em 2019
Falha no processo de gestão de segurança	O Comitê Gestor de Segurança da Informação foi devidamente instituído. Entretanto, constatou-se que no exercício de 2017 não se reuniu com a frequência prevista em norma instituidora (Art. 7º da Resolução nº 22 de 16 de outubro de 2014-TJTO), ou seja, ordinariamente uma vez por semestre.	- Realização das reuniões previstas para exercício de 2019; - Publicação das Portarias: nº 1660/2019 e 2361/2019[32] as quais criam novas políticas e definem um grupo de trabalho para apoio ao Comitê Gestor da Segurança da Informação; - Criação do fluxo do processo de monitoramento da Política de Segurança da Informação.
Achado: 19	**Critério: NC 05/IN01/DSIC/GSIPR[33]**	
Descrição	Situação em 2018	Providência tomada em 2019
Ausência de equipe de tratamento e resposta a incidentes de segurança em redes computacionais (ETIR).	Não foi constatada a instituição de equipe de tratamento e resposta a incidentes de segurança em redes computacionais (ETIR) e definida a sua autonomia.	Após decisão de reunião do CGSI, foi criado, por meio da Portaria nº 2361/2019[34], um Grupo de Trabalho de apoio ao Comitê Gestor de Segurança da Informação Multidisciplinar (GT-CGSI) para atuar como ETIR, até que sobrevenha sua inserção na estrutura organizacional do PJTO.
Achado: 20	**Critério: NC 18/IN01/DSIC/GSIPR[35]**	
Descrição	Situação em 2018	Providência prevista para 2020
Ausência de ações de conscientização dos	Não foram constatadas ações de conscientização dos	Elaboração de minuta de norma de PSI para campanha de conscientização de SI

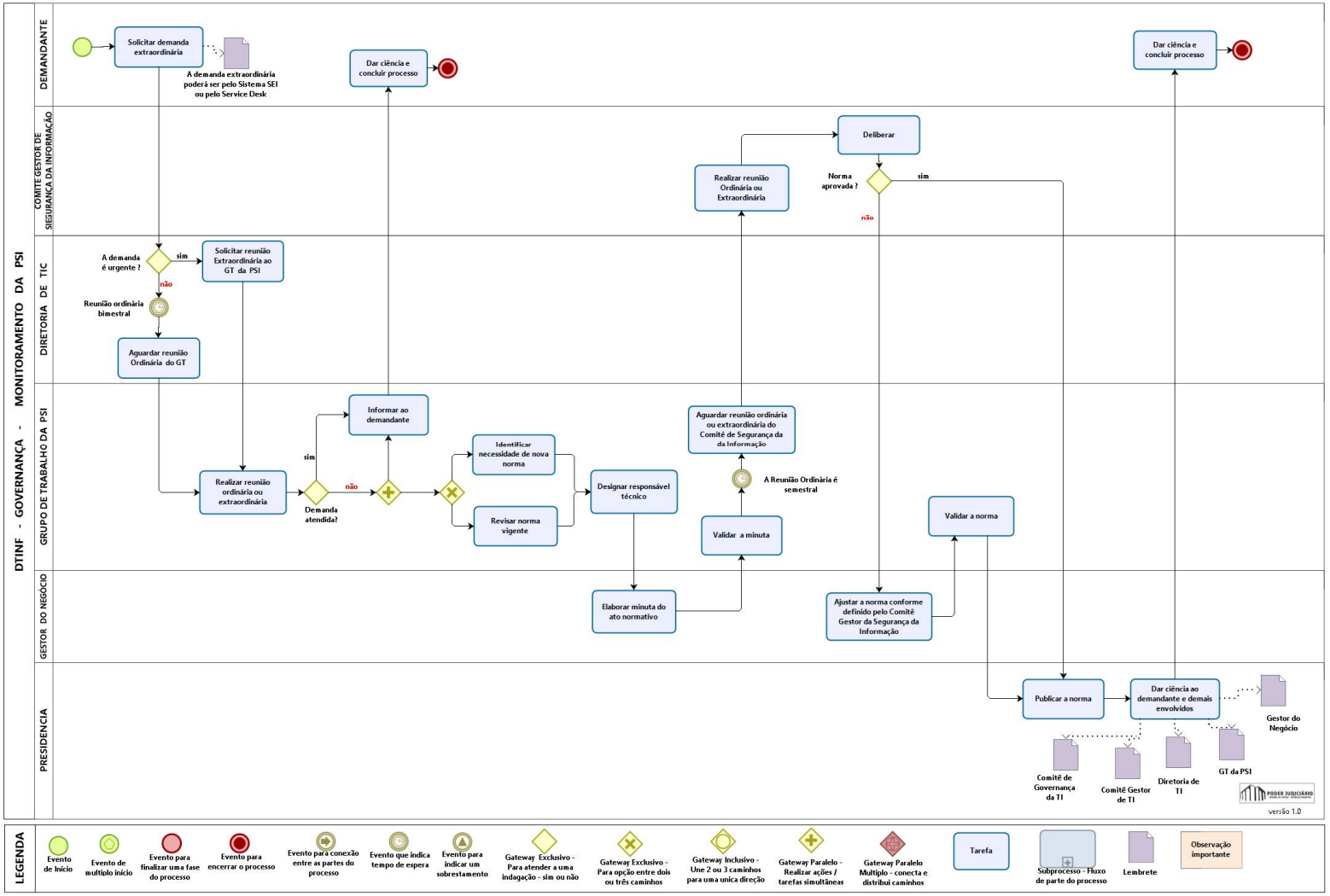
[31] http://wwa.tjto.jus.br/elegis/Home/Imprimir/899
[32] http://wwa.tjto.jus.br/elegis/Home/Imprimir/2020
[33] http://dsic.planalto.gov.br/legislacao/copy_of_nc_05_etir.pdf
[34] http://wwa.tjto.jus.br/elegis/Home/Imprimir/2020
[35] http://dsic.planalto.gov.br/legislacao/nc_18_atividades_ensino.pdf

colaboradores quanto à segurança da informação.	colaboradores quanto à segurança da informação.	de TIC e submetida ao CGSI para análise e deliberação.

4.3. Mapeamento dos fluxos de processos para a Gestão da Política de Segurança da Informação

O Escritório de Projetos do PJTO, vinculado à COGES, é a unidade organizacional responsável pela elaboração dos fluxos de processos oficiais do PJTO. Dessa maneira, DTINF e COGES desenvolveram no ano de 2019, após a publicação da PSI, um fluxograma para o **Monitoramento da Política de Segurança da Informação**, o qual visa padronizar os procedimentos através da definição das etapas de fluxos de processos, com o objetivo de melhoria da comunicação, de aumento de produtividade e da redução de retrabalho, conforme podemos verificar na Figura 5.

Figura 5 - Fluxo do Processo de Monitoramento da PSI do PJTO



Conforme verifica-se na Figura 5, o fluxograma do monitoramento da PSI é composto de 19 processos, distribuídos entre 6 unidades, que são representadas por: Demandantes, CGSI, Diretorias, GT-CGSI, Gestor do Negócio e Presidência.

No Quadro 13 abaixo são apresentados os detalhamentos dos papéis e responsabilidades das unidades envolvidas no processo:

Quadro 13 - Papeis e responsabilidades no processo de monitoramento da PSI do PJTO

Papéis		**Responsabilidades**
Demandante	Usuários, Unidades organizacional	Criar as demandas e dar ciência dos atos praticados
Comitê Gestor de Segurança da Informação - CGSI	Comitê formado por Desembargador, Juízes Auxiliares, Diretores, e Chefes de Divisão afetos aos processos e macroprocessos de TIC do PJTO.	Realizar reuniões ordinárias e extraordinárias
		Deliberar e tratar de temas relevantes afetos a Política de Segurança da Informação.
		Aprovar normas de PSI
		Remeter para publicação via Presidência
Diretoria de Tecnologia da Informação e Comunicação - DTINF	Unidade demandada, que recebe e classifica a demanda afeta à Tecnologia da Informação do PJTO	Classificar a demanda, apresentá-la nas reuniões ordinárias ou convocar reuniões extraordinárias com o GT-CGSI.
		Propor sugestões ao GT-CGSI.
		Subsidiar tecnicamente o GT-CGSI.
		Manter registros sobre os resultados
Grupo de Trabalho de apoio ao Comitê Gestor de Segurança da Informação - GT-CGSI	Grupo formado por Diretores de Tecnologia da Informação, de Gestão de Pessoas, Judiciário e Administrativo	Realizar reunião ordinária ou extraordinária
		Dar ciência ao demandante das ações realizadas
		Analisar a necessidade de nova norma
		Revisar norma vigente
		Designar responsável técnico para atualização de norma e/ou criação de nova norma
		Validar minuta de norma
		Agendar reuniões ordinárias e/ou extraordinárias com o CGSI
		Remeter para publicação via Presidência
Gestor do negócio	Diretor, Chefe de Divisão, ou responsável que possua domínio sobre o tema	Elaborar minuta ou ato normativo
		Ajustar norma conforme deliberação do CGSI
		Subsidiar o GT-CGSI e ao CGSI
Presidência	Gabinete da Presidência	Publicar a norma via portaria
		Dar ciência ao demandante e às unidades das ações realizadas

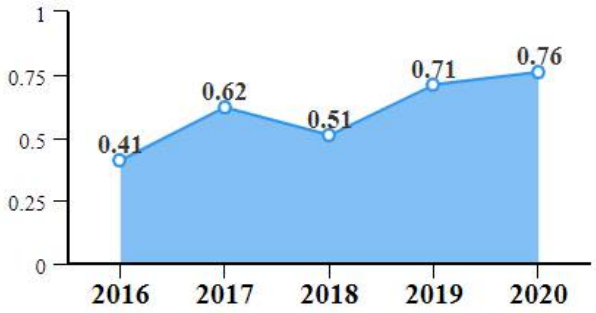
4.4. O iGovTIC-JUD

A Resolução do CNJ nº 211/2015 O CNJ, a qual instituiu a ENTIC-JUD prevê no seu art. 32, acerca da medição do nível do cumprimento das diretrizes estratégicas, bem como a análise da evolução da Governança, Gestão e Infraestrutura de Tecnologia da Informação e Comunicação (TIC) do Poder Judiciário.

O iGovTIC-JUD é o índice de governança de Tecnologia da Informação e Comunicação do Poder Judiciário e é mensurado anualmente, apresentando qual o nível de aderência dos Tribunais à Resolução nº 211/2015.

Através de uma consulta no painel do iGovTIC-JUD[36] do CNJ, verifica-se que a TIC do PJTO alcançou, no ano de 2019, o nível “Aprimorado”, mostrando uma evolução com relação aos anos de 2016, 2017 e 2018. O gráfico 1, apresenta os indicadores do iGovTIC-JUD de 2016 a 2020.

Gráfico 1 - iGovTIC-JUD da TIC do PJTO



O Gráfico 1 apresenta o índice iGovTIC-JUD definido pelo CNJ para área de TIC, no âmbito da DTINF do TJTO, no período de 2016 até 2020. Observa-se que na primeira medição, ocorrida no ano de 2016, a DTINF do TJTO alcançou índice de 0.41; em 2017, o índice subiu para 0.62. Contudo, em virtude de auditoria de conformidade, realizada pela Controladoria Interna do PJTO, conforme visto no item 5.2.2, no ano de 2018, a nota foi reduzida para 0.51.

No ano de 2019, a DTINF desenvolveu trabalhos afetos à segurança da informação, tais como: a) realização de reuniões do comitê de segurança da informação – CGSI; b) sugestão e aprovação de duas novas normas (Norma-TIC-07: Gestão de Riscos de Segurança da Informação e Norma-TIC-08: Gestão dos Processos de Backup.); c) criação dos fluxos de processos; d) criação do GT-CGSTI e e) publicação das portarias pertinentes. Tais ações contribuíram para o aprimoramento da gestão da segurança da informação, bem como na melhoria e composição da pontuação do iGovTIC-JUD.

Neste contexto, verificou-se uma evolução do índice de 0.51 em 2018, para 0.71 em 2019, fazendo com que a DTINF do TJTO mudasse do nível “Satisfatório” (2018) para o nível “Aprimorado” (2019), contribuído pela primeira vez, na composição da nota do PJTO no Prêmio CNJ de Qualidade[37].

---

36 https://paineis.cnj.jus.br/QvAJAXZfc/opendoc.htm?document=qvw_l%2FPainelCNJ.qvw&host=QVS%40neodimio03&anonymous=true&sheet=shIGTGraficos

37 https://www.cnj.jus.br/pesquisas-judiciarias/premio-cnj-de-qualidade/

Já no ano de 2020 o índice da DTINF subiu para 0.76, superando a meta definida no PETIC que era de 0.75, tendo como ações de destaque: a) Mapeamento de Processos de TIC; b) Gerenciamento de Serviços de TIC; c) Investimento em ativos de Segurança da Informação; d) instituição do Plantão de TIC e e) Minuta da Política de Gestão de Pessoas.

Neste Capítulo, nota-se a importância da PSI na conformidade com planejamento estratégico do PJTO no ciclo 2015 a 2020, uma vez que contribuiu com o atendimento de achados de auditoria de conformidade realizada pela Controladoria Interna do PJTO. Além disso, o mapeamento dos fluxos de processos, a atualização e criação de normas aplicadas à gestão da PSI contribuíram para a melhoria da pontuação do iGovTIC-JUD da DTINF do PJTO.

5. AVALIAÇÃO DO GRAU DE MATURIDADE DA SEGURANÇA DE INFORMAÇÃO NO ÂMBITO DO PJTO

O Poder Judiciário tocantinense está finalizando seu segundo ciclo do Planejamento Estratégico Institucional, sendo que os objetivos do Planejamento Estratégico do ciclo 2010 a 2014, referentes à TIC, constituíam em garantir a infraestrutura apropriada às atividades Administrativas e Judiciais do Poder Judiciário, onde se destacaram projetos como Sala Segura, Segurança de Rede e Consolidação de Servidores. Já no segundo ciclo 2015 a 2020, os objetivos priorizam a melhoria da infraestrutura e governança de TIC.

Tais objetivos estão alinhados à Resolução do CNJ nº 211/2015 e apresenta como pilar, a melhoria da infraestrutura e governança de TIC. Neste contexto, para a área de segurança, temos como objetivos:

- Política de Segurança da Informação para a TIC;
- Gestão de Riscos;
- Controles de Ativos;
- *Data Centers*;
- Campanha de Conscientização de Segurança da Informação e outros.

Ainda, no campo da conformidade com resoluções do CNJ, temos como referência as resoluções e metas:

- Resolução CNJ 45/2007, que trata do domínio JUS.BR;
- Metas Prioritárias de 2010, onde a Meta 09, tratava de assegurar velocidades adequadas às atividades das Unidades Judiciárias;
- Resolução CNJ 182/2013, que norteia o processo de contratação de STIC - Soluções de TIC e,
- Resolução CNJ 211/2015 que trata da Governança de TIC.

Dentro do contexto do processo de evolução e maturidade do PJTO no campo da Segurança da Informação, destacamos a criação do CGSI, as publicações das Portarias nº 3433 de 26 de junho de 2017 e nº 1660, de 12 de agosto de 2019, as quais atualizam a PSI contemplando novos conceitos, normas, mapeamento de fluxos de trabalho e ainda, a publicação da Portaria nº 2361, de 08 de Novembro de 2019, que cria o GT-CGSI.

Visando avaliar o grau de maturidade na Segurança da Informação do Poder Judiciário do Estado do Tocantins, foi realizado um estudo de caso, dentro de um ambiente formado por unidades com visão estratégica, tática e operacional da estrutura organizacional do Tribunal de Justiça do Estado do Tocantins, conforme segue:

5.1. Estudo de Caso

Para realização do estudo de caso, cujo objetivo é avaliar o grau de maturidade na Segurança da Informação do PJTO, foi elaborado um instrumento de pesquisa tendo como base o *framework* de conformidade com a norma ABNT 27002. Dessa forma, foram confeccionados formulários *web*, usando a plataforma do *Google*, com base técnica e conformidade com o teste desenvolvido por Sêmola (2014), através de adaptação do *framework* de conformidade com a ABNT 27002:2013.

Nesta pesquisa, foram distribuídos questionários via Sistema Eletrônico de Informações (SEI) para as áreas estratégicas, táticas e operacionais do PJTO.

Para a classificação da atuação das unidades organizacionais, dentro do campo de atuação estratégico, tático e operacional, foi realizada consulta interna via SEI à COGES, tendo recebido como resposta, a seguinte classificação:

- O nível **estratégico** do Poder Judiciário tocantinense é formado por:
    - Presidência do Tribunal de Justiça do Estado do Tocantins;
    - Vice-Presidência do Tribunal de Justiça do Estado do Tocantins;
    - Corregedoria Geral de Justiça;
    - Escola Superior da Magistratura Tocantinense - ESMAT;
    - Comissão Permanente de Segurança Institucional - COPESI;
    - Diretoria Geral;
    - Coordenadoria de Gestão Estratégica, Estatística e Projetos.
- O nível **tático** é formado por*:*
    - Diretorias de áreas;
    - Assessoria Militar;
    - Controladoria Interna;
    - Comitê Gestor de Segurança da Informação - CGSI;
    - Comitê Gestor de TIC.
- O nível **operacional** é formado por:
    - Chefias de divisões e serviços da DTINF.

O questionário de pesquisa esteve disponível no período de 01 a 10/06/2020, havendo um total de 42 respondentes, sendo quinze (15) respostas oriundas da área estratégica, treze (13) da área tática e quatorze (14) da operacional.

As unidades organizacionais que responderam os formulários compõem a cadeia de gestão das áreas meio e fim do PJTO.

5.1.1. A formalização do Instrumento de Pesquisa

Para a formalização do instrumento de pesquisa e sua aplicação nas unidades organizacionais do Poder Judiciário tocantinense, foram abertos três processos administrativos, do tipo requerimento, por meio do Sistema Eletrônico de Informações - SEI, e encaminhados à Diretoria Geral (DIGER), para conhecimento, manifestação e remessa às unidades organizacionais do Poder Judiciário.

A DIGER manifestou pelo envio dos autos à douta Presidência do TJTO e demais áreas conforme classificação acima.

A Presidência do TJTO acolheu o requerimento, autorizando a aplicação do instrumento de coleta de dados, o questionário *web*.

5.1.2. O Questionário de Pesquisa

O questionário de pesquisa foi baseado no *framework* de conformidade com a ABNT 27002 proposto por Sêmola (2014), formado por 59 (cinquenta e nove) questões, dentro do contexto dos 14 (quatorze) domínios de controles de segurança da informação. O sistema de pontuação do referido *framework* possui escala de *Likert* de três opções de respostas, conforme segue:

- **SIM**: representa 2 (dois) pontos, por atender na íntegra o controle;
- **SIM, porém desatualizada**: representa 1 (um) ponto, por estar desatualizada, e
- **NÃO**: representa 0 (zero), onde não soma e nem subtrai ponto.

Considerando que em alguns casos, os formulários de pesquisa foram encaminhados pelos respondentes originais a suas subunidades, houve um número de formulários respondidos superior à expectativa inicial.

Ressalta-se que foi informado nos requerimentos para aplicação dos instrumentos de pesquisa, que os dados coletados seriam utilizados unicamente para fins acadêmicos, na confecção do presente estudo.

5.1.3. O Resultado do Instrumento de Pesquisa

O resultado geral da pesquisa é formado por 42 respostas de formulários, onde quinze (15) deles são respostas das unidades organizacionais classificada como área estratégica, treze

(13) unidades classificadas como da área tática e quatorze (14) unidades da atuação operacional.

Considerando que cada formulário é composto por cinquenta e nove (59) questões ou controles, e que estas questões são organizadas em quatorze (14) domínios da segurança da informação, os resultados deste estudo serão apresentados com base nos quatorze (14) domínios.

Assim temos, na tabela 1, um dicionário de dados, contendo na primeira coluna o identificador do domínio, na segunda coluna a descrição do domínio e, na terceira coluna a quantidade de controles presentes naquele domínio e na quarta coluna a definição de sigla. A saber:

Tabela 1 – Representação dos domínios, descrição, quantidade de controles e sigla

Id do Domínio	Descrição do Domínio	Qtde de Controles	Sigla
01	Política de segurança da informação	1	POLSEGINFORMACAO
02	Organização da segurança da informação	6	ORGSEGINFORMACAO
03	Segurança em recursos humanos	4	SEGRECHUMANOS
04	Gestao de ativos	4	GESTATIVOS
05	Controle de acesso	6	CONTRACESSO
06	Criptografia	2	CRIPTOGRAFIA
07	Segurança física do ambiente	6	SEGFIAMBIENTE
08	Segurança nas operações	9	SEGOPERACOES
09	Segurança nas comunicações	5	SEGCOMUNICACOES
10	Aquisição, desenvolvimento e manutenção de sistemas	6	AQUIDEVSISTEMAS
11	Relacionamento na cadeia de suprimentos	3	CADSUPRIMENTOS
12	Gestão de incidentes de segurança da informação	2	GESTINCIDENTE
13	Aspectos da segurança da informação na gestão da continuidade do negócio	2	SEGCONTNEGOCIO
14	Conformidade	3	CONFORMIDADE

Assim, visando apresentar os resultados de forma simplificada, os dados foram tratados quali-quantitativamente, classificação em acordo com as percepções das áreas: estratégica, tática e operacional, dentro da estrutura organizacional do PJTO.

5.1.3.1.O Resultado na visão Estratégica

As unidades organizacionais classificadas como estratégicas, possuem representantes responsáveis pela garantia da missão, alcance da visão, tomada de decisão e definição das políticas e diretrizes de âmbito geral. O resultado da pesquisa foi obtido através de quinze (15)

respondentes. Na tabela 2, abaixo, temos a representação da frequência em porcentagem de todas as respostas.

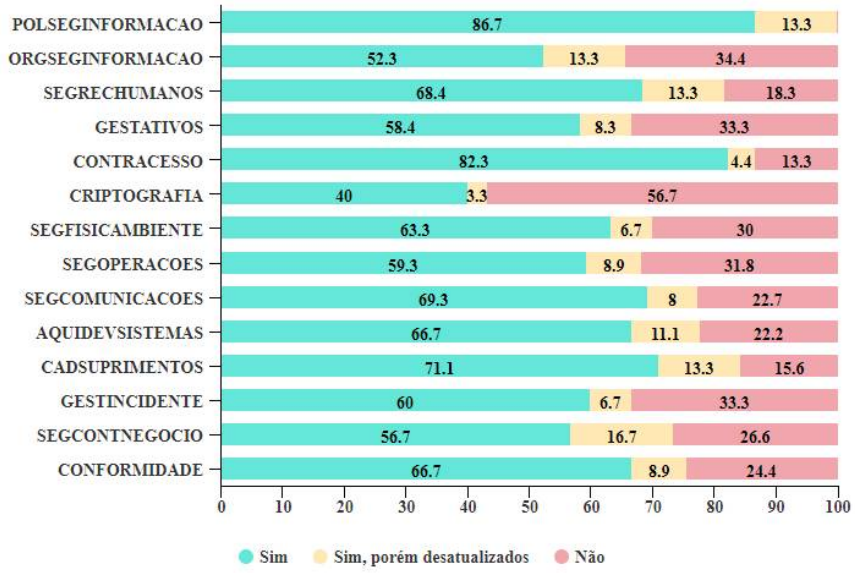
Tabela 2 – Representação da frequência das respostas na visão Estratégica

Sigla do Domínio	Sim	Sim, porém desatualizados	Não
POLSEGINFORMACAO	86.7 %	13.3 %	0 %
ORGSEGINFORMACAO	52.3 %	13.3 %	34.4 %
SEGRECHUMANOS	68.4 %	13.3 %	18.3 %
GESTATIVOS	58.4 %	8.3 %	33.3 %
CONTRACESSO	82.3 %	4.4 %	13.3 %
CRIPTOGRAFIA	40 %	3.3 %	56.7 %
SEGFIAMBIENTE	63.3 %	6.7 %	30 %
SEGOPERACOES	59.3 %	8.9 %	31.8 %
SEGCOMUNICACOES	69.3 %	8 %	22.7 %
AQUIDEVSISTEMAS	66.7 %	11.1 %	22.2 %
CADSUPRIMENTOS	71.1 %	13.3 %	15.6 %
GESTINCIDENTE	60 %	6.7 %	33.3 %
SEGCONTNEGOCIO	56.7 %	16.7 %	26.6 %
CONFORMIDADE	66.7 %	8.9 %	24.4 %

Na tabela 2, temos o campo sigla do domínio e sua identificação (onde o detalhamento está contido na tabela 1) e a frequência em porcentagem das respostas em conformidade com o *framework* da ABNT 27002, podendo ser: “Sim”, “Sim, porém desatualizados” e “Não”.

No Gráfico 2 apresenta o resultado em % da frequência das quinze (15) respostas obtidas no formulário respondido pela área estratégica.

Gráfico 2 – Resultado da frequência das respostas na visão Estratégica



5.1.3.2.O Resultado na visão Tática

As unidades organizacionais classificadas como táticas possuem representantes responsáveis pela articulação dos objetivos e desdobramentos até o nível operacional. A pesquisa do campo tático foi respondida por treze (13) respondentes (Apêndice 8), e na tabela 3 temos a representação da frequência em porcentagem de todas as respostas.

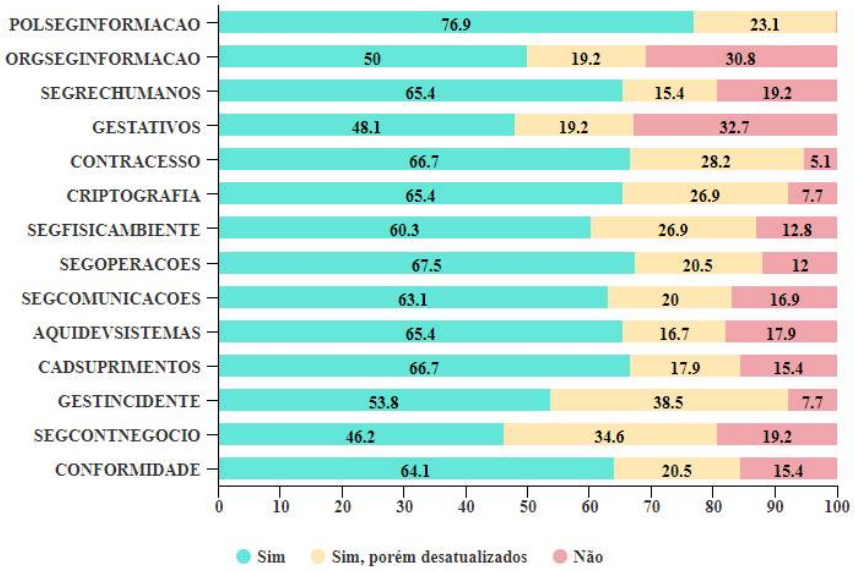
Tabela 3 – Representação da frequência das respostas na visão Tática

Sigla do Domínio	Sim	Sim, porém desatualizados	Não
POLSEGINFORMACAO	76.9 %	23.1 %	0 %
ORGSEGINFORMACAO	50 %	19.2 %	30.8 %
SEGRECHUMANOS	65.4 %	15.4 %	19.2 %
GESTATIVOS	48.1 %	19.2 %	32.7 %
CONTRACESSO	66.7 %	28.2 %	5.1 %
CRIPTOGRAFIA	65.4 %	26.9 %	7.7 %
SEGFIAMBIENTE	60.3 %	26.9 %	12.8 %
SEGOPERACOES	67.5 %	20.5 %	12 %
SEGCOMUNICACOES	63.1 %	20 %	16.9 %
AQUIDEVSISTEMAS	65.4 %	16.7 %	17.9 %
CADSUPRIMENTOS	66.7 %	17.9 %	15.4 %
GESTINCIDENTE	53.8 %	38.5 %	7.7 %
SEGCONTNEGOCIO	46.2 %	34.6 %	19.2 %
CONFORMIDADE	64.1 %	20.5 %	15.4 %

Na tabela 3 é apresentada a frequência em porcentagem das respostas em conformidade com o *framework* da ABNT 27002 na visão Tática.

No Gráfico 3 temos a representação gráfica em % do resultado da frequência das treze (13) respostas obtidas no formulário respondido pela área Tática.

Gráfico 3 – Resultado da frequência das respostas na visão Tática



5.1.3.3.O Resultado na visão Operacional

As unidades organizacionais classificadas como operacional formam a base da organização, sendo os responsáveis pela área de execução das atividades definidas no planejamento estratégico. A pesquisa do campo operacional foi respondida por quatorze (14) respondentes, e na tabela 4 temos a representação da frequência em porcentagem de todas as respostas.

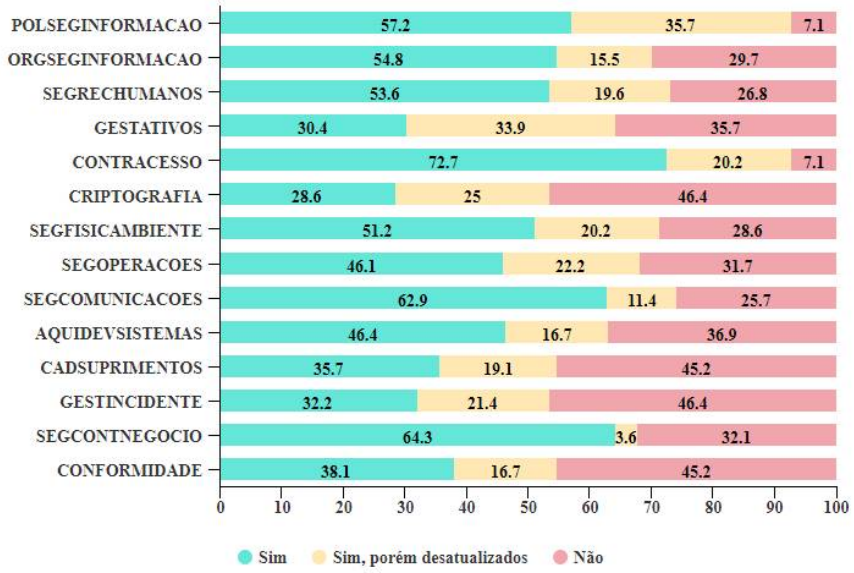
Tabela 4 – Representação da frequência das respostas na visão Operacional

Sigla do Domínio	Sim	Sim, porém desatualizados	Não
POLSEGINFORMACAO	57.2 %	35.7 %	7.1 %
ORGSEGINFORMACAO	54.8 %	15.5 %	29.7 %
SEGRECHUMANOS	53.6 %	19.6 %	26.8 %
GESTATIVOS	30.4 %	33.9 %	35.7 %
CONTRACESSO	72.7 %	20.2 %	7.1 %
CRIPTOGRAFIA	28.6 %	25 %	46.4 %
SEGFIAMBIENTE	51.2 %	20.2 %	28.6 %
SEGOPERACOES	46.1 %	22.2 %	31.7 %
SEGCOMUNICACOES	62.9 %	11.4 %	25.7 %
AQUIDEVSISTEMAS	46.4 %	16.7 %	36.9 %
CADSUPRIMENTOS	35.7 %	19.1 %	45.2 %
GESTINCIDENTE	32.2 %	21.4 %	46.4 %
SEGCONTNEGOCIO	64.3 %	3.6 %	32.1 %
CONFORMIDADE	38.1 %	16.7 %	45.2 %

Na tabela 4, temos a frequência em porcentagem das respostas que, conforme o *framework* da ABNT 27002 na visão Operacional.

O Gráfico 4 demonstra o resultado da frequência em % das quatorze (14) respostas obtidas no formulário respondido pela área Operacional.

Gráfico 4 – Resultado da frequência das respostas na visão Operacional



5.1.3.4. Consolidação dos Resultados

Após a apresentação dos resultados sob o prisma dos quatorze (14) domínio da segurança da informação, de forma setorizada, faz-se necessário apresentar uma visão geral de todas as frequências das respostas resultantes da pesquisa, que foi respondida por um total de 42 respondentes das unidades organizacionais estratégicas, táticas e operacionais. A compilação dos dados foi realizada através de média simples, resultando na tabela 5, conforme segue:

Tabela 5 - Consolidação das frequências de todas as respostas

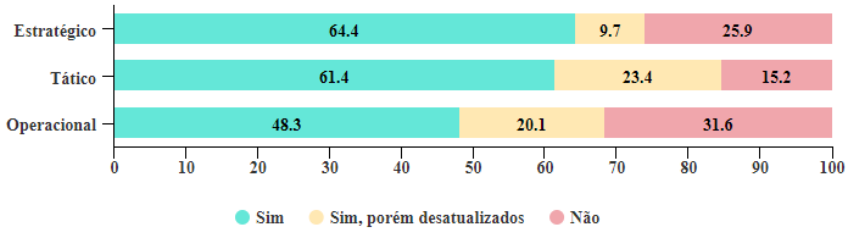
	Sim	**Sim, porem desatualizada**	**Não**
Estratégico	64,4 %	9,7 %	25,9 %
Tático	61,4 %	23,4 %	15,2 %
Operacional	48,3 %	20,1 %	31,6 %

A tabela 5 apresenta as percepções dos respondentes, evidenciando uma lacuna de impressão entre as áreas setoriais, como por exemplo, enquanto as áreas Estratégicas e Táticas

apresentam proximidade da frequência de respostas “SIM”, com percentuais de 64,4% e 61,4%, respectivamente, a área Operacional apresenta, no mesmo quesito, o percentual de 48,3%, abaixo das demais.

Assim, visando representar graficamente, com base na tabela 5, formada pelas três visões das áreas institucionais e suas respectivas médias de frequência em % para cada tipo de resposta, temos a Gráfico 5 com a consolidação dos resultados, a saber:

Gráfico 5 – Resultado da frequência: Estratégica, Tática e Operacional



Desta maneira é possível apresentar, através do Gráfico 5, uma visão ampla e consolidada, baseada na frequência das respostas das unidades organizacionais do TJTO, representantes das áreas estratégica, tática e operacional, no ano de 2020.

5.1.4. Análise do sistema de pontuação do *framework* da ABNT 27002

O sistema de pontuação presente no teste de conformidade do *framework* da ABNT 27002, possui um índice que define a percepção do grau de maturidade em segurança da informação de uma instituição. Tal metodologia é representada por três intervalos de pontuação, que classificam os três eventuais cenários em que a instituição se encontra no tocante à segurança da informação.

Com base nas respostas do instrumento de pesquisa e na metodologia de pontuação aplicada no teste de conformidade do *framework* da ABNT 27002, desenvolvido por Sêmola (2014), foi possível obter a pontuação das respostas para cada área de atuação, sendo elas: estratégica, tática e operacional. Assim, temos na tabela 6, o seguinte resultado:

Tabela 6 – Pontuação de todas respostas

Área	Pontuação alcançada
Estratégica	81.27
Tática	84.92
Operacional	70.63

Após a aplicação do *framework* da ABNT 27002, com a obtenção da pontuação por área de atuação, estratégica, tática e operacional, temos o Quadro 14, contendo o resultado situacional de acordo com o intervalo de pontos alcançados:

Quadro 14 - Pontuação do *framework* da ABNT 27002 conforme as áreas (adaptação do Autor)

Pontuação	Situação conforme teste do *framework* da ABNT 27002	Área do PJTO
De 0 a 38	A situação não é confortável para as organizações público e/ou privado; A Segurança não está sendo tratada como prioridade; Ausência ou ineficiência dos controles recomendado pela norma; Desconhecimento dos riscos pela alta gestão; A segurança não é considerada pelos clientes como fator crítico de sucesso; Ações isoladas e não coordenadas não geram o impacto e resultado esperado.	-
De 39 a 77	A organização mostra bom nível de consciência, mas também deficiência na estrutura, gestão ou falta de recursos financeiros para a continuidade; A organização pode ter adotado quase a totalidade dos controles, mas os requisitos podem estar desatualizados ou inativos; Alerta para a necessidade de priorização organizacional e financeira visando a evolução dos controles, caso contrário pode ocorrer estagnação do processo.	**Operacional**
De 78 a 118	A organização entende que a segurança da informação, aplicação dos controles, impacta diretamente no sucesso da área de negócio; Apesar de não ocorrer uniformização em 11 domínios, a organização está consciente da importância para a imagem e saúde do negócio; O processo de maturidade contínua será alcançado com a análise de riscos e gestão por um *Security Officer*.	**Estratégica Tática**

No Quadro 14 temos a coluna “Pontuação” contendo o intervalo da pontuação, onde o primeiro intervalo vai de 0 a 38 pontos; o segundo, de 39 até 77 pontos e, por fim, o terceiro, que vai de 78 até 118 pontos. Já na coluna “Situação conforme teste do *framework* da ABNT 27002”, temos as características que definem o grau de maturidade de uma instituição. Na terceira coluna, temos o campo “Área do PJTO” que indica as áreas pesquisadas, ou seja, estratégica, tática e operacional e em que situação elas se encontram.

Assim, após a aplicação do *framework* da ABNT 27002, com a obtenção da pontuação por área de atuação, podemos perceber que as áreas estratégicas e táticas estão classificadas no terceiro intervalo, com 81.27 e 84.92 pontos, respectivamente. Dessa maneira, as unidades das áreas estratégicas e táticas demonstram convergência de entendimento no tocante ao cenário da segurança da informação no âmbito do Poder Judiciário tocantinense. Entretanto, as unidades das áreas operacionais alcançaram 70.63 pontos, ficando classificada no segundo intervalo, apresentando uma percepção diferente das demais áreas, quanto ao grau de maturidade com relação à segurança da informação.

5.2. Considerações sobre o resultado do teste de *framework* da ABNT 27002

O estudo de caso foi desenvolvido com base no *framework* de conformidade com a ABNT 27002, aplicado às unidades que representam percepções das áreas estratégica, tática e operacional da estrutura organizacional do PJTO.

O resultado do estudo apresenta a convergência de visão das áreas estratégicas e táticas dentro da estrutura organizacional no que diz respeito aos itens: a) a segurança da informação, aplicação dos controles, impacta diretamente no sucesso da área de negócio; b) apesar de não ocorrer uniformização em 11 domínios, a organização está consciente da importância para a imagem e saúde do negócio; e c) o processo de maturidade contínua será alcançado com a análise de riscos e gestão por um *Security Officer*.

Contudo, o estudo de caso demonstrou uma percepção divergente vinda das unidades das áreas operacionais, pois, neste aspecto, a área operacional entende que: a) organização mostra bom nível de consciência, mas também deficiência na estrutura, gestão ou falta de recursos financeiros para a continuidade; b) a organização pode ter adotado quase a totalidade dos controles, mas os requisitos podem estar desatualizados ou inativos; e c) alerta para a necessidade de priorização organizacional e financeira visando a evolução dos controles, caso contrário pode ocorrer estagnação do processo.

Analisando todos os domínios e suas respectivas percepções por área de atuação dentro do PJTO, foi possível identificar quais domínios e quais áreas possuem oportunidades em fazer o nivelamento do conhecimento, bem como promover o aprimoramento da segurança da informação do PJTO, conforme quadro abaixo:

Quadro 15 - Oportunidade de Aprimoramento da Segurança da Informação no PJTO

Descrição do Domínio	Área Aplicável	Sugestão de Aprimoramento
Política de segurança da informação	Operacional	Campanha de Conscientização
Segurança em recursos humanos	Operacional	Campanha de Conscientização
Gestão de ativos	Operacional	Campanha de Conscientização
Criptografia	Estratégico e Operacional	Campanha de Conscientização e Criação de Normas específicas
Segurança física do ambiente	Operacional	Campanha de Conscientização
Segurança nas operações	Operacional	Campanha de Conscientização
Aquisição, desenvolvimento e manutenção de sistemas	Operacional	Campanha de Conscientização e Criação de Normas específicas
Relacionamento na cadeia de suprimentos	Operacional	Campanha de Conscientização
Gestão de incidentes de segurança da informação	Tático e Operacional	Campanha de Conscientização e Criação de Normas específicas
Aspectos da segurança da informação na gestão da continuidade do negócio	Tático	Campanha de Conscientização
Conformidade	Operacional	Campanha de Conscientização

No Quadro 15 é apresentada a coluna “Descrição do Domínio” contendo a descrição dos domínios da ABNT 27002 que precisam de aprimoramento; a coluna “Área Aplicável” onde estão relacionadas quais áreas, por domínio, devem ter uma atuação mais efetiva e a coluna “Sugestão de Aprimoramento” que descreve as sugestões de eventuais ajustes que podem promover a conscientização das áreas e eventual evolução rumo ao aprimoramento da segurança da informação no PTJTO.

Esse Capítulo dedicou-se a fazer um estudo de caso, apresentando os resultados do processo da primeira avaliação do grau de maturidade da segurança da informação, considerando as percepções das unidades administrativas que representam as áreas: estratégica, tática e operacional do PJTO, realizada no ano de 2020.

Assim, foi possível ter a percepção da convergência no pensamento das unidades das áreas estratégica e tática do PJTO que, em resumo, entendem que a organização está consciente da importância da segurança da informação para a imagem institucional e que as unidades administrativas, que representam a área operacional, possuem um entendimento divergente, onde a organização apesar de ser consciente da importância da segurança da informação, ainda existem deficiências na estrutura organizacional e na priorização das áreas que sustentam o negócio, e que se não ocorrer uma evolução poderá entrar no processo de estagnação do processo de segurança da informação.

6. CONSIDERAÇÕES FINAIS

A realização do presente trabalho possibilitou fazer uma viagem no tempo, com análise do passado, avaliação do presente e projeção do futuro da segurança da informação no âmbito do Poder Judiciário tocantinense, sendo concebido e realizado a partir da premissa de que o desenvolvimento de uma PSI favorece o aperfeiçoamento da governança e da gestão da segurança da informação no PJTO.

Identificar e analisar os processos adotados na Política de Segurança da Informação (PSI), com base em normas da ABNT, bem como avaliar o grau de maturidade em segurança da informação, visando aperfeiçoamento da mesma no âmbito do Poder Judiciário do Estado do Tocantins (PJTO).

O objetivo de identificação e análise dos processos adotados na Política de Segurança da Informação (PSI), com base em normas da ABNT, bem como a avaliação do grau de maturidade em segurança da informação, foi devidamente alcançado, tendo sido desenvolvido ainda, o mapeamento dos fluxos de processos para a gestão da PSI, contribuindo para o aperfeiçoamento da mesma no âmbito do Poder Judiciário do Estado do Tocantins.

Os Planejamentos Estratégicos presentes nos ciclos 2010 a 2014 e 2015 a 2020, promoveram a criação do CGSI e do CGTIC, onde foi possível desenvolver a primeira PSI para o PJTO, através a publicação da Portaria nº 3433/2017. Assim, No ano de 2019, o CGSI promoveu ações com foco no cumprimento de requisitos da Resolução do CNJ de nº 211/2015, tendo como destaque a aprovação e publicação de portarias que tratam de temas como: a) Gestão de Riscos de Segurança da Informação; b) Gestão dos Processos de *Backup*; e c) Criação do Grupo de Trabalho de Apoio ao Comitê Gestor de Segurança da Informação Multidisciplinar (GT-CGSI) presentes nas publicações das Portarias de nº 1660 e 2361 de 2019 do TJTO.

O resultado prático deste trabalho de dissertação serviu de base para as atividades do CGSI, CGTIC, DTINF e COGES bem como contribuiu em "aprimorar a segurança da informação" presente no artigo 3º e, atender os macroprocessos de segurança da informação, artigo 12º da a Resolução do CNJ de nº 211/2015. Tais ações somaram na nota geral da DTNF promovendo a evolução do iGovTIC-JUD de 0.51 para 0.71, fazendo com que a DTINF mudasse do nível "Satisfatório" para o nível "Aprimorado", fato importante para a melhoria da nota do TJTO no Prêmio CNJ de Qualidade.

No ano de 2020, foi realizada a primeira pesquisa para avaliação do grau de maturidade das áreas estratégica, tática e operacional da estrutura organizacional do PJTO com relação à segurança da informação, visando avaliar o quanto o Poder Judiciário tocantinense está em

conformidade com a Resolução CNJ nº 211/2015 e com os controles de segurança da informação contidos na ABNT 27002.

A pesquisa, fruto deste trabalho, foi elaborada e aplicada com base nos requisitos do *framework* de conformidade com a ABNT 27002, supedaneada no modelo proposto por Sêmola (2014) onde foi realizado um estudo de caso, dentro de um escopo formado por unidades administrativas com representação na área estratégica, tática e operacional.

A partir da análise dos resultados obtidos, constatou-se como positivo o fato das unidades do campo estratégico e tático estarem conscientes da importância da segurança da informação para a imagem institucional. Destaca-se também, o fato das unidades do campo operacional mostrarem preocupação com as deficiências ainda existentes na estrutura organizacional, bem como com a priorização das áreas que sustentam o negócio. Assim, este trabalho indicou os pontos a serem tratados para o aprimoramento da segurança da informação no PJTO.

Embora os objetivos deste trabalho terem obtido êxito no ano de 2020, verifica-se a necessidade de engajamento para a manutenção e o aprimoramento futuro da segurança da informação no âmbito do Poder Judiciário do Estado do Tocantins. Pois, novos desafios estão previstos para os próximos anos, como é o caso da adequação e conformidade com a Lei Geral de Proteção da Dados (LGPD) - Lei Nº 13.709 e do Comitê de Segurança Cibernética do Poder Judiciário (CSCPJ) criado pelo CNJ a partir da Portaria nº 242, de 10 de novembro de 2020.

Nota-se, ainda como ação para promoção da melhoria dos processos de segurança, a necessidade de reestruturação no organograma do Poder Judiciário tocantinense, contemplando uma área dedicada à segurança da informação, para atuar em ações alinhadas à segurança de redes, continuidade do negócio, gestão de riscos, estratégias para a recuperação de desastres e política de segurança da informação.

Posto isto, diante da atual realidade, com base nos princípios da segurança da informação, governança judiciária e melhoria da infraestrutura e governança de TIC, o PJTO trabalha na busca contínua para assegurar sua missão que é **garantir a cidadania através de distribuição de uma justiça célere, segura e eficaz.**

Faz-se necessário mencionar a entrada em vigor da Lei Geral de Proteção da Dados (LGPD), Lei Nº 13.709, de 14 de agosto de 2018, que dispõe sobre o tratamento de dados pessoais e que altera a Lei 12.965, de 23 de abril de 2014, que versa sobre o Marco Civil da Internet, a qual tem como objetivo a regulamentação da privacidade no Brasil, demandando a adoção urgente de boas práticas para garantir o gerenciamento da privacidade para evitar

sanções da Autoridade Nacional de Proteção de Dados - ANPD[38], que é vinculada à Presidência da República e possui autonomia técnica e decisória, conforme os artigos 55-A e 55-B da Lei Nº 13.709.

Referindo-se à LGPD, o CNJ baixou a Recomendação de nº 73/2020[39], a qual faz menção à adoção de medidas destinadas a instituir um padrão nacional de proteção de dados pessoais existentes nas suas bases, contemplando minimamente: a) a organização da comunicação; b) o tratamento do direito do titular; c) a gestão do consentimento; d) a retenção de dados e cópia de segurança; e) a gestão de contratos; f) o plano de respostas a incidentes de segurança com dados pessoais.

Ressalta-se também que o CNJ por meio da Portaria de nº 242, de 10 de novembro de 2020, instituiu o Comitê de Segurança Cibernética do Poder Judiciário (CSCPJ) que será formado por representantes de vários Tribunais, determinando aos Tribunais a adoção de protocolo de prevenção a incidentes cibernéticos no âmbito do Poder Judiciário (PPICiber/PJ).

O art. 3º da portaria do CSCPJ prevê criação de atos normativos como: a) protocolo de prevenção e gerenciamento de crise para o enfrentamento de ilícitos cibernéticos no âmbito do Poder Judiciário; b) protocolo de investigação para ilícitos cibernéticos que possam afetar o Poder Judiciário, e c) minuta da Estratégia da Segurança Cibernética e da Informação do Poder Judiciário.

Assim, verifica-se estarmos diante de novos desafios a serem encarados pelo Poder Judiciário, devendo o PJTO se adequar às recomendações supracitadas, tornando-se imperioso que, no novo ciclo de planejamento estratégico que compreenderá o período de 2021 a 2026, sejam contempladas ações para a evolução da gestão da segurança da informação, em conformidade com essas novas demandas, ou seja, a LGPD e o CSCPJ.

Desta feita, observa-se a necessidade de evolução da Gestão da Segurança da Informação no âmbito do Poder Judiciário tocantinense, no sentido de que a segurança da informação seja inserida como área estratégica do PJTO, visando o fortalecimento do CGSI e a busca contínua de revisão, atualização e criação de novas normas complementares para o aprimoramento da segurança da informação.

Fazendo um exercício de futurologia, não causaria espécie o surgimento ainda, de novas demandas afetas ao PJTO no tocante a a) gestão de riscos; b) tratamento de incidentes de

[38] http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm
[39] https://atos.cnj.jus.br/atos/detalhar/3432

segurança; c) segurança dos serviços em nuvem; e d) proteção de dados, o que reforça a premente necessidade do aprimoramento da segurança da informação no âmbito do PJTO.

Diante da instituição do CSCPJ, ocorrida em novembro de 2020, de onde exsurgirão novas definições e/ou diretrizes acerca da segurança da informação é possível a continuidade da presente pesquisa, pois tais definições oportunizarão a elaboração de um *framework* de conformidade para avaliação do grau de maturidade em segurança da informação, específico para os Tribunais de Justiça.

A transformação digital e disrupção tecnológica colocam a maioria das organizações sob pressão por conta das incertezas e mudanças constantes. Os recentes desafios enfrentados pelo Poder Judiciário brasileiro por conta de tentativas de ataques e eventuais interrupções dos serviços demostraram possíveis falhas de segurança no ambiente computacional. Tais ocorrências reforçam a relevância deste trabalho, da importância da área de TIC e sobretudo, da segurança da informação no cumprimento de normas e asseguramento da continuidade dos serviços administrativos e judiciais em meio eletrônico do PJTO.

7. REFERÊNCIAS BIBLIOGRÁFICAS

ABNT NBR ISO/IEC 17799: **Tecnologia da Informação – Código de prática para a gestão da segurança da informação**. Rio de Janeiro, 2005.

ABNT NBR ISO/IEC 27001: **Tecnologia da informação – Técnicas de segurança - Sistemas de gestão da segurança da informação - Requisitos,** 2ª Edição, 2013.

ABNT NBR ISO/IEC 27002: **Tecnologia da informação: técnicas de segurança: código de prática para a gestão da segurança da informação**. Rio de Janeiro, 2013.

ABNT NBR ISO/IEC 27005: **Tecnologia da Informação - Técnicas de Segurança – Gestão de Riscos de Segurança da Informação**. Rio de Janeiro, 2011.

ARAUJO, M. T.; FERREIRA, F.N.F**. Política de segurança da informação: guia prático para a elaboração e implementação**. Rio de Janeiro: Ciência Moderna, 2008.

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

FONTES, Edison Luiz Gonzaga. **Políticas e normas para a segurança da informação**. Rio de Janeiro: Brasport, 2012.

FONTES, Edison Luiz Gonzaga. **Segurança da Informação**. Saraiva SA, 2017.

MALDONADO, V.N; BLUM, R. O. **LGPD – Lei Geral de Proteção a Dados Comentada.** São Paulo: Thomson Reuters Brasil, Ed. 2019.

NOCÊRA, Rosaldo de Jesus. **Gerenciamento de Projetos - Teoria e Prática**, Santo André - SP, Ed. do Autor, 2009.

RAMOS, Anderson et al. **Security Officer - 1: guia oficial para a formação de gestores em segurança da informação**, 2. Ed. -Porto Alegre, RS: Zouk 2008.

SÊMOLA, M. **Gestão da Segurança da Informação - Uma Visão Executiva** – 2. ed. São Paulo: Elsevier, 2014.

SILVA, E. L; MENEZES, M. E. **Metodologia da pesquisa e elaboração de dissertação.** Florianópolis: UFSC, 4. Ed. 2005.

WASLAWICK, Raul Sidnei. **Metodologia de Pesquisa para ciência da computação**. 2. Ed. Rio de Janeiro: Elsevier, 2014.

Referências Consultadas

CNJ. (2013) **Dispõe sobre as normas técnicas de auditoria, inspeção administrativa e fiscalização nas unidades jurisdicionais vinculadas ao Conselho Nacional de Justiça (Processo CNJ nº 349.544).** 2013. Disponível em: < https://atos.cnj.jus.br/atos/detalhar/1680>. Acesso em 10/01/2020.

CNJ. (2015) **Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD)**. 2015. Disponível em: <http://www.cnj.jus.br/atos-normativos?documento=2227>. Acesso em 02/01/2020.

CNJ. (2015) 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**. Disponível em: <https://www.cnj.jus.br/wp-content/uploads/2015/12/164c053661476944a507e8a5dcc03003.pdf>. Acesso em: 02/01/2020.

CNJ. (2020) Conselho Nacional de Justiça. Recomendação n. 73, de 20 de ago de 2020. Dispõe sobre a **Recomenda aos órgãos do Poder Judiciário brasileiro a adoção de medidas preparatórias e ações iniciais para adequação às disposições contidas na Lei Geral de Proteção de Dados – LGPD.** Disponível em: < https://atos.cnj.jus.br/atos/detalhar/3432>. Acesso em: 10/11/2020.

CNJ. (2020) Conselho Nacional de Justiça. Portaria n. 242, de 10 de nov de 2020. Institui **o Comitê de Segurança Cibernética do Poder Judiciário.** Disponível em: < https://atos.cnj.jus.br/atos/detalhar/3566>. Acesso em: 21/12/2020.

PRESIDÊNCIA DA REPUBLICA. (2009) Gabinete de Segurança Institucional. **Criação de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR**. Disponível em: < http://dsic.planalto.gov.br/legislacao/copy_of_nc_05_etir.pdf>. Acesso em: 03/01/2020.

PRESIDÊNCIA DA REPUBLICA. (2013) Gabinete de Segurança Institucional. **Diretrizes Para as Atividades de Ensino em Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública federal**. Disponível em: < http://dsic.planalto.gov.br/legislacao/nc_18_atividades_ensino.pdf>. Acesso em: 03/01/2020.

TJTO, **Política de Segurança da Informação (PSI), no âmbito do Poder Judiciário do Estado do Tocantins e dá outras providências.** 2017. Disponível em <http://www.tjto.jus.br/images/tic/PORTARIA_PSI.pdf>. Acesso em: 02/01/2020.

TJTO. (2019) Tribunal de Justiça do Tocantins. Portaria Nº 1660, de 12 de agosto de 2019. **Normas complementares para Política de Segurança da Informação (PSI)**. Disponível em: <http://wwa.tjto.jus.br/elegis/Home/Imprimir/1199>. Acesso em: 02/01/2020.

TJTO. (2019) Tribunal de Justiça do Tocantins. Portaria Nº 2361, de 08 de novembro de 2019. **Designa membros para o Comitê Gestor de Segurança da Informação Multidisciplinar (CGSI) e cria o Grupo de Trabalho de Apoio ao Comitê Gestor de Segurança da Informação Multidisciplinar (GT-CGSI).** Disponível em: <http://wwa.tjto.jus.br/elegis/Home/Imprimir/2020>. Acesso em: 02/01/2020.

TJTO. (2017) Tribunal de Justiça do Tocantins. Portaria Nº 3433, de 26 de junho de 2017. Dispõe sobre a **Política de Segurança da Informação (PSI)**. Disponível em: <http://wwa.tjto.jus.br/elegis/Home/Imprimir/1199>. Acesso em: 02/01/2020.

TJTO. (2016) Tribunal de Justiça do Tocantins. Resolução Nº 11, de 02 de junho de 2016. Dispõe sobre o **Comitê de Governança de Tecnologia da Informação e Comunicação (CGTIC)**. Disponível em: < http://wwa.tjto.jus.br/elegis/Home/Imprimir/1101>. Acesso em: 06/01/2020.

TJTO. (2014) Tribunal de Justiça do Tocantins. Resolução Nº 22, de 16 de outubro de 2014. **Institui Comitê Gestor de Segurança da Informação Multidisciplinar no âmbito do Poder Judiciário do Estado do Tocantins, e adota outras providências**. Disponível em: <http://wwa.tjto.jus.br/elegis/Home/Imprimir/899>. Acesso em: 02/01/2020.

TJTO. (2011) Tribunal de Justiça do Tocantins. Resolução Nº 1, de 15 de fevereiro de 2011. **Implanta o Processo Eletrônico no âmbito do Poder Judiciário do Estado do Tocantins em primeiro e segundo graus de jurisdição.** Disponível em: <http://wwa.tjto.jus.br/elegis/Home/Imprimir/365>. Acesso em: 02/01/2020.

TJTO. (2011) Tribunal de Justiça do Tocantins. Instrução Normativa Nº 8, de 07 de dezembro de 2011. **Dispõe sobre a sistematização das regras necessárias à implementação do Sistema Eletrônico de Informações – SEI, no âmbito do Poder Judiciário do Estado do Tocantins.** Disponível em: <http://wwa.tjto.jus.br/elegis/Home/Imprimir/425>. Acesso em: 02/01/2020.

TJTO. (2009) Tribunal de Justiça do Tocantins. Resolução Nº 17, de 23 de setembro de 2009. **Dispõe sobre a organização e funcionamento das unidades integrantes dos Serviços Auxiliares do Tribunal de Justiça do Estado do Tocantins e dá outras providências.** Disponível em: <http://wwa.tjto.jus.br/elegis/Home/Imprimir/339>. Acesso em: 02/01/2020.

TJTO. (2016) Tribunal de Justiça do Tocantins. **PETIC – Planejamento Estratégico de Tecnologia da Informação e Comunicação**. Disponível em: < http://www.tjto.jus.br/tic/index.php/component/jdownloads/category/56-petic-2016-2020?Itemid=404>. Acesso em: 03/01/2020.

TJTO. (2017) Tribunal de Justiça do Tocantins. **PDTIC – Plano Diretor de Tecnologia da Informação e Comunicação**. Disponível em: < http://www.tjto.jus.br/tic/index.php/component/jdownloads/category/68-plano-diretor-de-tic-pdti?Itemid=404. Acesso em: 03/01/2020.

TJTO. (1996) Tribunal de Justiça do Tocantins. **Lei Complementar Nº 10, institui a Lei Orgânica do Poder Judiciário do Estado do Tocantins e dá outras Providências**. Disponível em: <http://www.tjto.jus.br/joomlatools-files/docman-files/arquivos/legislacao_interna/leis/lei_complementar_10_96.pdf>. Acesso em: 24/02/2020.

APÊNDICES

APÊNDICE A – Artigos Publicados

1. Mapping Of Information Technology Risks In The Judiciary Tocantinense

Mapeamento de Riscos de Tecnologia da Informação no Judiciário 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

2. Gerenciamento Remoto de Recursos de Softwares no Tribunal de Justiça do Tocantins

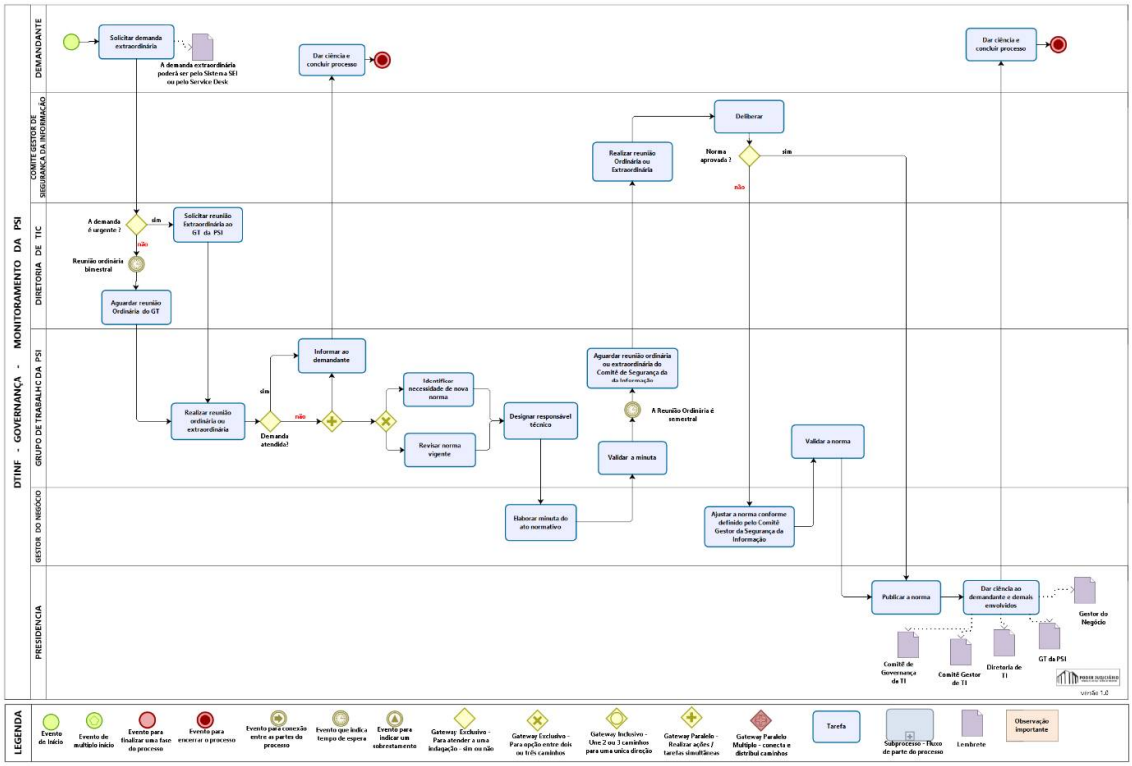
Remote Management of Software Resources in the Court of Justice of Tocantins

Tiago Souza Luz [1], Marcelo Leal de Araújo Barreto[2], Alice Carla de Sousa Setúbal[3], Gentil Veloso Barbosa[4]

[1]UFT – Universidade Federal do Tocantins, Brazil
[2]TJTO – Tribunal de Justiça do Estado do Tocantins, Brazil

https://revista.unitins.br/index.php/humanidadeseinovacao/article/view/2525/1679

APÊNDICE B – Fluxo do Processo de Monitoramento da PSI do PJTO



APÊNDICE C – Questionário

Questionário para avaliar o grau de maturidade na Segurança da Informação do Poder Judiciário do Estado do Tocantins

Prezado(a) Magistrado(a) / Servidor(a) do Poder Judiciário do Estado do Tocantins.

O questionário a seguir é parte integrante de pesquisa de campo para fins de dissertação de Mestrado, tendo como tema "Gestão da Política de Segurança da Informação no Poder Judiciário do Estado do Tocantins", sob a orientação do Professor Gentil Veloso Barbosa, Dr.

Responda às questões, marcando a opção que melhor corresponde à sua percepção, diante das situações apresentadas.

Não é necessário identificar-se.

Este formulário tem como referência o *Framework* de conformidade com a norma ABNT 27002, desenvolvido por Sêmola (2014).

Sua colaboração é muito importante!

Para mensurar a pontuação de uma instituição, o sistema de pontuação desenvolvido por Sêmola (2014) considera que:

Pontuação do *framework* de conformidade com a ABNT 27002 proposto por Sêmola (2014)	
Resposta	**Pontuação**
SIM	Soma-se 2 pontos
SIM, porém desatualizados	Some-se 1 ponto
Não	Não soma e nem subtrai pontos

1. POLITICA DE SEGURANÇA DA INFORMAÇÃO

O domínio 1, verifica a existência de uma Política de Segurança da Informação na instituição.

1.1. Política de Segurança da Informação?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

2. ORGANIZAÇÃO DA SEGURANÇA DA INFORMAÇÃO

O domínio 2, verifica a existência de papeis, atribuições e gerenciamento de projetos

2.1. Um responsável pela gestão da política de segurança?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

2.2. Definição clara das atribuições de responsabilidades associadas à segurança da informação?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

2.3. Politica de segregação de função e responsabilidade?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

2.4. Acordos de cooperação com autoridades e grupos especiais

( ) Sim ( ) Sim, porém desatualizados ( ) Não

2.5. Prática de segurança em gerenciamento de projetos ?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

2.6. Política definida para uso de dispositivos móveis e trabalho remoto?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

3. SEGURANÇA EM RECURSOS HUMANOS

O domínio 3, versa sobre critérios de seleção, contratação, capacitação dos recursos humanos

3.1. Critérios de seleção e contratação de pessoal?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

3.2. Processo de capacitação e treinamento de usuários ?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

3.3. Processos disciplinares estabelecidos?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

3.4. Procedimentos definidos para encerramento de contratações e desligamentos?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

4. GESTÃO DE ATIVOS

O domínio 4, trata controles sobre inventários de ativos físicos, tecnológicos e humanos

4.1. Inventários de ativos físicos, tecnológicos e humanos?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

4.2. Critérios de classificação da informação?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

4.3. Mecanismos de segurança e tratamento de mídias?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

4.4. Procedimento de descarte de mídias?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

5. CONTROLE DE ACESSO

O domínio 5, versa sobre regras e controles de acessos a rede e aos sistemas

5.1. Requisitos de negócios para controle de acesso?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

5.2. Gerenciamento de acessos de usuários?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

5.3. Definição de responsabilidade dos usuários?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

5.4. Controle de acesso a rede?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

5.5. Controle de acesso ao sistema operacional?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

5.6. Controle de acesso a aplicações?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

6. CRIPTOGRAFIA

O domínio 6, trata das regras do uso de criptografia

6.1. Política para uso de controles criptográficos?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

6.2. Política de gestão do ciclo de vida das chaves criptográficas?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

7. SEGURANÇA FÍSICA DO AMBIENTE

O domínio 7, lida com a segurança física, manutenção e infraestrutura elétrica e lógica

7.1. Definição de perímetros e controles de acesso físico aos ambientes?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

7.2. Recursos para segurança e manutenção dos equipamentos?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

7.3. Estrutura para fornecimento adequado de energia?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

7.4. Segurança do cabeamento?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

7.5. Procedimentos para reutilização e alienação de equipamentos?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

7.6. Política de mesa limpa e tela limpa?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

8. SEGURANÇA NAS OPERAÇÕES

O domínio 8, verifica a segurança das operações, responsabilidades, procedimentos, gestão de mudanças e capacidades

8.1. Procedimentos e responsabilidades operacionais definidos e documentados?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

8.2. Processo de gestão de mudança?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

8.3. Processo de gestão de capacidade?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

8.4. Processos para segregação entre ambientes de desenvolvimento, teste e produção?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

8.5. Proteção contra código maliciosos e códigos móveis?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

8.6. Procedimentos para cópia de segurança?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

8.7. Procedimentos para monitoramento e registro de logs?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

8.8. Procedimentos para instalação e atualização de software?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

8.9. Procedimentos para auditoria em sistemas de informação?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

9. SEGURANÇA NAS COMUNICAÇÕES

O domínio 9, trata da segregação de redes, proteção de mensagens e acordos de confidencialidade.

9.1. Controles e gerenciamento de redes?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

9.2. Procedimento para segregação de redes?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

9.3. Política para transferência de informações?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

9.4. Procedimento para proteção de informações em mensagens eletrônicas?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

9.5. Acordos de confidencialidade e não divulgação padronizados?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

10. AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS

O domínio 10, verifica controles dos requisitos, garantia, desenvolvimento, documentação, aceitação e testes nos sistemas

10.1. Requisitos de segurança de sistemas?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

10.2. Processos para garantia de segurança de aplicações?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

10.3. Política e procedimento para desenvolvimento de seguro de sistemas?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

10.4. Procedimentos para controle de mudanças em sistemas?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

10.5. Testes documentados de aceitação e segurança de sistemas?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

10.6. Procedimentos de proteção a dados para teste?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

11. RELACIONAMENTO NA CADEIA DE SUPRIMENTOS

O domínio 11, verifica requisitos de entregas dos produtos e serviços junto aos fornecedores

11.1. Requisitos de segurança para relacionamento com fornecedores?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

11.2. Requisitos de segurança para a cadeia de suprimento de produtos e serviços?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

11.3. Procedimentos de gerenciamento da entrega de serviços?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

12. GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

O domínio 12, verifica a existência de notificação e registros dos incidentes de segurança

12.1. Mecanismos de notificação de fragilidade e eventos de segurança da informação?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

12.2. Procedimentos para gestão de incidentes de segurança da informação e melhorias?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

13. ASPECTOS DA SEGURANÇA DA INFORMAÇÃO NA GESTÃO DA CONTINUIDADE DO NEGÓCIO

O domínio 13, trata dos controles de redundância e disponibilidade

13.1. Procedimentos e requisitos para a gestão da continuidade da gestão da segurança da informação?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

13.2. Redundância para garantia de disponibilidade de recursos de processamento da informação?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

14. CONFORMIDADE

O domínio 14, observa o grau de conformidade com o Sistema de Gestão da Segurança da Informação, definido na NBR ISO/IEC 27002:2013, bem como as regulamentações institucionais pertinentes à organização.

14.1. Requisitos de conformidade legal e contratual documentados?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

14.2. Controles para a proteção da privacidade e direitos individuais definidos e implementados?

( ) Sim ( ) Sim, porém desatualizados ( ) Não

14.3. Procedimentos para analisar criticamente o enfoque e a implementação da segurança no PJTO?

( ) Sim ( ) Sim, porém desatualizados ( ) Não