UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
DEPARTAMENTO DE FINANÇAS E CONTABILIDADE
CURSO DE CIÊNCIAS CONTÁBEIS

ISABELA FELIX SERAFIM

SEGURANÇA DA INFORMAÇÃO NA ADMINISTRAÇÃO PÚBLICA: O CASO DA CONTROLADORIA GERAL DO ESTADO DA PARAÍBA

JOÃO PESSOA
2017

ISABELA FELIX SERAFIM

SEGURANÇA DA INFORMAÇÃO NA ADMINISTRAÇÃO PÚBLICA: O CASO DA CONTROLADORIA GERAL DO ESTADO DA PARAÍBA

Monografia apresentada ao Curso de Ciências Contábeis, do Centro de Ciências Sociais Aplicadas, da Universidade Federal da Paraíba, como requisito parcial a obtenção do grau de Bacharel em Ciências Contábeis.

Orientador Prof.: Dr. Tiago Henrique de Souza Echternacht

JOÃO PESSOA
2017

Dados Internacionais de Catalogação na Publicação (CIP)

S481s Serafim, Isabela Felix.
Segurança da Informação na Administração Pública: o caso da Controladoria Geral do Estado da Paraíba. / Isabela Felix Serafim. – João Pessoa, 2017.
69f.: il.

Orientador(a): Profº Dr. Tiago Henrique de Souza Echternacht.
Trabalho de Conclusão de Curso (Ciências Contábeis) – UFPB/CCSA.

1. Tecnologia da Informação. 2. Segurança da Informação. 3. Política de Segurança da Informação. I. Título.

UFPB/CCSA/BS CDU:657(043.2)

Gerada pelo Catalogar - Sistema de Geração Automática de Ficha Catalográfica do CCSA/UFPB, com os dados fornecidos pelo autor(a)

ISABELA FELIX SERAFIM

SEGURANÇA DA INFORMAÇÃO NA ADMINISTRAÇÃO PÚBLICA: O CASO DA CONTROLADORIA GERAL DO ESTADO DA PARAÍBA

Esta monografia foi julgada adequada para a obtenção do grau de Bacharel em Ciências Contábeis, e aprovada em sua forma final pela Banca Examinadora designada pela Coordenação do Curso de Ciências Contábeis da Universidade Federal da Paraíba.

BANCA EXAMINADORA

Presidente: Professor(a). Dr Tiago Henrique de Souza Echternacht (Orientador)
Instituição: UFPB

Membro: Professor(a). MS. Ionara Stéfani Viana De Oliveira (Membro)
Instituição: UFPB

Membro: Professor(a). MS. Fabrício Do Nascimento Santos (Membro)
Instituição: UFPB

João Pessoa, 19 de maio de 2017.

AGRADECIMENTOS

Primeiramente devo agradecer a Deus, por ter me concedido discernimento em momentos de dificuldade, por permitir que não tivesse perdido a fé ao longo da minha trajetória no curso.

Agradecer aos meus pais e irmã, por acreditarem em mim, no meu potencial, por sempre estarem presente, por sempre se esforçarem para que eu tivesse uma boa educação.

A meu namorado Guilherme, por sempre estar comigo, por sempre me incentivar a ser uma pessoa melhor e apoiar minhas decisões.

A minha querida e amada amiga Dyliane, por sempre ser solicita aos meus pedidos de ajuda.

Aos meus colegas de turma, que me proporcionaram experiências inesquecíveis.

Ao meu orientador professor Tiago Ecthernat, por abdicar de seu tempo de lazer, para dar orientações, por ser um excelente orientador, amigo e psicólogo, por todo o auxílio para a realização desta pesquisa e por todos os conhecimentos obtidos nesse tempo

A professora Carla Janaina, que é sempre solicita e de uma simplicidade inexplicável.

Aos demais professores do curso que engradeceram meu conhecimento.

Ao gestor da organização pesquisada, pela simplicidade de atender e por ter disponibilizado um pouco de seu tempo, para que eu pudesse realizar a pesquisa.

As minhas chefes Érika e Dayanne por todo apoio no estágio e no meu desenvolvimento profissional.

RESUMO

O presente trabalho tem como objetivo geral identificar a existência de políticas de segurança da informação adotadas em um órgão da administração pública estadual. A metodologia utilizada foi descritiva, revisão bibliográfica e qualitativa com estudo de caso realizado na Controladoria Geral do Estado da Paraíba (CGE-PB), a coleta de dados foi realizada através de um questionário e uma entrevista semiestruturada, ambos realizados com o dirigente máximo desta organização, para obter conhecimento de sua percepção sobre diversos pontos da implementação da segurança da informação, as análises de dados utilizadas foram: análise descritiva para o questionário e análise qualitativa para a entrevista, na análise qualitativa foi utilizado o software MAXQDA. A pesquisa concluiu que existem algumas Políticas de Segurança da Informação (PSI) implantadas na CGE-PB, como backup, antivírus, controles de acesso, porém foi constatado que existem algumas dificuldades para uma boa prática de PSI como capacitação dos prestadores de serviço, a falta de interesse dos funcionários e a falta de um manual contendo todas as PSI's e sendo amplamente divulgado para todos os colaboradores da organização.

Palavras-chave: Tecnologia da Informação. Segurança da Informação. Política de Segurança da Informação.

ABSTRACT

The present work has as general objective to identify the existence of information security policies adopted in a state public administration body. The methodology used was descriptive, bibliographical and qualitative review with a case study carried out at the General Comptroller's Office of the State of Paraíba (CGE-PB), data collection was performed through a questionnaire and a semi-structured interview, both performed with the maximum leader of this Organization, to obtain knowledge of their perception on several points of the implementation of information security, the data analyzes used were: descriptive analysis for the questionnaire and qualitative analysis for the interview, in the qualitative analysis was used the MAXQDA software. The research concluded that there are some Information Security Policies (PSI) deployed in CGE-PB, such as backup, antivirus, access controls, but it has been found that there are some difficulties for a good PSI practice such as training of service providers, Lack of interest of the employees and the lack of a manual containing all the PSI's and being widely divulged to all the collaborators of the organization.

Keywords: Information Technology. Information Security. Information Security Policy.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS

ABNT – Associação Brasileira de Normas Técnicas

CGE – Controladoria Geral do Estado

IBGC – Instituto Brasileiro de Governança Corporativa

ITGI – IT Governance Institute

LAI – Lei de Acesso à Informação

LRF – Lei de Responsabilidade Fiscal

PSI – Políticas de Segurança da Informação

SERPRO – Serviço Federal de Processamento de Dados

SIAFEM – Sistema Integrado de Administração Financeira para Estados e Munícipios

SIAFI – Sistema Integrado de Administração Financeira do Governo Federal

STN – Secretaria do Tesou Nacional

TI – Tecnologia da Informação

TCU – Tribunal de Contas da União

SUMÁRIO

1 INTRODUÇÃO

A Tecnologia da Informação - TI está mudando a forma como os indivíduos e as organizações vêm realizando suas atividades, por meio desta ferramenta estão sendo criados novos mercados, produtos, negócios e empregos, como descrevem Turban e Volonino (2013).

Para O' Brien (2010), estão relacionados a TI todos os sistemas de informações que estejam baseados em *hardware* e *software* de computador, internet, redes de telecomunicações, técnicas de administração de dados via computador e outras áreas da TI que transformem recursos de dados em informações.

As mudanças socioeconômicas e políticas ocorridas devido ao surgimento de inovações da tecnologia, trouxeram diversas possibilidades para a modernização das organizações. Estas inovações atingiram todos os setores, inclusive a administração pública, sinalizando que as organizações deveriam se adequar a esta nova realidade de mercado e, consequentemente, exigindo da administração pública um novo modelo de gestão, que trabalhe de forma integrada e orientada para alcançar a excelência (PEREIRA, 2008).

A modernização da administração pública, como afirma Pereira (2012, p.31), busca "de forma permanente a melhoria da qualidade da oferta de serviços à população, aperfeiçoar o sistema de controle social da administração pública, elevar a transparência, entre outros". Nesse contexto de inovações, essas mudanças foram indispensáveis para um novo modelo de gestão pública e para incentivar o controle social sobre os recursos públicos.

Com o avanço da tecnologia e os objetivos traçados para a modernização da gestão pública, é essencial revisar as estratégias governamentais, frente ao desenvolvimento de um novo relacionamento de transparência entre o governo e o cidadão, e os servidores e as pessoas que utilizam seus serviços, afirmam Kanane, Fiel Filho e Pereira (2010).

Segundo Corbari e Macedo (2011, p.194), "para alcançar a transparência, é necessário que os órgãos públicos disponibilizem informações, claras, corretas e oportunas de todos os atos praticados". Desta forma, o desafio das organizações é tratar um conjunto de dados relevantes, que logo em seguida é transformada em conhecimento, e é de grande valor, pois dão suporte ao processo decisório e auxiliam a organização a otimizar seu desempenho (CARAPETO; FONSECA 2014).

A informação pode ser considerada um ativo, e é tão valiosa quanto qualquer outro bem de um órgão. Os ativos estão sujeitos a ameaças tanto acidentais como propositais, desta maneira muitas ameaças podem surgir, diante de alguma vulnerabilidade nos processos e sistemas onde são tratadas as informações. Por isto, a organização deve ter implantada uma

política de segurança da informação eficaz, para proteger seus ativos de possíveis ameaças e vulnerabilidades (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ISO/IEC 27002:2013).

A Controladoria Geral do Estado da Paraíba é um órgão público que manuseia informações da administração pública direta e indireta, e posteriormente no final de cada exercício pública em portais de transparência essas informações consolidadas.

Diante de todo o contexto apresentado, este trabalho visa identificar a existência de políticas de segurança da informação adotadas na Controladoria Geral do Estado, demonstrando a percepção da alta administração sobre políticas de segurança da informação, as ações preventivas que o órgão possui e verificar se existem dificuldades para boas práticas de segurança da informação.

1.1 Tema e problema de pesquisa

A proposta do presente estudo mostra parte do processo estratégico da administração pública e sua modernização, e a relevância da informação como um recurso dos negócios que precisa ser adequadamente gerenciada, sendo vital para a sobrevivência das empresas contemporâneas. Todas as organizações sejam públicas ou privadas manuseiam e transmitem informações, para proteger a informação das ameaças e vulnerabilidades, é necessário que as organizações possuam um sistema de segurança da informação eficaz (ISO/IEC 27002:2013). Nessa linha de raciocínio e a partir das considerações teóricas, apresenta-se a seguinte questão de pesquisa: Quais são as políticas de segurança da informação adotadas na Controladoria Geral do Estado da Paraíba para boas práticas de segurança da informação?

1.2 Objetivos

A pesquisa se apresenta estruturada em um objetivo geral e três objetivos específicos, conforme observado a seguir.

1.2.1 Objetivo Geral

Identificar a existência de políticas de segurança da informação adotadas na Controladoria Geral do Estado da Paraíba - CGE.

1.2.2 Objetivos Específicos

- Apresentar a percepção da alta administração da organização a respeito do papel das políticas de segurança da informação;
- Verificar a existência de implementação de procedimentos ou planos de tratamento que evitem os riscos, ameaças e vulnerabilidades;
- Verificar se existem dificuldades para uma boa prática de políticas segurança da informação na CGE.

1.3 Justificativa

As organizações armazenam a maior parte de suas informações por meio de formato eletrônico em sistemas de informações, que podem estar conectados através de redes de telecomunicações em diversas localidades, diante disto as informações tornam-se cada vez mais vulneráveis, pois as ameaças não ficam limitadas a apenas um lugar, podendo acontecer o uso indevido de informações em qualquer ponto de acesso à rede (LAUDON; LAUDON, 2014).

Para minimizar os riscos não basta ter foco apenas nos meios eletrônicos, de acordo com Laudon e Laudon (2014, p.255) é necessário "promover a cultura de mentalidade de segurança". Os colaboradores da organização devem ter conhecimento sobre suas responsabilidades para o alcance da segurança da informação, que visa garantir a continuidade da empresa e a proteção da informação como um bem essencial para a conservação dos negócios (FONTES, 2006).

A informação pode ser considerada essencial para o ramo empresarial, segundo Fontes (2006, p.2) "a informação é um bem, tem valor para empresa e deve ser protegida". É necessário que os gestores implantem políticas de segurança da informação, visando minimizar os possíveis riscos que a organização esteja exposta.

A política de segurança da informação é um conjunto de normas bem elaboradas, que limitam determinadas ações ou pessoas a manusear funções e informações em um sistema, com a finalidade de alcançar objetivos específicos de segurança (GOODRICH e TAMASSIA, 2013).

Para ser alcançada a segurança da informação é necessária a implantação de controles adequados, contendo procedimentos, processos, políticas, funcionários, estrutura organizacional e sistemas de informações. Estes controles devem ser definidos,

implementados, monitorados, averiguados adequadamente e aperfeiçoados quando houver necessidade, para assegurar que os objetivos da organização e a segurança da informação estão sendo respeitados (ISO/IEC 27002:2013).

Para que as informações sejam consideradas seguras, devem atender os três princípios de segurança da informação: disponibilidade, integridade e confidencialidade, segundo KIM e SOLOMON (2014). Buscando estar em conformidade a esses princípios convém que as organizações disponham de políticas de segurança da informação.

Nos Estados Unidos, o resultado de uma pesquisa com os maiores varejistas na América no ano de 2016, por meio da BDO, uma das maiores empresas de contabilidade no mundo, perguntou quais os maiores fatores de riscos que os varejistas enfrentavam: em primeiro lugar, empatados, estavam as condições econômicas e a preocupação de privacidade relacionados com a violação de segurança da informação (BDO, 2016).

No Brasil, depois de mais de 5 anos de debates, o Projeto de Lei de Proteção de Dados Pessoais foi encaminhado pelo Poder Executivo para o Congresso Nacional, sendo recebido na Câmara dos Deputados como o PL 5.276/2016 (BRASIL, 2016). O Projeto de Lei 5276/2016 (BRASIL, 2016) sobre proteção de dados pessoais, tem como temas tratados em seu projeto a definição de dado pessoal e os identificadores eletrônicos, os conceitos de dados anônimos e dados sensíveis, a noção de legítimo interesse, os tópicos de segurança da informação e vazamento de dados, a transferência internacional de dados e as competências de uma autoridade de proteção de dados.

Diante disto, a relevância deste tema para o curso de Ciências Contábeis da Universidade Federal da Paraíba - UFPB agregará valor, à proporção que conseguir conscientizar os gestores públicos de controle do Estado da Paraíba que uma política de segurança da informação protegerá as informações públicas dos riscos e vulnerabilidades presentes na tecnologia da informação e ameaças físicas, tornando-se assim, seu fluxo de informações mais seguras para seu ambiente interno e externo.

2 FUNDAMENTAÇÃO TEÓRICA

O objetivo deste tópico foi estabelecer a relação teórica dos principais temas da pesquisa. Dessa forma, procura-se contemplar os seguintes assuntos: administração pública moderna. Governança de TI, sistemas de informações e segurança da informação.

2.1 Administração Pública Moderna

A administração pública tem como finalidade atender as demandas da sociedade, através de serviços públicos de qualidade, desenvolvendo um ambiente propício para a inclusão social e o fortalecimento da capacidade de elaboração de políticas públicas, segundo Corbari e Macedo (2011). A participação da sociedade no setor público vem aumentando cada dia mais, desta forma desenvolvendo uma nova gestão pública.

Para aperfeiçoar essa nova gestão e atender as finalidades da administração pública, segundo Oliveira e Paula (2014), buscou-se no setor público modernizar a gestão, através da inclusão de técnicas e ferramentas provenientes da iniciativa privada, de forma que a eficiência passou a ser entendida como essencial, idealizando assim uma boa prática de gestão pública.

Matias-Pereira (2012) afirma que a visão estratégica da nova administração pública consiste em ter habilidades gerenciais de interpretar corretamente as ameaças que devem ser evitadas ou neutralizadas, as oportunidades que devem ser usufruídas e possuir competência de ação, para pôr em prática tudo àquilo que pode ser aperfeiçoado.

A modernização da administração pública visa alcançar um modelo de gestão que possa atingir seus objetivos, usando como enfoque questões de sustentabilidade, como por exemplo, aprimorar a qualidade se serviços ofertados a população, promover a transparência e combater a corrupção, desenvolver o sistema de controle social, entre outros (MATIAS-PEREIRA, 2008). Ou seja, a nova administração pública está mais voltada para promover uma cultura participativa da sociedade.

Nesse sentido, as leis que regulamentam a administração pública estão cada vez mais voltadas para a adoção da transparência pública governamental, supervisionando o gerenciamento dos recursos públicos e a sua devida prestação de contas. Através da transparência pública busca-se desenvolver o princípio da publicidade e assegurar o acesso as informações públicas, desta forma, possibilitando o controle social. Existem diversos tipos de informações públicas, porém as produzidas a partir da contabilidade detêm grande relevância,

pois é com base nessas informações que a população tem conhecimento de como estão sendo aplicados os recursos públicos, afirmam Frey, Marcuzzo e Dumke (2015).

A Lei 101/2000 – Lei de Responsabilidade Fiscal – LRF (BRASIL, 2000) sancionada em 2000, traz em seu artigo 48 instrumentos necessários para a elaboração e ampla divulgação de relatórios e demonstrativos dos órgãos públicos, incluindo a divulgação através de meios eletrônicos para garantir o acesso público. De acordo com Frey, Marcuzzo e Dumke (2015), a LRF foi um marco normativo relacionado à transparência dos recursos públicos.

A partir de novembro de 2011, a Lei 12.527/2011, Lei de Acesso a Informação – LAI (BRASIL, 2011), entrou em vigor garantindo a toda a população brasileira acesso às informações públicas, independente de solicitações, tornando-se assim obrigatório que os governos disponibilizassem suas informações, através dos portais de transparência pública. Esta lei reforça o conceito da nova administração pública, que tem o enfoque mais voltado para fins gerenciais, visando desenvolver uma cultura de transparência e controle social na administração pública.

2.1.1 Controle na administração pública

O controle é uma ferramenta essencial para a administração pública, pois sua influência sobre o governo dificulta o abuso de poder, de modo que o gestor atue na defesa do interesse social, através de uma fiscalização que tem como finalidade orientar, corrigir e até mesmo punir. Além disso, é indispensável para auxiliar a participação social frente ao acompanhamento e execução do orçamento público, visando certificar-se sobre a autenticidade das operações realizadas, afirma Lima (2008).

De acordo com o Tribunal de Contas da União (2014) o controle pode ser classificado quanto à posição, sendo dividido em controle interno e externo, o controle interno é feito por parte integrante do próprio órgão controlado, e o controle externo é exercido por outro componente que não faz parte do órgão que está sendo controlado.

A controladoria é um órgão de controle, que visa promover a transparência da gestão pública, através das funções do controle interno, ouvidoria e prevenção, correção e combate à corrupção, afirma Matias-Pereira (2008).

De acordo com a Controladoria Geral do Estado da Paraíba – CGE/PB, sua missão é:

> Acompanhar, avaliar, fiscalizar, orientar e controlar os Órgãos do Poder Executivo Estadual, visando a maximização do desempenho e da qualidade da Gestão Pública, com ênfase nos resultados, em cumprimento a dispositivos legais, utilizando recursos humanos qualificados, técnicas eficientes e eficazes, com suporte tecnológico adequado, objetivando a otimização e transparência da ação governamental perante a Sociedade.

A CGE-PB acompanha todos os órgãos públicos estaduais, é perceptível a relevância desse órgão para a tomada de decisão na esfera estadual, pois trabalha com diversas informações, que ao final de cada ano são consolidadas e disponibilizadas para livre acesso em portais de transparência pública.

2.2 Governança de TI

De acordo com Instituto Brasileiro de Governança Corporativa – IBGC (2015) a governança corporativa é um sistema que busca orientar, monitorar e incentivar as empresas, envolvendo os relacionamentos entre diretoria, conselho de administração e todas as demais partes interessadas na organização. Além disso, a governança corporativa possui como base quatro princípios: transparência, equidade, prestação de contas e responsabilidade corporativa, a adequação a esses princípios resulta no fortalecimento da confiança nas relações internas e com terceiros.

O sistema de governança no setor público reflete a forma como diversos colaboradores se organizam, interagem e atuam para obter boas práticas de governança. Envolvendo grande parte das estruturas administrativas, métodos de trabalho, os documentos, o compartilhamento de informações e o comportamento de pessoas envolvidas direta e indiretamente, na avaliação, no direcionamento e no monitoramento da organização, segundo o TCU (2013).

Segundo o IT Governance Institute – ITGI (2003) a governança de TI está inserida na governança corporativa, buscando alcançar os objetivos de TI, minimizar os riscos de TI e manter a continuidade através dos objetivos da organização. A governança corporativa está mais voltada para a empresa como um todo, possibilitando que existam outros tipos de governança que atendam aos demais setores da organização, como, por exemplo, a governança de TI que é indispensável para quem trabalha com base em informações, e principalmente para o setor público que trabalha com algumas informações que tem obrigatoriedade de ser disponibilizados em portais de transparência pública e que são bases para tomadas de decisões dos governantes.

De acordo com a Resolução do TCU n° 247/2011 a governança de TI é um:

> Conjunto de diretrizes, estruturas organizacionais, processos e mecanismos de controle que visam a assegurar que as decisões e ações relativas à gestão e ao uso da TI mantenham-se alinhadas às necessidades institucionais e contribuam para o cumprimento da missão e o alcance das metas organizacionais. (TRIBUNAL DE CONTAS DA UNIÃO, 2011)

De acordo com a ISO/IEC 38.500 (p.3, 2009) a Governança de TI "significa avaliar direcionar o uso da TI para dar suporte à organização e monitorar seu uso para realizar os planos. Inclui a estratégia e as políticas de uso da TI dentro da organização".

Diante dos conceitos expostos, é perceptível que a TI não é mais uma simples ferramenta de gestão, tornou-se mais complexa devido ao desenvolvimento dos processos organizacionais, necessitando de um enfoque maior dentro das instituições, visando assegurar que sua missão e seus objetivos de negócio sejam alcançados com o auxílio da TI, mas para isso é necessário que haja um bom gerenciamento de recursos de TI e pessoas capacitadas e orientadas na área, ou seja, convém que as organizações disponham de uma Governança de TI.

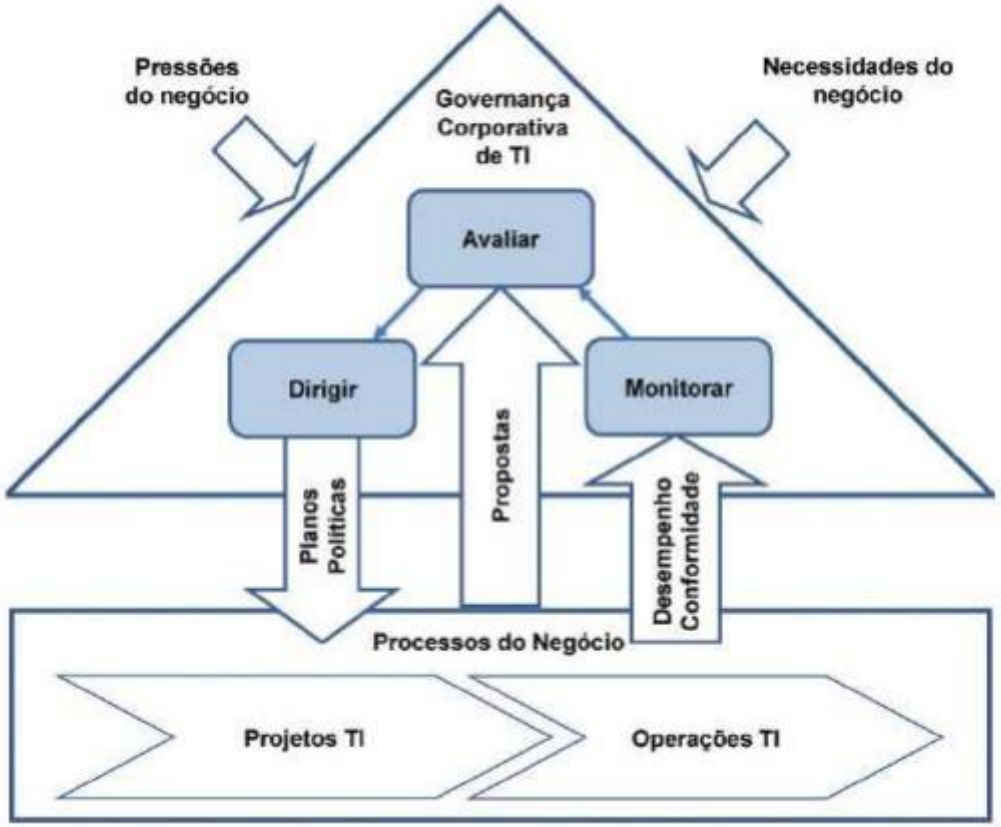
Conforme Okano et al. (2016), a TI proporciona suporte a todos os funcionários, programas e sistemas, ou seja, a TI está presente em todos os departamentos da organização, interagindo na maior parte dos processos e atividades, alinhado com o planejamento estratégico organizacional, diante deste contexto é perceptível a necessidade da governança de TI para direcionar e conduzir a organização a alcançar seus objetivos.

Uma boa governança de TI auxilia a alta administração no processo de tomada de decisão e contribui para a organização atingir suas metas, através do alinhamento da TI com os objetivos de negócio afirma Weill e Ross (2006).

A responsabilidade pela governança de TI, de acordo com ABNT NBR ISO/IEC 38500 (2009, p.3) é do dirigente que é conceituado como "membro da mais alta direção de uma organização, incluem proprietários, membros do conselho de administração, entre outros, parceiros, executivos seniores ou similares". Ou seja, a responsabilidade de adotar boas práticas de governança de TI é da alta administração.

Conforme mostra a figura a seguir, a norma ISO apresenta três atividades principais: avaliar, dirigir (orientar) e monitorar, convém aos dirigentes das organizações realizarem essas atividades para executar uma boa governança de TI.

Figura 1 - Modelo de Governança Corporativa de TI



Fonte: ABNT ISO/IEC 38.500 (p.7, 2009)

A atividade de avaliação consiste em examinar e avaliar a atual e futura utilização de TI, inserindo propostas e estratégias para melhorar seu desempenho, levando em consideração as variáveis internas e externas que influenciam o negócio, convém que a avaliação seja feita de forma continua, conforme as variáveis sofrerem alterações ao longo do tempo, além disto, nesta etapa é necessário que os dirigentes considerem as necessidades e os objetivos atuais e futuros da organização. (ABNT, 2009)

A tarefa de dirigir uma governança de TI tem como objetivo atribuir responsabilidades e exigir a preparação e adoção de planos e políticas, os planos devem estabelecer como serão utilizados os investimentos nos projetos e operações de TI e as políticas determinam uma conduta sólida no uso da TI. É dever dos dirigentes, ainda nesta tarefa, certificar que a transição dos projetos até entrar efetivamente em operação seja devidamente planejada e gerenciada, considerando os impactos nos negócios, na atividade operacional, nos sistemas de TI e na estrutura existente. Além disto, é dever dos dirigentes disseminar uma cultura de boa governança de TI dentro da organização, determinando que as informações sejam acessíveis em tempo adequado. (ABNT, 2009)

Na atividade de monitoramento, é de responsabilidade dos dirigentes realizarem o monitoramento por meio de sistemas de mensuração adequado, assegurando que o desempenho está em conformidade com os planos, particularmente no que corresponde aos objetivos do negócio. Nesta atividade também é necessário que os dirigentes assegurem que a TI está de acordo com a legislação e práticas internas de trabalho. (ABNT, 2009)

2.3 Tecnologia da Informação na Administração Pública

A tecnologia da informação é uma ferramenta indispensável para as organizações, auxilia as empresas a operar de forma adequada diante das necessidades de mercado e tomar decisões em um ambiente competitivo (BALTZAN, 2016).

Os órgãos públicos estão sujeitos a atender às exigências por parte da população, que estão relacionadas à orçamento público participativo, maior grau de transparência das contas públicas e melhorias nos serviços públicos que são prestados. Para que essas demandas sócias sejam atendidas é indispensável à utilização de novas tecnologias da informação e comunicação, afirmam Albano e Reinhard (2015).

De acordo com Bueno, Brelàz e Salinas (2016) o desenvolvimento da TI contribui significativamente para o controle social, pois possibilita a participação da população em debates, que por motivos externos, como falta de tempo e recursos financeiros, que em condições normais não participavam, assim, facilitando o acesso à informação pública, através de portais, aproximando a população da participação em processos decisórios e a possibilitando a melhoria na gestão de políticas públicas.

No 2° parágrafo do artigo 8° da LAI (BRASIL, 2011) estabelece que “os órgãos e entidades públicas deverão utilizar todos os meios e instrumentos legítimos de que dispuserem, sendo obrigatória a divulgação em sítios oficiais da rede mundial de computadores (internet) ”. Sem a TI e os sistemas de informações o desenvolvimento de portais de transparência, o tratamento adequado das informações e pincipalmente o acesso a essas informações seria inviável.

Através dos sistemas de informações a TI vêm sendo integrados a todas as áreas que compõe a organização, como por exemplo: contabilidade, produção, recursos humanos, entre outros. Os sistemas de informações coletam, processam, armazenam e analisam dados de acordo com os objetivos da organização (TURBAN, McLEAN e WETHERBE, 2004).

Com a finalidade de aperfeiçoar os fluxos de informações e conhecimentos, a adoção a sistemas de informações dentro das organizações se tornam cada vez mais relevante, para

que os dados passem por todos os departamentos da organização de maneira continua e uniforme, afirma Martins et al (2012).

O setor público dispõe de um sistema de informações denominado Sistema Integrado de Administração Financeira do Governo Federal – SIAFI (BRASIL, 2012), onde são feitos todos os registros e a contabilização de toda execução orçamentária, financeira e patrimonial afirma a Secretaria do Tesou Nacional - STN (2012).

De acordo com o Manual do SIAFI (BRASIL, 2012, p.3), disponibilizado pelo STN, o SIAFI tem como objetivos:

> - Prover de mecanismos adequados ao registro e controle diário da gestão orçamentária, financeira e patrimonial, os Órgãos Central, Setorial, Seccional e Regional do Sistema de Controle Interno e órgãos executores;
> - Fornecer meios para agilizar a programação financeira, com vistas a otimizar a utilização dos recursos do Tesouro Nacional;
> - Permitir que a contabilidade pública seja fonte segura e tempestiva de informações gerenciais destinada a todos os níveis da administração pública federal;
> - Integrar e compatibilizar as informações disponíveis nos diversos Órgãos e Entidades participantes do sistema;
> - Permitir aos segmentos da sociedade obter a necessária transparência dos gastos públicos;
> - Permitir a programação e o acompanhamento físico-financeiro do orçamento, em nível analítico;
> - Permitir o registro contábil dos balancetes dos Estados, Municípios e de suas supervisionadas;
> - Permitir o controle da dívida interna e externa, do Governo Federal, bem assim a das transferências negociadas. (BRASIL, 2012, p.3)

Com base no SIAFI (BRASIL, 2012) foi desenvolvido pelo Serviço Federal de Processamento de Dados - SERPRO o Sistema Integrado de Administração Financeira para Estados e Munícipios – SIAFEM, de acordo com a Secretaria de Estado da Fazenda (ALAGOAS, 2009).

Os sistemas de informação, sejam eles públicos ou privados, auxiliam no processamento dos dados, tornando informações compreensíveis, possibilitando uma base confiável para o processo de tomada de decisão.

2.4 Segurança da Informação

De acordo com Santos, Santos e Carreira (2016) a segurança da informação, foi tratada por muito tempo como uma técnica, sem muita relevância para as empresas, porém os problemas com a segurança da informação tomaram grandes proporções no ramo empresarial,

o que eram problemas com antivírus, *firewall* e rede de dados, passou a ser espionagem, invasão de privacidade, roubo de dados, entre outros, tornando as empresas vulneráveis a quaisquer tipos de ataque.

A segurança da informação é conceituada no Art. 2o do decreto no 3.505, 06/2000 (BRASIL, 2000) como:

> Proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento. (BRASIL, 2000)

Questões relacionadas à segurança da informação vêm tomando cada vez mais espaço entre as empresas, pois aplicada de maneira adequada, visa proteger a organização de possíveis ameaças que comprometam os negócios. É relevante salientar que a segurança da informação não abrange somente a área da TI, abrange também questões de segurança do espaço físico.

Para Goodrich e Tamassia (2013) a tendência natural é associar segurança da informação com um contexto totalmente digital, porém o acesso à informação digital encontra-se em algum espaço físico e para acessar a informação é necessária uma interface entre o espaço físico e digital, portanto devem ser incluídas nas políticas de segurança da informação – PSI's das organizações medidas corretivas e preventivas para proteção da interface física, por exemplo, proteção dos locais onde estão os computadores, detectar acesso de pessoas não autorizadas, alarmes, entre outros.

Segundo Sêmola (2014, p.15) o maior desafio das organizações é identificar "ameaças, vulnerabilidades, riscos, sensibilidades e impactos, a fim de permitir adequado dimensionamento e modelagem da solução". Dessa forma, é importante que as empresas tenham adotadas PSI's para garantir que suas informações não sofram nenhuma alteração indesejada ou inadequada.

De acordo com TCU (2012):

> Política de segurança de informações 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. (TRIBUNAL DE CONTAS DA UNIAO, 2012, p. 10)

É perceptível que as PSI's são extremamente necessárias para a continuidade das organizações, pois visam proteger todas as etapas pela qual a informação passa na entidade, sejam elas físicas ou por meio de tecnologia.

O sucesso da PSI está relacionado diretamente ao comprometimento e à atuação da alta administração, quanto maior o envolvimento da alta administração com os procedimentos de preparação e adoção de políticas, maior será a probabilidade de a PSI ser eficaz e efetiva, é necessário que esse envolvimento seja instituído formalmente e por escrito, assegurando o cumprimento pela alta administração (TCU, 2012).

A segurança da informação, além de proteger as informações, redes de telecomunicações, operações de comércios eletrônicos, entre outros, visa atender princípios básicos para que a informação seja considerada segura, que são: a confidencialidade, integridade, disponibilidade (TURBAN; VOLOVINO, 2013).

O TCU (2012) dispõe de conceitos para os três princípios, o princípio da integridade visa garantir a fidedignidade da informação, de forma que ela não seja alterada acidentalmente ou propositalmente, e que seja apresentada ao destinatário conforme foi enviada pelo transmissor. O princípio da confidencialidade consiste em garantir que tenham acesso às informações apenas pessoas autorizadas. O princípio da disponibilidade objetiva assegurar que as informações estejam acessíveis aos sistemas de informações e pessoas, sempre que for solicitado.

De acordo com a ISO 38.500 (ABNT, 2009, p.4) "um sistema de gestão da segurança da informação bem sucedido requer apoio de todos os funcionários da organização". Ou seja, as pessoas estão ligadas diretamente a todos os princípios da segurança da informação, por isso é relevante o desenvolvimento de uma cultura e de um manual formalmente instituído sobre suas reponsabilidades diante da segurança da informação dentro da organização, para incentivar o apoio dos colaboradores.

A ampla disponibilização de um manual de PSI para todos os usuários internos e externos da organização é um procedimento indispensável para que a implantação de segurança da informação ocorra com sucesso. Todos que compartilham de alguma rotina, seja ela direta ou indireta, com a organização devem ter conhecimento e acesso as PSI's, pois é fundamental que fique definido com clareza, os impactos provenientes da utilização imprópria dos sistemas de informações e as medidas corretivas e preventivas que são de responsabilidade de cada funcionário para o controle efetivo dos ativos computacionais e informacionais. (TCU, 2012)

3 METODOLOGIA

Nesta seção, serão descritas a caracterização utilizada para realização da pesquisa, a tipologia de pesquisa, população e amostra, a delimitação do estudo, bem como os procedimentos metodológicos para aplicação do estudo de caso.

3.1 Tipologia de Pesquisa

Para a realização da pesquisa, quanto aos seus objetivos, pode ser caracterizada como descritiva, pois de acordo com Gil (2009) o objetivo principal dessa tipologia de pesquisa é descrever características de uma determinada população ou fenômeno. A presente pesquisa busca demonstrar os conceitos, dificuldades e relevância da implementação da segurança da informação para uma organização pública.

Quanto aos procedimentos, as tipologias utilizadas podem ser caracterizadas como pesquisa bibliográfica e estudo de caso. A pesquisa bibliográfica como afirma Beuren (2009) contempla todo o material que seja relacionado ao tema da pesquisa que já tenha se tornado público, como por exemplo: livros, pesquisas, jornais, monografias, entre outros. Com relação à tipologia caraterizada como estudo de caso, de acordo com Silva (2006, p. 57) "é um estudo que analisa um ou poucos fatos com profundidade". As ideias iniciais para o estudo de caso surgem, primeiramente, com o escopo do estudo, como uma investigação empírica conforme Yin (2010, p.39) o estudo de caso "investiga um fenômeno contemporâneo em profundidade e em seu contexto de vida real, especialmente quando os limites entre o fenômeno e o contexto não são claramente evidentes", ou seja, o estudo de caso busca aprofundar o conhecimento em determinado fenômeno, no caso desta pesquisa aprofundar o conhecimento sobre segurança da informação.

A abordagem do problema é considera qualitativa, pois neste tipo de estudo conforme Sampieri et al. (2013, p.376), busca "compreender e aprofundar os fenômenos, que são explorados a partir da perspectiva dos participantes em um ambiente natural e em relação ao contexto". Estes mesmos autores, caracterizam o enfoque qualitativo como entender, descrever e interpretar os fenômenos, através das concepções e dos significados obtidos pelas experiências dos participantes, visando compreender as experiências, pontos de vistas e opiniões dos indivíduos diante do fenômeno estudado.

Assim, a opção pela abordagem qualitativa, do tipo estudo de caso, caracteriza-se pela necessidade de estudos no âmbito estadual de Políticas de Segurança da Informação no

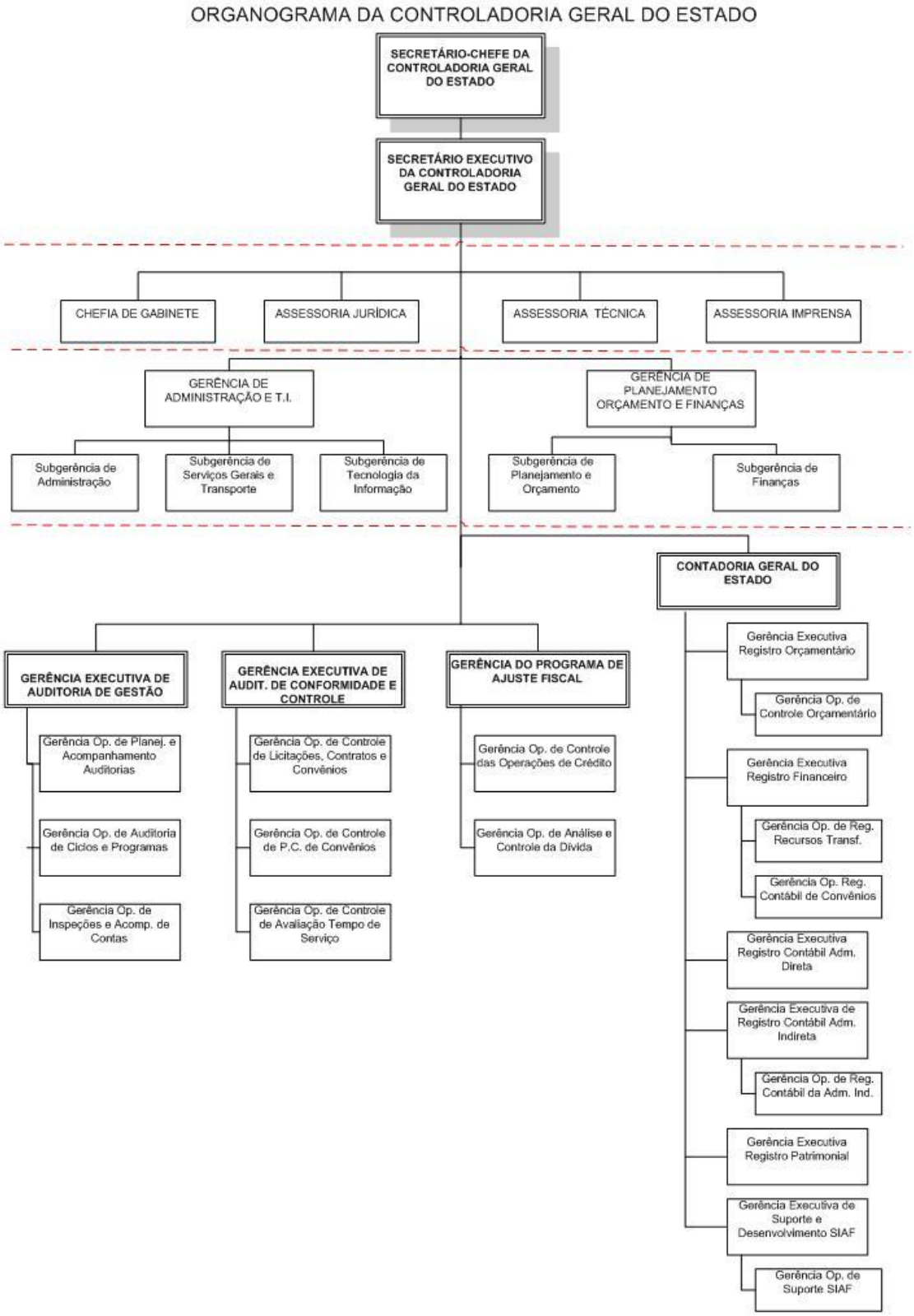
setor público, de maneira a permitir um conhecimento detalhado da realidade na implementação de novas estratégias nessa área.

3.2 Procedimentos Metodológicos

O caso foi selecionado, na cidade de João Pessoa, aplicado em um órgão da administração pública estadual, a Controladoria Geral do Estado da Paraíba, situada em João Pessoa, dispõe de orçamento anual de R$ 18.620.689,00 (dezoito milhões e seiscentos e vinte mil e seiscentos e oitenta e nove reais), conta com cerca de 152 prestadores de serviço, por uma amostra não probabilística, que, conforme Sampieri et al. (2013, p.405-406), é conhecida como "guiadas por um ou vários propósitos". Esse mesmo autor classifica o tipo de amostras, e a escolhida foi amostra de especialistas, com a participação de um especialista no tema da área de gestão pública e contabilidade do setor público.

Um dos critérios de seleção do respondente teve como base, o conhecimento e experiência profissional do gestor em relação à administração no âmbito público, além de seu posicionamento na alta administração da organização estudada, dessa forma a amostra pode ser caracterizada como, por especialistas, para colher suas perspectivas sobre assunto. Para realizar a coleta de dados, foi realizada a amostra por acessibilidade na organização pública, visto que o pesquisador utilizou de sua rede de contatos profissionais para conseguir realizar a entrevista conforme Sampieri et al. (2013). Foram utilizados, para prover maior consistência às informações levantadas, alguns critérios para a seleção do respondente, dentre os quais, os estabelecidos no questionário adaptado do Tribunal de Contas da União (Anexo A) sobre governança de políticas de segurança da informação, no qual o entrevistado deveria fazer parte da alta administração da organização estudada, pois a responsabilidade de uma boa Governança de TI e da segurança da informação é atribuída à alta administração.

Figura 2 - Organograma da Controladoria Geral do Estado



Fonte: PARAÍBA. Controladora Geral do Estado – Estrutura.

A figura 2, mostra a estrutura hierárquica da CGE-PB, é perceptível que a alta administração é composta pelo Secretário Chefe da Controladoria Geral do Estado e pelo

Secretário Executivo da Controladoria Geral do Estado, porém na realização da coleta de dados o cargo de Secretário Executivo estava vago, desta forma as informações foram obtidas, mediante o Secretário Chefe, gestor principal responsável pelo gerenciamento da Controladoria Geral do Estado. Esses documentos foram obtidos por meio de questionário e pela gravação digital de voz, por meio da entrevista semiestruturada.

3.3 Coleta de Dados

A coleta de dados foi executada em dois momentos: na primeira etapa, foram realizadas a análise documental da unidade, a aplicação do questionário e, posteriormente, a entrevista. Essa entrevista foi efetuada com base num roteiro semiestruturado, contemplando questões sobre políticas de segurança da informação, resistência na implementação da segurança da informação, qualidade das informações prestadas, conhecimento dos funcionários sobre as políticas adotadas, suas responsabilidades, bem como os benefícios da implementação de políticas, suas dificuldades, e as considerações como gestor numa posição primordial dentro da organização para adoção das políticas. Esse roteiro teve como objetivo guiar o tema, permitindo que o entrevistado pudesse se expressar livremente e se aprofundar sobre o assunto e a sua experiência no tema.

No caso específico desta pesquisa, a técnica de coleta de dados da entrevista se justifica, conforme Selltiz et al. (1967, p.273), por ser uma técnica que se enquadra para obter as “informações sobre o que as pessoas sabem, creem, esperam, sentem ou desejam, pretendem fazer ou fizeram, bem como sobre suas explicações ou razões a respeito das coisas precedentes”. A entrevista foi preparada conforme o roteiro questionário utilizado pelo Tribunal de Contas da União, com adaptações de alguns livros de segurança da informação. Em uma primeira etapa, conforme a recomendação de Cash Jr. e Stewart (2015, p.157), foi aplicado um pré-teste para “detectar possíveis problemas com perguntas e opções de resposta”, uma dificuldade encontrada na primeira entrevista foi o fator tempo. Os pontos que necessitavam de aperfeiçoamento foram discutidos e assim, foi reestruturada uma nova entrevista e reagendada, para ser feita novamente de forma presencial, que para Cash Jr. e Stewart (2015, p.158) “a probabilidade de obter respostas adequadas é maior” e por permitir a observação de todas as expressões seja gestos, visual, postura do entrevistado. A entrevista reestruturada foi realizada em outro ambiente de trabalho do gestor, que é uma faculdade privada, onde ele atua como professor, pois devido a questões de disponibilidade na controladoria, constatou-se que seria melhor realizar neste outro local de trabalho, em que

atua como docente, entre o intervalo de suas aulas. Foi estabelecido, que a entrevista seria no máximo de 30 minutos, porém o entrevistado não colocou nenhum obstáculo quanto ao tempo, sendo assim a entrevista durou mais de 20 minutos, com todos os pontos abordados perguntados.

A partir da entrevista, foi iniciada a coleta do questionário, com base noApêndices A, sobre a Governança de TI e controle na gestão, adotados na CGE-PB.

3.4 Tratamento e análise dos dados

O tratamento dos dados coletados a partir da entrevista realizada com o diretor da Controladoria Geral do Estado da Paraíba se deu em duas etapas: a primeira consistiu na categorização das áreas das Políticas de Segurança da Informação, em seções do questionário, para posterior análise descritiva das informações, e a segunda consistiu na transcrição das entrevistas para elaborar a análise, conforme procedimentos do *software* selecionado para análise do conteúdo das respostas obtidas na entrevista.

A análise descritiva do questionário buscou identificar a existência das políticas de segurança da informação na controladoria geral do estado, por meio da percepção do gestor principal, quanto aos itens de cada seção dos questionários e das entrevistas, tais como: liderança da alta administração, estratégias e planos de adoção das políticas de segurança de informação, informações referente à informatização dos processos organizacionais, o acesso à informação e sua divulgação, o conhecimento e a disseminação das políticas de segurança da informação aos prestadores de serviço da CGE-PB, bem como os processos.

Quanto à segunda etapa do tratamento dos dados será adotada a análise de conteúdo, Bardin (2011) afirma que a análise de conteúdo consiste em um conjunto de técnicas para analisar comunicações, em que Flick (2013) concorda que o uso de *softwares* para analisar os dados pode ser empregado para ligar segmentos de dados relevantes, entre si, criar categorias ou conjuntos ou redes de informação.

Nesse sentido, o processo para a análise do conteúdo das entrevistas e das observações ocorreu a partir da obtenção do relatório gerado pelas entrevistas, ocorreu por meio do *software* MAXQDA, versão demonstrativa. O MAXQDA é utilizado para a análise qualitativa de dados não estruturados, através da atribuição de categorias, codificação de segmentos de texto é possível apresentar os reultados, a partir disto é produzido diferentes

tipos de figuras que demonstram a frequência em que as codificações foram abordadas na entrevista (VERBI SOFTWARE, 2016).

O MAXQDA proporcionou a análise do conteúdo do texto obtido pela entrevista transcrita, de modo qualitativo. Posteriormente, à codificação seguiu-se a análise e comparação dos dados apresentados nas tabelas e mapas que o programa oferece para a mais correta visualização dos resultados.

4 RESULTADOS

Esta sessão do trabalho consiste em demonstrar os resultados obtidos e a análise dos dados, foram estruturados de uma maneira que ofereçam uma visão sobre o nível de adoção relacionado às práticas da governança corporativa e de TI e controles de gestão na Controladoria Geral do Estado, com os seguintes aspectos:

- Perfil do respondente;
- Liderança da alta administração;
- Estratégias e planos;
- Informações;
- Pessoas;
- Processos;
- Implementação de Políticas de Segurança da Informação na Controladoria Geral do Estado da Paraíba.

4.1 Perfil do Respondente

O respondente trabalha em cargo comissionado de confiança de Secretário Chefe da Controladoria Geral do Estado da Paraíba, tem experiência na profissão há três anos, quando questionado se possuía familiaridade na área de segurança da informação e se já havia participado de algum evento de capacitação, assinalou que sim e afirmou já ter participado do CONIP - Congresso de Informática e Inovação na Gestão Pública.

4.2 Liderança da Alta Administração

Este tópico de liderança da alta administração tem como objetivo avaliar a percepção do dirigente máximo da organização frente ao sistema de governança corporativa e de TI, aos riscos de TI, ao pessoal de TI, ao monitoramento da governança e da gestão de TI e sobre a capacidade da auditoria interna avaliar a gestão de TI.

Quadro 1 - Com relação ao sistema de governança corporativa

Nível de adoção da prática	Não se aplica	Não adota	Iniciou plano para adotar	Adota parcialmente	Adota integralmente
A organização define e comunica formalmente papéis e responsabilidades para a governança corporativa.				X	
A organização dispõe de um comitê de direção estratégica formalmente instituído, que auxilia nas decisões relativas às diretrizes, estratégias, políticas e no acompanhamento da gestão institucional.				X	
A organização realiza avaliações sobre a definição e compreensão dos papéis e responsabilidades organizacionais.					X
A organização dispõe de um código de ética formalmente instituído, bem como divulga e monitora o seu cumprimento.				X	
A organização dispõe de uma política corporativa de gestão de continuidade do negócio formalmente instituída como norma de cumprimento obrigatório.				X	

Fonte: Elaboração própria (2017).

De acordo com o respondente, no Quadro 1, a CGE dispõe parcialmente de um comitê de direção estratégica, de um código de ética, de uma política corporativa de gestão de continuidade do negócio, ambos formalmente instituídos, como norma de cumprimento obrigatório, bem como define e comunica parcialmente papéis e responsabilidades para a governança corporativa, e realiza integralmente avaliações sobre a definição e compreensão dos papéis e responsabilidades de seus colaboradores.

Quadro 2 - Com relação ao sistema de governança de TI.

Nível de adoção da prática	Não se aplica	Não adota	Iniciou plano para adotar	Adota parcialmente	Adota integralmente
A organização define e comunica formalmente papéis e responsabilidades mais relevantes para a governança e a gestão de TI.				X	
A organização dispõe de um comitê de TI formalmente instituído, composto por representantes de áreas relevantes da organização.				X	
O comitê de TI realiza as atividades previstas em seu ato constitutivo.				X	
A organização prioriza as ações de TI com apoio do comitê de TI (ou colegiado equivalente), que atua como instância consultiva da alta administração.					X

Fonte: Elaboração própria (2017).

Conforme o Quadro 2, o órgão define e comunica parcialmente de maneira formal papéis e responsabilidades mais relevantes para a governança e a gestão de TI, e dispõe parcialmente de um comitê de TI formalmente instituído que realiza as atividades previstas em seu ato constitutivo de forma parcial, com o apoio deste comitê de TI adota integralmente a priorização das ações de TI.

Quadro 3 - Com relação aos riscos de TI.

Nível de adoção da prática	Não se aplica	Não adota	Iniciou plano para adotar	Adota parcialmente	Adota integralmente
A organização define formalmente as diretrizes para gestão dos riscos de TI aos quais o negócio está exposto.				X	
A organização define e comunica formalmente papéis e responsabilidades pela gestão de riscos de TI.				X	
A organização define formalmente os níveis de risco de TI aceitáveis na consecução de seus objetivos (apetite a risco).				X	
A organização toma decisões estratégicas considerando os níveis de risco de TI definidos.					**X**

Fonte: Elaboração própria (2017).

De acordo com o quadro 3, a organização define de forma parcial as diretrizes e atribuições para seus colaboradores relacionadas à gestão de risco de TI, e os níveis de riscos de TI aceitáveis. A mesma adota integralmente estratégias que consideram os níveis de riscos de TI.

Quadro 4 - Com relação ao pessoal de TI.

Nível de adoção da prática	Não se aplica	Não adota	Iniciou plano para adotar	Adota parcialmente	Adota integralmente
A organização define formalmente diretrizes para garantir o desenvolvimento de competências e a retenção de gestores de TI.		X			
A organização define formalmente diretrizes para garantir o desenvolvimento de competências e a retenção de pessoal técnico de TI.		X			
A organização define formalmente diretrizes para avaliação e incentivo ao desempenho de gestores de TI.				X	
A organização define formalmente diretrizes para avaliação e incentivo ao desempenho de pessoal técnico de TI.				X	

Fonte: Elaboração própria (2017).

A CGE-PB, consoante ao quadro 4, não adota e nem define diretrizes para garantir o desenvolvimento de competências e a retenção de gestores e pessoal técnico de TI, porém define parcialmente diretrizes para avaliação e incentivo ao desempenho de gestores e técnicos de TI.

Quadro 5 - Com relação ao monitoramento da governança e da gestão de TI.

Nível de adoção da prática	Não se aplica	Não adota	Iniciou plano para adotar	Adota parcialmente	Adota integralmente
A organização define formalmente diretrizes para avaliação da governança e da gestão de TI.				X	
A organização realiza avaliação periódica de governança e de gestão de TI.				X	
A organização realiza avaliação periódica de sistemas de informação.				X	
A organização realiza avaliação periódica de segurança da informação.				X	
A organização realiza avaliação periódica de contratos de TI.					X

Fonte: Elaboração própria (2017).

A organização, de acordo com o quadro 5, define parcialmente diretrizes para avaliação da governança e da gestão de TI, realiza avaliação parcial periódica de governança e de gestão de TI, de sistemas de informação, de segurança da informação e realiza integralmente avaliação periódica de contratos de TI.

Quadro 6 - Com relação à auditoria interna.

Nível de adoção da prática	Não se aplica	Não adota	Iniciou plano para adotar	Adota parcialmente	Adota integralmente
A auditoria interna possui pessoal capacitado para avaliar a governança e a gestão de TI. Informe o quantitativo de pessoal da auditoria interna capacitado para avaliar a governança e a gestão de TI: _____				X	
A auditoria interna monitora as ações de governança e de gestão de TI.				X	
A organização aprova, de forma periódica, plano de auditoria que inclua avaliação da governança e da gestão de TI.				X	
A auditoria interna avalia a gestão de riscos de TI.				X	
A auditoria interna avalia os riscos considerados críticos para o negócio e a eficácia dos respectivos controles.				X	

Fonte: Elaboração própria (2017).

Com relação à auditoria interna, quadro 6, o entrevistado informou que dispõe de duas pessoas capacitadas para avaliar a governança e a gestão de TI e o nível de adoção desse item na percepção do gestor é parcial. De acordo com os demais itens, a auditoria interna da CGE-PB monitora e avalia parcialmente as ações de governança e de gestão de TI e os riscos considerados críticos para o negócio e a eficácia dos controles, além disto, a organização aprova parcialmente, de forma periódica, plano de auditoria que inclua avaliação da governança e da gestão de TI.

4.3 Estratégias e Planos

Foi questionado ao gestor sobre o nível de adoção de estratégias e planos organizacionais, sendo segregado em duas partes: processos e plano vigente, visando avaliar a relação do planejamento estratégico institucional.

Quadro 7 - Com relação ao planejamento estratégico institucional.

(continua)

Nível de adoção da prática Processo	Não se aplica	Não adota	Iniciou plano para adotar	Adota parcialmente	Adota integralmente
A organização executa periodicamente processo de planejamento estratégico institucional.				X	
O processo de planejamento estratégico institucional prevê a participação das áreas mais relevantes da organização.					X
O processo de planejamento estratégico institucional prevê a participação da área de TI.					X
O processo de planejamento estratégico institucional está formalmente instituído como norma de cumprimento obrigatório.				X	
Nível de adoção da prática Plano vigente	Não se aplica	Não adota	Iniciou plano para adotar	Adota parcialmente	Adota integralmente
A organização possui plano estratégico institucional vigente, formalmente instituído pelo seu dirigente máximo.				X	
O plano estratégico institucional vigente contém pelo menos um indicador de resultado para quantificar o cumprimento de cada objetivo estratégico estabelecido.					X
O plano estratégico institucional vigente contém metas associadas aos indicadores de resultado.				X	

Quadro 7 - Com relação ao planejamento estratégico institucional.

(conclusão)

Nível de adoção da prática Plano vigente	Não se aplica	Não adota	Iniciou plano para adotar	Adota parcialmente	Adota integralmente
O plano estratégico institucional vigente estabelece as ações (atividades e projetos) consideradas necessárias para o alcance das metas fixadas.				X	
Nível de adoção da prática Plano vigente	Não se aplica	Não adota	Iniciou plano para adotar	Adota parcialmente	Adota integralmente
A execução do plano estratégico institucional vigente é acompanhada periodicamente quanto ao alcance das metas estabelecidas, para correção de desvios				X	
O plano estratégico institucional vigente está publicado na internet para acesso livre. Informe a url (completa) do plano estratégico institucional vigente: _____	X				

Fonte: Elaboração própria (2017).

Relacionado aos processos, de acordo com o quadro 7, a CGE executa e institui parcialmente processo de planejamento estratégico institucional como norma de cumprimento obrigatório, porém adota integralmente a participação da área de TI e das áreas mais relevantes da organização no processo de planejamento estratégico institucional.

Conforme o quadro 7, em relação ao plano estratégico institucional vigente, a organização adota parcialmente esse tipo de plano, instituído pelo seu dirigente máximo, que estabelece de forma parcial as ações consideradas necessárias para o alcance das metas fixadas. Esse plano é constituído de pelo menos um indicador de resultado adotado integralmente para quantificar o cumprimento de cada objetivo estratégico estabelecido e de metas associadas aos indicadores de resultado adotados parcialmente. Apesar de ser em forma parcial, nota-se que há o acompanhamento quanto ao alcance das metas estabelecidas, para correção de desvios é executado parcialmente.

De acordo com o dirigente máximo da CGE, a publicação do plano estratégico institucional vigente não é uma política adotada pela organização, não havendo a disponibilidade de encontrar tal plano na internet para acesso livre.

4.4 Informações

Este tópico de informações visa avaliar o nível de adoção referente à informatização dos processos organizacionais e o acesso a informação e sua divulgação, de acordo com a percepção do dirigente máximo da CGE.

Quadro 8 - Com relação à informatização dos processos organizacionais.

Nível de adoção da prática	Não se aplica	Não adota	Iniciou plano para adotar	Adota parcialmente	Adota integralmente
A organização identifica e mapeia os principais processos de negócio.				**X**	
Os principais processos de negócio da organização são suportados por sistemas informatizados.					**X**
Há catálogo publicado com informações atualizadas de cada um dos sistemas informatizados.			**X**		
A organização designa formalmente responsáveis da área de negócio para a gestão dos respectivos sistemas informatizados.				**X**	

Fonte: Elaboração própria (2017).

Conforme o quadro 8, a organização identifica e mapeia os principais processos de negócio e designa formalmente responsáveis da área de negócio para a gestão dos respectivos sistemas informatizados, ambos são adotados parcialmente. A CGE iniciou um plano para adotar catálogo publicado com informações atualizadas de cada um dos sistemas informatizados, porém a instituição adota de forma integral o fato de que os principais processos de negócio da organização são suportados por sistemas informatizados.

Quadro 9 - Com relação ao acesso a informações e a sua divulgação.

Nível de adoção da prática	Não se aplica	Não adota	Iniciou plano para adotar	Adota parcialmente	Adota integralmente
A organização cataloga as informações de interesse coletivo ou geral por ela produzidas ou custodiadas.					X
A organização publica conjuntos de dados aderentes aos princípios de dados abertos.				X	

Fonte: Elaboração própria (2017).

Na percepção do gestor, conforme quadro 9, a CGE cataloga integralmente as informações de interesse coletivo ou geral por ela produzidas ou custodiadas, e publica conjuntos de dados que aderem parcialmente aos princípios de dados abertos.

4.5 Pessoas

Está parte do questionário, busca avaliar o nível de adoção referente ao desenvolvimento e desempenho de competências de TI dos colaboradores da organização.

Quadro 10 - Com relação ao desenvolvimento de competências de TI.

Nível de adoção da prática	Não se aplica	Não adota	Iniciou plano para adotar	Adota parcialmente	Adota integralmente
A organização define as competências necessárias para o pessoal de TI executar suas atividades.				X	
A organização define critérios para avaliação e atendimento dos pedidos de capacitação.				X	
A organização elabora, periodicamente, plano de capacitação para suprir as necessidades de desenvolvimento de competências de TI.				X	
A organização acompanha a execução do plano de capacitação, com identificação e correção de desvios.				X	

Fonte: Elaboração própria (2017).

De acordo com o Quadro 10, o órgão define parcialmente competências necessárias para o pessoal de TI e critérios para avaliação e atendimento dos pedidos de capacitação, além de elaborar parcialmente planos de capacitação parar suprir necessidades de competências de TI, bem como acompanha parcialmente a execução dos planos de capacitação.

No que diz respeito a adoção parcial relacionados aos itens de capacitação, justifica-se de acordo com a entrevista quando o gestor é questionado sobre quais seriam as dificuldades da implementação de políticas de segurança da informação, ele afirma que a maior é:

> A capacitação de pessoal... por conta de um outro componente inerente a administração pública, que é a questão da rotatividade de pessoal. Existe uma figura desse... do corpo funcional da administração pública que são os servidores comissionados, e os servidores comissionados, sempre que há mudança de governo, como são servidores tidos de confiança do gestor de plantão, normalmente há mudança, há uma rotatividade, então isso gera uma demanda praticamente de quatro em quatro anos, por capacitação.

Quadro 11 - Com relação ao desempenho do pessoal de TI.

Nível de adoção da prática	Não se aplica	Não adota	Iniciou plano para adotar	Adota parcialmente	Adota integralmente
A organização estabelece metas de desempenho para o pessoal de TI.		X			
A organização avalia periodicamente o desempenho do pessoal de TI.				X	
A organização estabelece benefício, financeiro ou não, em função do desempenho alcançado pelo pessoal de TI.				X	

Fonte: Elaboração própria (2017).

Conforme o quadro 11, a organização não adota o estabelecimento de metas para o desempenho do pessoal de TI, porém avalia parcialmente o desempenho do pessoal de TI de forma periódica e estabelece parcialmente benefício, financeiro ou não, em função do desempenho alcançado pelo pessoal de TI.

4.6 Processos

O tópico de processos visa analisar diante da percepção do gestor da organização o nível de adoção relacionado a segurança da informação, contendo questões referente a gestão de riscos de TI e gestão corporativa de segurança da informação.

Quadro 12 - Com relação à gestão de riscos de TI.

Nível de adoção da prática	Não se aplica	Não adota	Iniciou plano para adotar	Adota parcialmente	Adota integralmente
A organização identifica os riscos de TI dos processos críticos de negócio.				X	
A organização avalia os riscos de TI dos processos críticos de negócio.				X	
A organização trata os riscos de TI dos processos críticos de negócio com base em um plano de tratamento de risco.				X	
A organização executa um processo de gestão de riscos de TI.				X	
O processo de gestão de riscos de TI está formalmente instituído como norma de cumprimento obrigatório.				X	

Fonte: Elaboração própria (2017).

De acordo com o quadro 12, os riscos referentes à TI dos processos críticos de negócio da CGE são identificados, avaliados e tratados com base em um plano de tratamento

de risco. Todas essas etapas ocorrem de forma parcial. Além disso, a organização executa um processo de gestão de riscos de TI, que está formalmente instituído como norma de cumprimento obrigatório, sendo esse processo adotado parcialmente.

Quadro 13 - Com relação à gestão corporativa da segurança da informação, parte I.

Nível de adoção da prática Políticas e Responsabilidades	Não se aplica	Não adota	Iniciou plano para adotar	Adota parcialmente	Adota integralmente
A organização dispõe de uma política de segurança da informação formalmente instituída como norma de cumprimento obrigatório.				X	
A organização dispõe de comitê de segurança da informação formalmente instituído, responsável por formular e conduzir diretrizes para a segurança da informação corporativa, composto por representantes de áreas relevantes da organização.				X	
A organização possui gestor de segurança da informação formalmente designado, responsável pelas ações corporativas de segurança da informação.				X	
A organização dispõe de política de controle de acesso à informação e aos recursos e serviços de TI formalmente instituída, como norma de cumprimento obrigatório.				X	
A organização dispõe de política de cópias de segurança (backup) formalmente instituída como norma de cumprimento obrigatório.				X	

Fonte: Elaboração própria (2017).

De acordo com o quadro 13, a CGE dispõe de uma política de segurança da informação parcialmente instituída como norma de cumprimento obrigatório. Quando questionado na entrevista sobre a política de segurança da informação, o gestor afirmou que:

> Sim, nós temos implantados, né, na Controladoria Geral do Estado, parcialmente, uma política de segurança de informação, mas isso está distribuído, essa política está distribuída em vários normativos, em decreto governamental ou em portarias da própria controladoria. Nós estamos fazendo um trabalho visando uniformizar, ou seja, consolidar essa política em um único instrumento, né, de forma que fique mais claro, mais palatável para todos os colaboradores a como devemos nos portar diante de cada ação tomada no que diz respeito a produção de informações e tomada de decisão com base nelas.

A organização dispõe parcialmente de um comitê de segurança da informação e de um gestor de segurança da informação, ambos formalmente instituídos. Além desses itens, a CGE também dispõe de uma política de controle de acesso à informação e aos recursos e serviços de TI, adotada parcialmente.

No último item do quadro 13, o respondente afirma que a organização dispõe parcialmente de uma política de cópias de segurança (backup) formalmente instituída como norma de cumprimento obrigatório.

Quadro 14 - Com relação à gestão corporativa da segurança da informação – parte II (continua)

Nível de adoção da prática Controles e Atividades	Não se aplica	Não adota	Iniciou plano para adotar	Adota parcialmente	Adota integralmente
A organização executa processo de gestão de ativos, assegurando a definição de responsabilidades e a manutenção de inventário dos ativos.				X	
O processo de gestão de ativos está formalmente instituído como norma de cumprimento obrigatório.				X	
A organização executa processo para classificação e tratamento de informações.				X	
O processo para classificação e tratamento de informações está formalmente instituído como norma de cumprimento obrigatório.				X	
A organização implementa controles para garantir a proteção adequada ao grau de confidencialidade de cada classe de informação.				X	
A organização executa processo de gestão de riscos de segurança da informação.				X	
O processo de gestão de riscos de segurança da informação está formalmente instituído como norma de cumprimento obrigatório.				X	
A organização executa processo de gestão de vulnerabilidades técnicas de TI, com objetivo de reduzir o risco de exploração de vulnerabilidades conhecidas.				X	
O processo de gestão de vulnerabilidades técnicas de TI está formalmente instituído como norma de cumprimento obrigatório.				X	
A organização executa processo de monitoramento do uso dos recursos de TI, com objetivo de detectar atividades não autorizadas				X	
O processo de monitoramento do uso dos recursos de TI está formalmente instituído como norma de cumprimento obrigatório.				X	
A organização executa processo de gestão de incidentes de segurança da informação.				X	
O processo de gestão de incidentes de segurança da informação está formalmente instituído como norma de cumprimento obrigatório.				X	

Quadro 14 - Com relação à gestão corporativa da segurança da informação – parte II (conclusão)

Nível de adoção da prática Controles e Atividades	Não se aplica	Não adota	Iniciou plano para adotar	Adota parcialmente	Adota integralmente
A organização possui equipe de tratamento e resposta a incidentes de segurança em redes computacionais, formalmente instituída				X	
A organização realiza, de forma periódica, ações de conscientização, educação e treinamento em segurança da informação para seus colaboradores.				X	
A organização utiliza sistema criptográfico, aderente ao processo de certificação digital da ICP-Brasil, para garantir a autenticidade (autoria e integridade) das informações.	X				

Fonte: Elaboração própria (2017).

De acordo com o quadro 14, a organização executa processo de gestão de ativos, esse processo está formalmente instituído como norma de cumprimento obrigatório, ambos adotados parcialmente, assegurando a definição de responsabilidades e a manutenção de inventário dos ativos.

A organização executa e institui parcialmente, quadro 14, como norma de cumprimento obrigatório, o processo para classificação e tratamento de informações, além disto a CGE implementa parcialmente controles para garantir a proteção adequada ao grau de confidencialidade de cada classe de informação.

A organização executa e instituí parcialmente o processo de gestão de riscos de segurança da informação, como norma de cumprimento obrigatório, além disto executa e instituí parcialmente processo de gestão de vulnerabilidades técnicas de TI, com objetivo de reduzir o risco de exploração de vulnerabilidades conhecidas. Na entrevista o gestor foi questionado se a CGE estava preparada para lidar com riscos, ameaças e vulnerabilidades ele afirmou que:

> Eu diria que sim, a política de segurança da informação da controladoria, eu acho que já tem uma maturidade satisfatória e aí eu acho que também há de se registrar a importância que nós temos algo que nos passe essa tranquilidade, nós temos o apoio logístico da Companhia de Processamento de Dados do Estado, a CODATA, que nos dá todo suporte tecnológico pra você ter uma ideia, até o backup, o backup não e feito local, isso é uma das regras de segurança da informação, o backup de nossas bases de dados não são feitos no espaço físico da controladoria, mas sim na base de dados, ou seja, na sede da Companhia de Processamento de Dados para termos uma certa segurança que se algo acontecer localmente, até, Deus o livre, um incêndio, a gente vai perder o computador, mas não vai perder a informação, que as informações vão estar protegidas em outro ambiente.

A CGE, quadro 14, executa e instituí parcialmente o processo de monitoramento do uso dos recursos de TI, com objetivo de detectar atividades não autorizadas, como norma de cumprimento obrigatório.

Na percepção do gestor, a organização executa e instituí processo de gestão de incidentes de segurança da informação e possui equipe de tratamento e resposta a incidentes de segurança em redes computacionais, ambos adotados parcialmente, como norma de cumprimento obrigatório. Na entrevista foi indagado ao gestor se ele conseguia detectar ações preventivas e corretivas com relação a segurança da informação na CGE, ele afirmou que:

> [...] É importante para isso a gente ter esses antídotos para esses possíveis ataques e ter questão de backup, antivírus atualizado e ter também uma estrutura de TI, que nos permita essa tranquilidade, saber que opa, peraí, aconteceu alguma coisa, mas eu tenho um backup, tenho as pessoas que vão recuperar e não vamos sofrer solução de continuidade em relação a produção da informação ou tomada de decisão com base nela.

Conforme o quadro 14, a organização realiza parcialmente de forma periódica ações de conscientização, educação e treinamento em segurança da informação para seus colaboradores. Na percepção do gestor não se aplica a CGE, a utilização de sistema criptográfico, aderente ao processo de certificação digital da ICP-Brasil, para garantir a autenticidade das informações.

4.7 Implementação de Políticas de Segurança da Informação na Controladoria Geral do Estado da Paraíba

As subseções anteriores apresentaram a análise descritiva do questionário aplicado na Controladoria Geral do Estado da Paraíba, em que se verificou a implementação de políticas de segurança da informação por meio da categorização das áreas de Políticas de Segurança da Informação como seções do questionário.

De acordo com a codificação feita a partir do *software* de análise qualitativa MAXQDA, existem nove codificações para a governança de TI e controle da gestão na CGE, e estas podem ser visualizadas por meio da Figura 3. São elas: a qualidade das informações prestadas, Ações preventivas, as responsabilidades dos funcionários, o conhecimento dos funcionários, a resistência na implementação da Segurança da Informação, os benefícios da implementação da Segurança da Informação, as dificuldades na implementação, a políticas de segurança da informação, e ainda, a percepção do gestor.

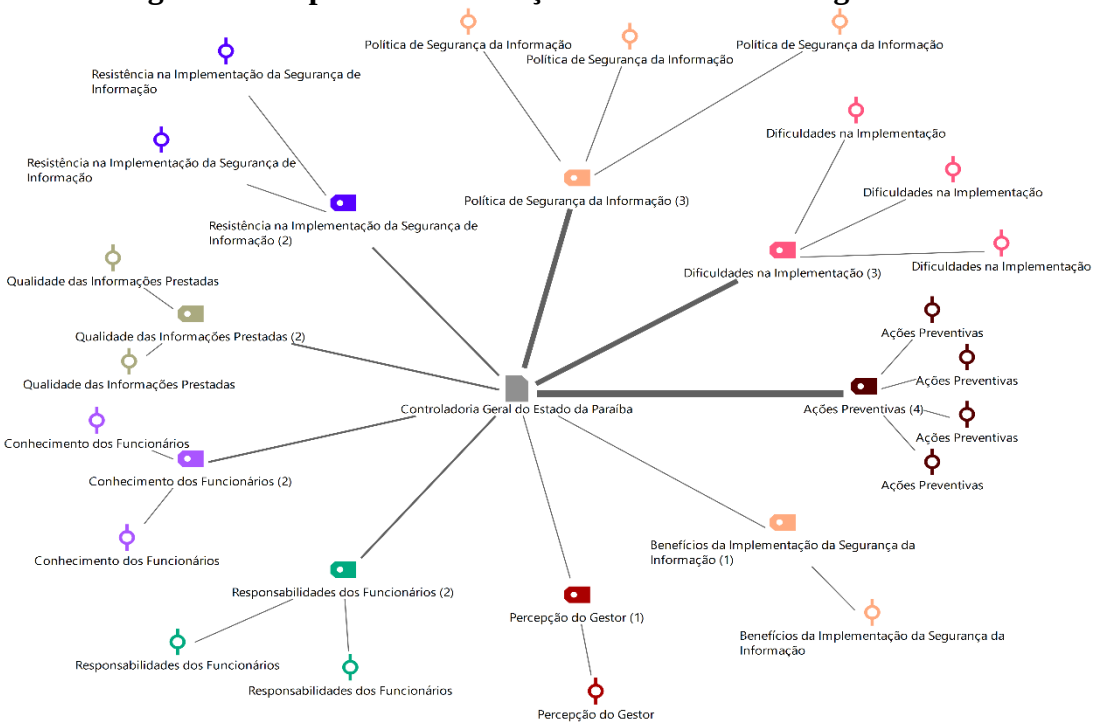
Figura 3 - Frequência dos códigos - "Governança de TI e controle da gestão"

Sistema de Códigos	Controladoria Geral do Estado da Paraíba	SOMA
Governança de TI e Controle Social		0
Ações Preventivas		4
Política de Segurança da Informação		3
Dificuldades na Implementação		3
Responsabilidades dos Funcionários		2
Qualidade das Informações Prestadas		2
Conhecimento dos Funcionários		2
Resistência na Implementação da Segurança de Informação		2
Benefícios da Implementação da Segurança da Informação		1
Percepção do Gestor		1
SOMA	20	20

Fonte: Elaboração Própria (2017)

A governança de TI e controle da Gestão na Controladoria do Estado da Paraíba, também pode ser demonstrada, por meio do mapa gerado a partir das respostas da entrevista, pelo software MAXQDA, como mostra a figura 4.

Figura 4 - Mapa da Governança de TI e controle da gestão na CGE-PB



Fonte: Elaboração Própria (2017)

Pode ser observado através das Figuras 3 e 4, tanto pelo número de frequências apresentados, quanto, pelas linhas mais grossas e escuras nas ligações, que os procedimentos e padrões mínimos adotados para boas práticas de Segurança da Informação na Controladoria Geral do Estado da Paraíba, conforme o gestor, centram-se principalmente nas: Ações

preventivas, políticas de segurança da informação e dificuldades em sua implementação. O quadro 15, apresenta todas essas percepções do gestor da Controladoria Geral do Estado da Paraíba.

Quadro 15 - Principais Desafios da Implementação de Políticas de Segurança na CGE

Ações preventivas	Políticas de segurança da informação	Dificuldades em sua implementação
"Ações preventivas, estruturadas, e tem algumas ações preventivas lúdicas.". "Processo de backup diário."	"A consciência da política da segurança da informação, ela vai dar credibilidade, vai dar robustez, segurança para a própria organização."	"Capacitação de pessoal, posso dizer que é a maior por conta e também por conta de um outro componente inerente a administração pública, que é a questão da rotatividade de pessoal."
"Apoio logístico da Companhia de Processamento de Dados do Estado, a CODATA, que nos dá todo suporte tecnológico. "... "o backup não e feito local, o backup de nossas bases de dados não são feitos no espaço físico da controladoria, mas sim na base de dados, ou seja, na sede da Companhia de Processamento de Dados para termos uma certa segurança que se algo acontecer localmente."	"Parcialmente, uma política de segurança de informação, mas isso está distribuído, essa política está distribuída em vários normativos, em decreto governamental ou em portarias da própria controladoria. Nós estamos fazendo um trabalho visando uniformizar, ou seja, consolidar essa política em um único instrumento".	"Corpo funcional da administração pública que são os servidores comissionados, e os servidores comissionados, sempre que há mudança de governo, como são servidores tidos de confiança do gestor de plantão, normalmente há mudança, há uma rotatividade, então isso gera uma demanda praticamente de quatro em quatro anos, por capacitação. "
"Controlamos esses níveis de acesso através de senha, então tem senhas que permitem acessar informações na sua totalidade, outros só conseguem acessar uma parte da informação ou só consegue executar uma parte da tarefa, Até isso coincide, também, com a própria concepção de controle. "	"Nós temos três gerências, que são as três macros funções da Controladoria Geral do Estado, e cada uma atua no âmbito da sua competência, então assim, a gerência de contabilidade ou a Controladoria Geral do Estado, então, tem a política de segurança da informação. "	"Pela experiência de coordenar as atividades na administração pública, acho que a dificuldade que a gente se depara em sentido maior é conscientizar os servidores públicos, as pessoas, da importância de observar a segurança da informação".
"Ação preventiva é mais em sentido das experiências, das ações que nos trouxeram algum problema no passado, a gente tenta trabalhar para que não tenhamos que conviver com ela no futuro novamente."		

Fonte: Elaboração Própria (2017).

A percepção do gestor da alta administração da organização, sobre o aspecto das ações previstas no papel da segurança da informação, tem como ponto central, o *backup* (cópias de segurança) dos dados, que é feito com o apoio da Companhia de Processamento de

Dados do Estado, a CODATA na base de dados da organização, salvaguardando assim os dados.

Quanto à existência e adoção de políticas segurança da informação na CGE, o gestor, destaca que existe em vários documentos, decretos, separados, porém, sua busca é na consolidação dessas políticas, em um documento específico e uniforme, para toda organização.

No aspecto, das dificuldades de implantação, dos procedimentos ou planos de tratamento que evitem os riscos, ameaças e vulnerabilidades, foi destacado que, um dos obstáculos é a rotatividade de funcionário não efetivos, isto ocorre devido as funções comissionadas, sendo assim, possuindo pouco tempo para consolidar as políticas de segurança. Outro aspecto, é a resistência dos servidores, quanto aos conhecimentos de políticas de segurança da informação, essa questão envolve a cultura organizacional da própria organização.

5 CONSIDERAÇÕES FINAIS

A informação é um ativo relevante que pode trazer grandes impactos para as organizações, e neste cenário de constantes evoluções da tecnologia da informação, os gestores devem buscar sempre aperfeiçoar seus mecanismos de segurança da informação, visando alcançar seus objetivos e proteger suas organizações de riscos, ameaças e vulnerabilidades.

Devido a relevância deste assunto, a presente pesquisa teve como objetivo principal identificar se a CGE-PB dispõe de políticas de segurança da informação, por meio da coleta e análise de dados, é possível afirmar que há uma adoção de políticas de segurança da informação, porém não existe um manual específico com essas políticas, elas estão definidas através de portarias e decretos, porém o gestor afirma que tem uma pretensão futura de consolidar essas políticas de segurança da informação em um único instrumento.

No contexto da percepção sobre a segurança da informação, de acordo com a análise de dados, a alta administração da CGE, acredita que as políticas de segurança da informação são valiosas e necessárias para dar suporte ao processo de tomada de decisão, além de melhorar a comunicação interna e externa da organização.

Com relação aos planos de tratamento de riscos, ameaças e vulnerabilidade, o gestor afirmou ter uma política de segurança da informação, que dispõe de maturidade satisfatória para lidar com o tratamento de riscos, além disso possui um processo de gestão de riscos e incidentes e assegurou ter ações preventivas como backup, antivírus, controle de níveis de acesso através de senha e uma estrutura de TI na organização.

Após a análise de dados é possível afirmar que a maior dificuldade encontrada, para uma boa prática de segurança da informação é a capacitação dos servidores, pois existe uma rotatividade dos servidores públicos, devido a organização dispor de alguns cargos comissionados e quando há mudança de governo pode ser que haja mudança de funcionários, desta forma, tendo que iniciar o processo de capacitação toda vez que houver mudança de funcionários. Além disto, é perceptível outras dificuldades, como, por exemplo, a falta de conhecimento, falta de cultura organizacional relacionada a segurança da informação, desconhecimento dos funcionários as políticas de segurança da informação.

Deste modo, conclui-se que as políticas de segurança da informação que devem ser adotados para boas práticas de Segurança da Informação na CGE-PB são: elaborar de forma integrada e divulgar amplamente dentro da organização um manual contendo as políticas de

segurança da informação e a disponibilizar cursos de capacitação para os servidores, para desenvolver e despertar a cultura de segurança da informação.

Como proposta para novos estudos, recomenda-se elaborar um estudo semelhante comparando os órgãos da esfera municipal e estadual, ou fazer com mais de uma empresa no setor privado, visando apresentar como está o nível de adoção da segurança da informação nas empresas, podendo ampliar também para a percepção dos colaboradores de uma determinada empresa frente a segurança da informação.

REFERÊNCIAS

ALAGOAS. Secretaria de Estado da Fazenda. **Manual de Orientação do SIAFEM**. 2009. Disponível em: <http://www2.sefaz.al.gov.br/legislacao/manual_de_orientacao_do_siafem.pdf>. Acesso em: abr.2017.

ALBANO, Cláudio Sonaglio; REINHARD, Nicolau. **Desafios para governos e sociedade no ecossistema brasileiro de dados governamentais abertos**. Disponível em: <http://bibliotecadigital.fgv.br/ojs/index.php/cgpc/article/view/41150/56628>. Acesso em: abr.2017.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 27002: **Tecnologia da Informação-Técnicas de Segurança – Código de Prática para controles de segurança da informação** – Apresentação. Rio de janeiro, setembro/2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISSO/IEC 38.500**. Governança Corporativa de Tecnologia de Informação. 2009. Disponível em: <http://www.abntcatalogo.com.br/norma.aspx?ID=40015>. Acesso em: abr.2017.

BALTZAN, Paige. **Tecnologia orientada para gestão.** 6. ed. Porto Alegre: AMGH, 2016.

BARDIN, L. **Análise de Conteúdo**. 1.ed. Edições 70-Brasil. 2011.

BEUREN, Ilse Maria (Org.). **Como elaborar trabalhos monográficos em contabilidade: teoria e prática**. 3. ed. São Paulo: Atlas, 2009.

BRASIL, CAMÂRA. **Projeto de Lei n° 5.276/16, 2016**. Disponível em: < http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1457459>. Acessado em: fev. 2017.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 5.276, de 2016**. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378>. Acesso em: abr.2017.

BRASIL. Ministério da Fazenda. **Sistema Integrado de Administração Financeira do Governo Federal – SIAFI**. 2012. Disponível em: <https://manualsiafi.tesouro.fazenda.gov.br/pdf/020000/020800/020801>. Acesso em: abr.2017.

BRASIL. Presidência da República. **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. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/d3505.htm>. Acesso em: abr.2017.

BRASIL. Presidência da República. **Lei nº 12.527, de 18 de Novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5o, no inciso II do § 3o do art. 37 e no § 2o do art. 216 da Constituição Federal; altera a Lei no 8.112, de 11 de dezembro de 1990; revoga a Lei no 11.111, de 5 de maio de 2005, e dispositivos da Lei no 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: abr.2017.

BRASIL. Presidência da República. **Lei Complementar nº 101, de 4 de Maio de 2000**. Estabelece normas de finanças públicas voltadas para a responsabilidade na gestão fiscal e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/LCP/Lcp101.htm>. Acesso em: abr.2017.

BRASIL. Tribunal de Contas da União. **Boas práticas em segurança da informação.** 4. ed. Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2012. Disponível em: <http://www4.planalto.gov.br/cgd/assuntos/publicacoes/2511466.pdf>. Acesso em: abr.2017.

BRASIL, Tribunal de Contas da União. **Perfil de governança de TI – ciclo 2016.** Disponível em < http://portal.tcu.gov.br/comunidades/fiscalizacao-de-tecnologia-da-informacao/atuacao/perfil-de-governanca-de-ti/>. Acesso em: fev. 2017.

BUENO, Ricardo Luiz Pereira; BRELÀZ, Gabriela de; SALINAS, Natasha Schmitt Caccia. **Administração pública brasileira no século 21: seis grandes desafios**. Revista Serviço Público Brasília 67 (Especial) 7-28 2016-7. Disponível em: <https://revista.enap.gov.br/index.php/RSP/article/viewFile/1152/776>. Acesso em: abr.2017.

CARAPETO, Carlos; FONSECA, Fátima. **Administração pública: modernização, qualidade e inovação**. 3. ed. Lisboa: Sílabo, 2014.

CORBARI, Ely Célia; MACEDO, Joel de Jesus. **Gestão pública: planejamento, processos, sistemas de informação e pessoa**. Curitiba: Ibpex, 2011.

FLINK, U. **Introdução à Metodologia de Pesquisa**: **um guia para iniciantes**. Porto Alegre: Pensa, 2013.

FONTES, Eduardo. **Segurança da informação: o usuário faz a diferença**. São Paulo: Saraiva, 2006.

FREY, Márcia Rosane; MARCUZZO, Juliana Luiza; DUMKE, Adalgisa. **Análise do Processo de Transparência na Gestão Orçamentária e Fiscal dos Municípios do Rio Grande do Sul (RS) com mais de 50.000 Habitantes**. XV Convenção de Contabilidade do Rio Grande do Sul. Ago.2015. Bento Gonçalves-RS. Disponível em: <http://www.crcrs.org.br/convencao/arquivos/trabalhos/cientificos/analise_processo_transparencia_gestao_orcamentaria_781.pdf>. Acesso em: abr.2017.

GIL, Antonio Carlos. **Como elaborar projeto de pesquisa.** 4. ed. São Paulo: Atlas, 2009.

GOLD, Alana. **100 Percent of retailers disclose cyber risks — bdo usa report.** Disponível em: < https://www.bdo.com/news/2016-may/100-percent-of-retailers-disclose-cyber-risks#sthash.ZupMFkeC.dpuf >. Acesso em: fev. 2017.

GOODRICH, Michael T.; TAMASSIA, Roberto. **Introdução à segurança de computadores.** Porto Alegre: Bookman, 2013.

KANANE, Roberto; FIEL FILHO, Alécio; Ferreira, Maria das Graças. **Gestão pública: planejamento, processos, sistemas de informação e pessoa**. São Paulo: Atlas, 2010.

KIM, David; SOLOMON, Michael G. **Fundamentos de segurança de sistemas de informação.** Rio de Janeiro: Ltc, 2014.

LAUDON, Kenneth C.; LAUDON, Jane P. **Sistemas de informações gerenciais.** 11. ed. São Paulo: Pearson Education do Brasil, 2014.

LIMA, Helton R. **Controle Externo, Administração Pública e a Transparência Administrativa**. Revista da AGU, Brasília, ano 8, set. 2008. Disponível em: <http://www.escola.agu.gov.br/revista/2008/Ano_VIII_setembro_2008/Controle_externo_Helton.pdf>. Acesso: abr.2017.

MATIAS-PEREIRA, José. **Curso de administração pública: foco nas instituições e ações governamentais**. São Paulo: Atlas, 2008.

MATIAS-PEREIRA, José. **Curso de gestão estratégica na administração pública.** São Paulo: Atlas, 2012.

O'BRIEN, James A. **Sistemas de informação e as decisões gerenciais na era da internet.** 3. ed. São Paulo: Saraiva, 2010.

OKANO, Marcelo Tsuguio et al. **Governança de TI**: **Um panorama acadêmico de artigos nos últimos 20 anos**. XII Simpósio de Excelência em Gestão e Tecnologia. Associação Educacional Dom Bosco. 2014. Disponível em: <http://www.aedb.br/seget/arquivos/artigos16/17124228.pdf>. Acesso em: abr.2017.

OLIVEIRA, K. P.; PAULA, Ana Paula P. **Herbert Simon e os limites do critério de eficiência na nova administração pública**. Cadernos Gestão Pública e Cidadania, São Paulo, v. 19, n. 64, jan./jun. 2014

PARAÍBA, Controladoria Geral do Estado. **Missão.** Disponível em: <http://www.cge.pb.gov.br/site/paginasub/missao.asp>. Acessado em: fev.2017.

PARAÍBA, Controladoria Geral do Estado. **Estrutura**. Disponível em: <http://www.cge.pb.gov.br/site/paginasub/estrutura.asp >. Acessado em: fev. 2017.

SAMPIERI, R. H., COLLADO, C. F., LUCIO, P. B. **Metodologia de Pesquisa.** 5. ed. Porto Alegre: Penso, 2013.

SANTOS, Rodrigo Costa dos; SANTOS, Manuela Fernandes dos; CARREIRA, Fernando Spencer. **Campanha de Conscientização em Segurança da Informação**: **Um Estudo de Caso**. XII Simpósio de Excelência em Gestão e Tecnologia. Associação Educacional Dom Bosco. 2014. Disponível em: < http://www.aedb.br/seget/arquivos/artigos16/382440.pdf>. Acesso em: abr.2017.

SELLTIZ, C. et al. **Métodos de Pesquisa das Relações Sociais**. São Paulo: Herder, 1967.

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

SILVA, Antonio Carlos Ribeiro da. **Metodologia da pesquisa aplicada à contabilidade: orientações de estudo, projetos, artigos, relatórios, monografias, dissertações, teses**. 2. ed. São Paulo: Atlas, 2006.

STEWART, C. J.; CASH JUNIOR, W. B. **Técnicas de entrevista**: **estruturação e dinâmica para entrevistados e entrevistadores**. 14.ed. Porto Alegre: AMGH, 2015.

TRIBUNAL DE CONTAS DA UNIÃO. **Controles na Administração Pública**. Aula 2. Abril.2015. Disponível em: <http://portal.tcu.gov.br/biblioteca-digital/controles-na-administracao-publica-1.htm>. Acesso em: abr.2017.

TRIBUNAL DE CONTAS DA UNIÃO. **Resolução TCU nº 247, de 7 de dezembro de 2011**. Dispõe sobre a Política de Governança de Tecnologia da Informação do Tribunal de Contas da União (PGTI/TCU). Disponível em: <http://portal.tcu.gov.br/comunidades/governanca-de-ti/normas-e-referencias-internas/>. Acesso em: abr.2017.

TURBAN, E; MCLEAN, E; WETHERBE, J. **Tecnologia da informação para gestão**. Transformando os negócios da economia digital. 3°Edição. Porto Alegre. Editora Bookman, 2004.

TURBAN, Efraim; VOLONINO, Linda. **Tecnologia da informação para gestão: em busca do melhor desempenho estratégico operacional**. 8. ed. Porto Alegre: Bookman, 2013.

TURBAN, Efraim; VOLONINO, Linda. **Tecnologia da informação para gestão: transformando os negócios na economia digital**. 3. ed. Porto Alegre: Bookman, 2004.

WEILL, Peter; ROSS, Jeanne W. **Governança de TI, tecnologia da informação.** São Paulo: M. Books, 2006.

YIN RK. **Estudo de caso**: **planejamento e métodos**. Porto Alegre: Bookman, 2010.

VERBI Software. Consult. Sozialforschung. **MAXQDA 12: guia de introdução**. Berlin: GmbH, 2016. Disponível em: <http://www.maxqda.com/wp/wp-content/uploads/sites/2/Getting-Started-Guide-MAXQDA12-ptbr.pdf>. Acesso em: abr.2017.

APÊNDICE A: ENTREVISTA SEMIESTRUTURADA

Isabela: Boa noite, aqui quem fala é Isabela Felix Serafim, realizando uma entrevista para o trabalho de conclusão de curso de Ciências Contábeis da UFPB, tendo como entrevistado Respondente 1, Secretário Chefe da Controladoria Geral do Estado da Paraíba.

Questão 1 - Na sua percepção, descreva a importância das políticas de segurança da informação para a sua organização.

Respondente 1: A segurança da informação para a organização é estritamente valiosa e necessária, porque sem essa política não poderíamos tomar decisões ou fazer uso das informações para tomada de decisão com a certeza de estarmos orientando a gestão pública nas melhores práticas, ou seja, nas melhores tomadas de decisão.

Isabela: A organização dispõe parcialmente de uma política de segurança da informação, assim como foi respondido no questionário. Você tem algum plano de melhoria para essa política? E qual seria esse plano?

Respondente 1: Sim, nós temos implantados, né, na Controladoria Geral do Estado, parcialmente, uma política de segurança de informação, mas isso está distribuído, essa política está distribuída em vários normativos, em decreto governamental ou em portarias da própria controladoria. Nós estamos fazendo um trabalho visando uniformizar, ou seja, consolidar essa política em um único instrumento, né, de forma que fique mais claro, mais palatável para todos os colaboradores a como devemos nos portar diante de cada ação tomada no que diz respeito a produção de informações e tomada de decisão com base nelas.

Isabela: Cite algumas dificuldades encontradas para estabelecer uma política de segurança da informação no órgão público que você trabalha.

Respondente 1: Bom, pela experiência de coordenar as atividades na administração pública, acho que a dificuldade que a gente se depara em sentido maior é conscientizar os servidores públicos, as pessoas, da importância de observar a segurança da informação, eu digo até, por quê? A gente tem, nós tínhamos a foi publicada em 2011 a lei de acesso a informação, e ela disciplina como deve se dar a cessão de informações para o cidadão de uma forma geral, mas, também, nesse próprio texto legal, existem casos que pode-se negar a informação, em função de proteção de sigilo e tal, também, eu... informações estratégicas para o governo, para

administração pública, né? Então essa fase de capacitar, conscientizar os servidores públicos da necessidade de observar a política de segurança de informação, não só a informação como produto, mas, também, a informação sistêmica, ou seja, observar a questão de acessos inadequados ou a alimentação também de sistema de forma inadequada, esse é um dos aspectos.

Isabela: Das dificuldades citadas qual seria a maior e por quê?

Respondente 1: A capacitação de pessoal, posso dizer que é a maior por conta e também por conta de um outro componente inerente a administração pública, que é a questão da rotatividade de pessoal. Existe uma figura desse.do corpo funcional da administração pública que são os servidores comissionados, e os servidores comissionados, sempre que há mudança de governo, como são servidores tidos de confiança do gestor de plantão, normalmente há mudança, há uma rotatividade, então isso gera uma demanda praticamente de quatro em quatro anos, por capacitação.

Isabela: No seu ponto de vista quais os benefícios que a implementação efetiva da segurança da informação pode trazer para a organização?

Respondente 1: Várias, várias, eu começaria dizendo pela própria melhoria da comunicação interna, ou seja, se há uma efetiva consciência da segurança da informação, para o produto, internamente, da organização, eu acho primeiro que tem esse benefício interno, da comunicação interna, e por fim depois os procedimentos, a segurança dos procedimentos, de dar segurança para a tomada de decisão e quando tiver que se relacionar com um público externo, a organização também vai estar mais confortável para esse posicionamento, nesse sentido.

Isabela: Na sua percepção, onde há mais resistência na implementação da segurança da informação, na alta gestão ou entre os demais funcionários?

Respondente 1: Eu não acredito que seja uma resistência, no sentido da implantação da segurança de informação, mas eu atribuiria mais, às vezes, por falta de conhecimento, a falta de cultura organizacional pela segurança da informação, quando se tem essa consciência, aí é mais fácil, logicamente, essa... a adoção dessa prática tem que ser capitaneada pela alta gestão, não dá para você implementar uma política dentro de um órgão, sem a contribuição efetiva da alta gestão. E os demais funcionários e servidores, normalmente seriam inseridos no processo, então eu não vejo como resistência, mas como uma dificuldade essa questão

cultural, eu acho que a gente tem que trabalhar essa questão da importância dessa política para a organização no âmbito interno como também no âmbito externo.

Isabela: E qual seria uma forma para superá-la?

Respondente 1: Capacitação. Capacitação. Eu acho que conscientização faz parte desse contexto. Só para ilustrar, há bem pouco tempo nós tivemos uma demanda de um órgão para averiguar uma questão de um acesso inadequado à base de dados de um órgão que estava com suspeita que poderia ter violado o banco de dados, e aí nós precisamos *startar* a nossa auditoria com especialistas em tecnologia da informação para poder dar um parecer de forma conclusiva, então nesse contexto e após esse trabalho, aí foi aproveitada a oportunidade para trabalharmos a questão da necessidade de se implementar uma política de segurança de informação no órgão em questão. Então é assim que a gente tenta conduzir.

Isabela: Seus subordinados conhecem a política de segurança da informação?

Respondente 1: Eu diria que parcialmente, alguns aqueles que estão na linha, os gerentes, aqueles que, realmente, conduzem o processo, tem uma consciência melhor, mas ainda temos aqueles servidores que não desempenham funções de gerência, e tal, aí eu acho que ainda precisamos trabalhar muito nesse sentido.

Isabela: Existe alguma política adotada definindo responsabilidade aos membros da organização?

Respondente 1: Sim. Existe sim. Em relação a política de segurança da informação, também.

Isabela: Você acha que os funcionários cumprem essa política?

Respondente 1: Se a gente for fazer um levantamento eu creio que encontremos ainda falhas não no sentido de não cumprir, mas por... alguns casos, mas por desconhecer a norma de forma profunda e comete aqueles vícios que a gente só trabalhando a capacitação de forma continuada para superar.

Isabela: Na sua percepção é importante que todos tenham acesso e conhecimentos políticos de segurança da informação?

Respondente 1: importantíssimo.

Isabela: Por quê?

Respondente 1: Como eu falei, eu acho que a consciência da política da segurança da informação, ela vai dar credibilidade, vai dar robustez, segurança para a própria organização.

Isabela: Quais as gerencias compartilham o desenvolvimento de política de segurança da informação na controladoria geral do estado?

Respondente 1: Nós temos três gerências, que são as três macro funções da Controladoria Geral do Estado, e cada uma atua no âmbito da sua competência, então assim, a gerência de contabilidade ou a Controladoria Geral do Estado, então, tem a política de segurança da informação. Basicamente é aquela tutelada no âmbito do Sistema Integrado de Administração Financeira – Siafi – temos a gerência de auditoria, que aí temos um sistemas próprios para a gestão de risco e tal e tomada de decisão sob a ótica da auditoria, também passa por essa política, também tem que ter essa consciência, e ainda temos a questão da gerência, a gestão dessa dívida pública, que aí também tem todo um sistema para gestão de dívida pública que também tem que estar aderente as políticas de segurança e mais com a informação que eles trabalham, a dívida pública consome alguns milhões por ano dos cofres do governo do estado e nós temos que ter confiança e segurança nas informações que consumimos e que produzimos.

Isabela: De que forma envolver todos da organização no que diz respeito ao aperfeiçoamento da segurança da informação?

Respondente 1: Nós trabalhamos, uma forma que a gente entende que é uma maneira de tentar atingir esse objetivo, é fazermos sempre que nós vamos discutir inovações, alterações na política de segurança da informação, nós procuramos sempre reunir os gerentes das áreas envolvidas para discutir a alteração em si, eles já participam da discussão, e aí depois uma vez definido qual vai ser a estratégia a ser adotada, ele fica incumbido de disseminar essa... de difundir esse conhecimento com esse aperfeiçoamento na sua gerência nesse sentido.

Isabela: Você consegue identificar ações preventivas detectáveis e corretivas com relação a segurança da informação na sua organização? Cite algumas.

Respondente 1: Até fazer que tem várias, tem umas assim, ações preventivas, estruturadas, e tem algumas ações preventivas lúdicas, só para exemplificar, certa vez eu cheguei na organização, e uma servidora chegou na minha sala dizendo, ‘ah, respondente 1, aconteceu uma tragédia’. Aí eu disse: ‘o que foi?’. ‘Ah um hacker invadiu a página da controladoria na internet, e tal, está mexendo com os arquivos’. Eu disse: ‘tá, tudo bem’. Aí depois eu mantive

o equilíbrio porque eu sabia que nós tínhamos ações preventivas e ações que me permitiam ter a tranquilidade necessária porque as informações por nós produzidas, elas passam por um processo de backup diário, ai então bom, aí o máximo, de manhã cedo, o máximo, a gente pede esse trabalho de início da manhã de recuperar a base, *startei* o pessoal da gerência de tecnologia da informação, que foram averiguar o que tinha acontecido, na verdade, era a questão de um vírus, e aí descobriram qual era o computador que estava infectado, desconectaram o computador da rede, e aí fizeram o trabalho de saneamento do vírus e aí restabeleceu o backup, e tal, e o processo foi continuado tanto... é importante para isso a gente ter esses antídotos para esses possíveis ataques e ter questão de backup, antivírus atualizado e ter também uma estrutura de TI, que nos permita essa tranquilidade, saber que opa, peraí, aconteceu alguma coisa, mas eu tenho um backup, tenho as pessoas que vão recuperar e não vamos sofrer solução de continuidade em relação a produção da informação ou tomada de decisão com base nela.

Isabela: Qual dessas ações você acha mais eficaz e por quê?

Respondente 1: A mais eficaz, né? Eu não... ficaria difícil dizer que é a mais, mais eficaz, mas assim o que nos dá tranquilidade quando acontece alguma vulnerabilidade é sabermos que temos backup, eu acho que isso nos passa tranquilidade, mas em relação a eficácia é aquela questão de ter cada vez mais, toda vez que acontece um incidente a gente tenta aprimorar os controles no âmbito de proteger a informação, para que essa eventualidade não torne acontecer. Então essa ação preventiva é mais em sentido das experiências, das ações que nos trouxeram algum problema no passado, a gente tenta trabalhar para que não tenhamos que conviver com ela no futuro novamente.

Isabela: As informações estão sujeitas a riscos a ameaças e vulnerabilidades, na sua percepção a organização tem capacidade de lidar através da atual política de segurança da informação de forma eficaz se ocorrer qualquer uma dessas situações?

Respondente 1: Eu diria que sim, a política de segurança da informação da controladoria, eu acho que já tem uma maturidade satisfatória e aí eu acho que também há de se registrar a importância que nós temos algo que nos passe essa tranquilidade, nós temos o apoio logístico da Companhia de Processamento de Dados do Estado, a CODATA, que nos dá todo suporte tecnológico pra você ter uma ideia, até o backup, o backup não e feito local, isso é uma das regras de segurança da informação, o backup de nossas bases de dados não são feitos no espaço físico da controladoria, mas sim na base de dados, ou seja, na sede da Companhia de

Processamento de Dados para termos uma certa segurança que se algo acontecer localmente, até, Deus o livre, um incêndio, a gente vai perder o computador, mas não vai perder a informação, que as informações vão estar protegidas em outro ambiente, tá?

Isabela: Você vê os procedimentos de segurança da informação como uma forma de contribuir para a melhoria da qualidade das informações divulgadas em portais de transparência, por quê?

Respondente 1: Você fez a pergunta que eu venho a bater muito nessa tecla, nós trabalhamos com... temos um grupo, no estado, permanente, que trabalha melhorias, a gente trabalha o ano todo pensando em melhorias de como melhorar a qualidade da informação produzida e disponibilizada no Portal de Transparência do governo, recentemente até dia 9 de dezembro do ano passado nós fizemos uma nova versão do portal e já estamos trabalhando pra 9 de dezembro, Dia Internacional de Combate a Corrupção, então já estamos com essa data pra lançar a nova versão, já estamos trabalhando agora para dia 9 de dezembro termos uma nova versão para lançar e ofertar à sociedade. Então, falar da importância da segurança da informação, como uma contribuição efetiva para melhoria das informações, da qualidade das informações no portal de transparência, para mim isso é fundamental. Eu costumo dizer que não adianta ter um portal de transparência, bonito, com a identidade visual moderna, e quando você vai cruzar as informações, informação de receita, numa consulta dá um valor, em outra dá outro valor, a despesa idem, você não tem uma serie histórica que permita fazer uma avaliação temporal mínima, então eu acho que isso... e inconsistente. Então assim, posso lhe afirmar que as informações disponibilizadas no portal de transparência do governo do estado nós não fazemos para atender uma exigência de lei de responsabilidade fiscal ou do tribunal de contas, ou da lei de acesso a informação. É curioso se você faz uma pesquisa no âmbito do próprio estado, quantos servidores, quantos gestores tomam decisões baseadas nas informações disponibilizadas no portal de transparência, então, ou seja, para tomar uma decisão com base no portal de transparência eu tenho que ter certeza que aquela informação é uma informação válida.

Isabela: As informações para serem consideradas seguras devem atender três princípios básicos, são eles: disponibilidade, a informação é acessível para os usuários autorizados, sempre que as solicitarem; integridade, somente usuários autorizados podem alterar informações; e confidencialidade, somente usuários autorizados podem visualizar a informação. O órgão em que trabalha atende a esses três princípios?

Respondente 1: Sim, nós controlamos esses níveis de acesso através de senha, então tem senhas que permitem acessar informações na sua totalidade, outros só conseguem acessar uma parte da informação ou só consegue executar uma parte da tarefa, Até isso coincide, também, com a própria concepção de controle, o controle a gente costuma dizer que se você quer maximizar controle, em qualquer esfera, então você tem que segregar as ações para que ninguém permita... possa fazer tudo na totalidade de forma que possa tornar vulnerável a informação ou a produção dela. Tá?

Isabela: Na sua percepção de gestor existe algum desses princípios que aplicados a sua organização seja falho e precise de melhoria?

Respondente 1: Por incrível que pareça pode parecer assim, pelo fato de ser o gestor do órgão, eu queira estar dando essa resposta no sentido de melhorar a imagem da organização, mas com toda sinceridade, no âmbito da Controladoria Geral do Estado, esses três princípios estão presentes no nosso dia a dia. As informações, elas tem que estar disponíveis, tem que ser integras e confiáveis. Então isso é uma premissa, afinal de contas nós somos um órgão de controle, né, se nós não tivéssemos essa concepção, esse entendimento, seria ruim até para o desempenho do próprio papel da instituição.

ANEXO A: QUESTIONÁRIO

Pesquisa Acadêmica sobre a Disciplina Sistemas de Informações Contábeis/Tecnologia da Informação

Senhor Secretário Chefe da Controladoria Geral do Estado – CGE /PB,

Esta pesquisa tem por objetivo subsidiar a elaboração do Trabalho de Conclusão de Curso em Ciências Contábeis de Isabela Félix, sob a orientação da Prof. Dr. Tiago Henrique de Souza Echternacht, do Departamento de Finanças e Contabilidade da Universidade Federal da Paraíba.
Todas as informações recebidas serão tratadas com confidencialidade e compromentemo-nos, encaminhar ao final da pesquisa, um resumo do resultado obtido para que V. Sa possa compartilhar conjuntamente deste esforço desenvolvido.
Por oportuno, agradecemos a preciosa colaboração de VSª e colocamo-nos a disposição para outros esclarecimentos que se façam necessários.

Isabela Felix Serafim - isabelafelixserafim@gmail.com
Prof. Tiago Henrique de Souza Echternacht — tiagoechternacht@gmail.com

QUESTIONÁRIO: SEGURANÇA DA INFORMAÇÃO

PARTE I – INFORMAÇÕES GERAIS

1. Caracterização do entrevistado (nome, cargo e função que ocupa; tempo);

1.1 Perfil do Respondente:

1.1.2 Nome: _____

1.1.3 Cargo: _____

1.1.4 Tempo de Trabalho _____

1.2 Função Comissionada

( ) Sim (especificar_____)

( ) Não

1.3 Servidor/Funcionário de carreira?

( ) Sim

( ) Não (especificar_____)

1.4 Familiaridade com o tema Segurança da Informação.

1.4.1 Você já participou de algum evento de capacitação (palestra, seminário, congresso, curso de especialização, mestrado, doutorado etc.) sobre o tema Segurança da Informação?

( ) Sim (especificar _____)

( ) Não

2. Perfil da organização:

2.1 Nome da organização:_____

2.2 Número de servidores/funcionários:_____

2.3 Número total de colaboradores:_____

2.4 Orçamento total anual:_____

2.5. Onde é o principal local de sua organização?

(Marque apenas uma opção)

Local:

2.6 A organização conta com múltiplos locais de trabalho:

( ) Não.

( ) Sim, na mesma cidade.

( ) Sim, em cidades diferentes.

Parte II – Boas Práticas de Segurança da Informação. Governança Corporativa e de TI

1) LIDERANÇA DAALTA ADMINISTRAÇÃO

Com relação ao sistema de governança corporativa:	Nível de adoção da prática				
	Não se aplica	Não adota	Iniciou plano para adotar	Adota parcialmente	Adota integralmente
a. a organização define e comunica formalmente papéis e responsabilidades para a governança corporativa.	○	○	○	○	○
b. a organização dispõe de um comitê de direção estratégica formalmente instituído, que auxilia nas decisões relativas às diretrizes, estratégias, políticas e no acompanhamento da gestão institucional.	○	○	○	○	○
c. a organização realiza avaliações sobre a definição e compreensão dos papéis e responsabilidades organizacionais.	○	○	○	○	○
d. a organização dispõe de um código de ética formalmente instituído, bem como divulga e monitora o seu cumprimento.	○	○	○	○	○
e. a organização dispõe de uma política corporativa de gestão de riscos formalmente instituída como norma de cumprimento obrigatório.	○	○	○	○	○

Com relação ao sistema de governança de TI:	Nível de adoção da prática				
	Não se aplica	Não adota	Iniciou plano para adotar	Adota parcialmente	Adota integralmente
a. a organização define e comunica formalmente papéis e responsabilidades mais relevantes para a governança e a gestão de TI.	○	○	○	○	○
b. a organização dispõe de um comitê de TI formalmente instituído, composto por representantes de áreas relevantes da organização.	○	○	○	○	○
c. o comitê de TI realiza as atividades previstas em seu ato constitutivo.	○	○	○	○	○
d. a organização prioriza as ações de TI com apoio do comitê de TI (ou colegiado equivalente), que atua como instância consultiva da alta administração.	○	○	○	○	○

Com relação aos riscos de TI:	Nível de adoção da prática				
	Não se aplica	Não adota	Iniciou plano para adotar	Adota parcialmente	Adota integralmente
a. a organização define formalmente as diretrizes para gestão dos riscos de TI aos quais o negócio está exposto.	○	○	○	○	○
b. a organização define e comunica formalmente papéis e responsabilidades pela gestão de riscos de TI.	○	○	○	○	○
c. a organização define formalmente os níveis de risco de TI aceitáveis na consecução de seus objetivos (apetite a risco).	○	○	○	○	○
d. a organização toma decisões estratégicas considerando os níveis de risco de TI definidos.	○	○	○	○	○

Com relação ao pessoal de TI:	Nível de adoção da prática				
	Não se aplica	Não adota	Iniciou plano para adotar	Adota parcialmente	Adota integralmente
a. a organização define formalmente diretrizes para garantir o desenvolvimento de competências e a retenção de gestores de TI.	○	○	○	○	○
b. a organização define formalmente diretrizes para garantir o desenvolvimento de competências e a retenção de pessoal técnico de TI.	○	○	○	○	○
c. a organização define formalmente diretrizes para avaliação e incentivo ao desempenho de gestores de TI.	○	○	○	○	○
d. a organização define formalmente diretrizes para avaliação e incentivo ao desempenho de pessoal técnico de TI.	○	○	○	○	○

Com relação ao monitoramento da governança e da gestão de TI:	Nível de adoção da prática				
	Não se aplica	Não adota	Iniciou plano para adotar	Adota parcialmente	Adota integralmente
a. a organização define formalmente diretrizes para avaliação da governança e da gestão de TI.	○	○	○	○	○
b. a organização realiza avaliação periódica de governança e de gestão de TI.	○	○	○	○	○
c. a organização realiza avaliação periódica de sistemas de informação.	○	○	○	○	○
d. a organização realiza avaliação periódica de segurança da informação.	○	○	○	○	○
e. a organização realiza avaliação periódica de contratos de TI.	○	○	○	○	○

Com relação à auditoria interna:	Nível de adoção da prática				
	Não se aplica	Não adota	Iniciou plano para adotar	Adota parcialmente	Adota integralmente
a. a auditoria interna possui pessoal capacitado para avaliar a governança e a gestão de TI. Informe o quantitativo de pessoal da auditoria interna capacitado para avaliar a governança e a gestão de TI: _____	○	○	○	○	○
b. a auditoria interna monitora as ações de governança e de gestão de TI.	○	○	○	○	○
c. a organização aprova, de forma periódica, plano de auditoria que inclua avaliação da governança e da gestão de TI.	○	○	○	○	○
d. a auditoria interna avalia a gestão de riscos de TI.	○	○	○	○	○
e. a auditoria interna avalia os riscos considerados críticos para o negócio e a eficácia dos respectivos controles.	○	○	○	○	○

2) ESTRATÉGIAS E PLANOS

Com relação ao planejamento estratégico institucional:	Nível de adoção da prática				
	Não se aplica	**Não adota**	**Iniciou plano para adotar**	**Adota parcialmente**	**Adota integralmente**
Processo					
a. a organização executa periodicamente **processo** de planejamento estratégico institucional.	○	○	○	○	○
b. o **processo** de planejamento estratégico institucional prevê a participação das áreas mais relevantes da organização.	○	○	○	○	○
c. o **processo** de planejamento estratégico institucional prevê a participação da área de TI.	○	○	○	○	○
d. o **processo** de planejamento estratégico institucional está formalmente instituído como norma de cumprimento obrigatório.	○	○	○	○	○
Plano Vigente					
e. a organização possui **plano** estratégico institucional **vigente**, formalmente instituído pelo seu dirigente máximo.	○	○	○	○	○
f. o **plano** estratégico institucional **vigente** contém pelo menos um indicador de resultado para quantificar o cumprimento de cada objetivo estratégico estabelecido.	○	○	○	○	○
g. o **plano** estratégico institucional **vigente** contém metas associadas aos indicadores de resultado.	○	○	○	○	○
h. o **plano** estratégico institucional **vigente** estabelece as ações (atividades e projetos) consideradas necessárias para o alcance das metas fixadas.	○	○	○	○	○
i. a execução do **plano** estratégico institucional **vigente** é acompanhada periodicamente quanto ao alcance das metas estabelecidas, para correção de desvios.	○	○	○	○	○
j. o **plano** estratégico institucional **vigente** está publicado na internet para acesso livre. Informe a URL (completa) do plano estratégico institucional vigente:	○	○	○	○	○

3) INFORMAÇÕES

Com relação à informatização dos processos organizacionais:	Nível de adoção da prática				
	Não se aplica	Não adota	Iniciou plano para adotar	Adota parcialmente	Adota integralmente
a. a organização identifica e mapeia os principais processos de negócio.	○	○	○	○	○
b. os principais processos de negócio da organização são suportados por sistemas informatizados.	○	○	○	○	○
c. há catálogo publicado com informações atualizadas de cada um dos sistemas informatizados.	○	○	○	○	○
d. a organização designa formalmente responsáveis da área de negócio para a gestão dos respectivos sistemas informatizados.	○	○	○	○	○

Com relação ao acesso a informações e a sua divulgação:	Nível de adoção da prática				
	Não se aplica	Não adota	Iniciou plano para adotar	Adota parcialmente	Adota integralmente
a. a organização cataloga as informações de interesse coletivo ou geral por ela produzidas ou custodiadas.	○	○	○	○	○
b. a organização publica conjuntos de dados aderentes aos princípios de dados abertos.	○	○	○	○	○

4) PESSOAS

Com relação ao desenvolvimento de competências de TI:	Nível de adoção da prática				
	Não se aplica	Não adota	Iniciou plano para adotar	Adota parcialmente	Adota integralmente
a. a organização define as competências necessárias para o pessoal de TI executar suas atividades.	○	○	○	○	○
b. a organização define critérios para avaliação e atendimento dos pedidos de capacitação.	○	○	○	○	○
c. a organização elabora, periodicamente, plano de capacitação para suprir as necessidades de desenvolvimento de competências de TI.	○	○	○	○	○
d. a organização acompanha a execução do plano de capacitação, com identificação e correção de desvios.	○	○	○	○	○

Com relação ao desempenho do pessoal de TI:	Nível de adoção da prática				
	Não se aplica	Não adota	Iniciou plano para adotar	Adota parcialmente	Adota integralmente
a. a organização estabelece metas de desempenho para o pessoal de TI.	○	○	○	○	○
b. a organização avalia periodicamente o desempenho do pessoal de TI.	○	○	○	○	○
c. a organização estabelece benefício, financeiro ou não, em função do desempenho alcançado pelo pessoal de TI.	○	○	○	○	○

5) PROCESSO

Com relação à gestão de riscos de TI:	Nível de adoção da prática				
	Não se aplica	Não adota	Iniciou plano para adotar	Adota parcialmente	Adota integralmente
a. a organização identifica os riscos de TI dos processos críticos de negócio.	○	○	○	○	○
b. a organização avalia os riscos de TI dos processos críticos de negócio.	○	○	○	○	○
c. a organização trata os riscos de TI dos processos críticos de negócio com base em um plano de tratamento de risco.	○	○	○	○	○
d. a organização executa um processo de gestão de riscos de TI.	○	○	○	○	○
e. o processo de gestão de riscos de TI está formalmente instituído como norma de cumprimento obrigatório.	○	○	○	○	○

Com relação à gestão corporativa da segurança da informação:	Nível de adoção da prática				
	Não se aplica	Não adota	Iniciou plano para adotar	Adota parcialmente	Adota integralmente
Políticas e Responsabilidades					
a organização dispõe de uma política de segurança da informação formalmente instituída como norma de cumprimento obrigatório.	○	○	○	○	○
a organização dispõe de comitê de segurança da informação formalmente instituído, responsável por formular e conduzir diretrizes para a segurança da informação corporativa, composto por representantes de áreas relevantes da organização.	○	○	○	○	○
a organização possui gestor de segurança da informação formalmente designado, responsável pelas ações corporativas de segurança da informação.	○	○	○	○	○
a organização dispõe de política de controle de acesso à informação e aos recursos e serviços de TI formalmente instituída, como norma de cumprimento obrigatório.	○	○	○	○	○
a organização dispõe de política de cópias de segurança (backup) formalmente instituída como norma de cumprimento obrigatório.	○	○	○	○	○
Controles e Atividades					
a organização executa processo de gestão de ativos, assegurando a definição de responsabilidades e a manutenção de inventário dos ativos.	○	○	○	○	○
o processo de gestão de ativos está formalmente instituído como norma de cumprimento obrigatório.	○	○	○	○	○
a organização executa processo para classificação e tratamento de informações.	○	○	○	○	○
o processo para classificação e tratamento de informações está formalmente instituído como norma de cumprimento obrigatório.	○	○	○	○	○
a organização implementa controles para garantir a proteção adequada ao grau de confidencialidade de cada classe de informação.	○	○	○	○	○
a organização executa processo de gestão de riscos de segurança da informação.	○	○	○	○	○
o processo de gestão de riscos de segurança da informação está formalmente instituído como norma de cumprimento obrigatório.	○	○	○	○	○
a organização executa processo de gestão de vulnerabilidades técnicas de TI, com objetivo de reduzir o risco de exploração de vulnerabilidades conhecidas.	○	○	○	○	○
o processo de gestão de vulnerabilidades técnicas de TI está formalmente instituído como norma de cumprimento obrigatório.	○	○	○	○	○
a organização executa processo de monitoramento do uso dos recursos de TI, com	○	○	○	○	○

objetivo de detectar atividades não autorizadas.					
o processo de monitoramento do uso dos recursos de TI está formalmente instituído como norma de cumprimento obrigatório.					
a organização executa processo de gestão de incidentes de segurança da informação.					
o processo de gestão de incidentes de segurança da informação está formalmente instituído como norma de cumprimento obrigatório.					
a organização possui equipe de tratamento e resposta a incidentes de segurança em redes computacionais, formalmente instituída.					
a organização realiza, de forma periódica, ações de conscientização, educação e treinamento em segurança da informação para seus colaboradores.					
a organização utiliza sistema criptográfico, aderente ao processo de certificação digital da ICP-Brasil, para garantir a autenticidade (autoria e integridade) das informações.					