UNIVERSIDADE FEDERAL DA PARAÍBA

CENTRO DE CIÊNCIAS APLICADAS A EDUCAÇÃO

DEPARTAMENTO DE CIÊNCIAS EXATAS

BACHARELADO EM SISTEMAS DE INFORMAÇÃO

A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO TRIBUNAL DE JUSTIÇA DA PARAÍBA:

Uma análise baseada na NBR ISO 27002

AUTOR: Fabiano Santana Ferreira

Orientador: Prof. Dr. Hermann Hrdlicka

RIO TINTO - PB

2015

FABIANO SANTANA FERREIRA

A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO TRIBUNAL DE JUSTIÇA DA PARAÍBA:
Uma análise baseada na NBR ISO 27002

Monografia apresentada para obtenção do título de Bacharel à banca examinadora no Curso de Bacharelado em Sistemas de Informação do Centro de Ciências Aplicadas e Educação (CCAE), Campus IV da Universidade Federal da Paraíba.
Orientador: Prof. Dr. Hermann Hrdlicka.

RIO TINTO - PB
2015

F383p Ferreira, Fabiano Santana.

A política de segurança da informação do Tribunal de Justiça da Paraíba: uma análise baseada na NBR ISO 27002. / Fabiano Santana Ferreira. – Rio Tinto: [s.n.], 2015.

79 f.: il.

Orientador(a): Prof. Dr. Hermann Hrdlicka.
Monografia (Graduação) – UFPB/CCAE.

1. Segurança da informação. 2. Tribunal de justiça - Paraíba. 3. Sistemas de informação.

UFPB/BS-CCAE CDU: 004.056:657.6(043.2)

FABIANO SANTANA FERREIRA

A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO TRIBUNAL DE JUSTIÇA DA PARAÍBA:

Uma análise baseada na NBR ISO 27002

Trabalho de Conclusão de Curso submetido ao Curso de Bacharelado em Sistemas de Informação da Universidade Federal da Paraíba, Campus IV, como parte dos requisitos necessários para obtenção do grau de BACHAREL EM SISTEMAS DE INFORMAÇÃO.

Assinatura do autor: _____

APROVADO POR:

Orientador: Prof. Dr. Hermann Hrdlicka
Universidade Federal da Paraíba – Campus IV

Prof. Dra. Adriana Clericuzi
Universidade Federal da Paraíba – Campus IV

Prof. M. Joelson Nogueira de Carvalho
Universidade Federal da Paraíba – Campus IV

RIO TINTO - PB

2015

A Minha família e aos amigos, colegas e professores, minha eterna gratidão por compartilhar comigo seus conhecimentos.

AGRADECIMENTOS

A Deus, à minha Família (Pais, Esposa, (Luzia) e Filhos (Éryka e Gabriel)) por estarem comigo desde o início desta caminhada.

Aos grandes amigos que fiz amigos esses que devo eterna gratidão por, em momentos difíceis, estarem prontos a me e compartilhar de seus conhecimentos.

Ao Professor Hermann, por me orientar na elaboração deste trabalho, além de ministrar aulas de forma a agregar mais conhecimentos compartilhando sua experiência profissional, acadêmica e de vida com todos que assistiram a suas aulas.

A todos os amigos, funcionários, professores e colegas que fazem parte do DCE da Universidade Federal da Paraíba que de uma forma ou de outra, contribuíram para a conclusão deste trabalho.

RESUMO

Garantir a segurança da informação é um ponto fundamental que deve ser tratado independente do tipo de organização, visto que a informação sempre foi um ativo primordial para as organizações; protegê-la se tornou indispensável para assegurar vantagens competitivas. Porém, para garantir essa segurança é preciso implementar controles e políticas capazes de garantir atributos básicos de segurança (confidencialidade, integridade, disponibilidade e autenticidade). No estudo de caso tratado neste trabalho – Tribunal de Justiça da Paraíba, a política de segurança da informação, como elemento fundamental em qualquer sistema ou plano de segurança, precisa estar alinhada com as melhores práticas reconhecidas mundialmente. Para o entendimento acerca do assunto foi realizado um levantamento bibliográfico em livros, leis, normas e etc, para verificar o grau de alinhamento ou conformidade da política de segurança daquele tribunal (em fase de implantação) com os elementos de diagnóstico apresentados pela ISO 27002.

Palavras chave: Segurança; Informação; política; política de segurança da informação.

ABSTRACT

Ensuring the security of information is a fundamental point that must be, independent of the type of industry, because the information has always been a key asset for organizations; protect it became essential to get competitive advantages. However, security´s assurance needs controls capable of ensuring basic security attributes policies (confidentiality, integrity, availability and authenticity). In the case study treated in this work - Court of Paraiba, the security´s police of information, known as a fundamental element in any system or security, needs to be aligned with the best practices recognized worldwide. For the understanding of this subject, a bibliography research was made based on books, laws, rules, etc., to verify the degree of alignment or conformity of that court security policy (under implementation) with diagnostic evidence submitted by ISO 27002.

Keywords: Security; Information; policy; information security policy.

LISTA DE FIGURAS

LISTA DE GRÁFICOS

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE SIGLAS

ABNT	Associação brasileira de normas técnicas
APF	Administração publica federal
CNJ	Conselho Nacional de Justiça
DITEC	Diretoria de tecnologia da informação
IEC	*International Electrotechnical Commission – Comissão Eletrotécnica Internacional*
IN	Instrução Normativa
ISO	*International Organization for Standardization – Organização*
PSI	Política de segurança da informação
TCU	Tribunal de Contas da União
TI	Tecnologia da Informação
TJMT	Tribunal de Justiça de Mato Grosso
TJPB	Tribunal de Justiça da Paraíba
TJSP	Tribunal de Justiça de São Paulo
CMMI	Capability Maturity Model - Integration – Modelo de Maturidade em Capacitação - Integração
COBIT	Control Objectives for Information and relface faated Technology – Objetivo de Controle para Tecnologia da Informação e Áreas Relacionadas
ITIL	Information Technology Infrastructure Library – Biblioteca de Infraestrutura de TI

SUMÁRIO

1 INTRODUÇÃO

Nos últimos tempos o mundo deparou-se com inúmeras denúncias de violação de privacidade feita pelo governo americano, como mostra (GROSSMANN, 2013).

Esse fato é percebido pelo crescimento no índice médio dos incidentes de segurança em relação entre os anos 2011 e 2013 (não temos ainda disponíveis os dados de 2.014); de outra maneira pode, de certa forma, explicar que empresas e pessoas estão investindo mais em mecanismos de segurança, fazendo com que se identifique um maior número de incidentes.

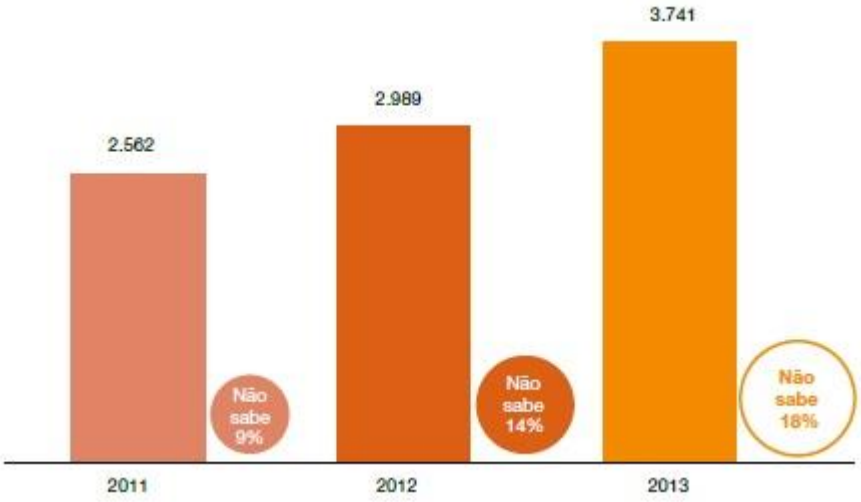

Figura 1 - Número médio de incidentes nos últimos anos
Fonte: (PWC, 2014)

Grosso modo, a motivação da espionagem é obter informações para obter vantagem competitiva, acesso a contas de clientes em bancos, ou neutralizar alguma ação de mercado; algumas evidências brasileiras importantes relaciona um dos bens não renováveis na escala humana e de alto valor internacional: o petróleo, e os trâmites entre Petrobras e o Ministério de Minas e Energia (GANDRA, 2013); outra, no setor bancário, apontou falhas de segurança nas aplicações em *smartphones* de clientes do Banco do Brasil: alguns clientes tiveram acesso a dados de outros clientes (CAMPI, 2013).

A justiça brasileira também tem sido objeto de ataques: o site do Tribunal de Justiça de São Paulo ficou fora do ar cerca de duas horas quando um grupo de *hackers* assumiu o ataque em solidariedade a ação de reitegração de posse de pinheirinho (VASCONCELLOS, 2012). O mesmo aconteceu com o site do Tribunal de Justiça do Rio de Janeiro (TJRJ) que ficou fora

do ar por um bom tempo, vitimado por conta de grupo *hacker* que assumiu a autoria do ato, apesar do tribunal negar o ataque afirmando que a página estava em manutenção (RODRIGUES, 2013).

A figura a seguir mostra o poderio de um tipo específico diferentes fontes de ataque, onde se destacam aqueles causados por hackers, e outros por funcionários e ex-funcionários apresentada na pesquisa global de seguraça da informação junto a empresas nos cinco continentes e realizada pela PWC junto a empresas , uma empresa internacional de auditoria. (2014).

Figura 2 - Estimativa da provável origem dos incidentes
Fonte: (PWC, 2014, p. 13)

Nota-se que o percentual relativo ao ataque de hackers é mais que o dobro das ações praticadas por concorrentes e equivale, no ambiente interno, aos ataques sofridos por funcionários atuais. Isso faz pensar que esse crescente aumento dos incidentes em segurança da informação implica na necessidade em se ter, nas organizações, um ambiente tecnológico com a qual sejam desenvolvidos processos cada vez mais eficientes para manter as informações seguras. Mas, também, que uma política de segurança adequada seja eficaz para diminuir o percentual de incidentes causados por funcionários – por dolo ou por desconhecimento de boas práticas de segurança no ambiente de trabalho.

A 10ª Pesquisa Nacional sobre Segurança da Informação, mostra, dentre outras, as medidas de segurança que dominam os relatos de planejamento de segurança nas organizações para os próximos 12 meses, onde se enfatiza a necessidade de uma política de segurança adequada (Módulo, 2007).

Os percentuais podem ser vistos na figura 3.

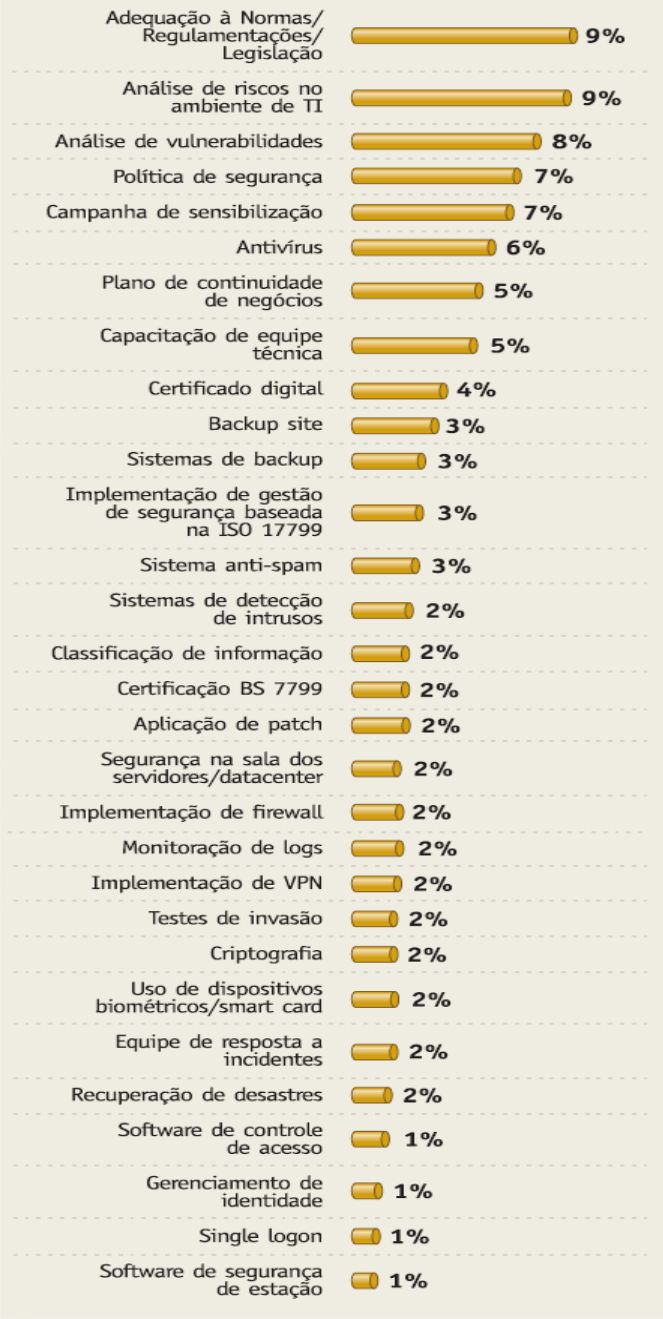

Figura 3 - Principais medidas de segurança por segmento
Fonte (Módulo, 2007, p. 17)

As notícias e as pesquisas nos apontam que se deve refletir quão seguro são os sistemas de informação nas organizações, sejam elas públicas ou privadas, pois a informação tratada

nesses sistemas revela-se em um ativo essencial: portanto é indispensável protegê-la. Nesse contexto, identifica-se uma grande batalha onde um grupo desenvolve mecanismos que visam proteger e outro que tem por objetivo acessar informações por meios ilícitos.

> É interessante observar que o crescimento da importância e até mesmo da dependência do papel da tecnologia nos negócios, somado ao aumento da facilidade de acesso e ao avanço das técnicas usadas para ataques e fraudes eletrônicos, resultam no aumento do número de incidentes de segurança, o que faz com que as organizações devam ser protegidas da melhor maneira possível. Afinal de contas, é o próprio negócio, em forma de bits e bytes, que está em jogo. (NAKAMURA & GEUS, 2007, p. 29)

Portanto, é necessário conhecer a importância da segurança da informação e adotar as melhores práticas adotadas mundialmente, em qualquer ambiente de negócios, em empresas (públicas ou privadas) e seu porte (grandes, médias, pequenas e microempresas), que visam lucro ou não, e principalmente na esfera governamental.

Nakamura & Geus explicam que o fato de se obter vantagem competitiva por intermédio da velocidade e eficiencia nos processos, é uma das estratégia de negócios nos dias de hoje, mas desde que sejam seguros contra ataques e outras contingências, pois senão as organizações correm o risco de incorrerem em grandes prejuízos e provável perda de oportunidades (NAKAMURA & GEUS, 2007).

Como diferentes conceitos são recorrentes em diferentes textos que pululam a internet, livros e artigos, possuindo o mesmo sentido, neste trabalho define-se a informação como sendo parte do conhecimento formada por um conjunto organizado de dados, que transmite uma mensagem sobre um determinado fenômeno ou evento, e permite, dentre outros, resolver problemas e tomar decisões. Deve-se salientar que, porém um dado pode existir sem que necessariamente a informação exista, assim como a informação pode haver sem conhecimento, porém não há conhecimento sem informação (CAMPOS, 2007).

Para que a segurança em sistemas de informação seja eficaz é necessário, antes de mais nada, que se desenvolva um sistema de segurança capaz de detectar vulnerabilidades e prescrever ações de proteção. Desse modo entende-se que a segurança da informação deve ser constituída por controles e políticas de que visam garantir a confidencialidade, a integridade, a disponibilidade, a autenticiade e não repúdio – e nada melhor do que pré-estabelecer uma orientação para o assunto: a politíca de segurança da informação (PSI), aqui entendida como

um conjunto de diretrizes, na qual estabelce o uso adequado dos recursos de TI assim como os direitos e deveres das partes interessadas (*stakeholders*), como bem explica Campos:

> Atualmente, a PSI é adotada em grande parte das organizações em todo o mundo, inclusive no Brasil. esmo aquelas empresas que ainda não tem uma politica efetiva, reconhecem a necessidade de elaborar e implementar uma. Revistas e sites especializados recomendam a utilização de políticas de segurança da informação. As normas ISO 27001 e ISO 27002, ambas específicas sobre segurança da informação, indicam que a política de segurança da informação é um controle essencial. diante de tantas recomendações, é apenas lógico imaginar que deve haver um bom motivo para implementação dessa política na organização. (CAMPOS, 2007, p. 131).

Essa política é fundamental em todas as organizações, por isso a Administração Pública Federal (APF) estabeleceu normas para desenvolver e implantar tais políticas de segurança em suas organizações. Por exemplo, O Decreto n.º 3.505, de 13 de junho de 2000, instituiu a PSI nos órgãos e entidades da APF. De maneira geral, os objetivos expostos nesse decreto, dizem respeito à necessidade capacitar e conscientiza as pessoas que fazem parte das APF, no tocante a segurança da informação, além mostrar a importância da implementação de uma PSI. Outros exemplos que tratam a respeito da segurança da informação em instituições públicas e instituições que fazem parte do judiciário brasileiro podem ser vistas como apêndice deste relatório, tendo como fonte o trabalho de Araujo (ARAÚJO, 2012), atualizado pelo autor deste trabalho, com base em duas fontes distintas[1]·.

O objeto deste trabalho é o Tribunal de Justiça da Paraíba (TJPB) onde um grupo está desenvolvendo, atualmente, sua política de segurança e se espera é que esteja de acordo com as melhores práticas adotadas mundialmente, assim como sugere o Conselho Nacional de Justiça (CNJ) em sua resolução 90, de 29 de setembro de 2009, que dispõe sobre os requisitos de nivelamento de tecnologia da informação no âmbito do poder judiciário, a seguir:

> CAPÍTULO V GESTÃO DE TIC
>
> **Art. 10.** A estrutura organizacional, o quadro de pessoal, a gestão de ativos e os processos do setor responsável pela gestão de trabalho da área de TIC do Tribunal deve-

[1] http://dsic.planalto.gov.br/legislacaodsic, e http://www.cnj.jus.br/programas-de-a-a-z/eficiencia-modernizacao-e-transparencia/comite-nacional-da-tecnologia-da-informacao-e-comunicacao-do-poder-judiciario/resolucoes.

> rão estar adequados às melhores práticas preconizadas pelos padrões nacionais e internacionais para as áreas de governança e de gerenciamento de serviços de TIC.
> **Art. 11**. O Tribunal deve elaborar e manter um Planejamento Estratégico de TIC - PETI, alinhado às diretrizes estratégicas institucionais e nacionais. Parágrafo único. Deverá ser elaborado, com base no PETI, o plano diretor de Tecnologia da Informação e Comunicação (PDTI).
> **Art. 12**. O Tribunal deverá constituir comitê ou comissão responsável por orientar as ações e investimentos em TIC, observado o planejamento de que trata o artigo anterior.
> **Parágrafo único**. Recomenda-se que a composição de tal comitê ou comissão seja multidisciplinar.
> **Art. 13**. O Tribunal deve elaborar e aplicar Política de Segurança da Informação, por meio de um Comitê Gestor, alinhada com as diretrizes nacionais.
> **Art. 14**. As aquisições de equipamentos e contratação de serviços na área de TIC devem atender aos padrões recomendados pelo Comitê Nacional de Gestão de Tecnologia da Informação e Comunicação do Poder Judiciário e aprovado pela Comissão de Tecnologia e Infraestrutura do CNJ. (Redação dada pela Resolução n° 136, de 13.07.11)
> **Art. 15**. O Superior Tribunal de Justiça - STJ, o Tribunal Superior do Trabalho - TST, o Conselho da Justiça Federal - CJF, o Conselho Superior da Justiça do Trabalho - CSJT, o Tribunal Superior Eleitoral - TSE, o Superior Tribunal Militar - STM, os Tribunais de Justiça e os Tribunais de Justiça Militar poderão propor ao CNJ normas específicas sobre TIC para o respectivo segmento e recomendar uso de estruturas e serviços de tecnologia disponíveis. Parágrafo único. O CNJ manterá banco de melhores práticas e definirá requisitos para atestar conformidade de sistemas de automação judicial, conferindo selo a esse respeito.

Uma vez considerada a importância de uma PSI nos meios regidos pela Administração Pública Federal, estabelece-se as perguntas que orientaram este trabalho como sendo:

Será que existem divergências entre a PSI do TJPB com a principal referencia do assunto: a NBR-ISO_27002?

Qual seria o nível de alinhamento observado – Alto, Médio ou Baixo?

A pesquisa enquadra-se como sendo de cunho exploratório, com razoável investigação sobre o assunto em livros, artigos de periódicos, adotará os parâmetros da NBR-ISO-27002, e legislações brasileiras aplicáveis para avaliar um caso específico: a PSI do TJPB. A fundamentação com base nesse levantamento bibliográfico (modelos, leis, resoluções, etc.) auxilia-

rá, sobremaneira, na construção de um quadro auxiliar de análise onde será possível identificar fatores presentes e ausentes na PSI do TJPB, segundo as boas práticas vigentes.

1.1 Justificativas

Independente da organização, a informação deve ser tratada como ativo primordial e a segurança da mesma um requisito fundamental para sua sobrevivência.

No ambito da administração pública especificamente no poder judiciário, o Conselho Nacional de Justiça, instituição pública que visa aperfeiçoar o sistema judiciario brasileiro, por meio da resolução nº 90 de Setembro de 2009 dispõe sobre o nivelamento dos requisitos de tecnologias de informação para os diferentes tribunais; e em complemento, o Plano Estratégico Nacional . Assim como, visando adequar-se ao que sujere a resolução nº 99 de Novembro de 2009 que institui diretrizes para o planejamento estratégico de tecnologia da informação e comunicação do poder judiciario nos diferentes estados, no caso, a Paraiba.. Sendo assim, o Tribunal de Justiça da Paraíba órgão que visa ser reconhecido como instituição confiável, acessível e justa. Sabendo disso, é fundamental garantir os princípios básicos da segurança de informação.

Para garantir que os princípios básicos da segurança de informação sejam alcançados na abrangência do Tribunal de Justiça da Paraíba, mas em consonância com aquele Plano Estratégico mencionado, é necessário que uma política de segurança de informação siga as orientações do CNJ, das normas complementares 03/IN01/DSIC/GSIPR de 30 de junho de 2009 e 17/IN01/DSIC/GSIPR de 10 de abril de 2013, do decreto nº 7.845 de 14 de novembro de 2012. Em complemento, essa política ainda em construção deverá adotar as melhores praticas adotadas mundialmente em seu conteúdo, especialmente aqueles ditados pela norma NBR/ISO/27002:2005.

Com isso pode-se afirmar que este trabalho é inédito e de suma importância não só para universo acadêmico, mas também para toda a sociedade que utiliza os serviços oferecidos pelo tribunal de justiça da Paraíba, pois o mesmo visa ser reconhecido como instituição que presta serviço de excelência.

Também se constitui em justificativa a contribuição que oferece aos desenvolvedores dessa política, como forma de antecipar possíveis descaminhos proporcionados por uma política ineficaz baseada em práticas que não foram adotadas em sua construção.

Por fim, e não menos importante, é o aprendizado na realização de avaliações de políticas que o aluno obteve, fazendo um trabalho constante junto ao grupo desenvolvedor da PSI do TJPB, facilitado por ter sido estagiário naquele tribunal.

1.2 Objetivos

O Presente trabalho tem como objetivo:

- Criar um quadro comparativo com os fatores mencionados na bibliografia consultada, se possível amparando a avaliação de outros tribunais mencionados.
- Analisar a PSI do TJPB.
- Levantar possíveis pontos que deveriam estar incluídos na PSI do TJPB, considerando o padrão da norma brasileira NBR ISO 27002.

Não é foco deste, propor uma nova PSI para o tribunal de justiça da Paraíba.

1.3 DESENHO DA PESQUISA

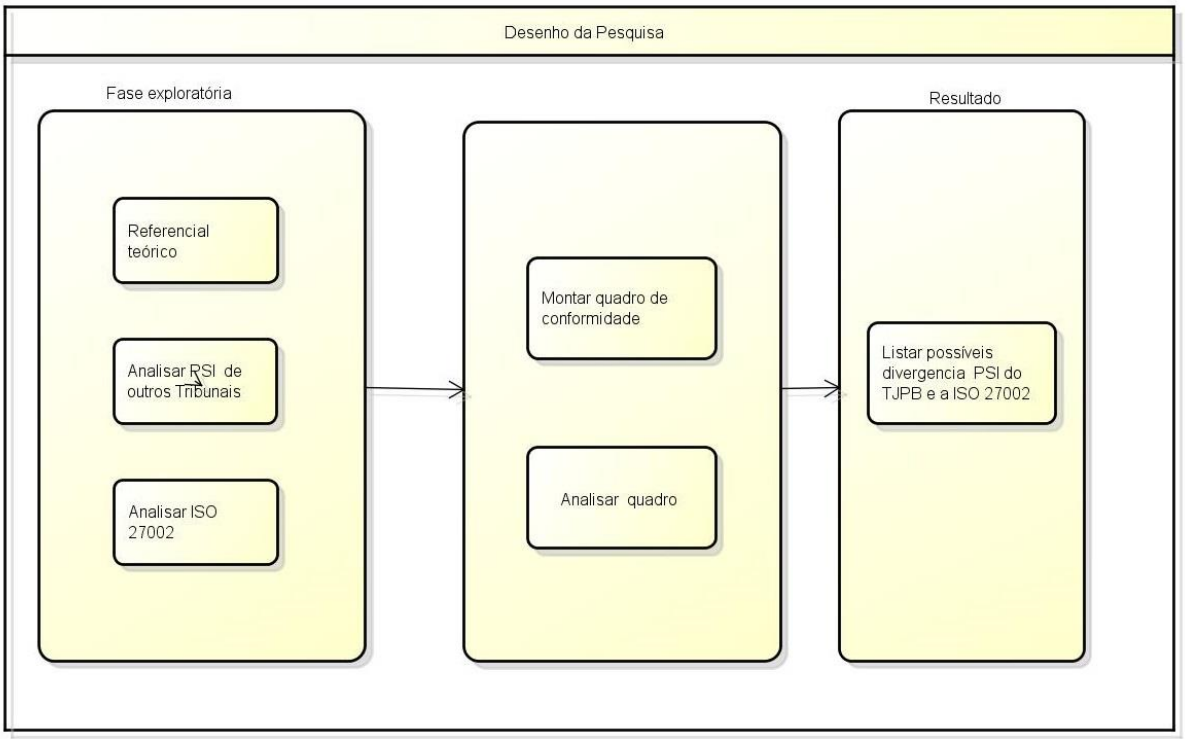

Figura 4 - Desenho da Pesquisa
Fonte: Desenvolvida pelo autor.

1.4 ORGANIZAÇÃO DO TRABALHO SEGUE ABAIXO

- No capítulo 2 encontra-se a fundamentação teórica do assunto tratado na pesquisa, onde o autor procurou estabelecer os principais conceitos que norteiam uma política de segurança de informação.
- O capítulo 3 apresenta a metodologia de pesquisa adotada no presente trabalho, o mesmo buscou apresentar o estudo de caso como técnica adotada.
- No capítulo 4 a pesquisa de campo é revelada, por meio da descrição da organização objeto deste estudo, sua estrutura organizacional, a atual situação da política de segurança, para, finalmente, apresentar os resultados comparativos com a norma NBR/ISO/IEC 27002.
- O capítulo 5 discorre-se sobre as considerações finais acerca da pesquisa, mostrando que os objetivos foram alcançados, logo após será apresentada as lições aprendidas.
- O capítulo 6 publica as bibliografias que foram usadas como base para o presente trabalho.

2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo apresentam-se os conceitos que norteiam uma política de segurança de informação, ou seja, serão apresentadas as definições do que é política, segurança, informação dentre outras definições.

2.1 Informação e Segurança da Informação

2.1.1 Conceito de informação

De acordo com Campos, a definição de informação é ambígua e incerta podendo variar dependendo da área de trabalho, cultura e ciências. No entanto, na literatura a um entendimento de que a informação é composta, em sua essencia, de dados e faz parte do conhecimento (CAMPOS, 2007).

Para Stair e Reynolds "é um conjunto de fatos organizados de modo a terem valor adicional além dos fatos propriamente ditos" (STAIR & REYN0LDS, 2006).

Para Stoner: "Informações são dados analisados ou processados que informam que os recebe sobre uma informação" (STONER J. A., 1982).

Para a ABNT

> É um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e, consequentemente, necessita ser adequadamente protegida. [...] A informação pode existir em diversas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas. Seja qual for a forma de apresentação ou o meio através do qual a informação é compartilhada ou armazenada, é recomendado que ela seja sempre protegida adequadamente. (ABNT, 2005) .

Explica-se: a informação é essencial para a organização, pois auxilia aos gestores a criarem vantagens competitivas a partir da detecção tanto de oportunidades quanto de prováveis ameaças. A informação e o conhecimento serão os diferencias das empresas e dos profissionais que pretedem destacar-se no mercado e manter a sua competitividade (REZENDE & Abreu, 2000).

Informações há muitas, algumas são muito importantes, outras não; assim, quanto mais importantes para a organização, tanto mais devem impactar na sua sobrevivência, por isso é importante classificar a informação segundo os interesses da organização, como será visto a seguir.

2.1.2 Classificação da informação

Para (SPANCESKI, 2004)" A classificação da informação é importante para que as organizações possam determinar o nível de proteção que suas informações, de modo que a segurança de informações importantes para as organizações possa ser assegurada".

A classificação da informação é uma atividade específica e de fundamental importância, uma vez que se faz necessária às organizações definirem o grau de importância de acordo com o tipo de negócio a que pertencem.

O grau de sigilo é o elemento fundamental quando se classifica a informação. Assim, para garantir a proteção da informação é necessário definir o nível proporcional ao seu grau de sigilo, como bem explica a ABNT abaixo:

> A informação possui vários níveis de sensibilidades e criticidade. Alguns itens podem necessitar um nível adicional de proteção ou tratamento especial. Convém que um sistema de classificação da informação seja usado para definir um conjunto apropriado de níveis de proteção e determinar a necessidade de medidas especiais de tratamento. (ABNT NBR ISO/IEC-27002, 2005, p.23).

Em complemento, para Laureano e Moraes, "Nem toda informação é crucial ou essencial a ponto de merecer cuidados especiais, porém uma determinada informação pode ser tão vital que o custo de sua integridade" (LAUREANO & MORAES, 2005). Com isso entende-se que ah necessidade em classificar de acordo com seu grau de sigilo.

- **Secreta –** Informação interna, restrita a um determinado grupo da organização. Segundo Laureano e Moraes, esse tipo de informação deve ser preservado a qualquer custo, pois é considerada de suma importância para a empresa, e, portanto, é preciso manter acesso limitado e seguro (LAUREANO & MORAES, 2005).

- **Confidencial –** A informação na qual deve ser controlada sua divulgação, ficando restrita ao conhecimento interno da empresa. Ela pode ser acessada pelos colaboradores da organização. Para Laureano e Moraes pode haver comprometimento caso

as informações sejam acessadas de forma não auterizada (LAUREANO & MORAES, 2005) e (LYRA, 2008).

- **Interna –** Informação na qual é de interesse exclusivo dos usuários internos da empresa, ficando o acesso de outros usuários. Lyra enfatiza que, se a informção for divulgada, não trará consequencias vitais (LYRA, 2008). "Sua integridade é importante, mesmo que não seja vital." (LAUREANO & MORAES, 2005)

- **Pública –** Laureano e Moraes mostram que este tipo de informação pode ser divulgado, sem restrição e sem causar prejuízo à empresa **(**LAUREANO & MORAES, 2005**).** "São informações que, se forem divulgadas fora da organização, não trarão impactos para o negócio" (LYRA, 2008).

Para a Administração Pública Federal (APF), as informações devem ser classificadas da conforme orientações da LEI Nº 12.527, DE 18 DE NOVEMBRO DE 2011. Especificamente na seção II que dispõe acerca:

Da Classificação da Informação quanto ao Grau e Prazos de Sigilo

> Art. 23. São consideradas imprescindíveis à segurança da sociedade ou do Estado e, portanto, passíveis de classificação as informações cuja divulgação ou acesso irrestrito possa:
> I - pôr em risco a defesa e a soberania nacionais ou a integridade do território nacional;
> II - prejudicar ou pôr em risco a condução de negociações ou as relações internacionais do País, ou as que tenham sido fornecidas em caráter sigiloso por outros Estados e organismos internacionais;
> III - pôr em risco a vida, a segurança ou a saúde da população;
> IV - oferecer elevado risco à estabilidade financeira, econômica ou monetária do País;
> V - prejudicar ou causar risco a planos ou operações estratégicos das Forças Armadas;
> VI - prejudicar ou causar risco a projetos de pesquisa e desenvolvimento científico ou tecnológico, assim como a sistemas, bens, instalações ou áreas de interesse estratégico nacional;
> VII - pôr em risco a segurança de instituições ou de altas autoridades nacionais ou estrangeiras e seus familiares; ou
> VIII - comprometer atividades de inteligência, bem como de investigação ou fiscalização em andamento, relacionadas com a prevenção ou repressão de infrações.

> Art. 24. A informação em poder dos órgãos e entidades públicas, observado o seu teor e em razão de sua imprescindibilidade à segurança da sociedade ou do Estado, poderá ser classificada como ultrassecreta, secreta ou reservada.
> § 1o Os prazos máximos de restrição de acesso à informação, conforme a classificação prevista no caput vigora a partir da data de sua produção e são os seguintes:
> I - ultrassecreta: 25 (vinte e cinco) anos;
> II - secreta: 15 (quinze) anos; e
> III - reservada: 5 (cinco) anos.
> § 2o As informações que puderem colocar em risco a segurança do Presidente e Vice-Presidente da República e respectivos cônjuges e filhos(as) serão classificadas como reservadas e ficarão sob sigilo até o término do mandato em exercício ou do último mandato, em caso de reeleição.
> § 3o Alternativamente aos prazos previstos no § 1o, poderá ser estabelecida como termo final de restrição de acesso a ocorrência de determinado evento, desde que este ocorra antes do transcurso do prazo máximo de classificação.
> § 4o Transcorrido o prazo de classificação ou consumado o evento que defina o seu termo final, a informação tornar-se-á, automaticamente, de acesso público.
> § 5o Para a classificação da informação em determinado grau de sigilo, deverá ser observado o interesse público da informação e utilizado o critério menos restritivo possível, considerados:
> I - a gravidade do risco ou dano à segurança da sociedade e do Estado; e
> II - o prazo máximo de restrição de acesso ou o evento que defina seu termo final.

A informação tem papel importante para gestão, com isso entende-se que é necessário tratá-la de acordo com grau de sigilo e garantir que a mesma permaneça segura.

2.1.3 Conceito de Segurança

A necessidade de segurança é um fato indispensável em qualquer área, apesar de nem sempre ser tratada como se deve. Neste contexto, a fim de se conhecer mais a fundo a importância da mesma, faz-se necessário defini-la adequadamente.

> Segurança seria uma condição relativa à proteção na qual se é capaz de neutralizar ameaças discerníveis contra a existência de alguém ou de alguma coisa com razoável expectativa de sucesso. Em termos organizacionais, segurança é obtida através de padrões e medidas de proteção para conjuntos definidos de informações, siste-

> mas, instalações, comunicações, pessoal equipamento ou operações. (CEPIK, 2003 p.138).

O conceito de segurança é um tema aberto e sua definição depende do contexto na qual estejam inseridos, por falta de uma definição consensual, alguns autores consideram a definição associada a valores intangíveis. No dicionário Houaiss encontra-se a seguinte definição: segurança consiste na ação ou efeito de assegurar e garantir alguma coisa, estado, qualidade ou condição de uma pessoa ou coisa que está livre de perigos, de incertezas, assegurada de danos e riscos eventuais.

Para (MONTEIRO, 2009) "Segurança é o estado ou condição que se estabelece num determinado ambiente, através da utilização de medidas ".

Segurança no âmbito dos negócios faz com que haja novas possibilidades e a liberdade necessária capaz de garantir potencias oportunidades ao negócio.

> Uma solução de segurança é imensurável e não resulta em melhorias nas quais todos podem notar que alguma coisa foi feita. Pelo contrário, a segurança tem justamente o papel de evitar que alguém perceba que alguma coisa está errada. O fato é que ninguém percebe a existência da segurança, apenas a inexistência dela, quando um incidente acontece e resulta em prejuízos gigantescos. (NAKAMURA & GEUS, 2007 p. 52).

Com intuito de delimitar o entendimento do que vem ser segurança, que por sua vez tornar-se muito genérico, este trabalho focará nas definições encontradas na literatura para área mais específica de segurança. Na qual conhecida por segurança da informação. Com isso a necessidade de mostrar sua definição e os princípios que a norteiam.

2.2 Princípios da segurança da informação

A informação, por ser um ativo primordial em qualquer organização, a mesma deve ser preservada independente da forma que a mesma se encontre, seja impressa, escrita em papel, armazenada eletronicamente e etc. Com isso é necessário proteger adequadamente a informação.

Para o TCU, a segurança das informações tem por objetivo garantir e garantir a preservação da confidencialidade, integridade, disponibilidade e autenticidade das informações processadas pela organização (TCU, 2012).

Atualmente a família ISO 27000 é considerada a principal referência a ser seguida pelas organizações quando se quer implantar segurança da informação. Em particular a ISO/IEC 27002 explica:

> A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimento, estruturas organizacionais e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos. (ABNT, 2005, p. x)

A proteção dos ativos deve ser um item a ser implantada em todos os setores de uma organização, neste sentido é preciso estabelecer um nível de segurança a fim de garantir a proteção dos mesmos.

Conforme mostra Campos (2007), um sistema de segurança da informação é formado por três princípios básicos, que são eles: confidencialidade, integridade e disponibilidade. Esse sistema tem a finalidade de garantir que os princípios sejam mantidos (CAMPOS, 2007). Já Loudon (2003) sugere que o sistema de segurança da informação deve garantir que a informação seja verificável, completa, útil e eficaz (LAUDON, 2003, p.3-18).

Seguindo o mesmo entendimento Nakamura e Geus (2007) afirmam ser indispensável garantir a confidencialidade, disponibilidade e integridade da informação, para que se possa ter um bom funcionamento das organizações. Para (BEAL, Segurança da Informação: Princípios e melhores práticas para a proteção dos ativos de informação nas organizações, 2005) segurança da informação pode ser entendida como o processo de proteger informações das ameaças para garantir os três atributos básicos e fundamentais.

Lyra (2008) e a Instrução Normativa GSI 01 (2008), que estabelece diretrizes para a elaboração da PSI e comunicação nos órgãos e entidades da administração pública federal, em seu item II, conceituam segurança da informação como sendo ações que visam garantir além da tríade, citada acima, a autenticidade como sendo um atributo fundamental. Uma das principais orientadoras de segurança na informação, a norma ABNT ISO/IEC 27002 (ABNT, 2005) define segurança da informação como a preservação dos atributos básicos, já mostrados

além da possibilidade de inclusão de demais propriedades, sendo elas: responsabilidade, não repúdio e confiabilidade.

A Figura a seguir mostra os atributos de segurança da informação.

Figura 5 - Atributos de Segurança da Informação
Fonte: http://www.skylan.com.br/img/pilares_da_seguranca.png

Se um ou mais desses atributos forem violados, desrespeitados ou etc. implica em dizer que houve quebra da segurança da informação, ou seja, aconteceu um incidente de segurança da informação (CAMPOS, 2007), portanto faz-se necessário conhecer mais a fundo cada atributo.

Concluindo esse tópico a Brazil IT Snapshot (2014) apresenta os resultados de sua pesquisa a cerca do tema segurança, a pesquisa revela que o tema vem ganhando importância cada vez maior nas corporações, é também aquele sobre o qual as empresas exibem maior grau de maturidade. É um ponto que o Brazil IT Snapshot já havia destacado em 2013 e que se confirma ano de 2014. (Brazil IT Snapshot, 2014).

2.2.1 Conceito de Confidencialidade

Segundo (CAMPOS, 2007), “O princípio da confidencialidade é garantido quando apenas as pessoas explicitamente autorizadas podem ter acesso à informação”.

Conforme (TCU, 2012), “Manter a confidencialidade pressupõe assegurar que as pessoas não tomem conhecimento de informações, de forma acidental ou proposital, sem que possuam autorização para tal procedimento”.

A (INSTRUÇÃO NORMATIVA GSI Nº01, 2008), define confidencialidade como sendo "propriedade de que a informação não esteja disponível ou revelada à pessoa física, sistema, órgão ou entidade não autorizado e credenciado;".

Neste contexto entende-se que garantindo a confidencialidade faz-se necessário suprimir, bloquear, não permitir o acesso a informação a quem não seja devidamente autorizada.

2.2.2 Conceito de Integridade

Conforme mostra o (TCU, 2012) integridade "Consiste na fidedignidade de informações. Sinaliza a conformidade de dados armazenados com relação às inserções, alterações e processamentos autorizados efetuados".

Campos define integridade como sendo o princípio na qual a informação deve está intacta, sou seja, deve ser garantido a não violação, gravação ou exclusão da mesma (CAMPOS, 2007). Na esfera pública integridade é a "propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental (INSTRUÇÃO NORMATIVA GSI Nº01, 2008).".

Com isso entende-se que garantir a integridade é assegurar que as informações não foram alteradas por pessoas ou sistemas não autorizados, ou seja, os mesmos devem ser mantidos em seu formato original.

2.2.3 Conceito de Disponibilidade

Disponibilidade é a "propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade." (INSTRUÇÃO NORMATIVA GSI Nº01, 2008) e se relaciona com a prestação contínua do serviço público, como apresenta o TCU:

> Consiste na garantia de que as informações estejam acessíveis às pessoas e aos processos autorizados, a qualquer momento requerido, durante o período acordado entre os gestores da informação e a área de informática. Manter a disponibilidade de informações pressupõe garantira prestação contínua do serviço, sem interrupções no fornecimento de informações para quem de direito. (TCU, 2012, p. 26)

Campos (2007) enfatiza que "O princípio da disponibilidade é garantido quando a informação está acessível, por pessoas autorizadas, sempre que necessário." (CAMPOS, 2007)

2.2.4 Conceito de Autenticidade

Outro conceito importante, a autenticidade é a "propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;" (INSTRUÇÃO NORMATIVA GSI Nº01, 2008); de outro modo, pode-se dizer que é a garantia na qual a informação tem, onde a mesma possa ser manipulada apenas por quem esteja autorizado. Para o TCU, garantir autenticidade é garantir com exatidão a fonte da informação (TCU, 2012, p. 25).

Com a garantia desses atributos, a segurança de informação será capaz de trazer grandes benefícios para qualquer organização, é notório que ao garanti-los haverá um maior controle dos recursos de informática fazendo com que sistemas críticos estejam sempre em produção.

2.2.5 Não-Repúdio

Segundo definição relatada por (RESS, 2011) o "Não Repúdio é a capacidade de garantir que um usuário ou sistema realmente realizou uma operação em um sistema da informação, não permitindo a existência de dúvidas ou questionamentos sobre a sua realização." Ou seja, é a garantia de autenticidade dadas pelas partes envolvidas.

2.3 Sistema de Segurança de Informações / TIC

Segundo (ABNT NBR ISO/IEC-27001, 2006) "Um sistema de gestão da segurança da informação (SGSI) é projetado para proteger os ativos de informação e proporcionar confiança às partes interessadas". Além do mais, o mesmo pode ser entendido como um conjunto de processos e procedimentos, baseado em normas e na legislação, que uma organização implementa para prover segurança no uso de seus ativos tecnológicos. (ABNT NBR ISO/IEC-27001, 2006).

Sendo assim, Almeida (2013) afirma que "o SGSI torna-se pré-requisito a ser em ambientes corporativos, educacionais, industriais, governamentais e qualquer outro que tenha por objetivo resguardar ambientes que criam, manipulam ou destroem informações relevantes.".

Um fator importante exposto pelo mesmo autor é que deve ser levado em consideração quando se pensa na implementação e manutenção do SGSI, é a estruturação da equipe de colaboradores. Seguindo esse entendimento fica claro que em uma estrutura bem definida os

possíveis problemas quanto à responsabilidades poderão ser sanados. Ainda segundo Almeida (2013):

> "Existe um equívoco muito grande em pensar que os profissionais de segurança se reportam ao departamento de TI, na realidade ele independe deste departamento e se reporta diretamente ao corpo executivo. Caso isto não ocorra o SGSI fica sob as demandas da TI e limita-se em suas tarefas se tornando parte estendida de um departamento, perdendo eficácia e consequente credibilidade no âmbito da empresa. As consequências desta submissão ao departamento de TI condicionam o SGSI a "não identificar" problemas no próprio departamento de tecnologia por motivos óbvios. Para que não ocorram tais fatos é necessário, que, a diretoria da empresa entenda a distinção dos departamentos e a importância do SGSI ser autônomo em suas atividades dentro da organização. Em muitos casos é bem difícil, por diversos motivos, dentre eles a acessibilidade a este corpo executivo pode ser dificultada até a burocratização criada por diversos departamentos que veem o SGSI como um risco."

Portanto, é de fundamental importância ter o apoio da direção para que a SGSI tenha o sucesso esperado.

A Figura 6 a seguir, mostra uma estrutura de sistema de gestão de segurança.

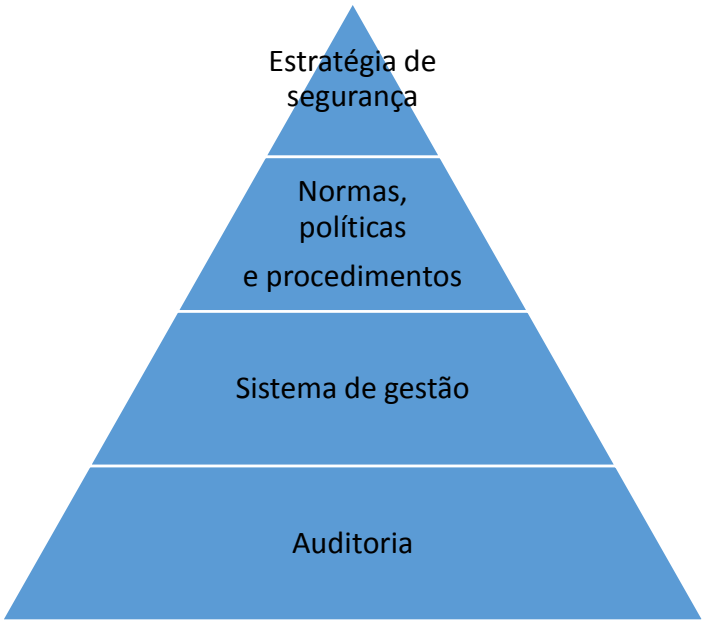

Figura 6 - Estrutura de um sistema de gestão da segurança
Fonte: Adaptado de: http://pt.dreamstime.com/foto-de-stock-estrutura-do-sistema-de-gestão-da-segurança-image12059840

A figura mostra que é fundamental o apoio da diretoria ao SGSI no âmbito da organização. Pois como a (ABNT NBR ISO/IEC-27001, 2006) ressalta: "a adoção de um SGSI deve ser uma decisão estratégica para uma organização". Observa-se no topo da pirâmide a estratégia de segurança que é de responsabilidade da direção defini-la, assim como plano de ação, pois a mesma mostra aonde se quer chegar. Logo em seguida, são mostradas as normas, políticas e procedimentos referem-se os meios que devem ser seguidos para alcançar os objetivos, definindo a estrutura do pessoal, assim como as responsabilidades. A seguir no sistema de gestão são definidas as responsabilidades e por fim na auditoria serão avaliados os processos.

2.4 Política, Diretrizes, Normas e procedimentos.

A importância de uma política é fundamental para a tomada de decisão e mais, é importante conhecer suas diferentes nuances em Administração, cada um com seu sentido e campo de aplicação.

Para Pontes, a distinção entre políticas, diretrizes, normas e procedimentos é necessária uma vez que elas fazem parte de um conjunto de regras formais que servem como ferramenta para a avaliação e execução dos processos organizacionais e auditorias periódicas. (PONTES, 2014, p. 21).

Nas subseções seguintes será mostrado às principais definições no que diz respeito à política.

2.4.1 Conceito de Política

Na literatura existem diversas variações quanto à definição do termo política, isso se dá pelo fato do conceito se aplicar em diversos contextos. Para (BETHLEM, 1981) *apud* (UMEDA & TRINDADE, 2004) mostra que uma das maiores dificuldades em se conceituar política, de forma mais precisa, parte da distinção que há na língua inglesa entre *politcs e policy*, ficando o primeiro termo voltado para a ciência de governar e o segundo referindo-se a administração de empresas.

No dicionário (HOUAISS, 2009) encontra-se as seguintes definições de política:

1. Arte ou ciência de governar
2. Arte ou ciência da organização, direção e administração de nações ou Estados; ciência política.
3. Orientação ou método político

> 4. Arte de guiar ou influenciar o modo de governo pela organização de um partido, influência da opinião pública, aliciação de eleitores etc.
> 5. Prática ou profissão de conduzir negócios políticos
> 6. Cerimônia, cortesia, urbanidade.
> 7. Fig. habilidade no relacionar-se com os outros, tendo em vista a obtenção de resultados desejados.

Diante do exposto, fica clara a diversidade de conceitos e campos de aplicação, que ora enfocam o termo Política no ambiente social/governamental,ora se aplicada nas organizações, ou ainda em regras de etiqueta e relacionamentos inter-humanos. Umeda e Trindade (2004) ratificam essa ideia de diversidade e complexidade: "mesmo os teóricos discordam entre si sobre qual a acepção mais correta ou que oferecerá maior contribuição à organização".

Para Steiner e Miner, não existe consenso quanto ao sentido da política organizacional, e mais, há ocasiões em que é difícil distinguir políticas de estratégias. Para os autores, as políticas dirigem a ação ou o pensamento para o atingimento de um objetivo e metas, e explicam como esses devem ser atingidos, de forma a assegurar coerência de propósitos e evitar decisões que possam resolver problemas operacionais imediatos em detrimento ao alcance de objetivos estratégicos de maior prazo (STEINER & MINER, 1981, p. 25).

As possíveis definições de política apresentadas até aqui, referem-se de forma genérica no sentindo amplo do termo. Este trabalho tem foco na segurança da informação, mais especificamente a PSI.

Para Caruso e Steffen (2006) a "Política de segurança é um conjunto de diretrizes gerais destinadas a governar a proteção a se dada a ativos da companhia." Os autores fazem a seguinte ressalva: caso uma política de segurança eficiente seja posta em prática ela pode se concentrar em três aspectos: redução da probabilidade de ocorrência; de danos causados por eventuais ocorrências e criação de procedimentos para se recuperarem de eventuais danos.

Para Ferreira (2003) *apud* Monteiro (2009) e Pontes (2014) "política é o texto de alto nível de documentação, que dá direcionamento geral e significado aos objetivos..".

Percebe-se, diante do exposto, quão difícil é conseguir definir o que é uma política, que pode ser entendida como um guia, uma orientação, que tem como objetivo auxiliar a direção a tomar decisões acertadas. Neste trabalho usaremos o seguinte conceito de politica definido por Caruso e Steffen (2006), "política é um conjunto de diretrizes".

Quanto à classificação de políticas, segundo Ferreira (2003) existem três tipos de politicas: regulatórias, consultivas e informativas.

A Política Regulatória é um documento criado com intuito de fornecer a organização uma série de especificações legais, na qual devem ser muito bem detalhadas, deixando claro o que deve ser feito e quem deve fazer. Esse tipo de política mostra as necessidades legais que devem ser implementadas nas organizações.

Por sua vez, a Política Consultiva indica quais são as ações ou métodos que devem ser adotado para concretização de determinadas tarefas. O principal objetivo desse tipo de politica é conscientizar os funcionários da organização das atividades do dia-a-dia.

Finalmente, a Política Informativa caracteriza-se por não haver riscos, caso nenhuma ação seja cumprida ou realizada. Esta politica diferencia das demais por não ser tão rigorosa.

2.4.2 Conceito de Diretriz

De maneira geral pode se afirmar que diretrizes são regras genéricas, na qual a partir delas as normas e procedimentos são elaboradas, elas desempenham seu papel no nível estratégico e por esse motivo as mesmas complementam a política da organização. Segundo (CAMPOS, 2007, p. 137) "As diretrizes informam qual é a visão da organização sobre um determinado tema geral [...] a diretriz informa qual é a visão da organização".

Já o CNJ (2012) estabelece que as diretrizes façam parte da base da gestão de segurança da informação e que as mesmas orientem a criação das normas e dos procedimentos. (CNJ, 2012) .

Para a (ABNT, 2005) "Diretriz é uma descrição que orienta o que deve ser feito e como, para se alcançarem os objetivos estabelecidos nas políticas.".

Por tanto, entende-se que as diretrizes embasam as normas a partir dos objetivos definidos na política.

2.4.3 Conceito de Norma

Da mesma forma que diretrizes compõe a política, as normas completam e complementam, e fazem parte de alguma diretriz dentro da organização, mas apresentam características específicas, elas definem comportamentos dentro da organização, ou seja, as normas por estarem em um nível diferente das diretrizes são elaboradas com foco específico de acordo com a diretriz na qual a mesma faz parte.

Uma norma conforme definição mostrada a seguir, é:

> Documento estabelecido por consenso e aprovado por um organismo reconhecido, que fornece, para uso comum e repetitivo, regras, diretrizes ou características para

> atividades ou seus resultados, visando à obtenção de um grau ótimo de ordenação em um dado contexto. (ABNT, 2006).

Uma Norma segundo (CAMPOS, 2007, p. 138) "Informa o que a organização espera em termos de comportamento em um determinado assunto".

2.4.4 Conceito de Procedimento

Finalmente, os procedimentos encontram-se no nível operacional, com isso faz-se necessário descrevê-lo de acordo com a norma que o mesmo faz parte, pois seguindo o entendimento da hierarquia já dita, onde as diretrizes são compostas de normas e as normas são compostas de procedimentos e os procedimentos mostram como deve ser feito, ou seja, são mostrados os passos necessários na qual deve está bem claro (CAMPOS, 2007).

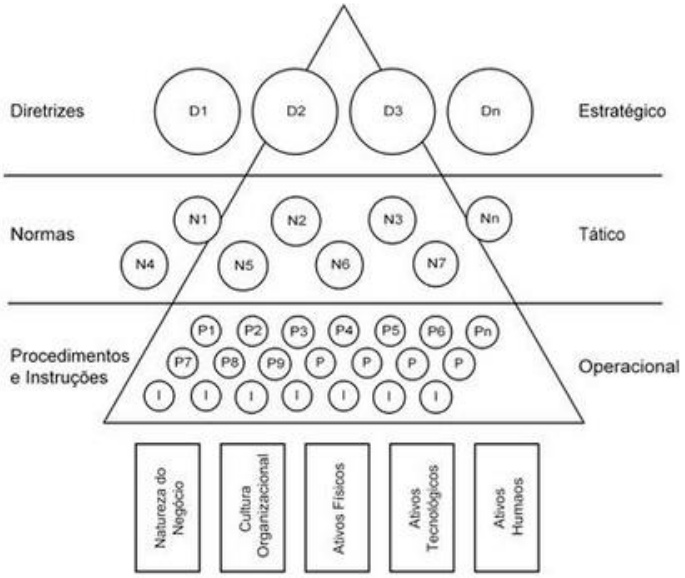

Figura 7 - Diagrama de conceito dos componentes da política e seus pilares
Fonte: (SEMOLA, 2003, versão kindle, posição 1835).

Diante do exposto foi possível conhecer os diferentes conceitos que são empregados a respeito do que vem a ser uma política, além de conhecer as definições ficou claro a importância da mesma para as organizações, seja ela publica ou privada. (CAMPOS, 2007) *apud* (MONTEIRO, 2009) "O objetivo de uma política é estabelecer um padrão de comportamento que seja conhecido por todos na organização."

A figura 7 mostrou a estrutura conceitual de uma política assim como a divisão por nível: Estratégico, Tático e operacional. Seguindo o mesmo entendimento deste trabalho, PONTES (2014) relata as seguintes definições:

- Nível estratégico: Algumas situações exigem decisões não programadas que podem afetar substancialmente uma organização. Novos desafios, oportunidades ou ameaças que podem impactar na sobrevivência da organização exigem ponderação e cuidado, e são conduzidas tendo como fundamento os valores da organização: uma decisão errada pode mudar completamente o rumo da organização. Assim são as políticas de segurança de informação.

- Nível tático: Nesse nível, a palavra é padronização: software, correio eletrônico, equipamentos, entre outras coisas, devem ser padronizados, pois assim todos os pontos da organização terão o mesmo nível de segurança e não haverá nenhuma vulnerabilidade aparente.

- Nível operacional: O essencial no nível operacional é o detalhamento, pois assim se garante a perfeição no atendimento e na continuidade dos negócios independente do fator humano. Se existe um padrão formalizado então esse padrão deve ser seguindo; na política de segurança a parte operacional vem para padronizar detalhes de configurações do ambiente. Pode-se criar um único padrão que sirva para toda organização, ou criar vários padrões para varias localidades da organização, isso vai de acordo com a necessidade que a organização apresenta; o essencial é saber que o padrão é importante. (PONTES, 2014, p. 22)

Um desenho bastante elucidativo a respeito das relações entre níveis organizacionais e a segurança da informação, com seus diferentes elementos orientadores/prescritores é apresentada na Figura 8, que compõe a política de segurança da informação no Governo do Rio Grande do Sul. Estas definições mostram o intuito em deixar clara a responsabilidade em cada nível.

Figura 8 - Segurança da Informação e níveis organizacionais no Governo do RS

Fonte: http://www.tic.rs.gov.br/conteudo/3264/cgtic-institui-a--politica-de-seguranca-da-informacao-para-administracao-publica-estadual

A Figura 9 a seguir mostra os fatores críticos em segurança da informação apresentados pela Brazil IT Snapshot (2014) e onde conscientizar os profissionais ou colaboradores é um dos elementos mais importantes.

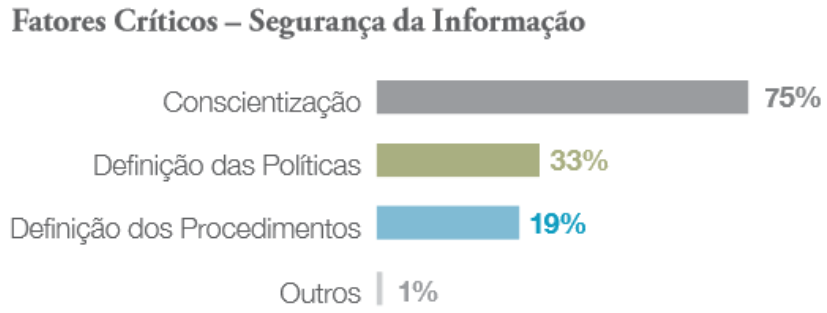

Figura 9 - Fatores Críticos - Segurança da Informação
Fonte: (Brazil IT Snapshot, 2014)

Observa-se que definir as políticas é um tópico que apresenta grande desafio, haja vista que a conscientização das profissionais, como já foi dito, revela-se como fator primordial para o sucesso da politica de segurança da informação como vimos anteriormente. Não basta desenvolver políticas, é preciso conscientizar as pessoas para absorver os conceitos nelas envolvidos. Outro ponto importante é a definição dos procedimentos necessários para a segurança informacional. A seguir serão apresentados os principais conceitos e definições encontradas, para que se possa definir uma política de sucesso.

2.5 Política de segurança de informação

Uma política de segurança de informação (PSI) é fundamental nas organizações, pois com ela definem-se regras para o acesso a informação, sua preservação e precaução, fazendo com que como pessoas, hardware, software, dentre outros, se integrem na organização para dirimir suas vulnerabilidades ou minimizar ataques internos ou externos.

Para (CAMPOS, 2007) "PSI é um conjunto de regras, normas e procedimentos", nesse sentido entende-se que ela estabelece regras gerais para o acesso à informação, onde o comprometimento parte da alta direção e é repassada aos níveis inferiores, fazendo com que os integrantes da organização devem interagir com recursos tecnológicos no que se refere à segurança da informação.

Uma definição mais precisa desenvolvida pelo TCU explica:

> Política de segurança da informação é um conjunto de princípios que norteiam a gestão de segurança de informações e que deve ser observado pelo corpo técnico e gerencial e pelos usuários internos e externos. As diretrizes estabelecidas nesta política determinam as linhas mestras que devem ser seguidas pela instituição para que sejam assegurados seus recursos computacionais e suas informações. (TCU, 2012, p. 10)

A PSI é um documento na qual sua atualização é indispensável para que o mesmo se mantenha efetivo, garantindo assim seu alinhamento contínuo às necessidades do negócio. Com isso, entendem-se da importância em se ter mecanismos com as quais seja garantida a atualização deste documento (BEAL, 2005).

Para a ABNT NBR ISO/IEC-27002 uma "Política de segurança da informação é documento aprovado pela direção e deve ser de conhecimento de todos que fazem parte da organização, na qual visa alinhar os requisitos do negócio da organização no que diz respeito a segurança da informação e com as leis e regulamentações pertinentes". (ABNT, 2005)

Já a norma complementar 03/IN01/DSIC/GSIPR, estabelece nos itens a seguir que:

- 2.1 A Política de Segurança da Informação e Comunicações declara o comprometimento da alta direção organizacional com vistas a prover diretriz as estratégicas, responsabilidades, competências e o apoio para implementar a gestão de segurança da informação e comunicações nos órgãos ou entidades da Administração Pública Fe deral, direta e indireta;
- 2.2 As diretrizes constantes na Política de Segurança da Informação e Comunicações no âmbito do órgão ou entidade visam viabilizar e assegurar a disponibilidade, integridade,confidencialidade e autenticidade da informação.(03/IN01/DSIC/GSIPR, 2009).

Para o TCU:

> A política de segurança de informações deve extrapolar o escopo abrangido pelas áreas de sistemas de informação e pelos recursos computacionais. Ela não deve ficar restrita à área de informática. Ao contrário, ela deve estar Integrada à visão, à missão, ao negócio e às metas institucionais, bem como ao plano estratégico de informática e às políticas da organização concernentes à segurança em geral. O conteúdo da PSI varia, de organização para organização, em função de seu estágio de maturidade,

> grau de informatização, área de atuação, cultura organizacional, necessidades requeridas, requisitos de segurança, entre outros aspectos. (TCU, 2012, p. 11)

2.5.1 Objetivos de uma PSI

Segundo a mesma ABNT (2005) o objetivo primordial da PSI é "prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações pertinentes." Além do mais fazer com que a utilização dos recursos tecnológicos de informática e o mais importante, as informações, independente do formato que as mesmas estejam (documentos físicos ou eletrônicos), sempre sejam de maneira adequada.

Sendo assim, e ainda seguindo o entendimento mostrado pela ABNT (2005), é indispensável o envolvimento, empenho e comprometimento da alta direção e que ela mostre para os demais envolvidos que a política está alinhada com os objetivos da organização com isso faz-se necessário à publicação.

2.5.2 Tópicos essenciais contidos em uma PSI

Levantamento feito com as principais referências bibliográficas apresenta os fatores essenciais de uma PSI, e estão resumidas no quadro abaixo.

Quadro 1 - Fatores essenciais de uma PSI segundo fontes pesquisadas

FATORES DE COMPARAÇÃO	Beal (2004)	ABNT (2005)	FREITAS & ARAUJO, 2008	GSI Nº01,2008	TCU (2012)
Referências Legais		X	X	X	X
Atribuição das responsabilidades	X	X	X	X	X
Definição do Escopo		X	X	X	X
Análise de Risco	X	X	X		X
Penalidade			X	X	X
Divulgação	X	X			X
Treinamento	X	X			X

No tocante às responsabilidades, todas as fontes apontam como essencial para se ter em uma PSI o item que trata das atribuições das responsabilidades, já que a adoção dele garante

que haverá pessoas de setores importantes da organização, ou seja, gestores de diversas áreas devem participar da elaboração da PSI, sendo que é necessário que a mesma seja aprovada pela mais alta direção.

Outo ponto importante mostrado no quadro revela a importância em se ter referências legais, este item é importante já que adotar as melhores práticas garante que a mesma seja menos sujeita a erro na elaboração.

Já no item análise de risco, a maioria das fontes adota como sendo fundamental para fazer parte de uma PSI.

Portanto o quadro resume sucintamente fatores importantes que, segundo os autores pesquisados, devem estar presente em uma PSI.

2.6 Modelos de Segurança da informação

Segundo FURTADO (2011) na literatura existem vários modelos que abrangem a segurança da informação, que possuem alinhamento com os da família 27000 os mais conhecidos são: CMMI COBIT e ITIL. Essa família é composta, dentre outras em desenvolvimento, por:

- ISO 27001: especificação do sistema de gestão de segurança da informação.
- ISO 27002: código e prática para gestão de segurança da informação.
- ISO 27003: guia de implementação do sistema de gestão de segurança da informação.
- ISO 27004: medidas e métricas utilizadas em segurança da informação
- ISO 27005: gestão de riscos em sistemas de gestão de segurança da informação
- ISO 27006: requisitos para auditoria e certificação de um sistema de gestão de segurança da informação. (CAMPOS, 2007, p. 126)

A primeira, conhecida como NBR ISO/IEC 27001 especifica os requisitos para um Sistema de Gestão de Segurança da Informação (SGSI). O documento desta norma está estruturado em oito seções, sendo que as três primeiras referem-se à Introdução, Objetivo, Referência Normativa e Termos e Definições. Os requisitos propriamente ditos se localizam nas seções finais.

> Esta Norma foi preparada para prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de

> Segurança da Informação (SGSI). A adoção de um SGSI deve ser uma decisão estratégica para uma organização. A especificação e a implementação do SGSI de uma organização são influenciadas pelas suas necessidades e objetivos, requisitos de segurança, processos empregados e tamanhos e estrutura da organização. É esperado que este e os sistemas de apoio mudem com o passar do tempo. É esperado que a implementação de um SGSI seja escalada conforme as necessidades da organização, por exemplo, uma situação simples requer uma solução de um SGSI simples. (ABNT NBR ISO/IEC-27001, 2006, p. V).

Portanto, a norma sugere que a organização estabeleça, identifique e gerencie os processos envolvidos em um SGSI, além de verificar suas interações. Salienta-se que essa norma prioriza o ciclo denominado PDCA (*Plan*, *Do*, *Check*, *Act*), uma ferramenta de gestão consagrada nas normas ISO que deve ser utilizada em qualquer área da empresa uma vez que possibilita melhoria contínua de processos e a solução de problemas (ABNT NBR ISO/IEC-27001, 2006).

Figura 10 - Ciclo PDCA
Fonte: http://www.profissionaisti.com.br/2010/10/conhecendo-a-abnt-nbr-isoiec-27001-parte-1/

Como visto na figura anterior, o ciclo PDCA se inicia pelo planejamento, logo após são executadas as ações planejadas; em seguida na fase de checagem será feita a comparação do que foi planejado no processo, e por fim toma-se uma ação de correção dos problemas e divergências encontradas, reiterando o ciclo.

> Plan (planejar) (estabelecer o SGSI): Estabelecer a política, objetivos, processos e procedimentos do SGSI, relevantes para a gestão de riscos e a melhoria da segurança da informação para produzir resultados de acordo com as políticas e objetivos globais de uma organização.
>
> Do (fazer) (implementar e operar o SGSI):Implementar e operar a política, controles, processos e procedimentos do SGSI.
>
> Check (checar) (monitorar e analisar criticamente o SGSI): Avaliar e, quando aplicável, medir o desempenho de um processo frente à política, objetivos e experiência prática do SGSI e apresentar os resultados para a análise crítica pela direção.
>
> Act (agir) (manter e melhorar o SGSI): Executar as ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e da análise crítica pela direção ou outra informação pertinente, para alcançar a melhoria contínua do SGSI. (ABNT NBR ISO/IEC-27001, 2006, p. VI)

2.6.1 Segurança da informação segundo a ISO/IEC 27002

No Brasil, a partir de 2007 a norma NBR ISO/IEC 27002:2005 (Tecnologia da informação – Técnicas de segurança – código de prática para a gestão da segurança da informação), passou a substituir à norma ISO/IEC 17799:2005, trata de técnicas de segurança no âmbito da tecnologia da informação. “Esta norma pode servir como um guia prático para desenvolver os procedimentos de segurança da informação da organização e as eficientes práticas de gestão da segurança.” (ABNT, 2005). Os objetivos definidos nessa norma configuram as melhores práticas quando se fala em gestão da segurança da informação.

A norma está dividida em 11 capítulos de controles de segurança da informação, que por sua vez são compostos por 39 categorias. Do capítulo um ao quatro a norma apresenta seu objetivo, termos e definições, a seguir será apresentada como a norma está estruturada:

- Capítulo 5– Políticas de Segurança da Informação (1)
- Capítulo 6 – Organizando a Segurança da Informação (2)
- Capítulo 7 – Gestão de Ativos (2)

- Capítulo 8 – Segurança em Recursos Humanos (3)
- Capítulo 9 – Segurança Física e do Ambiente (2)
- Capítulo 10 – Gestão das Operações e Comunicações (10)
- Capítulo 11 – Controle de Acessos (7)
- Capítulo 12 – Aquisição, Desenvolvimento e Manutenção de Sistemas. (6)
- Capítulo 13 – Gestão de Incidentes de Segurança da Informação (2)
- Capítulo 14 – Gestão da Continuidade do Negócio (1)
- Capítulo 15 – Conformidade (3)

> A ordem das seções nesta Norma não significa o seu grau de importância. Dependendo das circunstancias, todas as seções podem ser importantes. Portanto, convém que cada organização que utiliza esta Norma identifique quais são os itens aplicáveis, quão importantes eles são e a sua aplicação para os processos específicos do negócio. Todas as alíneas nesta Norma também não estão ordenadas por prioridade, a menos que explicado. (ABNT, 2005, p. 4)

Esta norma é um conjunto de recomendações gerais para melhores práticas da gestão da segurança de informação e procedimentos para a segurança da informação e essas orientações são aceitas mundialmente.

Um dos seus capítulos trata da gestão de continuidade do negócio, elemento principal de um sistema de segurança da informação, pois trata de ações após um incidente ou ataque que possa ter causado transtornos substanciais ou, inclusive, o risco de se perder o negócio. Esse tópico será apresentado a seguir.

2.7 Gestão de continuidade do negocio e sua importância

Para o TCU (2012) um Plano de Continuidade do Negócio (PCN) consiste no desenvolvimento de um conjunto de estratégias, procedimentos e planos que visam garantir os serviços essenciais, ou seja, no PCN são definidas as ações necessárias quando a instituição ou uma área específica se deparar com problemas que comprometam o andamento normal dos processos e a consequente prestação dos serviços (TCU, 2012).

O PCN estabelece que as estratégias e procedimentos adotados devam reduzir o impacto que por ventura venha sofrer diante do acontecimento de situações imprevisíveis, ocasional, inesperadas, desastres naturais, falhas de segurança, entre outras, até que a normalidade seja

estabelecida. Para o (TCU, 2012) "O Plano de Continuidade do Negócio é um conjunto de medidas que combinam ações preventivas e de recuperação. Obviamente, os tipos de riscos a que estão sujeitas as instituições variam no tempo e no espaço.".

Além do que foi exposto, a 06/IN01/DSIC/GSIPR estabelece que o PNC seja composto por: "Documentação dos procedimentos e informações necessárias para que aos órgãos ou entidades da APF mantenha seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo num nível previamente definido, em casos de incidentes".

O TCU (2012) mostra a seguir a importância de uma PCN:

> Atualmente, é inquestionável a dependência das instituições aos computadores, sejam eles de pequeno, médio ou grande porte. Esta característica quase generalizada, por si só, já é capaz de explicar a importância do Plano de Continuidade do Negócio, pois, se para fins de manutenção dos serviços, as instituições dependem de computadores e de informações armazenadas em meio eletrônico, o que fazer na ocorrência de situações inesperadas que comprometam o processamento ou disponibilidade desses computadores ou informações? Ao contrário do que ocorria antigamente, os funcionários não mais detêm o conhecimento integral, assim como a habilidade para consecução dos processos organizacionais, pois eles são, muitas vezes, executados de forma transparente. Além disso, as informações não mais se restringem ao papel, ao contrário, elas estão estrategicamente organizadas em arquivos magnéticos. Por conseguinte, pode-se considerar o Plano de Continuidade do Negócio quesito essencial para as instituições preocupadas com a segurança de suas informações. (TCU, 2012, p. 32)

Para Monteiro (2009) a importância de um PCN pode ser entendida pela seguinte definição: "Conjunto de procedimentos emergenciais a serem adotados na eventualidade da ocorrência de um determinado incidente de segurança da informação.". Seguindo o entendimento do autor:

> Um Plano de Continuidade de Negócios (PCN) deverá ser acionado sempre que houver um evento específico que possa causar interrupção da continuidade do negócio da organização. Premissas deverão ser adotadas na elaboração do PCN: - Os procedimentos de emergência devem ser feitos de modo a recuperar as condições de trabalho dentro de prazos que garantem o menor impacto ao negócio; - Todos os procedimentos deverão ser documentados; - Deverá ter treinamento constante para

> os responsáveis (operadores/ executores) dos procedimentos, afim de atualização dos mesmos; - Os procedimentos deverão ser testados e melhorados. (MONTEIRO, 2009, p. 55)

Neste contexto nota-se a importância em se ter o PNC na organização, seja ela publica ou privada, uma vez que se faz necessário garantir a continuidade do negócio minimizando as prováveis perdas, caso aconteça algum incidente.

2.8 Conclusão do capítulo

A política de segurança da informação está baseada em uma série de conceitos, definições e etc. Neste capítulo foram apresentados os tópicos que revelam a importância em se ter uma PSI independente da organização, uma vez que a mesma fornece um enquadramento para a implementação de mecanismos de segurança. Por tanto é preciso desenvolvê-la seguindo os conceitos apresentados e embasados nas principais referências do assunto e melhores modelos aceitos mundialmente, assim como bases legais: Leis, Normas, Decretos e Instruções Normativas.

No capítulo seguinte será apresentada a metodologia aplicada.

3 METODOLOGIA

A pesquisa enquadra-se, quanto à abordagem, como qualitativa; quanto aos objetivos, pesquisa exploratória; e quanto aos procedimentos, estudo de caso (SILVEIRA & CÓRDOVA, 2009); foi fundamentada em leis, instruções normativa, livros, artigos científicos e outros documentos disponíveis na internet para ser aplicada a um caso específico como forma de compreensão e revelação da conformidade de uma política em desenvolvimento com um padrão estabelecido, o que caracteriza um estudo de caso.

Gil (2002) define pesquisa exploratória como aquela que tem o objetivo de buscar uma maior familiarização do problema, assim como "aprimorar ideias ou descobrir intuições" (GIL, 2002)

Para Marconi & Lakatos pesquisa bibliográfica é:

> Um apanhado geral sobre os principais trabalhos já realizados, revestidos de importância, por serem capazes de fornecer dados atuais e relevantes relacionados com o tema. O estudo da literatura pertinente pode ajudar a planificação do trabalho, evitar publicações e certos erros, e representa uma fonte indispensável de informações, podendo até orientar as indagações. (MARCONI & LAKATOS, 2003, p. 158)

A pesquisa foi feita em fontes primárias e secundárias nos seguintes temas, políticas de segurança da informação, melhores práticas em segurança da informação, normas e metodologias de implantação de políticas de segurança a informação, assim como em leis, decretos, resoluções e instruções normativas. Além disso, foi realizado contato direto do pesquisador junto ao órgão responsável dentro do TJPB, o que Silveira e Cordova (2009, p. 39) apresentam como necessárias para a realização de um estudo de caso.

Portanto neste trabalho será dada mais ênfase nas seguintes fontes:

- NBR ISO/IEC 27002:2005 - Técnicas de segurança – Código de prática para gestão da segurança da informação.
- Decreto nº. 3505 de 2000, que institui a Política de segurança da informação nos órgãos da Administração Pública Federal.

- Norma complementar 03/IN01/2008/GSIPR/ DSIC que disciplina a gestão de segurança da informação e comunicações na administração pública federal, direta e indireta.
- TCU Boas práticas em segurança da Informação
- Resolução 99 de 24 de novembro de 2009 do CNJ que institui o planejamento estratégico de tecnologia da informação e comunicação no âmbito do poder judiciário
- Resolução 90 de 2009 do CNJ que dispõe sobre os requisitos de nivelamento de tecnologia da informação no âmbito do poder judiciário.

Com esse levantamento bibliográfico foi possível obter o nível de entendimento suficiente para criar um quadro de comparação entre a NBR ISO 27002:2005 e a PSI do TJPB. Outros tribunais foram comparados somente para se ter uma ideia da possível variação no alinhamento entre as políticas, uma vez que fazem parte do Sistema Judiciário Brasileiro. A importância desse quadro, é que ele fornece um nível alinhamento da PSI do TJPB que, para sociedade, é de grande importância ser reconhecido como uma instituição confiável, acessível e justa – e nada melhor do que ter uma imagem de segurança em seus sistemas informacionais.

O quadro é composto por 133 controles que podem receber uma pontuação de acordo com a existência ou não, esta pontuação foi definida da seguinte forma: 2 se o item estiver em sua totalidade; 1 se o item estiver em parte e 0 se o item não estiver presente.

O preenchimento do quadro foi feito por intermédio de análise desses fatores nas PSIs avaliadas; após o preenchimento foram efetuadas as somas parciais e totais de cada objeto analisado e onde se obteve a pontuação final comparada.

Para análise do resultado ficou estabelecido que se a pontuação estiver entre 180 e 266 pontos a mesma enquadra-se com aderente a norma NBR ISO (Aderência Alta); se a pontuação estiver entre 90 e 179 a mesma enquadra-se como insuficiente apesar de alguns controles estarem de acordo com norma (Aderência Média); se a pontuação estiver a baixo de 89 pontos a mesma enquadra-se como não-aderente a norma (Aderência Baixa), isso significa que é preciso rever a PSI e procurar revisar a fim de obter um nível satisfatório.

Um tratamento estatístico aprofundado poderia ter sido realizado, mas tendo em vista o caráter exploratório do trabalho, que buscou obter *insights* ou entender melhor o assunto, essa etapa foi descartada.

4 RESULTADOS

4.1 O TRIBUNAL DE JUSTIÇA DA PARAÍBA

4.1.1 Histórico, características das principais partes interessadas (*stakeholders*)

O Tribunal de Justiça da Paraíba foi criado em 30 de setembro de 1891, pelo decreto nº 69, o superior Tribunal de Justiça, pelo mesmo decreto foi designado o dia 15 de outubro de 1891 para que o mesmo seja instalado.

O mesmo está situado na Praça João Pessoa, s/n - CEP 58013-902 - João Pessoa (PB).

O TJPB tem por missão, concretizar a justiça por meio de uma prestação jurisdicional acessível, célere e efetiva. Já a visão pretende-se alcançar até o ano de 2018, o grau de excelência na prestação de seus serviços e ser reconhecido pela sociedade como uma instituição confiável, acessível e justa, na garantia do exercício pleno da cidadania e promoção da paz social.

Atributos de Valor para a Sociedade

- Credibilidade;
- Modernidade;
- Acessibilidade;
- Transparência;
- Credibilidade;
- Responsabilidade Social e Ambiental;
- Imparcialidade;
- Ética;
- Probidade.

Atributos Diferenciadores de Valor

- Comprometimento;
- Serviço de qualidade;
- Justiça humanizada;
- Impacto social;
- Eficiência e eficácia;
- Igualdade.

4.1.1.1 Organização Judiciária

Conforme a LEI Nº 9.316, DE 29 DE DEZEMBRO DE 2010, na qual dispõe da organização administrativa e divisão judiciária do estado da Paraíba, o poder judiciário está organizado com segue:

Art. 2º São órgãos do Poder Judiciário do Estado:

I – o Tribunal de Justiça;
II – o Tribunal do Júri;
III – os Juízes Substitutos e de Direito;
IV – a Justiça Militar;
V – os Juizados Especiais;
VI – a Justiça de Paz.

Art. 6º São órgãos do Tribunal de Justiça:

I – o Tribunal Pleno;
II – as Seções Especializadas;
III – as Câmaras Especializadas;
IV – o Conselho da Magistratura;
V – a Presidência do Tribunal de Justiça;
VI – a Vice-Presidência do Tribunal de Justiça;
VII – a Corregedoria-Geral de Justiça;
VIII – as Comissões;
IX – a Escola Superior da Magistratura;
X – a Ouvidoria de Justiça

A seguir será mostrado o organograma do TJPB que dispõe da divisão estrutural do mesmo.

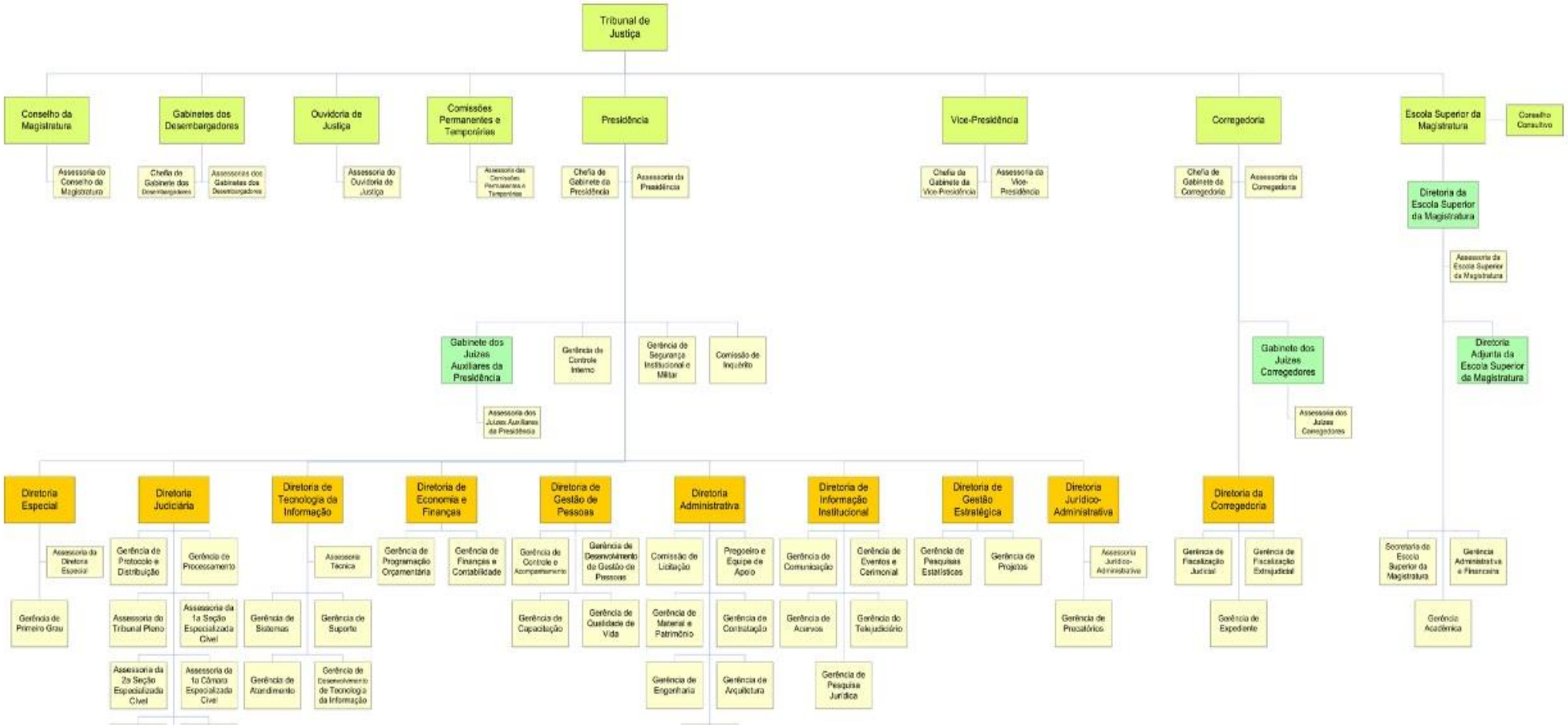

Figura 11 - Organograma TJPB

Fonte: http://www.tjpb.jus.br/wp-content/uploads/2012/05/organograma.pdf

A diretoria de tecnologia da informação (DITEC) é o órgão responsável em administrar os recursos de tecnologia da informação além de padronizar os métodos e as práticas dos processos de trabalho. A Figura 12 mostra a divisão da DITEC.

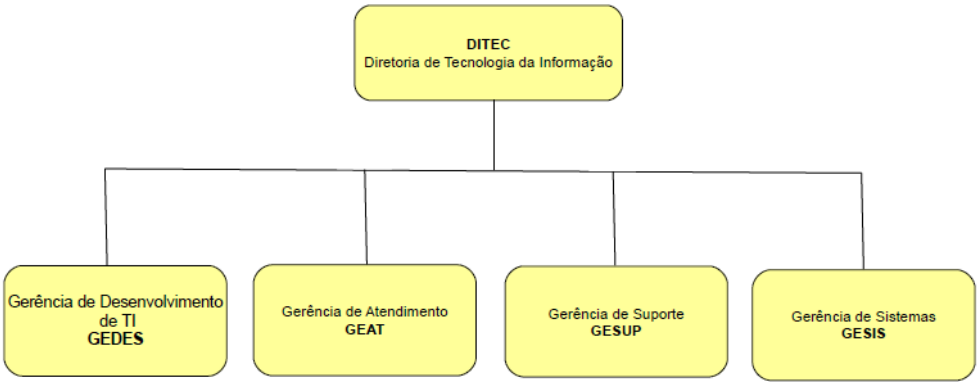

Figura 12 - Organograma DITEC
Fonte: http://www.tjpb.jus.br/wp-content/uploads/2012/05/organograma.pdf

A Diretoria de Tecnologia da Informação tem por missão administrar os recursos de tecnologia da informação e padronizar os métodos e as práticas dos processos de trabalho, especialmente.

- Planejar, organizar e dirigir às atividades de gestão de recursos de tecnologia da informação, inclusive a realização de projetos, a gestão de sistemas, as redes e os equipamentos e o suporte ao usuário;
- Normatizar os procedimentos para produtos e serviços de tecnologia da informação;
- Identificar a necessidade de contratação de equipamentos, sistemas e serviços de tecnologia da informação, bem como fiscalizar a execução dos contratos resultantes.

A LEI Nº 9.316, DE 29 DE DEZEMBRO DE 2010, estabelece as atribuições das gerências que fazem parte da DITEC.

A gerência de sistemas (GESIS) tem objetivo de planejar, desenvolver, homologar, manter e administrar ferramentas, linguagens de desenvolvimento, sistemas e aplicativos, e manter a respectiva documentação, além de realizar a manutenção do sítio na intranet e na internet.

A gerência de suporte (GESUP) é responsável pela administração e gerenciamento da infraestrutura de TI de todo o TJPB, além de prover a segurança de todos os sistemas que estão disponíveis para os funcionários e dos que estão disponíveis para a população. Outras atribuições referem-se à instalação de ferramentas e serviços necessários para novas tecnologias a

serem implantadas pela DITEC, atribuições mais específicas estão relacionadas aos controles de acesso a rede do TJPB, do servidor de arquivos e dos backups destes, do acesso dos funcionários de TI ao banco de dados do TJPB, do acesso dos funcionários de TI ao banco de dados do TJPB.

A gerência de atendimento (GEATE) de como objetivo receber sugestões, reclamações ou solicitações de suporte de tecnologia da informação, além de controlar, acompanhar e requisitar da unidade responsável informações sobre averiguações e providências tomadas no que se refere a demandas registradas.

E por fim, a gerência de desenvolvimento de tecnologia da informação (GEDES) esta, tem a responsabilidade de propor às políticas, as diretrizes, as normas e os procedimentos que disciplinem a utilização de recursos de tecnologia de informação, além de identificar as necessidades de tecnologia da informação junto aos usuários, também escopo da mesma realizar estudos de viabilidade, análise de projetos, bem como acompanhar a sua implementação e manutenção e por fim, prospectar novas tecnologias de desenvolvimento de sistemas processuais para o Poder Judiciário do Estado, e definir seus artefatos, produtos e requisitos mínimos.

Atualmente, o TJPB conta com cerca de 4.100 funcionários, distribuídos em cargos comissionados, efetivos e requisitados de outros órgãos.

Quadro 2 – Parâmetros mínimos recomendados para a força de trabalho em TIC

FORÇA DE TRABALHO TOTAL MÍNIMA RECOMENDADA PARA TIC		
Total de Usuários de recursos de TIC	% mínimo da força de trabalho de TIC (efetivos, comissionados e terceirizados)	Mínimo necessário de profissionais do quadro permanente
Até 500	7,00%	15
Entre 501 e 1.500	5,00%	35
Entre 1.501 e 3.000	4,00%	75
Entre 3.001 e 5.000	3,00%	120
Entre 5.001 e 10.000	2,00%	150
Acima de 10.000	1,00%	200

Fonte: Resolução 90, de 29 de setembro de 2009.

Como mostrado na figura anterior, o quantitativo de usuários enquadra-se no intervalo na qual são necessários pelo menos 3% de funcionários no setor de TI; atualmente o TJPB possui cerca de 100 funcionários alocados na função de TIC, o que indica que sua força de trabalho está aquém do mínimo recomendado pela mencionada resolução.

4.1.2 Implantação de Política de Segurança da Informação no TJPB.

O planejamento estratégico da organização é uma ferramenta de trabalho que facilita as organizações a trabalhar com situações de mudanças, constituindo-se em um instrumento de gestão. Sendo assim, o Plano Estratégico de Tecnologia da Informação (PDTI) tem o objetivo de planejar a utilização das informações em conjunto com os recursos de TI.

O PDTI do TJPB, para o período 2011-2014, foi desenvolvido em fevereiro de 2011 com auxílio de vários servidores, gestores e contratados da DITEC, e procurou estar em conformidade com as resoluções 90 e 99 do CNJ, que dispõem sobre os requisitos de nivelamento de TIC e instituiu o planejamento estratégico no âmbito do poder judiciário, respectivamente.

Seguindo o que foi designado nesse PDTI para a elaboração da PSI do TJPB, ficou responsável a DITEC, especificamente na gerência de suporte (GESUP), neste setor foi designado um servidor, do quadro efetivo, para fazer os levantamentos necessários em relação ao que deve compor uma PSI segundo as melhores práticas adotadas: leis, decretos, normas e resoluções, assim como as necessidades próprias do TJPB.

A PSI do TJPB deveria ser composta de um conjunto de regras e padrões que visassem principalmente assegurar que as informações e serviços importantes para a instituição recebam proteção, de forma a garantir a confidencialidade, integridade e disponibilidade das informações.

A PSI do TJPB, em fase de implantação propõe a criação de um comitê de segurança da informação (CSI) composto por:

I – um Desembargador;

II – um juiz auxiliar da Presidência;

III – um juiz da Corregedoria Geral de Justiça;

IV – Diretor de Tecnologia da Informação;

V – Gestor de Segurança da Informação;

VI – Diretor Administrativo;

VII – Diretor de Economia e Finanças;

VIII – Diretor de Gestão de Pessoas;

IX – um representante do Comitê de Magistrados para Tecnologia da Informação (CMTI);

X – um integrante da Diretoria de Processo Administrativo;

XII – Gerente de Suporte de Tecnologia de Informação

XIII – Diretor de Segurança Institucional

Além desses, mais três servidores da DITEC, com conhecimento em segurança da informação devem auxiliar a esse comitê.

O próximo item apresentará os resultados desta pesquisa, que, para enriquecimento de análise, contou com a comparação com outras duas políticas de tribunais encontradas na internet: são elas as políticas de TIC do Tribunal de Justiça de Mato Grosso (TJMT) e do Tribunal de Justiça de São Paulo (TJSP).

4.2 Grau de alinhamento

Para se conhecer o nível de alinhamento entre a PSI do TJPB com a ISO 27002 (ABNT, 2005) foi desenvolvido, como mencionado na metodologia, um quadro com todos os fatores apresentados no normativo da ABNT, onde foi possível verificar se determinado fator ou prática estava sendo consolidada na PSI do TJPB, que sabemos está em fase final de implementação.

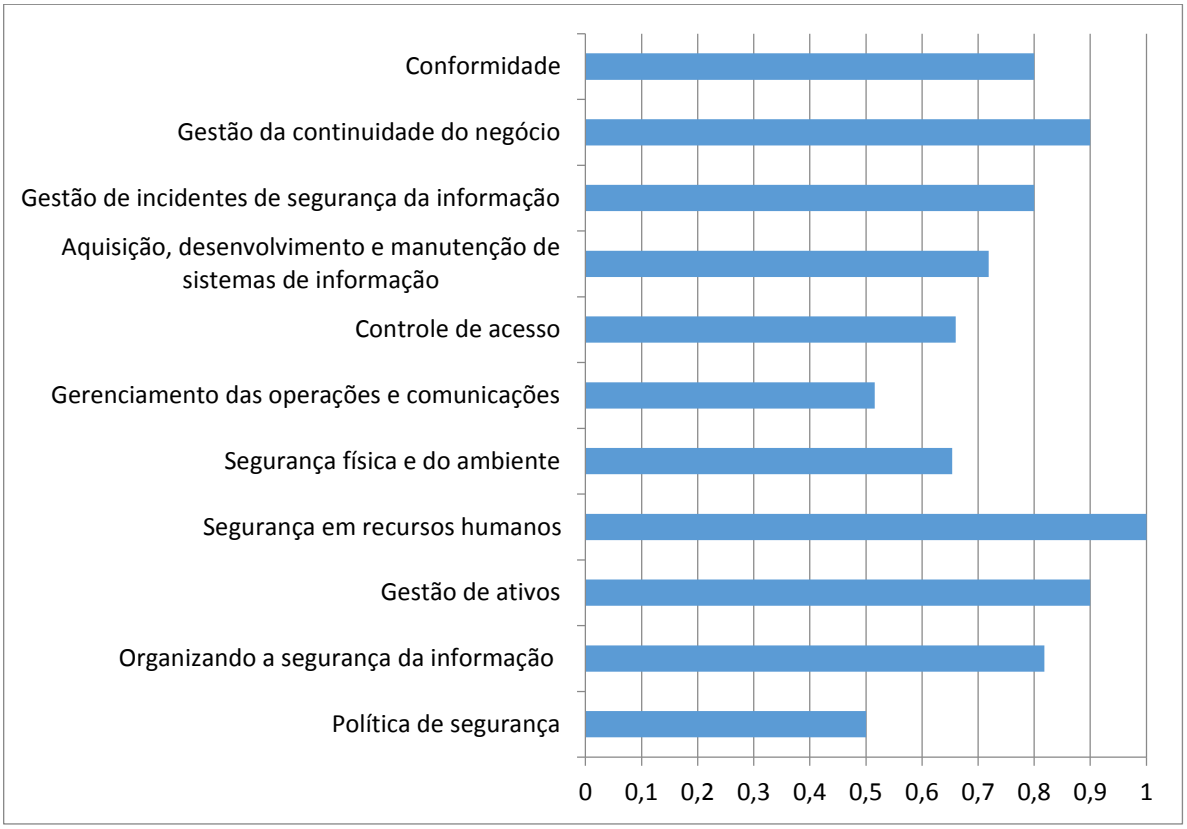

Gráfico 1 - Grau de alinhamento com as dimensões de segurança apresentadas pela ISO 27002 (1 = 100%)

Analisando o gráfico a cima notou-se o que a maioria dos itens apresentados estão com mais de 70% de alinhamento com a norma, isso mostra que após as próximas revisões, caso for aplicado novamente esse tipo de análise, e desde que o TJPB se oriente pelos parâmetros da NBR ISO 27002 ,o alinhamento tende à sua totalidade.

A conformidade, a gestão da continuidade do negócio, a gestão de incidentes de segurança da informação, a gestão de ativos, a organização da segurança da informação, são os itens que estão com alinhamentos mais próximos entre si, os mesmos atingiram uma pontuação considerável, mostrando que há preocupação em manter protegidos os ativos de acordo com as leis, normas, resoluções vigente.

O fator humano no TJPB é um ponto que está sendo levado em consideração com bastante ênfase, ou seja, o mesmo está seguindo totalmente o que a NBR ISO 27002 sugere, pois é sabido que esse fator tende a ser vulnerável quando se pensa em segurança da informação.

Quanto aos itens política de segurança de informação, infraestrutura, gerenciamento de partes externas, a responsabilidade pelos ativos, classificação da informação, controle de áreas seguras e a segurança de equipamentos temos os seguintes resultados apresentados no gráfico a seguir.

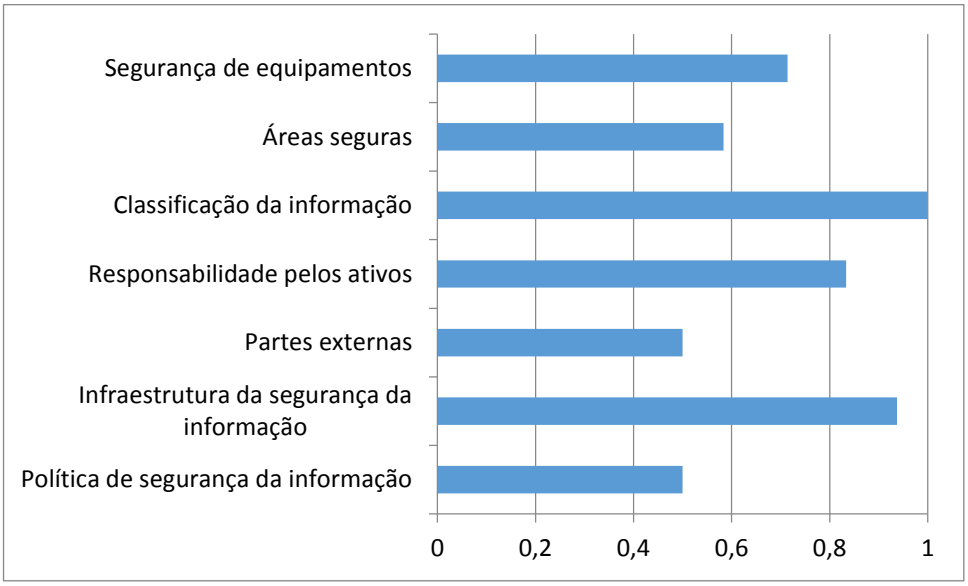

Gráfico 2 - Macro fatores: Segurança física, infraestrutura e política.

(1 = 100%)

Os itens que apresentam maior disparidade entre si, itens que obtiveram boa pontuação e itens que com pontuação baixa. A PSI do TJPB merece maior atenção por se tratar do do-

cumento crucial para a segurança, sendo que a mesma ainda não está aprovada, esse foi o fator negativo nesse tópico.

No entanto a classificação e a infraestrutura da segurança da informação revelaram-se por terem pontuação expressiva, isso mostra que o TJPB se preocupa em estabelecer grau de sigilo das informações, assim como manter meios de protegê-la.

Continuando a análise, o gráfico a seguir, nos mostra informações a cerca da segurança operacional e de comunicações.

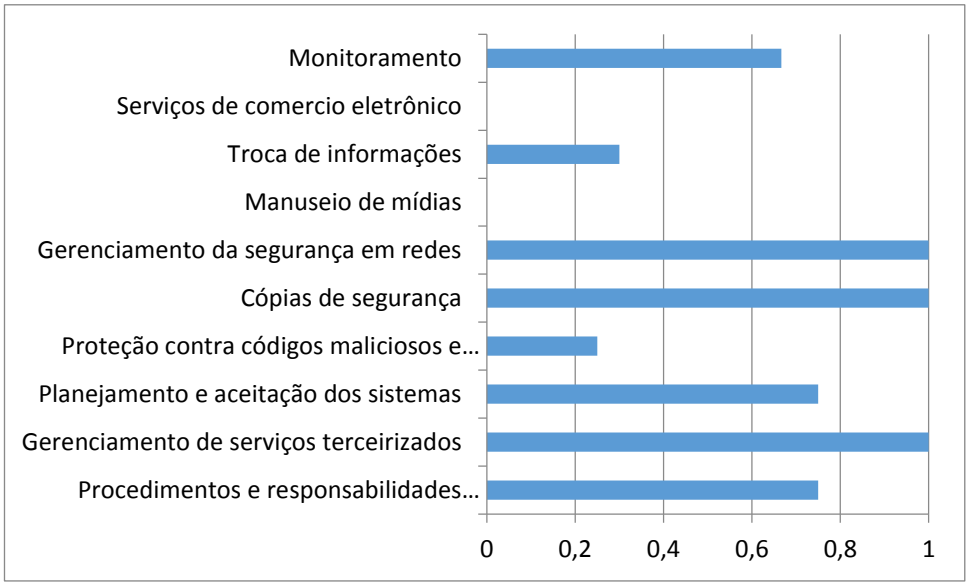

Gráfico 3 - Macro fatores: Segurança operacional e de comunicações.

(1 = 100%)

Neste gráfico em especial, pode ser visto dois itens que não tiveram pontuação, três com computação considerável e três com pontuação máxima. Um possível problema identifica-se nos itens com baixa pontuação, proteção contra códigos maliciosos e trocas de informação, além do manuseio de mídias. A proteção contra códigos maliciosos é fundamental para a segurança informacional, seja através de firewalls eficazes, e outras salvaguardas, portanto, longe de aspectos operacionais, a política deveria indicar a importância e atualidade de salvaguardas para o fim desejado.

A troca de informações é outro fator de segurança indiscutível ao considerarmos que tribunais trocam ou devem trocar informações sobre processos, ou acessar outros sistemas para obter a informação necessária - nesse ponto é importante para orientar ou inspirar salvaguardas adequadas.

O manuseio de mídias, por não estar presente na PSI do TJPB é outro item de interesse na segurança da informação, pois a cada dia novas mídias são desenvolvidas e essa PSI deveria orientar a limitação de uso de tais complementos. A NBR ISO 27002 recomenda que a política de segurança, no caso a PSI do TJPB, estabeleça e mantenha o gerenciamento de mídias removíveis, do descarte de mídias, dos procedimentos para tratamento de informações, assim como garantir a segurança da documentação dos sistemas, definindo claramente esses controles, além de aumentar o alinhamento com a norma, mostra um maior interesse do TJPB em preservar a segurança das informações contra divulgação não autorizadas, modificação entre outros problemas.

Finalmente, o item serviços de comércio eletrônico não se aplica ao TJPB, por esse motivo o mesmo não teve pontuação; porém, a política deveria abranger a questão do governo eletrônico e a acessibilidade para os cidadãos, pois a cada dia novos serviços são incorporados e disponibilizados na internet, agilizando o sistema e satisfazendo novas necessidades dos usuários. .

Ressalta-se, no gráfico, que as pontuações máximas foram atingidas pelos itens mais sensíveis desta dimensão, isso mostra que há esforços consideráveis nas maiorias dos itens.

O próximo Gráfico 4 nos mostra fatores importantes com pontuações máximas: Controle de acesso à aplicação e à informação, Gerenciamento de acesso do usuário e Requisitos de negócio para controle de acesso.

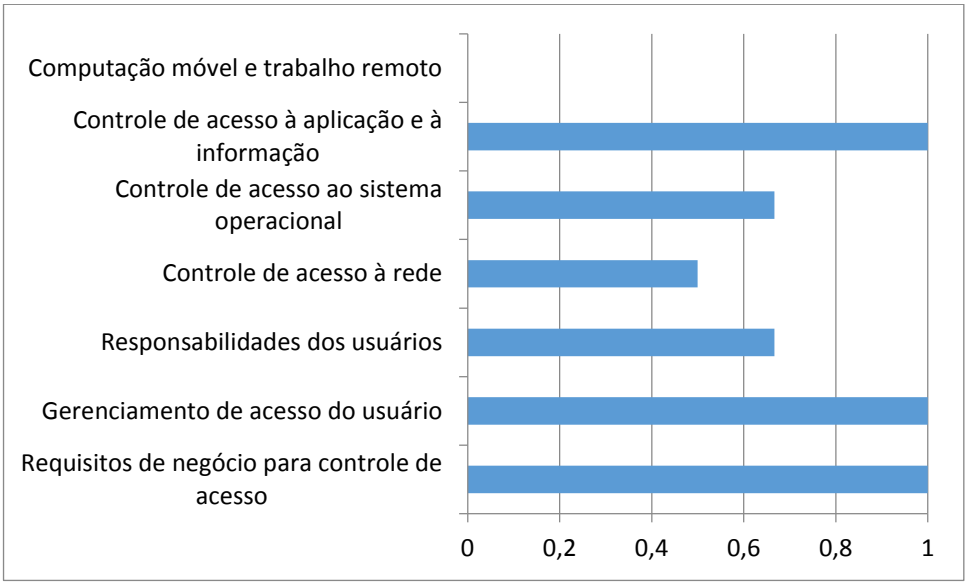

Gráfico 4 - Macro fatores: Controle de acesso

(1 = 100%)

Três itens do gráfico acima que merecem maior atenção, tanto por sua importância para o TJPB como pelo fato de ter obtido pontuação razoável; em complemento, tratam dos meios com que os sistemas e rede são acessados, e os deveres dos usuários, são eles: Controle de acesso à rede, controle de acesso à rede e responsabilidades dos usuários. Nota-se que a PSI em análise é omissa em alguns fatores e, portanto deverá ser revista e desenvolvida, para melhor se parametrizar à NBR ISO 27002.

De outra forma, a computação móvel e trabalho remoto não estão mencionados, o que indica que não está havendo um acompanhamento das tendências no trabalho, como o Home Office e as audiências remotas através de sistemas de vídeo-comunicação específicos para a área jurídica tão comum em países desenvolvidos. Além do mais, é preciso estabelecer e diferenciar o trabalho remoto citado acima que remete a prestação do serviço ao público, do trabalho remoto de suporte aos usuários do próprio tribunal, que apesar de ser utilizada não está presente na PSI. O TJPB deveria incluir essas possibilidades em sua PSI de forma a orientar a segurança e o estudo de alternativas às tendências mencionadas.

Por fim, o Gráfico 5 apresenta os resultados quanto à análise das orientações de salvaguardas que necessitam de maior reflexão e alinhamento às recomendações da NBR ISO 27002.

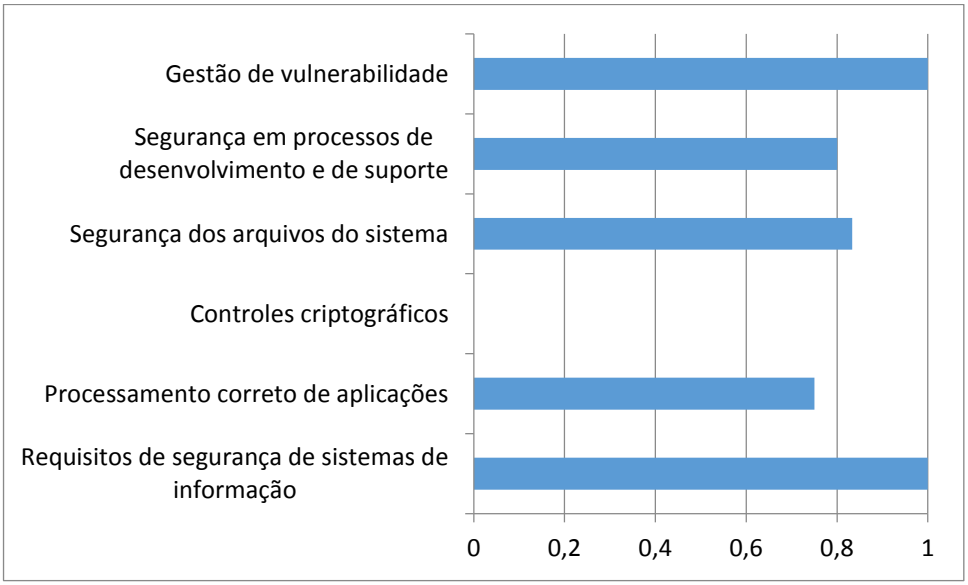

Gráfico 5 - Macro fatores: Aquisição, desenvolvimento e manutenção de sistemas.

(1 = 100%)

O gráfico denuncia que não foram identificados controles criptográficos definidos na PSI; esse é um ponto fundamental para preservação dos princípios de segurança. Porém o que

chama a atenção neste item é que, por conhecimento *in loco* do autor, o acesso a determinados sistemas se dá por meio de certificado digital.

É de se supor que, provavelmente, não houve uma interação entre o departamento que desenvolve os sistemas com o que está produzindo a PSI do TJPB; ou por essa tecnologia de segurança estar sendo introduzida atualmente no órgão, e a PSI do tribunal possuir certo tempo de desenvolvimento e não considerou a certificação digital, que é uma forma de criptografia.

A existência da criptografia é tão importante que alguns sistemas só permitem acesso através do certificado digital, meio que garante a autenticidade de quem acessa esses sistemas. A não inclusão desse tópico poderá ser corrigida, assim que a mesma for aprovada e tiver sua primeira revisão.

O Gráfico 6 apresenta resultados importantes para a melhoria contínua propagada pelo PDCA e que fundamenta a NBR ISO 27002: a existência de processos de auditorias, outro ponto essencial em uma PSI. Embora se apresente com mais de 70% alinhada, a PSI do TJPB deveria ser mais robusta, pois é o elemento de controle fundamental e garantidor da melhoria contínua da segurança informacional no tribunal.

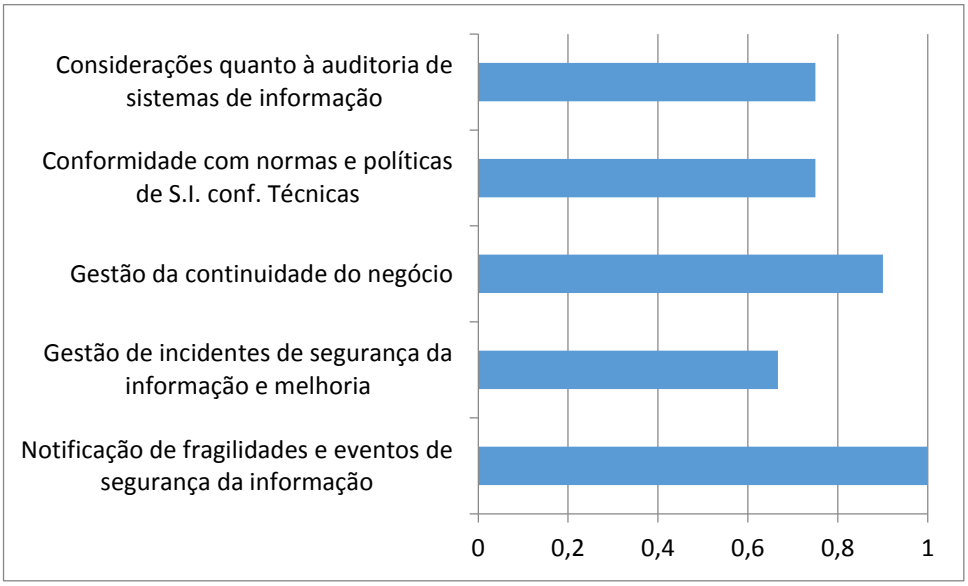

Gráfico 6 - Macro fatores: Conformidade, auditoria, continuidade e incidentes.
(1 = 100%)

Nota-se no Gráfico 6 que fatores como conformidade, gestão da continuidade do negócio e gestão de incidentes da segurança da informação estão parcialmente alinhados. Como não há, dentre todas as dimensões de segurança presentes na NBR ISO 27002 indicação de

qual é mais importante ou não, pois todos fazem parte da corrente de proteção aos sistemas informacionais do tribunal, verifica-se que a gestão de continuidade está bastante presente, mas a gestão de incidentes de segurança e melhoria não, o que faz pensar que o acerto nos macro fatores comparados relacionados à aquisição, desenvolvimento e manutenção de sistemas vistos no Gráfico 5 poderia melhorar esse fator de avaliação.

Ressalta o grau de alinhamento do fator relacionado à notificação de fragilidades que é perfeitamente justificável por se tratar de órgão público onde esse tipo de comunicação deve ser tratado com acuidade, haja vista as recomendações legais existentes e que impactarão individualmente e na equipe responsável pela segurança.

Finalmente, a conformidade com normas e políticas e conformidades técnicas indica que essas deveriam estar alinhadas para melhor eficácia. fazendo com que seja possível identificar o interesse em manter a PSI alinhada, revisada e que a mesma garanta a continuidade dos serviços do TJPB.

Os gráficos apresentados demonstram quais tópicos merecem maior atenção assim como quais estão de acordo com a norma.

Sendo que, além dos pontos relatados anteriormente, vale salientar que os pontos: Conformidade, Gestão da continuidade do negócio, Gestão de incidentes de segurança da informação, Gestão de ativos e organização da segurança da informação, são pontos que apesar de não estarem completamente de acordo com a norma, são bastante importantes para a organização, sendo assim eles devem ser melhorados um pouco mais, para estar realmente aderente a norma.

Porém há também fatores que precisam urgente de uma maior atenção, ou seja, pontos obtiveram uma pontuação relativamente baixa, são eles: Controle de acesso, segurança física e do ambiente, gerenciamento de operações e comunicações e política de segurança da informação. Eles estão em ordem decrescente de pontuação, o item PSI obteve este resultado, pois a mesma ainda está em fase de aprovação pela presidência do TJPB sendo esse o ponto crucial para se ter uma PSI adequada já que é necessário a aprovação da alta direção e nesse caso é o que falta para o TJPB afirmar que o mesmo dispõe de tal documento.

Outro ponto que merece atenção é acerca da segurança física do ambiente, já que esse merece, também, mais atenção por se tratar da forma como é obtido o acesso aos setores do tribunal, apesar do mesmo manter um certo nível de controle quanto a isso, vale salientar que por se tratar de repartição pública é fato que qualquer pessoa que necessite dos serviços do órgão terá acesso a todos os andares do prédio., sem dúvidas esse é a maior dificuldade em se

garantir controle total do trânsito de pessoas, no entanto há um maior controle em lugares críticos, como sala dos servidores, acesso a *switches* entre outros.

No parágrafo anterior discorreu a cerca da segurança física e do ambiente, outro ponto importante é o controle lógico de acesso à informação, apesar de o TJPB manter controle de acesso a maioria de seus sistemas, pois existe terminais de consulta onde qual quer pessoa pode acessar, Além do mais, nos principais prédios que fazem parte do judiciário paraibano existe ponto de acesso público a rede *wifi* do tribunal que pode identificado alguma vulnerabilidade e causar grandes danos a segurança do mesmo.

4.3 Pontos positivos e negativos

É fato que a criação de uma PSI totalmente aderente a norma ISO 27002 não é tarefa fácil por uma série de fatores; com a PSI do TJPB não é diferente. As análise dos gráficos que foram feitas anteriormente mostram isso: existem itens aderente à norma e outros não. A Tabela 2 apresenta alguns pontos positivos e negativos identificados.

Tabela 1- Resumo comparativo da política do TJPB com as dimensões relacionadas na ISO27002

PONTOS POSITIVOS	PONTOS NEGATIVOS
Na dimensão "Recursos Humanos" a política se mostra totalmente alinhada aos preceitos da ISO 27002.	Na dimensão relacionada à aquisição, desenvolvimento e manutenção de sistemas, a política não prevê controles criptográficos.
Na dimensão "Gestão da continuidade do negócio" a mesma visa manter seguro copias de segurança, acesso a redes.	A dimensão "segurança física e do ambiente" áreas segura é fácil ter acesso aos setores.
A dimensão "Gestão de ativos" se propõe manter a proteção adequada dos ativos da organização	Na dimensão "gerenciamento das operações e comunicação" não há controle no manuseio das mídias.
Na dimensão "Conformidade" aderente a leis, resoluções e etc.	A "Política de segurança da informação" ainda não obteve aprovação da presidência.

A dimensão "Organizando a Segurança da informação" garante a atribuição de responsabilidades adequadamente.	Na dimensão "Controle de acesso" não há menção a cerca do item computação móvel

4.4 Comparação entre PSIs de três tribunais de justiça

Para entender o acerto (ou não) do que foi observado na PSI do TJPB, foi realizada comparação (*benchmarking*) dessa PSI do TJPB com as PSIs do TJMT e TJSP, procurando saber qual estaria em melhor grau de nivelamento com os parâmetros da norma. O que se obteve está apresentado nos Gráficos 7e 8 abaixo:

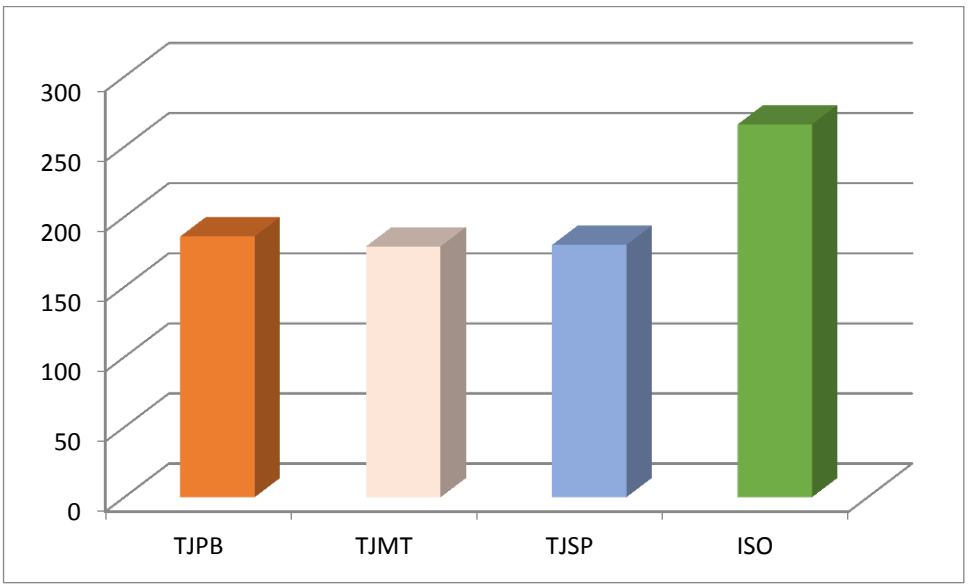

Gráfico 7 - Comparação do alinhamento com a ISO27002, por pontuação obtida.

Neste gráfico é possível analisar individualmente cada PSI, em termos de medidas absolutas, e compará-la com norma ISO 27002, assim como foi no tópico anterior. Nota-se que , ou seja, uma comparação em conjunto. A comparação feita entre as PSI do TJMT, TJSP e TJPB mostra que os mesmos estão seguindo o mesmo alinhamento, a pontuação dos mesmos são: TJPB=186=70% TJMT=179=67%, TJSP=180=68%. Porém a norma ISO 27002 totaliza 266 pontos, segundo as medidas utilizadas para a comparação descritas na metodologia.

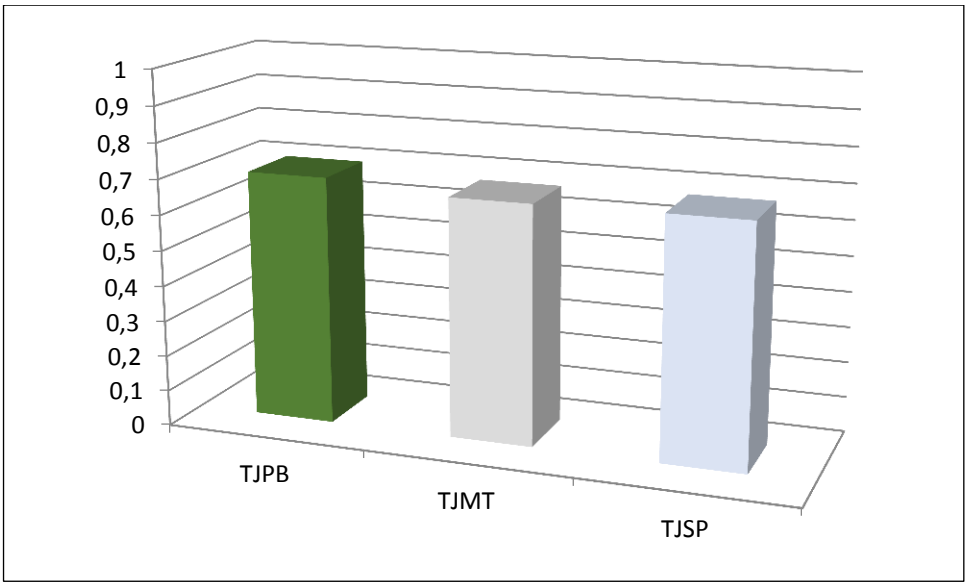

Gráfico 8 - Comparação do alinhamento das PSIs de diferentes tribunais de justiça (1 = 100%)

A partir da análise nas PSI's dos tribunais de MT, SP e PB e apresentação dos resultados no gráfico a cima, nota-se que os mesmos estão praticamente igualados nos total dos quesitos, mas ainda faltam em torno de 30% para se adaptarem ao padrão NBR ISO 27002.

Os resultados da comparação realizada nos macro-fatores presentes na NBR ISO 27002 entre as PSI dos tribunais informam que não estão totalmente: aderentes aos parâmetros orientadores de segurança: a troca de informações, o manuseio de mídias, os serviços de comercio eletrônico (ou sua adaptação: governo eletrônico), a computação móvel e trabalho remoto e os controles criptográficos.

A partir das análises realizadas é possível responder as questões que orientaram este trabalho:

Será que existem divergências entre a PSI do TJPB com a principal referencia do assunto: a NBR-ISO_27002? Qual seria o nível de alinhamento observado – Alto, Médio ou Baixo?

Como resposta à primeira chega-se à conclusão de que, ou seja, apesar de não estar totalmente em conformidade com NBR ISO 27002 não foram identificados pontos que a contrapõe.

Respondendo à segunda pergunta pode se afirmar, com base na categorização de alinhamento através de fatores presentes na NBR ISO 27002 caracterizados na metodologia apresentada (Médio = 90 e 179) e o resultado obtido para o TJPB (186), que sua PSI encontra-se altamente alinhada com a norma, embora com recomendações de melhoria principalmente nos quesitos de criptografia, tratamento de mídias, dentre outros.

Por fim, mas não tendo sido objetivo deste trabalho, a comparação das PSIs entre tribunais apontou similaridades nas pontuações obtidas com relação à NBR ISO 27002, sendo que o TJPB apresenta pequena margem comparativa favorável ao alinhamento. Não foi realizada a comparação entre macro-fatores de segurança informacional por fugir ao escopo deste trabalho.

4.5 Conclusão do capítulo

Neste capítulo foi possível conhecer melhor a estrutura do TJPB, sua missão, visão e principais informações. Além disso, a PSI foi analisada cuidadosamente com intuito de verificar a aderência da mesma com a NBR ISO 27002, seus resultados e gráficos explicativos, além disso, foi criada uma tabela com pontos positivos e pontos negativos percebidos na análise. Também foi realizada comparação, em termos absolutos e relativos, dos resultados de avaliação realizada junto às PSIs dos TJSP e TJMT.

No capítulo seguinte serão apresentadas as considerações finais e lições aprendidas, limitações e recomendações para trabalhos futuros.

5 CONSIDERAÇÕES FINAIS

Este trabalho apresentou os principais conceitos acerca de segurança da informação que podem ser aplicados em qualquer tipo de organização, seja ela publica ou privada. Essas definições, conceitos e práticas remetem à importância em se ter uma política de segurança da informação, além de mostrar a necessidade em se adotar referências mundialmente reconhecidas e aceitas nas principais instituições.

Os objetivos que nortearam este trabalho foram atingidos, pois a partir do levantamento bibliográfico feito, a exposição da importância do tema política de segurança da informação, a necessidade de alinhamento com as boas práticas internacionais presentes na NBR ISO 27002, a criação de planilha de fatores de análise para aplicar na PSI do TJPB, posteriormente em mais dois tribunais, chegou-se ao resultado de que a PSI objeto deste trabalho encontra-se altamente alinhada aos preceitos daquela norma internacional.

Da mesma forma, a criação de uma tabela com fatores positivos e negativos encontrados foi importante para o entendimento da PSI do TJPB. Os pontos negativos presentes, dentre outros, a falta de implementação de uma política de backup, definir claramente quais são as punições para possíveis violações, a criação de um portfólio dos problemas encontrados e solucionados referente à manutenção dos equipamentos, merecem tratamento. De outra forma, os fatores positivos relacionados com a preocupação se utilizar e-mail institucional, gerenciar o uso de redes sociais, estabelecer os deveres e responsabilidades dos usuários e gestores de TIC merecem destaque.

O presente trabalho teve caráter exploratório, descritivo de um caso apenas, e decorrente apenas do olhar do pesquisador, portanto sujeito a erros do pesquisador. Outra limitação do trabalho diz respeito ao acesso a informações que pudessem melhor explicar as diferentes pontuações obtidas, uma vez que a presente pesquisa foi realizada durante o estágio concedido naquele TJPB.

A metodologia também apresenta limitações por sua natureza, mas poderá ser replicada para abranger outros tribunais de forma a desenvolver um trabalho com ênfase estatística com intuito a entender o atual estágio de maturidade no desenvolvimento dessas políticas, podendo até traçar um panorama do nível de alinhamento do judiciário brasileiro em relação à NBR ISO 27002. Melhorias na metodologia aplicada são possíveis e bem-vindas.

Quanto à contribuição curricular do curso de Sistemas de Informação da UFPB Campus IV, o autor considera que as disciplinas ministradas foram de fundamental importância para a

elaboração deste trabalho, e seus professores capacitados e motivadores. As disciplinas que foram fundamentais para a elaboração desta pesquisa foram: Auditoria e segurança de sistemas, Gestão da qualidade, Gestão da informação, Gerência de redes, dentre outras.

6 Bibliografia

ABNT. (2005). *iso/iec 27002 - Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da Informação.* Rio de Janeiro: ABNT.

ABNT. (2006). *Perguntas Frequentes*. (Associação Brasileira de Normas Técnicas) Acesso em 08 de 10 de 2014, disponível em http://www.abnt.org.br/m2.asp?cod_pagina=963#

ABNT NBR ISO/IEC-27001. (2006). *Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos.* Rio de Janeiro: ABNT.

ALMEIDA, E. (16 de Outubro de 2013). *Sistema de Gestão de Segurança da Informação*. Acesso em 23 de Fevereiro de 2015, disponível em tiespecialistas: http://www.tiespecialistas.com.br/2013/10/sistema-gestao-seguranca-informacao-sgsi-i/

ARAÚJO, W. J. (2012). Leis, Decretos e Normas sobre Gestão da Segurança. *Inf. & Soc: Est, 22*, 13-24. Acesso em 26 de 11 de 2014, disponível em http://www.ies.ufpb.br/ojs/index.php/ies/article/viewFile/13675/8206

BEAL, A. (2004). *Gestão estratégica da informação : como transformar a informação e a tecnologia da informação em fatores de crescimento e de alto desempenho a tecnologia da informação em fatores de crescimento e de alto desempenho nas organizações.* São Paulo: Atlas.

BEAL, A. (2005). *Segurança da Informação: Princípios e melhores práticas para a proteção dos ativos de informação nas organizações.* São Paulo: Atlas.

BETHLEM, A. (JAN/MAR de 1981). Os conceitos de política estratégica. *Revista de Administração de Empresas, vol.21*, p.7-15.

Brasil. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. (2010). *Livro verde : segurança cibernética no Brasil / Gabinete de Segurança Institucional, Departamento de Segurança da Informação e Comunicações; organização Claudia Canongia e Raphael Mandarino Junior.* Brasília.

Brazil IT Snapshot. (2014). *promonlogicalis.* Acesso em 26 de 02 de 2015, disponível em http://www.br.promonlogicalis.com/globalassets/latin-america/advisors/pt/snapshot-2014.pdf

CAMPI, M. (10 de Dezembro de 2013). *Falha em app do Banco do Brasil expõe dados de correntistas*. Fonte: de INFO Online: http://info.abril.com.br/noticias/seguranca/2013/12/falha-em-app-do-banco-do-brasil-expoe-dados-de-correntistas.shtml

CAMPOS, A. (2007). *Sistemas de segurança da Informação: Controlando Riscos.* Florianópolis: Visual Books Ltda.

CARUSO, C. A., & STEFFEN, F. D. (2006). *Segurança em informática e de Informações.* São Paulo: Senac.

CEPIK, M. A. (2003). *Espionagem e democracia: agilidade e transparencia como dilemas na institucionalização de seviços de inteligência.* Rio de Janeiro: FGV. Acesso em 16 de 08 de 2014, disponível em http://books.google.com.br/books?id=xERuDA-Ra8wC&printsec=frontcover&dq=isbn:8522504377&hl=pt-BR&sa=X&ei=mKvvU9LcIsPesASMv4HgBw&ved=0CB0Q6AEwAA#v=onepage&q&f=false

CNJ. (Outubro de 2010). Segurança da Informação-Apresentação das diretrizes da Gestão de Segurança da informação. Brasília, Distrito Federal, Brasil.

CNJ. (Junho de 2012). *Diretrizes para a gestão de segurança da informação no âmbito do poder judiciário.* Acesso em 14 de 10 de 2014, disponível em http://www.cnj.jus.br/images/dti/Comite_Gestao_TIC/Diretrizes_Gestao_SI_PJ.pdf

FERREIRA, F. N. (2003). *Segurança da Informação.* Rio de Janeiro: Ciencia Moderna LTDA.

FONTES, E. (2012). *Políticas e normas para segurança da informação.* Rio de Janeiro: Brasport.

FRASER, B. Y. (09 de 1997). *RFC-2196 Site Security Handbook*. (SEI/CMU, Editor, & ITEF) Acesso em 15 de 09 de 2014, disponível em http://www.rfc-editor.org/rfc/rfc2196.txt

FREITAS, F., & ARAUJO, M. (2008). *POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO: Guia pratico para a elaboração e implementação.* (2 ed.). Rio de Janeiro: Ciência Moderna LTDA.

FURTADO, E. d. (2011). *ABNT NBR ISO/IEC 27002:2005: um norte para a gestão de segurança da informação na Organização: Auditoria de sistemas e de segurança.* Brasília: Monografia (especialização) – Universidade de Brasília. Instituto de Ciências Exatas. Departamento de Ciência da Computação.

GANDRA, A. (07 de 10 de 2013). *Secretário do Ministério de Minas e Energia diz que espionagem não afetará leilões*. Acesso em 10 de 08 de 2014, disponível em Da Agência Brasil, no Rio: http://noticias.uol.com.br/politica/ultimas-noticias/2013/10/07/secretario-do-ministerio-de-minas-e-energia-diz-que-espionagem-nao-afetara-leiloes.htm

GROSSMANN, L. O. (30 de 10 de 2013). *Espionagem dos EUA no Brasil deixa governo Dilma atordoado*. Acesso em 14 de 02 de 2014, disponível em convergenciadigital: http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=34222

HOUAISS, A. (2009). *Dicionário Houaiss eletronico* (Versão Monousuário 3.0 ed.). Rio de Janeiro: Objetiva.

InfoSec Council. (s.d.). *Formação de cultura em segurança da informação.* Acesso em 05 de 01 de 2015, disponível em Computer World: http://computerworld.com.br/estaticas/downloads/catalogo_parte1.pdf

INSTRUÇÃO NORMATIVA GSI Nº01. (13 de 06 de 2008). *Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.* Acesso em 21 de 08 de 2014, disponível em http://dsic.planalto.gov.br/documentos/in_01_gsidsic.pdf

LAUREANO, M. A. (s.d.). *Gestão da segurança da informção.* Acesso em 14 de 08 de 2014, disponível em www.mlaureano.org/: http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf

LAUREANO, M. A., & MORAES, P. E. (2005). Segurança como Estratégia de Gestão da Informação. *Segurança como Estratégia de Gestão da Informação*, 38-44. Acesso em 05 de 08 de 2014, disponível em http://www.mlaureano.org/projects/seguranca/economia_tecnologia_seguranca.pdf

LYRA, M. R. (2008). *Segurança e Auditoria em Sistemas de Informação.* Rio de Janeiro: Ciência Moderna Ltda.

MARCONI, M. A., & LAKATOS, E. M. (2003). *Fundamentos de metodologia científica* (5ª ed.). São Paulo: Atlas.

MARCONI, M., & LAKATOS, E. M. (2003). *Fundamentos de metodologia científica* (5ª ed.). São Paulo: Atlas.

Módulo. (19 de Novembro de 2007). *10ª Pesquisa Nacional sobre Segurança da Informação* . Acesso em 20 de 11 de 2014, disponível em www.modulo.com.br: http://www.modulo.com.br/media/10a_pesquisa_nacional.pdf

MONTEIRO, I. L. (23 de 06 de 2009). *Proposta de um guia para elaboração de políticas de segurança da informação e comunicações em órgãos da administração publica federal.* Acesso em 15 de 08 de 2014, disponível em http://dsic.planalto.gov.br/documentos/cegsic/monografias_1_turma/ina_lucia.pdf

MORAES, M. (04 de Outubro de 2013). *Espionagem abre discussão sobre preparo do Brasil para uma guerra cibernética.* Fonte: BBC Brasil em São Paulo: http://www.bbc.co.uk/portuguese/noticias/2013/10/131011_defesa_seguranca_cibernetica_brasil_mm.shtml

NAKAMURA, E. T., & GEUS, P. L. (2007). *Segurança de Redes em Ambientes.* São Paulo: Novatec Editora.

Network Working Group. (Setembro de 1997). *RFC-2196.* Acesso em 25 de 09 de 2014, disponível em https://www.ietf.org/rfc/rfc2196.txt

PONTES, M. V. (2014). *Política de segurança da informação: uma contribuição para o Campus IV.* Rio Tinto.

PWC. (2014). *Pesquisa Global de Segurança da Informação 2014*. (Price Waterhouse Cooper Serviços Profissionais Ltda.) Acesso em 14 de 10 de 2014, disponível em http://www.pwc.com.br/pt/publicacoes/servicos/consultoria-negocios/pesquisa-global-seguranca-informacao-14.jhtml

RESS, W. (09 de 2011). *Começando em segurança*. Acesso em 09 de 02 de 2015, disponível em https://msdn.microsoft.com/pt-br/library/ff716605.aspx#naorepudio

REZENDE, D. A., & Abreu, A. F. (2000). *Tecnologia da Informação Aplicada a Sistemas de Informação Empresariais.* São Paulo: Editora Atlas.

RODRIGUES, L. (09 de Setembro de 2013). *Site do Tribunal de Justiça do RJ está fora do ar*. Fonte: cbn.globoradio.globo.com: http://cbn.globoradio.globo.com/rio-de-janeiro/2013/09/09/SITE-DO-TRIBUNAL-DE-JUSTICA-DO-RJ-ESTA-FORA-DO-AR.htm

SEMOLA, M. (2003). *Gestão da Segurança da Informação uma visão executiva.* Rio de Janeiro: Elsevier.

SILVEIRA, D. T., & CÓRDOVA, F. P. (2009). *Métodos de Pesquisa.* (T. E. GERHARDT, & D. T. SILVEIRA, Eds.) Porto Alegre: ufrgs.

SPANCESKI, F. R. (2004). *Política de Segurança da informação – Desevolvimento de um modelo voltado para instituição de ensino.* JOINVILLE.

STAIR, R. M., & REYN0LDS, G. W. (2006). Principios de Sistemas de Informação-Uma Abordagem Gerencial. In: R. STAIR. São Paulo: Pioneira Thomson Learning.

STEINER, G. A., & MINER, J. B. (1981). *Políticas e Estratégias.* Rio de Janeiro: Editora Interciência Ltda.

STONER, J. A. (1982). *Administração.* Rio de Janeiro: Prentice Hall do Brasil Ltda.

TCU. (2012). *Boas práticas em segurança da Informação.* Tribunal De Contas da União, Brasília. Acesso em 20 de 08 de 2014, disponível em http://portal2.tcu.gov.br/portal/pls/portal/docs/2511466.PDF

TURBAN, E., R, K. J., & POTTER, R. E. (2005). *Tecnologia da Informação- Teória e Prática* (8a ed.). Rio de Janeiro: Elsevier.

UMEDA, G. M., & TRINDADE, C. C. (2004). Possíveis definições para as Políticas Empresariais: Um estudo Bibliográfico. *VII SEMEAD.*

VASCONCELLOS, M. d. (25 de janeiro de 2012). *Hackers afirmam ter tirado site do TJ-SP do ar*. Acesso em 14 de 08 de 2014, disponível em Revista Consultor Jurídico: http://www.conjur.com.br/2012-jan-25/hackers-afirmam-tirado-site-tj-sp-ar-nesta-terca-feira

7 APÊNDICES

7.1 APENDICE I – Relação de normas, diretrizes e outros documentos.

Instruções Normativas Normas, Decretos e Resoluções.	Ementa
Instrução Normativa Nº 4 - SLTI/MPOG, de 12 de novembro de 2010.	Dispõe sobre o processo de contratação de Soluções de Tecnologia da Informação pelos órgãos integrantes do Sistema de Administração dos Recursos de Informação e Informática (SISP) do Poder Executivo Federal. (Publicada no DOU Nº 218, de 16 Nov 2010- Seção 1)
Norma Complementar nº 01/IN01/DSIC/GSIPR	Disciplina a Gestão de Segurança da Informação e comunicações na Administração Pública Federal, direta e indireta, e dá outras providências. (Publicada no DOU Nº115, de 18 Jun 2008- Seção 1)
Norma Complementar nº 02/IN01/DSIC/GSIPR,	Metodologia de Gestão de Segurança da Informação e Comunicações. (Publicada no DOU Nº 199, de 14 Out 2008 - Seção 1)
Norma Complementar nº 03/IN01/DSIC/GSIPR,	Diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal. (Publicada no DOU Nº 125, de 03 Jul 2009 - Seção 1)
Norma Complementar nº 04/IN01/DSIC/GSIPR,	(Revisão 01) Diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC nos órgãos e entidades da Administração Pública Federal.(Publicada no DOU Nº 37, de 25 Fev 2013 - Seção 1)
Norma Complementar nº 05/IN01/DSIC/GSIPR,	Disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal. (Publicada no DOU Nº 156, de 17 Ago 2009 - Seção 1)
Norma Complementar nº 06/IN01/DSIC/GSIPR,	Estabelece Diretriz para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.(Publicada no DOU Nº 223, de 23 Nov 2009 - Seção 1)
Norma Complementar nº 07/IN01/DSIC/GSIPR	(Revisão 01) Estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. (Publicada no DOU Nº 134, de 16 Jul 2014 - Seção 1)
Norma Complementar nº 08/IN01/DSIC/GSIPR	Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal. (Publicada no DOU Nº 162, de 24 Ago 2010 - Seção 1)
Norma Complementar nº 09/IN01/DSIC/GSIPR	(Revisão 02) Estabelece orientações específicas para o uso de recursos criptográficos em Segurança da Informação e Comunicações, nos órgãos ou entidades da Administração Pública Federal (APF), direta e indireta. (Publicada no DOU Nº 134, de 16 Jul 2014 - Seção 1)
Norma Complementar nº 10/IN01/DSIC/GSIPR	Estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a Segurança da Informação e Comunicações (SIC), dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.(Publicada no DOU Nº 30, de 10 Fev 2012 - Seção 1)
Norma Complementar nº 11/IN01/DSIC/GSIPR	Estabelece diretrizes para avaliação de conformidade nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos ou entidades da Administração Pública Federal, direta e indireta – APF. (Publicada no DOU Nº 30, de 10 Fev 2012 - Seção 1)
Norma Complementar nº 12/IN01/DSIC/GSIPR,	Estabelece diretrizes e orientações básicas para o uso de dispositivos móveis nos aspectos referentes à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. (Publicada no DOU Nº 30, de 10 Fev 2012 - Seção 1)
Norma Complementar nº 13/IN01/DSIC/GSIPR,	Estabelece diretrizes para a Gestão de Mudanças nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal, direta e indireta (APF). (Publicada no DOU Nº 30, de 10 Fev 2012 - Seção 1)
Norma Complementar nº 14/IN01/DSIC/GSIPR	Estabelece diretrizes para a utilização de tecnologias de Computação em Nuvem, nos aspectos relacionados à Segurança da Informação e Comunicações (SIC), nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. (Publicada no DOU Nº 30, de 10 Fev 2012 - Seção 1)

Norma Complementar nº 15/IN01/DSIC/GSIPR	Estabelece diretrizes de Segurança da Informação e Comunicações para o uso de redes sociais, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. (Publicada no DOU Nº 119, de 21 Jun 2012 - Seção 1)
Norma Complementar nº 16/IN01/DSIC/GSIPR,	Estabelece as Diretrizes para o Desenvolvimento e Obtenção de Software Seguro nos Órgãos e Entidades da Administração Pública Federal, direta e indireta. (Publicada no DOU Nº 224, de 21 Nov 2012 - Seção 1)
Norma Complementar nº 17/IN01/DSIC/GSIPR	Estabelece Diretrizes nos contextos de atuação e adequações para Profissionais da Área de Segurança da Informação e Comunicações (SIC) nos Órgãos e Entidades da Administração Pública Federal (APF). (Publicada no DOU Nº 68, de 10 Abril 2013 - Seção 1)
Norma Complementar nº 18/IN01/DSIC/GSIPR	Estabelece as Diretrizes para as Atividades de Ensino em Segurança da Informação e Comunicações (SIC) nos Órgãos e Entidades da Administração Pública Federal (APF). (Publicada no DOU Nº 68, de 10 Abril 2013 - Seção 1)
Norma Complementar nº 19/IN01/DSIC/GSIPR	Estabelece Padrões Mínimos de Segurança da Informação e Comunicações para os Sistemas Estruturantes da Administração Pública Federal (APF), direta e indireta. (Publicada no DOU Nº 134, de 16 Jul 2014 - Seção 1)
Norma Complementar nº 20/IN01/DSIC/GSIPR	(Revisão 01) Estabelece as Diretrizes de Segurança da Informação e Comunicações para Instituição do Processo de Tratamento da Informação nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. (Publicada no DOU Nº 242, de 15 Dez 2014 - Seção 1)
Norma Complementar nº 21/IN01/DSIC/GSIPR	Estabelece as Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da Administração Pública Federal, direta e indireta. (Publicada no DOU Nº 196, de 10 Out 2014 - Seção 1)
Norma Complementar nº 01/IN02/NSC/GSIPR	Disciplina o Credenciamento de Segurança de Pessoas Naturais, Órgãos e Entidades Públicas e Privadas para o Tratamento de Informações Classificadas. (Publicada no DOU Nº 123, de 28 de junho de 2013 - Seção 1)
Decreto Nº 3.505, de 13 de junho de 2000.	Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.
Decreto Nº 7.724, de 16 de maio de 2012	Regulamenta a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art 5º, no inciso II do § 3º do art. 37 e no § do art. 216 da Constituição.
Decreto Nº 7.845, de 14 de novembro de 2012.	Regulamenta os procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento.
Decreto Nº 8.097, de 4 de setembro de 2013	Altera o Decreto nº 3.505, de 13 de junho de 2000, para incluir a Secretaria-Geral da Presidência da República no Comitê Gestor da Segurança da Informação.
Resolução Nº 12, de 14 de Fevereiro de 2006.	Cria o Banco de Soluções do Poder Judiciário e dá outras providências
Resolução nº 90, de 29 de setembro de 2009.	Dispõe sobre os requisitos de nivelamento de tecnologia da informação no âmbito do Poder Judiciário.
Resolução nº 136 -	Altera arts. 6º, 14, 17 e 18 da Resolução 90
Resolução nº 91, de 29 de setembro de 2009.	Institui o Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Poder Judiciário e disciplina a obrigatoriedade da sua utilização no desenvolvimento e manutenção de sistemas informatizados para as atividades judiciárias e administrativas no âmbito do Poder Judiciário.
Resolução nº 99, de 24 de novembro 2009.	Institui o Planejamento Estratégico de Tecnologia da Informação e Comunicação no âmbito do Poder Judiciário
Resolução nº 100, de 24 de novembro de 2009.	Dispõe sobre a comunicação oficial, por meio eletrônico, no âmbito do Poder Judiciário e dá outras providências.

Fonte:

7.2 APÊNDICE II – Planilha de avaliação de fatores de segurança

CONTROLES	CONFORMIDADES		
	TJPB	TJMT	TJSP
1. Política de segurança			
1.1. Política de segurança da informação			
1.1.1. Documento da política de segurança da informação	1	2	2
1.1.2. Análise crítica da política de segurança da informação	1	2	2
2. Organizando a segurança da informação			
2.1. Infraestrutura da segurança da informação			
2.1.1. Comprometimento da direção com a segurança da informação	2	2	2
2.1.2. Coordenação da segurança da informação	2	2	2
2.1.3. Atribuição de responsabilidade para a segurança da informação	2	2	2
2.1.4. Processo de autorização para os recursos de processamento da informação	2	2	2
2.1.5. Acordos de confidencialidade	2	1	2
2.1.6. Contato com autoridades	1	1	1
2.1.7. Contato com grupos especiais	2	0	0
2.1.8. Análise critica independente de segurança da informação	2	2	2
2.2. Partes externas			
2.2.1. Identificação dos riscos relacionados com partes externas	1	1	1
2.2.2. Identificando a segurança da informação quando tratando os clientes	1	2	1
2.2.3. Identificando segurança da informação nos acordos com terceiros	1	2	2
3. Gestão de ativos			
3.1. Responsabilidade pelos ativos			
3.1.1. Inventário dos ativos	2	2	2
3.1.2. Proprietário dos ativos	2	2	0
3.1.3. Uso aceitável dos ativos	1	2	1
3.2. Classificação da informação			
3.2.1. Recomendações para classificação	2	2	2
3.2.2. Rótulos e tratamento da informação	2	1	2
4. Segurança em recursos humanos			
4.1. Antes da contratação			
4.1.1. Papéis e responsabilidades	2	2	2
4.1.2. Seleção	2	0	1
4.1.3. Termos e condições de contratação	2	2	2
4.2. Durante a contratação			
4.2.1. Responsabilidades da direção	2	2	1
4.2.2. Conscientização, educação e treinamento em segurança da informação	2	2	2

4.2.3. Processo disciplinar	2	2	2
4.3. Encerramento ou mudança da contratação			
4.3.1. Encerramento de atividades	2	2	2
4.3.2. Devolução de ativos	2	2	2
4.3.3. Retirada de direitos de acesso	2	2	2
5. Segurança física e do ambiente			
5.1. Áreas seguras			
5.1.1. Perímetro de segurança física	1	1	1
5.1.2. Controles de entrada física	1	2	2
5.1.3. Segurança em escritórios, salas e instalações	1	1	2
5.1.4. Proteção contra ameaças externas e do meio ambiente	1	2	1
5.1.5. Trabalho em áreas seguras	1	1	2
5.1.6. Acesso do público, áreas de entrega e de carregamento	2	2	1
5.2. Segurança de equipamentos			
5.2.1. Instalação e proteção do equipamento	2	2	2
5.2.2. Utilidades	2	2	2
5.2.3. Segurança do cabeamento	2	2	2
5.2.4. Manutenção dos equipamentos	2	2	2
5.2.5. Segurança de equipamentos fora das dependências da organização	0	2	1
5.2.6. Reutilização e alimentação segura de equipamentos	0	1	1
5.2.7. Remoção de propriedade	2	1	1
6. Gerenciamento das operações e comunicações			
6.1. Procedimentos e responsabilidades operacionais			
6.1.1. Documentação dos procedimentos de operação	1	2	2
6.1.2. Gestão de mudanças	1	1	1
6.1.3. Segregação de funções	2	1	1
6.1.4. Separação dos recursos de desenvolvimento, teste e de produção	2	1	1
6.2. Gerenciamento de serviços terceirizados			
6.2.1. Entrega de serviços	2	1	2
6.2.2. Monitoramento e análise crítica de serviços terceirizados	2	2	2
6.2.3. Gerenciamento de mudanças para serviços terceirizados	2	2	2
6.3. Planejamento e aceitação dos sistemas			
6.3.1. Gestão de capacidade	1	1	1
6.3.2. Aceitação de sistemas	2	1	1
6.4. Proteção contra códigos maliciosos e códigos móveis			
6.4.1. Controle contra códigos maliciosos	1	1	1
6.4.2. Controle contra códigos móveis	0	0	0
6.5. Cópias de segurança			
6.5.1. Cópias de segurança das informações	2	2	2
6.6. Gerenciamento da segurança em redes			
6.6.1. Controles de redes	2	2	2
6.6.2. Segurança dos serviços de rede	2	2	2
6.7. Manuseio de mídias			

6.7.1. Gerenciamento de mídias removíveis	0	0	0
6.7.2. Descarte de mídias	0	0	0
6.7.3. Procedimentos para tratamento de informações	0	2	2
6.7.4. Segurança da documentação dos sistemas	0	1	1
6.8. Troca de informações			
6.8.1. Política e procedimentos para troca de informações	0	1	2
6.8.2. Acordos para troca de informações	1	1	2
6.8.3. Mídias em trânsito	0	0	0
6.8.4. Mensagens eletrônicas	2	2	2
6.8.5. Sistema de informações do negócio	0	0	0
6.9. Serviços de comercio eletrônico			
6.9.1. Comercio eletrônico	0	0	0
6.9.2. Transações on-line	0	0	0
6.9.3. Informações publicamente disponíveis	0	0	0
6.10. Monitoramento			
6.10.1. Registros de auditoria	2	2	2
6.10.2. Monitoramento de uso do sistema	2	2	2
6.10.3. Proteção das informações dos registros (logs)	1	2	1
6.10.4. Registros (log) de administrador e operador	1	2	1
6.10.5. Registros (logs) de falhas	2	2	1
6.10.6. Sincronização dos relógios	0	0	0
7. Controle de acesso			
7.1. Requisitos de negócio para controle de acesso			
7.1.1. Política de controle de acesso	2	2	1
7.2. Gerenciamento de acesso do usuário			
7.2.1. Registro de usuário	2	2	2
7.2.2. Gerenciamento de privilégios	2	2	2
7.2.3. Gerenciamento de senha do usuário	2	2	2
7.2.4. Análise crítica dos direitos de acesso de usuário	2	2	2
7.3. Responsabilidades dos usuários			
7.3.1. Uso de senhas	2	2	2
7.3.2. Equipamento de usuário sem monitoração	0	0	0
7.3.3. Política de mesa limpa e tela limpa	2	1	1
7.4. Controle de acesso à rede			
7.4.1. Política de uso dos serviços de rede	2	2	2
7.4.2. Autenticação para conexão externa do usuário	2	0	0
7.4.3. Identificação dos equipamentos em rede	1	1	1
7.4.4. Proteção e configuração de portas de diagnostico remota	0	0	0
7.4.5. Segregação de redes	0	0	0
7.4.6. Controle de conexão de rede	2	2	2
7.4.7. Controle de roteamento de redes	0	2	2
7.5. Controle de acesso ao sistema operacional			
7.5.1. Procedimentos seguros de entrada no sistema (log-on)	2	2	2
7.5.2. Identificação e autenticação de usuário	2	2	2
7.5.3. Sistema de gerenciamento de senha	2	1	1

7.5.4. Uso de utilitários de sistema	2	1	1
7.5.5. Desconexão de terminal por inatividade	0	0	0
7.5.6. Limitação de horário de conexão	0	0	0
7.6. Controle de acesso à aplicação e à informação			
7.6.1. Restrição de acesso à informação	2	2	2
7.6.2. Isolamento de sistemas sensíveis	2	2	1
7.7. Computação móvel e trabalho remoto		0	
7.7.1. Computação e comunicação móvel	0	0	0
7.7.2. Trabalho remoto	0	0	0
8. Aquisição, desenvolvimento e manutenção de sistemas de informação			
8.1. Requisitos de segurança de sistemas de informação			
8.1.1. Análise e especificação dos requisitos de segurança	2	2	2
Processamento correto de aplicações			
8.1.2. Validação dos dados de entrada	0	0	0
8.1.3. Controle de processamento interno	2	2	2
8.1.4. Integridade de mensagens	2	2	2
8.1.5. Validação de dados de saída	2	2	2
8.2. Controles criptográficos			
8.2.1. Política para o uso de controles criptográficos	0	0	0
8.2.2. Gerenciamento de chaves	0	0	0
8.3. Segurança dos arquivos do sistema			
8.3.1. Controle de software operacional	2	1	2
8.3.2. Proteção dos dados para teste de sistema	2	1	1
8.3.3. Controle de acesso ao código fonte de programa	1	1	1
8.4. Segurança em processos de desenvolvimento e de suporte			
8.4.1. Procedimentos para controle de mudanças	2	1	2
8.4.2. Análise crítica técnica das aplicações após mudanças no S.O.	2	2	2
8.4.3. Restrições sobre mudanças em pacotes de software	1	1	1
8.4.4. Vazamento de informações	1	1	1
8.4.5. Desenvolvimento terceirizado de software	2	1	2
8.5. Gestão de vulnerabilidade			
8.5.1. Controle de vulnerabilidades técnicas	2	1	1
9. Gestão de incidentes de segurança da informação			
9.1. Notificação de fragilidades e eventos de segurança da informação			
9.1.1. Notificação de eventos de segurança da informação	2	1	1
9.1.2. Notificando fragilidades de segurança da informação	2	1	1
9.2. Gestão de incidentes de segurança da informação e melhoria			
9.2.1. Responsabilidades e procedimentos	2	1	2
9.2.2. Aprendendo com os incidentes de segurança da informação	1	1	2
9.2.3. Coleta de evidências	1	2	2
10. Gestão da continuidade do negócio			
10.1. Aspectos da gestão da continuidade do negócio			

10.1.1. Incluindo S.I. no processo de gestão de continuidade de negócio	2	1	1
10.1.2. Continuidade de negócio e análise/avaliação de risco	2	2	2
10.1.3. Desenvolvimento e implementação de planos de continuidade relativos à S.I.	2	1	2
10.1.4. Estrutura do plano de continuidade do negócio	1	0	0
10.1.5. Testes, manutenção e reavaliação dos planos de continuidade do negócio	2	1	1
11. Conformidade			
11.1. Conformidade com requisitos legais			
11.1.1. Identificação da legislação vigente	2	2	2
11.1.2. Direitos de propriedade intelectual	2	2	2
11.1.3. Proteção dos registros organizacionais	2	2	2
11.1.4. Proteção de dados e privacidade da informação pessoal	2	2	2
11.1.5. Prevenção de mau uso de recursos de processamento da informação	2	2	2
11.1.6. Regulamentação de controles de criptografia	0	0	0
11.2. Conformidade com normas e políticas de S.I. conf. Técnicas			
11.2.1. Conformidade com as políticas e normas de segurança da informação	2	1	2
11.2.2. Verificação da conformidade técnica	1	2	2
11.3. Considerações quanto à auditoria de sistemas de informação			
11.3.1. Controles de auditoria de sistemas de informação	2	2	2
11.3.2. Proteção de ferramentas de auditoria de Sistemas de Informação	1	2	1
Total			**133**
TOTAL DE PONTOS	**185**	**178**	**179**
ALINHAMENTO TOTAL			
266			

Fonte: Adaptado de Pontes (2014)

Métricas adotadas:

Situação	**Métrica**
Possui	2
Possui em Parte	1
Não possui	0