UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE EDUCAÇÃO
MESTRADO PROFISSIONAL EM POLÍTICAS PÚBLICAS, GESTÃO E AVALIAÇÃO DA EDUCAÇÃO SUPERIOR

DIEGO CHAVES REINALDO DE SOUZA

SEGURANÇA DA INFORMAÇÃO: UMA METODOLOGIA PARA IMPLANTAÇÃO DE UM SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

JOÃO PESSOA
2020

DIEGO CHAVES REINALDO DE SOUZA

SEGURANÇA DA INFORMAÇÃO: UMA METODOLOGIA PARA IMPLANTAÇÃO DE UM SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Dissertação apresentada ao Programa de Pós-Graduação em Políticas Públicas, Gestão e Avaliação da Educação Superior da Universidade Federal da Paraíba como requisito parcial para obtenção do Título de Mestre.

Linha de Pesquisa: Políticas Públicas e Gestão da Educação Superior.

Orientador: Prof. Dr. Mariano Castro Neto

JOÃO PESSOA - PB

2020

Catalogação na publicação
Seção de Catalogação e Classificação

S729s Souza, Diego Chaves Reinaldo de.
Segurança da informação : uma metodologia para implantação de um sistema de gestão de segurança da informação / Diego Chaves Reinaldo de Souza. - João Pessoa, 2020.
107 f. : il.

Orientação: Mariano Castro Neto.
Dissertação (Mestrado) - UFPB/CE.

1. Segurança da informação. 2. Gestão da informação. 3. Análise de risco. 4. Gestão de segurança da informação. I. Castro Neto, Mariano. II. Título.

UFPB/BC CDU 004.056(043)

Elaborado por Larissa Silva Oliveira de Mesquita - CRB-15/746

DIEGO CHAVES REINALDO DE SOUZA

SEGURANÇA DA INFORMAÇÃO: UMA METODOLOGIA PARA IMPLANTAÇÃO DE UM SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Dissertação apresentada ao Programa de Pós-Graduação em Políticas Públicas, Gestão e Avaliação da Educação Superior da Universidade Federal da Paraíba, como requisito institucional para obtenção do Título de Mestre.

Aprovado em: 10 / 11 / 2020

Banca Examinadora:

Prof. Dr. Mariano Castro Neto – Orientador – MPPGAV/UFPB

Prof. Dr. Alisson Vasconcelos de Brito – Examinador Externo – PPGI/UFPB

Profa. Dra. Maria das Graças G. Vieira Guerra – Examinador Interno – MPPGAV/UFPB

Profa. Dra. Maria da Salete Barboza de Farias - Examinador Interno - MPPGAV/UFPB

AGRADECIMENTOS

Agradeço primeiramente a Deus pela vida, por nos proporcionar sabedoria e por ter me conduzido a este objetivo, a ele seja dado toda honra e toda gloria.

Aos meus pais e irmão, os quais estiveram sempre presentes me proporcionando orientações durante toda minha vida acadêmica e profissional.

Agradeço em especial a minha esposa Iris, pelas contribuições realizadas nesta pesquisa, pela paciência, incentivo, por ser uma mulher incrível e pela ajuda nos momentos difíceis desta caminhada.

Ao professor Dr. Mariano Castro Neto, pela disposição e por todas as orientações concebidas que contribuíram com maestria para a concretização desta pesquisa.

À professora Dra. Maria das Graças G. Vieira Guerra pela aceitação e disponibilidade em participar da banca examinadora e por ter contribuído com os aprimoramentos deste trabalho.

À professora Dra. Maria da Salete Barboza de Farias por ter aceite o convite para participar da banca examinadora e pelos ensinamentos de sala de aula.

Ao professor Prof. Dr. Alisson Vasconcelos de Brito, por aceitar o convite para participar da banca examinadora e pelas valiosas contribuições que engrandeceram enormemente a condução desta pesquisa.

A professora Dra. Maria Angeluce Soares Perônico Barbotin, por ter contribuído na etapa inicial de criação do projeto de pesquisa para seleção deste programa e por me proporcionar novas experiências de vida e profissional.

Ao colega de trabalho Jeruzalém, por todo incentivo e motivação para a realização deste mestrado.

Aos colegas da turma 5, pela amizade, pela troca de conhecimentos em sala de aulas e por todos os momentos vividos.

A todos os professores do MPPGAV.

Muita gratidão a todos vocês.

RESUMO

A segurança da informação é um tema que provoca diversas preocupações nos mais diversos tipos de organizações e entidades governamentais na busca por meios que ofereçam garantias de proteção contra eventuais ameaças a confidencialidade, integridade e disponibilidade dos dados, não somente no ambiente convencional, mas também no tecnológico e na sua rede de comunicação. Esta pesquisa tem como objetivo geral propor um modelo de sistema de gestão de segurança da informação (SGSI) baseado nas normas ABNT NBR ISO 27001 e ABNT NBR ISO 27002, possuindo uma abordagem qualitativa, do tipo exploratória, adotando como meio de informação para compor sua base teórica, a pesquisa documental e bibliográfica. Como instrumento de coleta de dados, foi utilizado o questionário, o qual objetivou identificar as principais ameaças à segurança da informação presente no ambiente de estudo desta pesquisa, bem como avaliar o conhecimento dos colaboradores a respeito da temática. Como parte do processo de análise de risco, foi utilizado o método *Facilitated Risk Analysis and Assessment Process* (FRAAP), uma metodologia desenvolvida através de métodos qualitativos que possui o objetivo de garantir que os riscos relacionados à segurança da informação sejam identificados, documentados e quais controles deverão ser estabelecidos como forma de reduzir os riscos a níveis aceitáveis. Espera-se obter respostas aos problemas inerentes à segurança da informação, sugerindo-se a adoção de uma Sistema de Gestão da Segurança da Informação (SGSI) baseado nas normas ABNT NBR ISO/IEC 27001 e 27002, o qual irá simplificar o processo de planejamento, implantação, análise crítica e modificação do sistema, auxiliando na adoção de um padrão de segurança a ser seguido.

Palavras-chaves: Gestão da informação. Segurança da informação. Análise de risco. Sistema de gestão de segurança da informação.

ABSTRACT

Information security is a topic that raises several concerns in the most diverse types of government organizations and entities in the search for means that offer guarantees of protection against any threats to confidentiality, integrity and availability of data, not only in the conventional environment, but also in the technology and its communication network. This research has as general objective to propose a model of information security management system (ISMS) based on the standards ABNT NBR ISO 27001 and ABNT NBR ISO 27002, having a qualitative approach, of the exploratory type, adopting as a means of information to compose its theoretical basis, documentary and bibliographic research. As a data collection instrument, the questionnaire was used, which aimed to identify the main threats to information security present in the study environment of this research, as well as to evaluate the knowledge of the collaborators regarding the theme. As part of the risk analysis process, the Facilitated Risk Analysis and Assessment Process (FRAAP) method was used, a methodology developed through qualitative methods that aims to ensure that risks related to information security are identified, documented and which controls should be established as a way to reduce risks to acceptable levels. It is expected to obtain answers to the problems inherent to information security, suggesting the adoption of an Information Security Management System (ISMS), based on the ABNT NBR ISO / IEC 27001 and 27002 standards, which will simplify the process of planning, implementation, critical analysis and modification of the system, helping to adopt a safety standard to be followed.

Keywords: Information management. Information security. Risk analysis. Information security management system.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE GRÁFICOS

LISTA DE SIGLAS E ABREVIATURAS

ABNT - Associação Brasileira de Normas Técnicas

APF - Administração Pública Federal

CCAE - Centro de Ciências Aplicadas e Educação

CERT- Centro de Estudos, Resposta e Treinamento de Incidentes de Segurança no Brasil

COBIT – Control Objectives for Information and Related Technology

CONSUNI - Conselho Universitário

DSIC - Departamento de Segurança da informação e Comunicações

FRAAP - Facilitated Risk Analysis And Assessment Process

GSI – Gabinete de Segurança Institucional

ICP – Infraestrutura de Chaves Públicas

IEC - International Electrotechnical Commission

IFES – Instituição Federal de Ensino Superior

ISO - International Standartization Organization

LAI - Lei de Acesso à Informação

LGPD – Lei Geral de Proteção de Dados

MEC - Ministério da Educação e Cultura

NBR - Norma Brasileira

MPPGAV - Mestrado Profissional em Políticas Públicas, Gestão e Avaliação da Educação Superior

PDCA – Plan, Do, Check, ACT (Planejar, Fazer, Checar, Agir)

PNSI - Política Nacional de Segurança da Informação

PSI - Política de Segurança da Informação

SGSI - Sistema de Gestão de Segurança da Informação

TI - Tecnologia da Informação

TIC - Tecnologia da Informação e Comunicação

TCU - Tribunal de Contas da União

UFPB - Universidade Federal da Paraíba

SUMÁRIO

1. INTRODUÇÃO

O avanço da tecnologia, o surgimento dos computadores, bem como a expansão da área de abrangência da Internet, Rede Mundial De Computadores, gerou mudanças na forma e desenvolvimento da informação, propiciando maior rapidez, aumento e eficiência na transmissão de dados, fazendo com que esta seja capaz de se propagar em alta velocidade.

Segundo Marciano e Marques (2006), devido às facilidades e benefícios, a sociedade passou a se tornar cada vez mais dependente dos computadores e das redes, surgindo assim diversos tipos de ameaças física, virtuais e humanas, que passaram a comprometer a segurança das pessoas e das informações.

Independentemente do tipo, segmento e porte das organizações, quer sejam elas públicas ou privadas, a informação tornou-se um capital precioso, fundamental na tomada de decisões, sendo vista como um recurso estratégico primordial ao desenvolvimento organizacional e por isto é um ativo que está constantemente sofrendo ameaças**.** O seu roubo ou sua perda pode acarretar prejuízos imensuráveis, colocando em risco as atividades do negócio (CHOO, 2003).

Desta forma, a preocupação em torno da segurança da informação propagada entre usuários conectados em redes de comunicação, fez surgir à definição de procedimentos, normas ou regras e a criação de sistemas, que tenham por objetivo regular meios no qual se deve agir diante dos recursos que tratam informações.

Neste sentido, às Instituições Públicas Federais passaram a regulamentar os procedimentos que devem ser realizados visando à segurança da informação, sendo orientadas por normas, leis e decretos elaborados pelo Governo Federal que possuem o objetivo de preservar a informação, abrangendo recursos computacionais, físicos e humanos.

Para Caruso e Steffen (2013), o valor da informação para uma organização torna-se superior aos seus produtos e serviços, não sendo o seu resultado final o bem mais valioso, mas sim, as informações relacionadas à forma como se chegou a este resultado, portanto é necessário protegê-la.

Assim, definir meios de gestão da segurança da informação é um fator fundamental que deve estar presente no processo de desenvolvimento institucional das organizações, pois elas estão inseridas em um cenário informacional e de fluxo

informacional, onde a todo o momento são produtoras, receptoras de dados, informações e conhecimentos que são disseminados aos tomadores de decisão (CAVALCANTE, 2009).

Neste cenário de evolução, estabelecer procedimentos de gestão da segurança da informação, é um desafio que precisa ser definido prioritariamente para o meio corporativo.

A interrupção de um negócio poderá ser ocasionada por diversos fatores que representam riscos para a segurança da informação, como o furto de equipamentos, desastres naturais ou ataques, os quais podem ocasionar prejuízos imensuráveis, portanto, é fundamental que as organizações definam estratégias de gestão da segurança da informação com o objetivo de estabelecer métodos contra eventuais ameaças que apresentem risco ao funcionamento do negócio.

Entretanto, vale ressaltar que, para que um negócio seja interrompido, não necessariamente precisa ocorrer alguma das ameaças acima citadas, basta que um funcionário mal intencionado ou que não tenha conhecimento suficiente sobre boas práticas em segurança da informação, realize alguma ação que venha a provocar falhas de segurança (CHOO, 2003).

Neste sentido, o elemento humano é um fator de extrema importância no processo de gestão da informação, pois mesmo que os controles de segurança tecnológica apresentem forte eficácia contra os riscos provocados pela internet, é necessário que os usuários cooperem para se alcançar o nível de segurança desejado. A organização deve ser responsável por estabelecer programas de conscientização ou caso contrário, aqueles que desconhecem os controles a serem seguidos no ambiente organizacional tornam-se pontos fracos, podendo ocasionar incidentes de segurança (FONTES, 2006).

Vários são os tipos de incidentes que ocorrem diariamente em todo o mundo, provocando diversas ameaças a informação, como fraudes financeiras, ataques de vírus, invasão de sistemas e roubo de identidade.

Segundo o relatório global publicado em 2019 pela empresa de cibersegurança Symantec, o Brasil é o terceiro pais que mais recebe ataques cibernéticos em dispositivos conectados à internet, ficando atrás apenas de países como a China, que ocupa o primeiro lugar e os Estados Unidos, em segundo. O relatório indica que de 2017 a 2018, o Brasil saiu da sétima para a terceira posição no ranking no principal

índice de segurança digital, e há anos na América Latina e Caribe lidera o primeiro lugar (SYMANTEC, 2019).

A empresa Kapersky Lab, indica que, no Brasil os crimes cibernéticos têm afetado cerca de 62 milhões de pessoas, ocasionando um prejuízo em torno de US$ 22 bilhões, perdendo apenas para a China, que obteve em 2018 US$ 66.3 bilhões. Outro dado alarmante é que, em pesquisas realizadas, a empresa afirma que um terço da população brasileira não sabe como proteger a sua privacidade e os seus dados online (KAPERSKY, 2019).

A partir dos fatos mencionados e compreendendo o valor e a importância que a informação representa para as organizações, esta pesquisa tem o objetivo de propor um modelo de sistema de gestão de segurança da informação (SGSI) baseado nas normas ABNT NBR ISO 27001 e ABNT NBR ISO 27002 para o Centro de Ciências Aplicadas e Educação (CCAE) da Universidade Federal da Paraíba (UFPB).

O processo de gestão da informação compreende as etapas do planejamento, execução e monitoramento das atividades relacionadas à segurança da informação, bem como a implementação de processos de melhoria contínua (MANOEL, 2014).

Deverá ser realizada uma análise dos riscos existentes no processo de gestão da informação nos ambientes que tratam com os mais variados tipos de informações, identificando as principais ameaças e controles que deverão ser estabelecidos, com o intuito de propor um Sistema de Gestão de Segurança da Informação (SGSI), o qual defina processos e procedimentos, de acordo com normas e legislação, para que a organização possa prover meios de segurança no uso dos ativos tecnológicos que lidam com informação.

1.2 ORIGEM DO TRABALHO

O foco desse estudo está centrado no CCAE, Campus IV da UFPB. Suas motivações estão relacionadas a observações empíricas do pesquisador, que atua como técnico de informática na UFPB, no setor de Gerência de Tecnologia da Informação e Comunicação, onde através das experiências vivenciadas no cotidiano profissional, pôde sentir a necessidade de realizar um estudo sobre a gestão de segurança da informação no referido centro, identificando as ameaças, os riscos existentes e propor um Sistema de Gestão de Segurança da Informação (SGSI) que venha garantir a

confidencialidade, integridade e disponibilidade dos dados, princípios fundamentais da segurança da informação.

A pesquisa em pauta objetiva proporcionar uma visão abrangente sobre a importância que a gestão da informação representa para uma organização e apresentar uma abordagem proativa referente à como se estabelecer processos que visem assegurar a proteção destas informações em um cenário complexo que é a modernização da sociedade.

Entende-se que a definição de métodos, que estabeleça a gestão da segurança da informação, dado o avanço informacional e a importância que as informações exercem sobre a sociedade, é condição essencial para que qualquer tipo de organização possa desenvolver suas atividades e seus objetivos, uma vez que sua implementação irá minimizar a exposição aos riscos e ameaças existentes.

1.3 PROBLEMATIZAÇÃO

A informação agrega um valor para a organização baseado no seu grau de importância e na influência que exerce sobre os processos e operações, e por isto, é um ativo que desperta o interesse de pessoas mal-intencionadas que desejam obter algum tipo de vantagem, explorando falhas e vulnerabilidades no seu acesso (Nakamura, 2007).

Definir meios que gerencie e ofereça segurança à informação, implica em atingir a perspectiva de negócio de forma que contemple as necessidades informacionais, integrando as atividades e recursos disponíveis, com o intuito de facilitar a obtenção do alcance da missão e dos objetivos institucionais.

Instituições educacionais como a UFPB, a todo o momento são alvos frequentes de ameaças que podem causar a violação dos seus dados e gerar grandes prejuízos, tanto as informações confidenciais, como a imagem da instituição.

Desta forma, as instituições de ensino, assim como qualquer outro tipo de organização, possui a necessidade de proteger suas informações e seus recursos tecnológicos informacionais que precisam ser satisfeitas, como a proteção dos servidores, regulamentação do acesso dos alunos aos computadores, senhas utilizadas, equipamentos eletrônicos e também as especificidades de cada setor presente na estrutura organizacional. E difícil imaginar o tamanho da gravidade caso ocorra à perda

de todas as informações relativas aos seus clientes, alunos, funcionários, fornecedores ou o registro funcional dos colaboradores.

A Universidade é composta por uma diversidade muito grande de ambientes, onde cada qual possui suas particularidades, existindo áreas administrativas que não devem ser acessadas por docentes ou por alunos e outras onde ocorre um grande fluxo de usuários, que ao não serem monitorados, podem trazer sérios riscos à segurança institucional.

A partir dessas discussões e atento às transformações tecnológicas referentes à segurança da informação, se problematizou acerca da necessidade de investigar as implicações que as ameaças à segurança da informação e o processo de gestão de segurança da informação podem refletir para uma instituição de ensino superior.

Neste sentido optou-se por iniciar a investigação a partir do seguinte questionamento: Como elaborar uma metodologia para implantação de um sistema de gestão para a segurança da informação no Centro de Ciências Aplicas e Educação da Universidade Federal da Paraíba?

1.4 OBJETIVOS

Na busca de respostas para essas questões definiram-se os objetivos gerais e específicos, que concretizam a finalidade deste estudo.

1.4.1 OBJETIVO GERAL

- ✓ Apresentar uma metodologia para implantação de um sistema de gestão de segurança da informação (SGSI) baseado nas normas ABNT NBR ISO 27001 e ABNT NBR ISO 27002.

1.4.2 OBJETIVO ESPECÍFICO

- ✓ Identificar as ameaças e os riscos a gestão da segurança da informação;
- ✓ Realizar uma análise de risco com foco na segurança da informação;
- ✓ Identificar o nível de conhecimento dos colaboradores acerca dos procedimentos relacionados à segurança da informação.

1.5 JUSTIFICATIVA

Estabelecer meios de gestão da informação nas organizações é uma necessidade que deve ser vista de forma estratégica, pois é primordial para a obtenção do sucesso, das oportunidades e das vantagens competitivas. A administração informacional, bem como os seus fluxos, representa uma atividade que está cada vez mais ganhando evidência em qualquer tipo de negócio.

O alto volume de informação que a todo o momento é criado, armazenado, processado e enviado por diferentes meios, torna evidente a necessidade de possuir um meio de gestão de segurança da informação eficaz e que ofereça garantias, sejam elas físicas ou tecnológicas.

A relevância acadêmica desta pesquisa justifica-se na perspectiva de fornecer uma análise dos riscos à segurança da informação presente no CCAE, compreender o nível de conhecimento dos colaboradores sobre o referido tema, visto que o elemento humano constitui-se como primordial no processo de gestão da informação em ambientes organizacionais e apresentar uma metodologia para implementação de um sistema de gestão de segurança da informação.

Novos elementos serão apresentados para compor uma proposta de metodologia para implantação de um SGSI, tomando-se como base os principais padrões e normas de segurança, que definem um conjunto de diretrizes as quais devem nortear o processo de Gestão de Segurança da Informação no ambiente corporativo. O processo de adoção do SGSI possui como objetivo realizar a padronização e documentação dos procedimentos, ferramentas e técnicas utilizadas, além da criação de indicadores, registros e a definição de um processo educacional de conscientização da organização e seus colaboradores.

Deste modo, justifica-se a importância desta pesquisa, bem como sua pertinência, pois a implantação de um SGSI na organização irá permitir ao usuário tomar conhecimento sobre os meios de proteção e segurança que são aplicados à informação. Para os profissionais técnicos, a existência de um SGSI irá permitir seguir um modelo de atuação em comum, evitando desta forma a adoção de um padrão não definido entre diferentes equipes, pois a contribuição dessa metodologia irá permitir desenvolver um projeto de segurança o qual deverá contribuir para uma visão única do sistema de segurança e dos diversos padrões e métodos que o compõem.

1.6 ADERÊNCIA DO TEMA DA PESQUISA COM O PROGRAMA

O Mestrado Profissional em Políticas Públicas, Gestão e Avaliação da Educação Superior (MPPGAV) do Centro de Educação da UFPB, possui o objetivo de preparar os servidores técnicos administrativos das Instituições Federal de Ensino Superior (IFES) do Estado da Paraíba, de modo a desenvolver reflexões críticas, produção e criação de projetos de inovação socialmente relevantes, apresentando novas formas de gestão, e tecnologias administrativas capazes de responder aos desafios da governança pública.

Nessa perspectiva, o presente estudo tem aderência especificamente à linha de pesquisa sobre Políticas Públicas e Gestão da Educação Superior, ao apresentar propostas de estudos sobre a gestão de segurança da informação no CCAE, realizando a pesquisa de fatores que implicam diretamente na segurança da informação das atividades desenvolvidas pelos colaboradores da referida unidade e apresentando metodologias que venham contribuir na melhoria dos problemas existentes.

1.7 ESTRUTURA DOS CAPÍTULOS

Na introdução, primeiro capítulo, apresenta-se a origem deste estudo e sua problematização. Objetivos geral e específicos, justificava e aderência do tema da pesquisa ao MPPGAV e linha de pesquisa e estrutura dos capítulos.

A segunda seção trata sobre a segurança da informação, discutindo aspectos relacionados à gestão da segurança da informação, expondo dados estáticos sobre a relevância deste tema, como também os princípios que servem como base para a implantação da segurança, as ameaças, os tipos de ataques mais comuns, vulnerabilidades, política de segurança da informação, as leis, normas e decretos existentes sobre a gestão da segurança da informação na Administração Pública Federal (APF).

O percurso metodológico, presente na terceira seção, é composto pela caracterização da pesquisa, campo de pesquisa, objeto de estudo, sujeitos da pesquisa e os procedimentos de coleta e análise dos dados.

A quarta seção apresenta o processo de análise de riscos que foi realizado após análise dos dados coletados através dos questionários.

O modelo de sistema de gestão da segurança da informação, encontra-se na quinta seção, onde é definido uma visão geral e suas fases de implantação.

Por fim, as Considerações Finais, Referências, Apêndices e Anexos.

2. SEGURANÇA DA INFORMAÇÃO

No decorrer dos anos, a informação vem se caracterizando quase que em sua totalidade em formato digital. Os sistemas digitais foram tão ampliados que as organizações passaram a ter sua base de funcionamento dependente de tecnologias. Por outro lado, a dependência do mundo tecnológico veio acompanhada de diversos fatores como furto, a perda ou alterações de informações, que colocaram em evidência o tema de segurança da informação (CÔRTES, 2008).

Conforme Silva e Stein (2007), a segurança da informação se tornou um elemento de destaque na sociedade moderna, onde todos desejam que seus dados pessoais não sejam violados e que somente as pessoas autorizadas consigam obter acesso.

Este cenário contemporâneo se apresenta como a era da *big* data, onde a todo o momento o alto volume de informações é criado, processado, armazenado e compartilhado entre vários tipos de entidades (SÊMOLA, 2014). Assim, é indispensável que as Instituições de Ensino Superior, enquanto disseminadoras do conhecimento e responsáveis pelo patrimônio documental, definam meios que gerencie a segurança das suas informações.

O reconhecimento do valor que as informações representam para as organizações é universalmente aceito e considerado um dos recursos mais importante e fundamental para o seu sucesso (MORESI, 200). Portanto, a informação é um fator estruturante e um instrumento de gestão para as organizações, a qual necessita ser devidamente protegida.

Segundo Davenport (1998), “grandes volumes de informação entram e saem das organizações sem que ninguém tenha plena consciência de seu impacto, valor ou custo”. Desta forma, o gerenciamento da informação e a adoção de estratégias de segurança, são fundamentais para a obtenção do sucesso e garantias das vantagens competitivas.

Fontes (2006) afirma que, a segurança da informação objetiva minimizar os riscos do negócio quanto ao uso dos recursos de informação presentes na organização, com o intuito de evitar perdas que comprometam seu funcionamento.

Já a norma (ABNT NBR ISO 27002:2013) define a segurança da informação como “a preservação da confidencialidade, da integridade e da disponibilidade da informação", os considerando como os três principais pilares fundamentais da segurança

da informação. Outras propriedades como autenticidade, responsabilidade, não repúdio e confiabilidade são aspectos de segurança, derivados dos pilares principais.

Na visão de Sêmola (2014), a segurança da informação é “uma área do conhecimento dedicada à proteção de ativos da informação contra acesso não autorizado, alterações indevidas ou sua indisponibilidade”. Sêmola define que ativo informacional, pode ser compreendido como tudo aquilo que manipula direta ou indiretamente a informação. Por sua vez a norma ABNT NBR ISO 27002 considera que ativos, “são objeto de ameaças, tanto acidentais como deliberadas, enquanto que os processos, sistemas, redes e pessoas têm vulnerabilidades inerentes”.

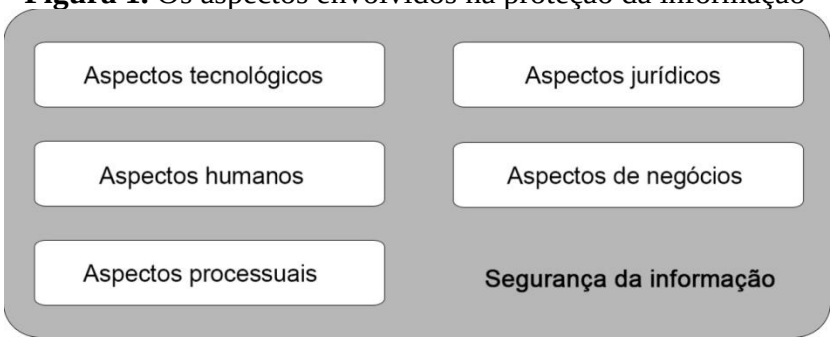
Anderson (2003) vai mais além ao afirmar que os conceitos sobre segurança da informação, em sua maioria, “apresentam as atribuições ou resultados esperados pela aplicação da segurança da informação” e define seu próprio conceito como sendo: “Um sentimento bem fundamentado da garantia de que os controles e riscos da informação estão bem equilibrados”.

Devido a sua importância, a segurança da informação é um tema multidisciplinar que deve envolver várias áreas de uma organização, como segurança em recursos humanos, controle organizacional, segurança física, controles técnicos, conformidade com leis e regulamentos e aspectos relativos à continuidade de negócio. Isto significa que uma única área ou departamento, dificilmente possui todo o conhecimento necessário à sua gestão.

Desta forma, a segurança da informação não deve ser compreendida como um objetivo em si, mas como um meio para a organização atingir seus objetivos estratégicos, sendo importante para os negócios, tanto do setor privado como do setor público, com o objetivo de evitar ou reduzir os riscos relevantes.

Nakamura (2007) enfatiza que o viés tecnológico é essencial para a proteção da informação, porém, reforça que outros elementos devem ser levados em consideração, como o fator humano e processual de uma organização, afirmando que ataques não tecnológicos podem comprometer o nível da segurança organizacional. Outros aspectos como o jurídico e de negócio, representados na figura 1, também devem ser envolvidos na proteção da informação.

Figura 1. Os aspectos envolvidos na proteção da informação



Fonte: Nakamura (2007, p. 30)

Dentre os aspectos citados, Santos (2011) destaca que o fator humano é a principal ameaça a qualquer tipo de segurança, pois todo o processo se inicia e termina com o usuário do sistema. Santos, enfatiza ainda que este é o elo mais fraco da corrente em um processo que envolve segurança da informação nas organizações.

A gestão da segurança da informação define três categorias fundamentais que norteiam seus procedimentos: Pessoas, Processos e Tecnologia. A tecnologia é fundamental, porém é incapaz de evitar todos os problemas caso não exista processos definidos, estudo de vulnerabilidades e a participação dos colaboradores, objetivando manter o ambiente seguro. Mitnick e Simon (2003) afirmam que "aqueles que acham que os produtos de segurança sozinhos oferecem a verdadeira segurança estão fadados a sofrer da ilusão da segurança". Reforçam ainda que, a segurança não deve ser vista como um problema para a tecnologia, mas sim para as pessoas e a direção.

Para que as organizações consigam alcançar o sucesso em segurança informacional, elas deverão investir tanto em técnicas, como nos recursos sócio-organizacional (CHOO, 2003). O viés tecnológico encontra-se sempre mais presente, devido às soluções tecnológicas que tratam do tema, mas é necessário incluir o aspecto humano como um grande elemento que precisa ser conquistado.

Neste sentido, nota-se que o Governo Federal vem realizando esforços na tentativa de enfrentar os desafios que o mundo globalizado e interconectado impõe, publicando leis, normas e decretos que objetivam lançar estratégias de segurança da informação, na tentativa de combater as ameaças e diminuir os riscos que a infraestrutura de tecnologia da informação e comunicação está exposta. Para o Governo Federal Brasileiro, a segurança da informação é definida como:

> [...] a 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).

Desta forma, foi criada a Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal (APF) 2015-2018, versão 1.0, complementando a Instrução Normativa GSI/PR nº 01/2008, com o objetivo de contemplar aspectos referentes à segurança da informação no cenário atual, nacional e mundial (BRASIL, 2015).

O Decreto nº 9.637, de 26 de Dezembro de 2018, institui a Política Nacional de Segurança da Informação (PNSI) no âmbito da APF, com o objetivo de promover a defesa cibernética e a proteção dos dados organizacionais na administração pública e define no seu Art. 4º os objetivos da PNSI: "[...] IV – fomentar a formação e a qualificação dos recursos humanos necessários à área de segurança da informação [...]". O Art. 12º apresenta que é de competência do Gabinete de Segurança Institucional da Presidência da República, para os fins deste decreto: "[...] III – elaborar e implementar programas sobre segurança da informação destinados à conscientização e à capacitação dos servidores públicos federais e da sociedade [...]".

A Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na APF, direta e indireta, por sua vez apresenta que:

> Art. 3º Ao Gabinete de Segurança Institucional da Presidência da República – GSI, por intermédio do Departamento de Segurança da informação e Comunicações – DSIC, compete:
> IV – Elaborar e implementar programas destinados à conscientização e a capacitação dos recursos humanos em segurança da informação e comunicações (Instrução Normativa GSI/PR nº1, 2008).

Desta forma, fica evidente a importância que o fator humano exerce nesse processo, onde mesmo que sejam desenvolvidas melhores tecnologias de segurança, as fragilidades serão cada vez mais voltadas para o elemento humano.

Neste sentido, a segurança da informação passou a ter uma abordagem necessária tanto na iniciativa privada, como na administração pública, sendo um elemento necessário que deve estar presente em todo o fluxo informacional, como

forma de garantir a proteção da informação de acordo com os requisitos de sigilo, integridade, autenticidade, disponibilidade e irretratabilidade da comunicação (BEAL, 2005).

Desta forma, observa-se que a informação ocupa um lugar de destaque nas organizações, sendo caracterizada como um recurso estratégico necessário para o desenvolvimento organizacional e mesmo que esteja atualmente com maior presença nos ambientes tecnológicos, sua manipulação é realizada pelas pessoas e sua segurança se processa por meios destas em ambiente convencional.

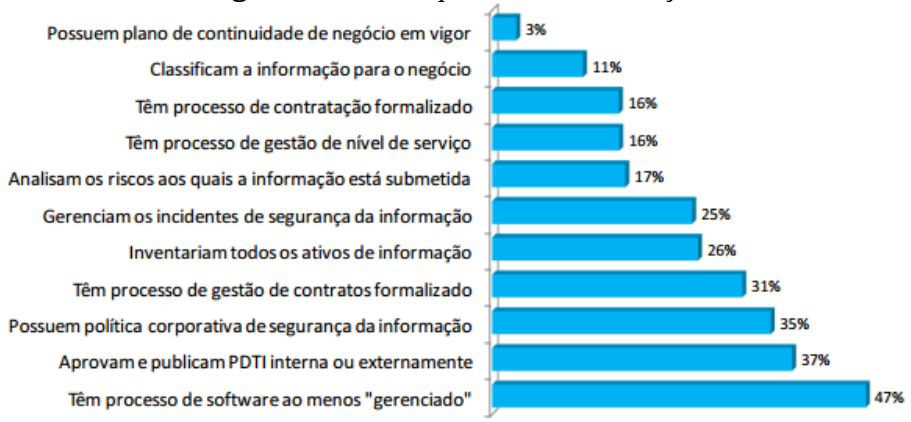
Apesar do processo de gestão e segurança da informação não estar limitado a aspectos da tecnologia, as fragilidades, riscos e ameaças à segurança podem ser decorrentes também de falhas encontradas na governança do ambiente de tecnologia da informação (TI). Neste sentido, o Tribunal de Contas da União (TCU), a partir de 2007 passou a realizar levantamentos, através de questionários, que possuem o objetivo de avaliar a situação da governança de TI nos órgãos da APF, estabelecendo-se como base a regulamentação existente em leis, normas técnicas, regulamentos e modelos de boas práticas.

No primeiro levantamento, ocorrido em 2007, participaram 255 órgãos da APF, onde através de questionários contendo 39 perguntas, elaboradas com base na norma 17799:2005, revelou um cenário preocupante quanto à governança de TI e a segurança da informação. Diante da situação exposta, o TCU (2012) através do Acórdão 1.603/2008-TCU-Plenário, determinou que novos levantamentos fossem realizados nos anos seguintes, ocorrendo em 2010, 2012, 2014 e 2016, se utilizando, como base para a elaboração dos questionários, a ABNT NBR ISO 27002 (substituta da 1779:2005) a qual estabelece critérios mais abrangentes.

O levantamento realizado em 2010, apreciado pelo Acórdão 2.308/2010-TCU-Plenário, foi baseado em um questionário contendo 30 questões e 152 subquestões, contando com 256 respondentes e abrangeu 301 organizações. O objetivo seria identificar os pontos mais vulneráveis na governança de TI da APF e identificar bons exemplos e modelos para serem divulgados. Esta pesquisa revelou alguns temas que merecem atenção, destacando índices relativos à gestão da informação, onde apenas 35% afirmaram que a instituição possui alguma política corporativa de segurança da informação, 26% realizam algum tipo de inventário dos ativos de informação, 25%

gerenciam os incidentes de segurança da informação e que apenas 17% analisam os riscos aos quais as informações estão submetidas, como pode ser observado na figura 2.

Figura 2. Temas que merecem atenção

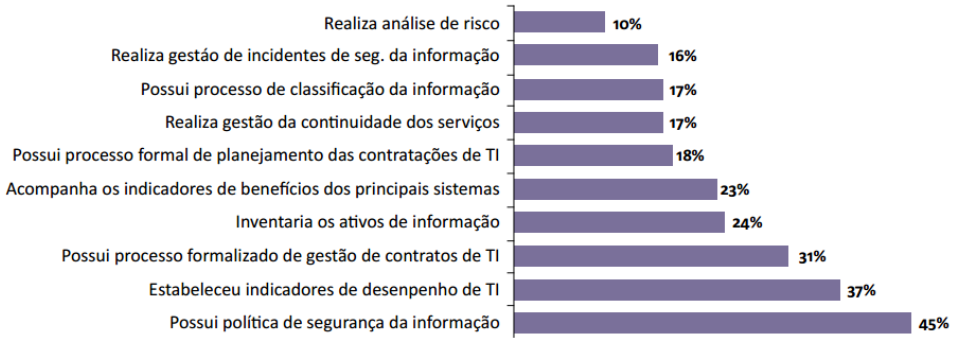


Fonte: TCU (2010)

Desta forma, o levantamento realizado em 2010 concluiu que não houve melhorias em relação aos indicadores de segurança da informação, quando comparados com os índices apresentados em 2007 e que 57% das instituições encontram-se em escala inicial no processo de governança de TI, 38% em nível intermediário e apenas 5% em estágio avançado.

Em 2012, o objetivo do levantamento, resultado do Acórdão 2.585/2012-TCU-Plenário, foi manter os dados atualizados em relação à Governança de TI na APF, observando os avanços ou retrocessos em comparação com os índices apresentados em 2010. Foram avaliadas 349 organizações, seguindo como referência o modelo de gestão COBIT 5, o qual esclarece a diferença entre governança e gestão de TI. Observa-se que houve um significativo avanço, com a evolução de diversos índices avaliados como observado na figura 3.

Figura 3. Aspectos que demandam atenção

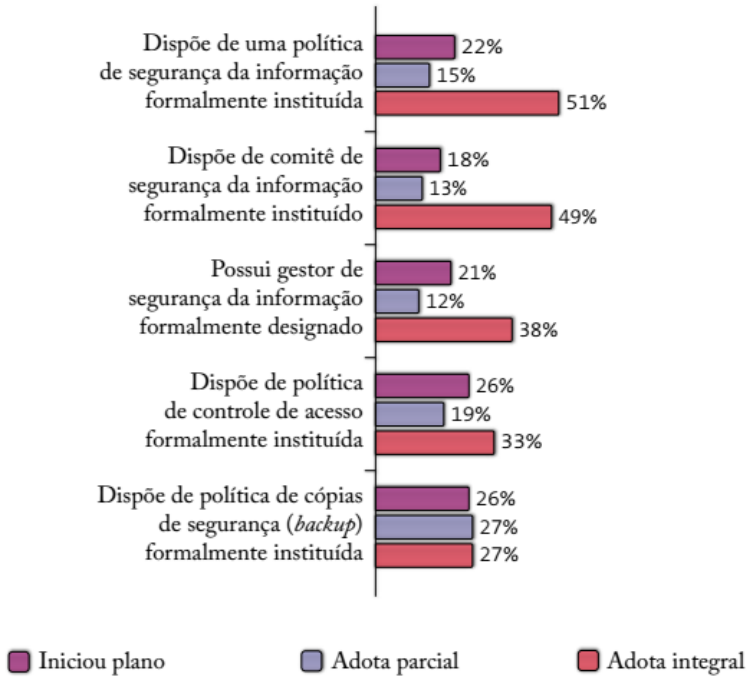


Fonte: TCU (2012)

Este levantamento concluiu que, metade das instituições que foram avaliadas passou para o nível intermediário em relação à governança de TI, apresentando um significativo avanço quando comparado aos números de 2010, onde este índice foi de 38%. Em estágio avançado o índice chegou a 16%, diante dos 5%, apresentado em 2010.

No levantamento realizado em 2014, resultado do Acórdão 3.117/2014-TCU-Plenário, os dados coletados mostraram que houve uma tendência de evolução da situação, mesmo ainda estando longe do nível ideal, pois muitas práticas fundamentais que agregam valor para a organização ainda não são realizadas. A partir de questionários eletrônicos, desenvolvidos com base nas práticas da ABNT NBR ISO 27002 – segurança da informação, do modelo de governança de TI - COBIT 5 e a ISO/IEC 38500 – governança corporativa de TI, foram avaliadas 372 organizações da APF. A figura 4 apresenta os resultados obtidos relativos à gestão corporativa da segurança da informação. Chama atenção o fato de que penas 27% das instituições possui uma política de copias de segurança *(backup)* integralmente instituída, fato este que pode levar à perda definitiva dos dados.

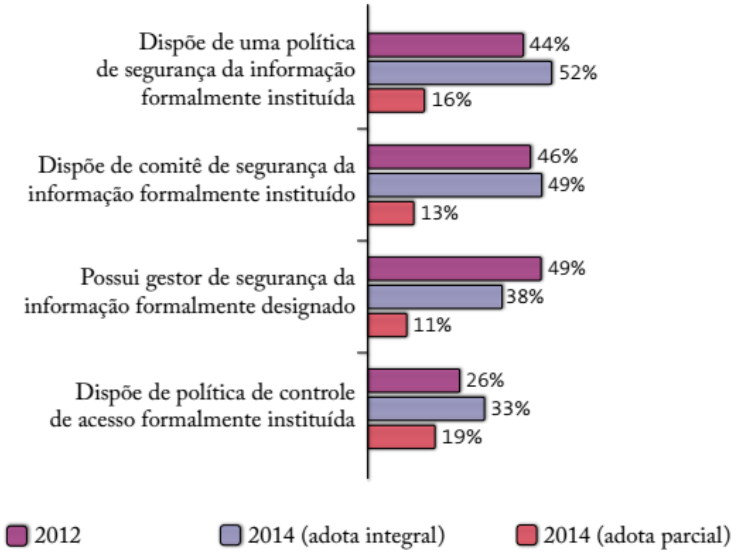
Figura 4. Resultado das práticas de gestão da segurança da informação



Fonte: TCU (2014)

A respeito da evolução no período de 2012 a 2014 representado na figura 5, observa-se que os indicadores apresentam evidências de que o nível de adoção das práticas está muito longe do esperado, situação que pode expor a APF a riscos como a indisponibilidade de serviços e a perda de integridade das informações.

Figura 5. Evolução da gestão de segurança da informação

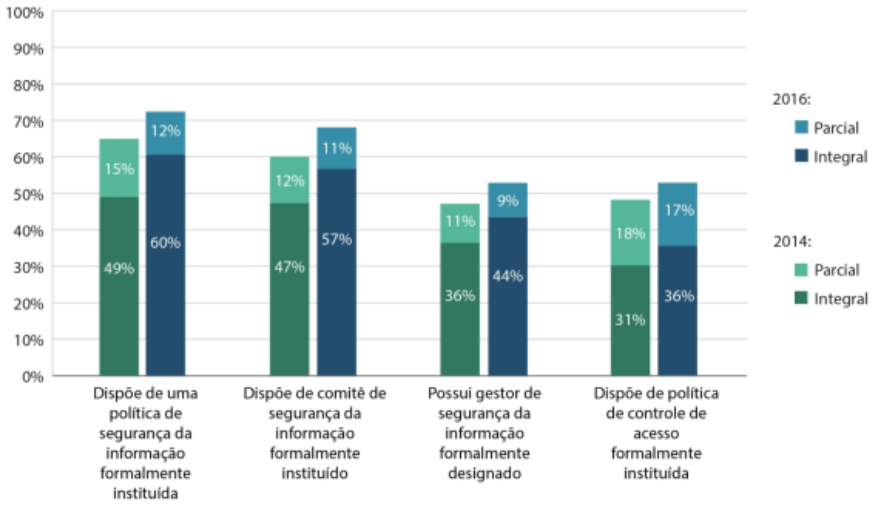


Fonte: TCU (2014)

Chama atenção o fato de apenas 52% das instituições possuírem sua política de segurança da informação, documento básico que norteia todo o processo de gestão da segurança da informação.

O último levantamento disponível pelo TCU foi realizado no ano de 2016, o qual analisou 376 órgãos da APF, de forma geral, observou-se que houve uma evolução, como se pode observar na figura 6, maior do que a obtida em 2014. Quanto ao aspecto da gestão da segurança da informação, os resultados apresentaram uma discreta evolução, indicando que o nível de adoção das práticas ainda continua muito distante do esperado, “situação que revela a existência de lacunas na formulação de políticas e na atribuição de responsabilidades concernentes à gestão corporativa de segurança da informação” (TCU, 2016).

Figura 6. Evolução da gestão da segurança da informação



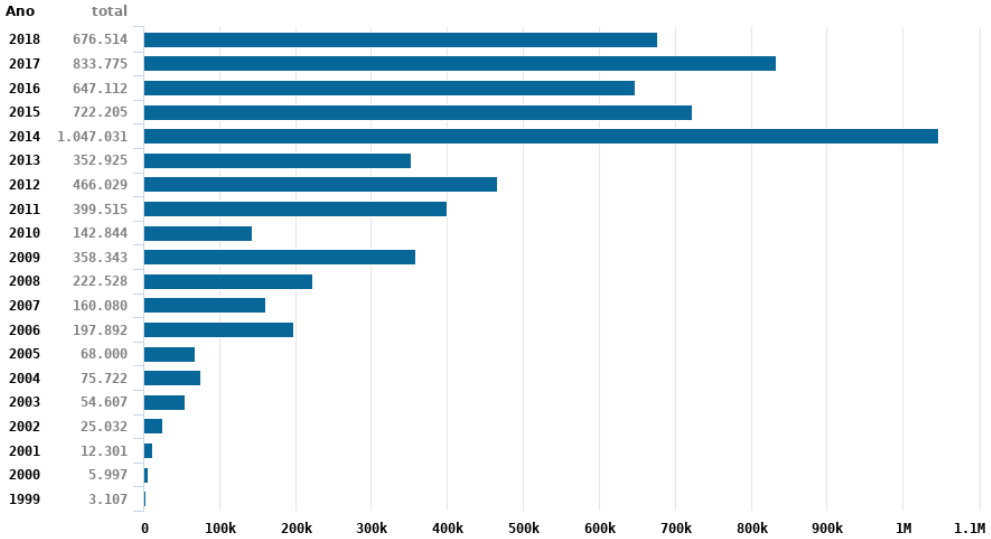
Fonte: TCU (2016)

Estes levantamentos serviram de alerta para indicar as fragilidades encontradas nos órgãos da APF quanto à governança de TI e a temas ligados a gestão da segurança da informação, sendo de fundamental importância, pois a partir dos anos 2000, houve um significativo aumento no número de ataques realizados por hackers direcionados aos mais diversos tipos de segmentos organizacionais do mundo, deixando sites, computadores e sistemas de grandes empresas inoperantes, ocasionando prejuízo econômico em torno de U$13.2 bilhões (GUIA DE SEGURANÇA, 2013).

Como forma de identificar e combater essas ameaças surgiu o CERT (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil), um grupo ligado ao Comitê Gestor da Internet no Brasil, que atua na resposta a incidentes de segurança ocorridos em computadores ligados à internet brasileira e também realiza trabalhos de conscientização sobre os problemas de segurança.

Segundo dados disponibilizados pelo CERT.br, de Janeiro a Dezembro de 2018, foram registradas 676.514 notificações de ataques, número 19% menor que o total registrado em 2017. Essas notificações são reportadas ao centro de forma voluntária através da internet e dentre as principais ocorrências destacam-se: tentativas de fraudes, computadores comprometidos, varreduras e propagação de códigos maliciosos, ataques a servidores web, dentro outros incidentes. A figura 7 representa as estatísticas de incidentes reportados ao CERT.br envolvendo ataques a computadores e sistemas de informação ao longo dos anos.

Figura 7. Incidentes Reportados ao CERT.br por Ano



Fonte: CERT.br (2019)

Esses incidentes são fortes ameaças à segurança da informação das instituições, sejam elas públicas ou privadas, como também são capazes de pôr em risco as pessoas que estão conectadas a rede, impactando de forma negativa os negócios organizacionais e a privacidade dos indivíduos. O CERT.br apresenta os tipos e descrição dos principais incidentes que foram reportados em 2018 como pode-se observar no quadro 1.

Quadro 1 – Categorias de incidentes reportados ao CERT.br

Tipo	Descrição
Worm	Notificações de atividades maliciosas relacionadas com o processo automatizado de propagação de códigos maliciosos na rede
Dos	(DoS -- *Denial of Service*): notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede.
Invasão	Um ataque bem sucedido que resulte no acesso não autorizado a um computador ou rede.
Web	Um caso particular de ataque visando especificamente o comprometimento de servidores Web ou desfigurações de páginas na Internet.
Scan	Notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.
Fraude	Segundo Houaiss, é "qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro". Esta categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem.
Outros	Notificações de incidentes que não se enquadram nas categorias anteriores.

Fonte: Adaptado para quadro de CERT.br (2019)

Segundo o CERT.br, a atividade de *Scan* foi responsável por 58,77% das ocorrências registradas em 2018, isto demonstra claramente que existem tentativas de

buscas de vulnerabilidades em computadores e sistemas presente nas organizações, em seguida com 23,42% estão os incidentes de *DoS*, os quais buscam ocasionar a indisponibilidade dos serviços e sistemas das instituições e empresas.

A Associação Brasileira de Normas Técnicas (ABNT) publicou normas ligadas diretamente à segurança da informação e as classificou como pertencente à família 27000, dando origem as normas ABNT NBR ISO 27001 e ABNT NBR ISO 27002. Regazzi Filho (2000) afirma que uma norma possui como fundamento a definição de regras, padrões e instrumentos de controle para regulamentar a forma a qual os produtos, processos e serviços são criados e atualizados.

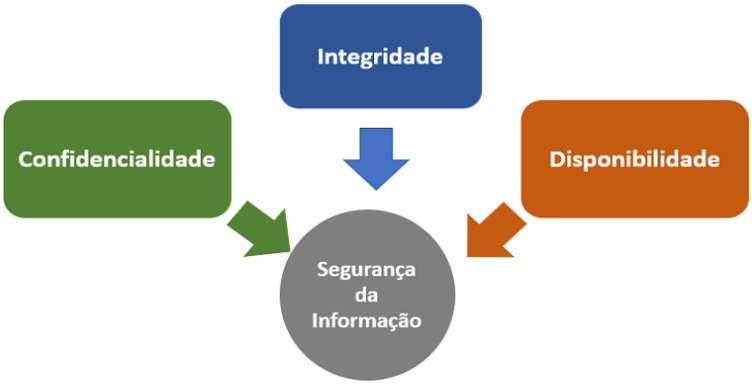
A ABNT NBR ISO 27001 contém os requisitos para se estabelecer um Sistema de Gestão de Segurança da Informação, enquanto que a ABNT NBR ISO 27002 estabelece as diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização.

Desta forma, a segurança da informação passou a ser vista como elemento primordial no planejamento estratégico de uma organização, com o objetivo de prevenir potenciais danos. O Governo Federal brasileiro há tempos vem tentando implementar procedimentos que visem diminuir tais problemas, publicando normas, decretos e leis que regulamentem a gestão de segurança da informação.

2.1 PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

A gestão da segurança da informação envolve três princípios básicos que devem ser estabelecidos como forma de oferecer garantias quanto à origem, uso e trânsito da informação, ou caso contrário, poderá ocorrer à quebra da sua segurança, também conhecido como incidente de segurança (CAMPOS, 2006). Dentre estes requisitos estão à garantia da confidencialidade, da integridade e da disponibilidade, os quais devem estar contidos no plano de gestão da segurança da informação das organizações, com o objetivo de implementar estratégias necessária à proteção da informação (ABNT NBR ISO 27002:2013).

Figura 8. Princípios da segurança da informação



Fonte: Oliveira (2019)

Desta forma, a segurança da informação nas organizações deve possuir a premissa de proteger a informação contra o acesso de usuários não autorizados (Confidencialidade), garantir a não violação da informação (Integridade) e assegurar o acesso aos usuários autorizados (Disponibilidade), sempre que for necessário (CAMPOS, 2006).

Assim, o princípio da confidencialidade objetiva garantir que apenas as pessoas autorizadas terão acesso ao conteúdo de determinada informação (ABNT NBR ISO 27002:2013). De acordo com Silva (2008) “ter confidencialidade na comunicação é ter a segurança de que o que foi dito a alguém ou escrito em algum lugar será escutado ou lido por quem tiver autorização para tal”. Portanto, a confidencialidade constitui um desafio para as organizações, visto que sua implementação deve estar presente em todo o ciclo de vida da informação e deve abranger os diferentes graus de importância que a informação possui.

Sua quebra ocorre quando o acesso não autorizado é realizado ao conteúdo informacional. Quando isto acontece, pode-se dizer que houve a perda do segredo da informação e que esta pode estar na iminência de ter seu conteúdo divulgado de forma indevida, ocasionando perdas inestimáveis (DANTAS, 2011).

Uma matéria publicada pela Folha de São Paulo em Julho de 2019, apresentou um relatório contendo dados de uma pesquisa anual realizada pela IBM, a qual avaliou mais de 500 empresas, sendo 35 no Brasil e mostrou que cada incidente de segurança no país gera um quantitativo de 26.523 registros de informações vazadas, ficando o Brasil atrás apenas de países como Oriente Médio (38.800), Índia (35.636) e EUA (32.434).

A pesquisa revelou ainda que cada incidente gera em média um prejuízo de R$ 5 milhões de reais e que os setores que sofrem o maior impacto financeiro por vazamento, são a Saúde, o Financeiro, a Energia, o Industrial e Farmacêutico. Dentre as principais causas de vazamentos de dados foram identificados os ataques criminosos (51%), falha em sistema (25%) e erro humano (24%). Outro dado negativo para o Brasil diz respeito ao tempo de resposta a incidente de segurança, em média as organizações demoram 111 dias para conter um vazamento (HERNANDES, 2019).

O segundo princípio da segurança da informação é a integridade, o qual deve estabelecer métodos que garantam que a informação não seja violada de forma não autorizada (BEAL, 2005). Garantir a integridade significa dizer que a informação deve permanecer em seu estado original conforme definido pelo seu proprietário sem sofrer qualquer tipo de alteração indevida, ou caso contrário, poderá ocorrer erros e fraudes que, como consequência, prejudicam a comunicação e a tomada de decisões.

De acordo com Silva (2008), existem várias formas de alteração da informação, podendo variar tanto no seu conteúdo, como no ambiente ao qual está inserida, ocorrendo a quebra da integridade sob dois aspectos:

a) Alterações do conteúdo – parte do conteúdo sofre algum tipo de inserção, substituição ou exclusão.
b) Alterações nos elementos que fornecem suporte a informação – alterações realizadas no ambiente físico e lógico onde a informação está armazenada.

Portanto, estabelecer a integridade, é garantir que apenas as pessoas ou sistemas autorizados serão capazes de realizar qualquer tipo de alteração na forma e no conteúdo da informação ou que as alterações causadas por erros em sistemas ou ambientes na qual a informação é armazenada ou processada não ocorra.

O terceiro princípio diz respeito à disponibilidade. Além de garantir que o acesso à informação seja realizado somente por usuários autorizados e que seu conteúdo não seja alterado de forma indevida, ela deverá estar sempre disponível no momento oportuno. Beal (2005) afirma que disponibilidade “é a garantia de que as informações e serviços importantes estejam disponíveis para os usuários quando requisitados”.

Como forma de garantir a disponibilidade, é fundamental que regras sejam criadas, que as organizações conheçam seus usuários e que algumas medidas devem ser levadas em consideração. Silva (2008) destaca algumas dessas medidas:

a) Configuração segura de um ambiente em que todos os elementos que fazem parte da cadeia de comunicação estejam dispostos de forma adequada para assegurar o êxito da leitura, do trânsito e do armazenamento da informação;
b) Cópias de segurança – *backup*. Isso permite que as informações estejam duplicadas em outro local para uso, caso não seja possível recuperá-las a partir de sua base original;
c) Definir estratégias para situações de contingência;
d) Estabelecer rotas alternativas para o trânsito da informação, para garantir seu acesso e a continuidade dos negócios, inclusive quando alguns dos recursos tecnológicos ou humanos, não estejam em perfeitas condições de funcionamento (SILVA, 2008).

A quebra da disponibilidade ocorre quando a informação não se encontra disponível no momento em que o usuário deseja utilizá-la, podendo ser ocasionada por um roubo de um documento, sistemas de computador indisponíveis, serviços inoperantes, dentre outros. Este princípio pode ser considerado o mais importante, pois as informações presentes nas organizações precisam estar disponíveis para uma pessoa ou equipe sempre que for necessário acessá-la, ao passo que ela também deve estar acessível apenas para os usuários autorizados. Desta forma, criar mecanismos de controle de acesso e de classificação da informação é fundamental para que não ocorra a quebra da confidencialidade, da integridade e da disponibilidade (DANTAS, 2011).

Algumas abordagens agregam ainda outros princípios que podem fazer parte do processo de proteção da informação, é o que define a ABNT NBR ISO 27002:2013, ao afirmar que outros elementos como a autenticidade, a responsabilidade, o não repudio e a confiabilidade também devem estar envolvidos.

A autenticidade visa garantir a fonte a qual a informação foi atribuída e que foi elaborada por quem tem permissão para tal procedimento, uma das formas de assegurar esse processo é através da assinatura digital (BEAL, 2005). A responsabilidade objetiva a coparticipação de todos os envolvidos no processo de criação, manipulação, transporte, armazenamento e descarte da informação. O não repudio possui o intuito de estabelecer métodos que façam com que o autor não seja capaz de negar a criação e assinatura do documento. Por fim, a confiabilidade deve oferecer garantias de que a informação é confiável (DANTAS, 2011).

Esses princípios devem ser encarados como de suma importância no processo de gestão da segurança da informação e garanti-los não é tarefa fácil, pois mesmo que a tecnologia ofereça um amplo auxilio, ela não é unicamente a solução para os problemas.

Ao serem preservados, espera-se que a segurança da informação seja garantida e

que não ocorra nenhum tipo de registros de incidentes de segurança, fortalecendo-se assim a informação organizacional contra os diversos tipos de ameaças e ataques ao qual a informação está suscetível.

2.2 AMEAÇAS

A informação conseguiu atravessar fronteiras com velocidades surpreendentes e ameaças foram surgindo como forma de inviabilizar o negócio. Sêmola (2014) define ameaça como sendo a exploração de vulnerabilidades realizadas por agentes externos a ativos de informação, como forma de comprometer o funcionamento normal da organização. Elas podem ser classificadas como: naturais, involuntárias ou voluntarias.

Como o próprio nome sugere, as ameaças naturais possuem origem em fenômenos da natureza como provocados por água, inundações, incêndios, descargas de energia, dentre outros fatores. Já as ameaças involuntárias são oriundas de forma acidental, sendo provocadas pela introdução incorreta de dados no sistema, configurações incorretas ou problemas de natureza elétrica. As ameaças voluntárias ocorrem de forma proposital, com a intenção de destruir, roubar ou adulterar o conteúdo de determinada informação, sendo muitas vezes provocados por pessoas mal intencionadas, como hacker, espiões, ladrões, entre outros (SÊMOLA, 2014).

No processo de identificação das ameaças, Peltier (2005) afirma que a criação de listas de ameaças é um elemento importante e que deve ser usado, porém observa que esta não deve ser a única fonte norteadora no processo de avaliação de riscos, pois não garante que todo o processo esteja assegurado. Outra forma de identificação é a observação de dados históricos, buscando identificar os tipos de eventos e com que frequência eles ocorreram.

Para construir o processo de identificação das principais ameaças presentes no objeto de estudo desta pesquisa, baseou-se na “Árvore de Ameaças” apresentada por Shahri e Ismail (2012), cujos nodos exemplificam os tipos de ameaças e as folhas apresentam as ameaças propriamente ditas.

Shahri e Ismail (2012) enfatizam que as organizações devem compreender quais são as potencias ameaças existentes no ambiente corporativo, pois é através deste conhecimento que será possível definir e fortalecer o nível de proteção adequado à informação. A figura 9 apresenta uma lista de possíveis ameaças.

Figura 9 – Lista de ameaças

Fonte: Shahri et. al. (2012)

A criação de árvores de ameaças poderá ser realizada pelo responsável da segurança organizacional ao ser feito uma análise do tipo e a frequência das ameaças mais recorrentes.

Dentre as principais ameaças, dados do Cert.Br indicam que os incidentes ocasionados por *malwares*, fazem parte de uma das categorias mais reportadas no ano de 2018, representando um total de 39.071 notificações. O termo *malware,* surge através da contração das palavras inglesas ***mal****icious soft****ware*** (software maliciosos), e se refere aos *softwares* indesejados que sofreram algum tipo de modificação no seu código, com o intuito de danificar dispositivos, roubar dados e ocasionar danos às pessoas (DANTAS, 2011). Os principais tipos de *malwares* são: vírus, *worms*, cavalo de Tróia, *Spyware* e *Adware*.

O **Vírus** é um programa de computador ou parte dele, que se propaga através de cópias de si mesmo com o objetivo de infectar outros programas, danificando sistemas e excluindo ou corrompendo arquivos (NAKAMURA, 2007).

O ***Worm*** é um programa que se propaga através de redes inteiras de dispositivos, enviando cópias de si mesmo entre computadores, difere do vírus por não inserirem copias de si em arquivos ou programas (MORIMOTO, 2010).

Similar ao vírus, o **Cavalo de Troia** é um tipo de *malware* que se oculta em programas, executando funções maliciosas sem o conhecimento do usuário. Seu principal objetivo é abrir portas, oferecendo algum tipo de acesso remoto à máquina infectada. Uma vez infectada, a máquina permite ao invasor o roubo de senhas, de informações, o envio de *spam* ou o uso da própria máquina para direcionar outros tipos de ataques (NAKAMURA, 2007).

Projetado para agir como espião, o ***Spyware*** é um *malware* que possui o objetivo de monitorar as atividades do sistema e enviar as informações para terceiros. Ele atua em segundo plano, fazendo com que o usuário não perceba seu funcionamento e desta forma consegue gravar as atividades do equipamento infectado online, incluído senhas, número de cartão de crédito, atividades no sistema, dentro outros (MORIMOTO, 2010).

Adware é um tipo de *software* que atua expondo propagandas indesejadas aos usuários de acordo com seu modo de navegação, efetuando desta forma monitoramento invisível e indevido.

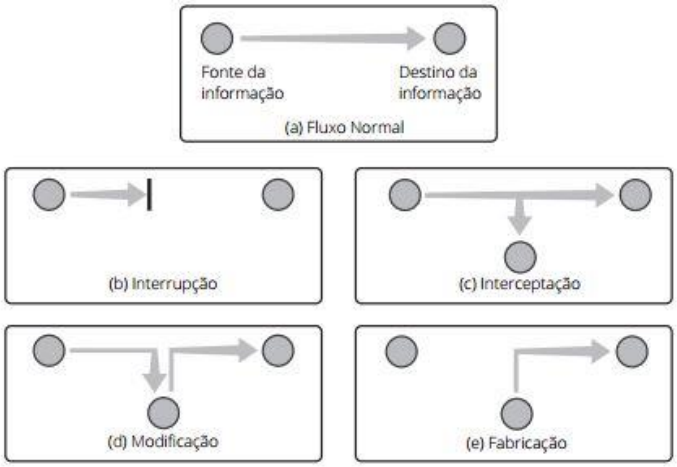
O Cert.Br apresenta também que outra ameaça denominada ***scan,*** é um mecanismo que vem sendo amplamente utilizados pelos atacantes, a qual consegue realizar uma varredura em redes de computadores na tentativa de identificar potenciais alvos e quais são as vulnerabilidades existentes nos serviços que por eles estão sendo

disponibilizados. Em 2018 o Cert.Br recebeu um total de 397.590 notificações de *scan*, o que corresponde a 58,77% do total de incidentes reportados.

2.3 ATAQUES

Ataque pode ser compreendido como qualquer tipo de ação que venha a comprometer a segurança de uma organização, seja este realizado por ações humanas ou tecnológicas. Enfatizando os ataques tecnológicos, estes podem ser realizados através de quatro modelos possíveis, podendo ocorrer por *interrupção*, o qual acontece destruição ou indisponibilidade de um ativo, *interceptação*, quando o acesso à informação é realizado por parte não autorizada, *modificação*, quando a informação é acessada por parte não autorizada e possui seu conteúdo alterado e, por fim, *fabricação ou personificação*, quando uma entidade se passa por outra para ter acesso à informação, conforme representeado na figura 10.

Figura 10. Modelo genérico de ataque



Fonte: Coelho et al (2014)

A figura 10 apresenta de forma genérica os possíveis ataques que podem ocorrer alterando o fluxo normal da informação.

2.3.1 TIPOS DE ATAQUE

Diversos são os tipos ataques que podem ocorrer à segurança da informação, existindo inúmeras técnicas, ferramentas e métodos que surgem a todo momento no

cenário mundial. Os ataques variam de acordo com a técnica aplicada e o objetivo ao qual se pretende alcançar, dentre os principais tipos estão:

a) Engenharia social

Este tipo de ataque se utiliza de técnicas que exploram as fragilidades humanas, afetando o componente mais frágil do sistema, o usuário. Se apropriando do fato de que os usuários sempre colaboram com os serviços da organização, o engenheiro social possui a habilidade de tentar ludibriar as pessoas com o intuito de assumir uma falsa identidade para ter acesso a computadores, sistemas, senhas ou informações sigilosas que comprometam a segurança. Um tipo de ataque clássico ocorre quando o atacante se passa por um alto funcionário que possui problemas urgentes de acesso ao sistema, colocando em jogo a confiança, a psicologia e tentando manipular as pessoas com o intuito de conseguir o acesso (NAKAMURA, 2007).

De acordo com Silva et. al (2003), a engenharia social pode ser definida "como um conjunto de ações que, unicamente através da interação humana, levam ao compromisso de informação confidencial".

Faz parte da natureza humana as ações de proferir ajuda entre colaboradores do ambiente organizacional e na tentativa de diminuir os riscos de sofrer ataque, pesquisas e informações sobre o ambiente computacional, atividades da instituição e funcionários, só devem ser respondidas pelo setor competente e nunca através de telefone ou e-mail onde não se tenha conhecimento real do remetente.

Afirma Eras (2004) que o termo engenharia social se refere à área que realiza o estudo das técnicas e práticas que são executas para obter informações importantes ou sigilosas pertencentes a uma organização, através da persuasão dos seus colaboradores.

No contexto da segurança da informação quanto ao uso de tecnologias, Hadnagy e Maxwell (2009) afirmam que o objetivo da engenharia social é conseguir realizar ações que venham a obter a quebra do valor da informação mediante a exploração da confiança das pessoas.

Quanto ao significado de cada palavra, em pesquisa realizada por Peixoto (2004), o termo Engenharia Social não possui a relevância negativa que aparenta ter visto que:

- Engenharia; refere-se à aplicação de conhecimentos científicos, empíricos e habilidades que são capazes de modificar recursos naturais de forma que atendam às necessidades humanas.
- Social; que interessa a sociedade. Sociável.

Porém, a engenharia social não é oriunda das ciências da natureza, mas sim das ciências humanas e sociais, de tal modo que ao realizar a junção dos termos anteriormente definidos isoladamente, passamos a obter uma ideia e significado diferente, referindo-se a engenharia social como: "A técnica que explora as fraquezas humanas e sociais, em vez de explorar unicamente a tecnologia" (NAKAMURA, 2007).

No âmbito das Ciências Políticas, a engenharia social é entendida como o modo de se aplicar técnicas as quais tenham o objetivo de manipular as pessoas, para que estas executem atos que normalmente não fariam, como a divulgação de informações pessoais ou corporativas pertencentes às organizações (HADNAGY; MAXWELL, 2009).

Normalmente o engenheiro social possui o perfil de uma pessoa que apresenta um comportamento agradável, educado, simpático e carismático, mas também por ser muito criativo e dinâmico (PEIXOTO, 2004).

Os ataques sempre buscam explorar a fragilidade e a ingenuidade das pessoas, e possuem duas características diferentes: a exploração do ambiente físico, como o local de trabalho, lixo, telefones; e o psicológico, objetivando meio de persuadir as pessoas ou simplesmente sendo gentil.

O ser humano possui algumas características comportamentais que o tornam alvo recorrente de ataques, como a facilidade de sofrer persuasão, a vontade de ser útil, a propagação de responsabilidades e a busca por novas amizades (SILVA FILHO, 2004).

A dependência que a sociedade passou a ter da informação e dos recursos tecnológicos fez com que a engenharia social se tornasse uma das principais ameaças à segurança das organizações.

b) Ataques físicos

O ataque físico constitui o método menos comum praticado contra as organizações. Seu objetivo principal é realizar uma tentativa de acesso direto aos sistemas, não sendo utilizadas técnicas de ataques remotos. Uma vez obtido o acesso, o

atacante poderá, além do roubo do equipamento, executar uma série de ações como: Copiar documentos, acessar informações privilegiadas, modificar arquivos, alterar configurações, ler e-mails de terceiros, destruir todas as informações, dentre outros (NAKAMURA, 2007).

Na tentativa de minimizar este tipo de ataque, as organizações devem realizar controles de acesso físico aos sistemas e aos ambientes restritos, exigindo o uso de crachás de identificação, oferecer treinamento contínuo aos colaboradores fazendo com que estes conheçam as normas de segurança institucional e que possam adotar práticas que diminuam os riscos, como não deixar a estação de trabalho desbloqueada ao se ausentar e evitar expor documentos oficiais em cima da mesa de trabalho.

c) Ataques por força bruta

Este tipo de ataque utiliza um método de criptoanálise que consiste em tentar decifrar as senhas criptografadas através de uma lista de senhas já conhecidas. Senhas mais comuns como, data de nascimento ou numeração sequencial com poucos dígitos, são facilmente descobertas pelos atacantes, onde consequentemente terão êxito no acesso aos mais diversos meios tecnológicos que exigem autenticação.

2.4 VULNERABILIDADES

Vulnerabilidades são fatores que estão relacionados diretamente com fragilidades, as quais podem colocar em risco as informações das organizações, podendo provocar danos. Sêmola (2014), afirma que as vulnerabilidades são fragilidades encontradas em ativos de informação, que ao serem explorados acarretam incidentes de segurança da informação. Já Beal (2005) define que as vulnerabilidades são pontos de fragilidade que são encontrados por ameaças que visam realizar ataque.

2.5 POLITICA DE SEGURANÇA DA INFORMAÇÃO

A política de segurança da informação, também referida como (PSI), é um documento que deve ser elaborado com o intuito de estabelecer métodos, procedimentos, princípios, compromissos, orientações e normas a serem seguidas por todos os colaboradores de uma organização (FONTES, 2006).

De acordo com Beal (2005) a política de segurança da informação, surge da real necessidade da afirmação de regras que regulamentem e discipline como deve ocorrer o acesso à informação organizacional, a forma de utilização de meios tecnológicos da instituição, bem como o processo de tratamento, manuseio e proteção dos dados. A autora ressalta ainda que "o comprometimento com a proteção da informação e dos sistemas de informação, deve surgir do mais alto nível da organização" motivado pela consequência dos graves problemas que podem resultar na divulgação, alteração indevida ou indisponibilidade da informação.

A norma ABNT NBR ISO 27002 (2005), enfatiza que o objetivo da política de segurança da informação é "prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações pertinentes". Assim, cabe à direção oferecer orientações claras sobre sua política alinhada com os objetivos da instituição, demonstrando o comprometimento com a segurança da informação que abranja toda a organização.

Desta forma, a UFPB, através da resolução 32/2014 (UFPB, 2014) aprovada pelo Conselho Universitário (CONSUNI), estabeleceu a sua Política de Segurança da Informação. O Capítulo I apresenta no seu Art. 1º que: "Fica estabelecida a Política de Segurança da Informação (PSI) da Universidade Federal da Paraíba, contendo as diretrizes de segurança da informação a serem observadas no âmbito desta Universidade". O Parágrafo Único, do referido Capítulo, acrescenta que: "As diretrizes estabelecidas na PSI/UFPB determinam as bases a serem seguidas pela UFPB com relação à segurança dos recursos de tecnologia da informação (TI) e informações geradas na UFPB". Já o artigo 2º acrescenta que: "A PSI consiste em um quadro de referência contendo princípios que norteiam a Gestão de Segurança da Informação e que devem ser observados por professores, alunos, servidores e demais usuários que interagem com os "ativos" de TI da UFPB" (UFPB, 2014).

A política de segurança da informação deve normatizar todos os assuntos que tratem sobre segurança da informação, como o uso do e-mail corporativo, o uso da internet, o acesso a computadores e sistemas dentre outros.

Para nortear estes objetivos, a norma internacional ABNT NBR ISO 27002, apresenta as boas práticas para apoiar a implantação do sistema de gestão de segurança da informação. Com o objetivo de estabelecer diretrizes e princípios em uma organização, a norma possui procedimentos que servem de base para a elaboração da

política de segurança da informação, a gestão de ativos, segurança em recursos humanos, segurança física e do ambiente, controle de acesso, gestão de incidentes, dentre outros procedimentos.

Desta forma, Sêmola (2014) destaca o papel fundamental que a política de segurança impõe no ambiente organizacional, sendo a base para as atividades que envolvem a questão de segurança.

É importante ressaltar que, para alcançar os resultados pretendidos em âmbito organizacional, é necessário que seus principais objetivos sejam entendidos e disseminados a todos da organização e não somente a determinados setores. Entretanto, segundo Silva (2012) este é um procedimento demorado e que requer um trabalho contínuo.

2.6 LEIS, NORMAS E DECRETOS SOBRE GESTÃO DA SEGURANÇA DA INFORMAÇÃO EM ORGÃOS DA ADMINISTRAÇÃO PÚBLICA FEDERAL

A relevância sobre o tema “segurança da informação” fez com que o governo Brasileiro publicasse diversas normas, leis e decretos, que fizeram com que o Brasil não possua uma única lei especifica que trate em sua plenitude sobre o tema, mais que no conjunto da sua legislação podem ser aplicadas (VIEIRA, 2008).

Com a massificação da informação digital, alguns problemas como o vazamento de informações sigilosas dos órgãos da APF, passaram a ser recorrentes e na tentativa de contornar esta situação, o Governo Brasileiro promulgou a Lei nº 9.983 de 14 de julho de 2000, a qual apresenta em seu Artigo 313-A e 313-B a seguinte redação:

> Art. 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano: Pena - reclusão, de 2 (dois) a 12 (doze) anos, e multa.
>
> Art. 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente: Pena – detenção, de 3 (três) meses a 2 (dois) anos, e multa (BRASIL, 2000).

Em 13 de Junho de 2000, o Decreto nº 3.505 foi criado com a finalidade de instituir a Política de Segurança da Informação nos órgãos e entidades da APF. Este decreto criou o Comitê Gestor da Segurança da informação (CGSI), o qual deve ser

composto por 17 Órgãos: Advocacia Geral da União (AGU); Ministério da Justiça (MJ); Ministério da Comunicação (MC); Ministério da Defesa (MD); Secretaria de Comunicações da Presidência da República (SECOM/PR); dentre outros. Seu objetivo é "assessorar a Secretaria-Executiva do conselho de Defesa Nacional na consecução das diretrizes da Política, bem como na avaliação e análise de assuntos relativos aos objetivos estabelecidos nesse Decreto".

Em 26 de Dezembro de 2018, o então Presidente Michel Temer, em um dos últimos atos do seu mandato, publicou o Decreto nº 9.637, o qual revogou o Decreto nº 3.505 e criou a Política Nacional de Segurança da Informação (PNSI). Este ato normativo regula a forma de gerenciamento da segurança da informação no âmbito da Administração Pública Federal, objetivando abranger, de acordo com os incisos presentes no Art. 2º, a segurança cibernética, a defesa cibernética, a segurança física e a proteção dos dados organizacionais, com a finalidade de garantir os princípios da confidencialidade, integridade, disponibilidade e autenticidade da informação em território nacional (BRASIL, 2018).

O ato normativo em questão apresenta como princípios, a soberania nacional, o respeito e a promoção dos direitos humanos e das garantias fundamentais, destacando a liberdade de expressão, a proteção dos dados pessoais, da privacidade, o acesso à informação e a prevenção e tratamento de incidentes em segurança da informação.

Em 28 de Junho de 2001, foi publicada a Medida Provisória nº 2.200, a qual definiu a Infraestrutura de Chaves Públicas Brasileiras – ICP - Brasil, e dá outras providencias, definindo em seu Artigo 1º que: "Fica instituída a Infraestrutura de Chaves Pública Brasileira – ICP - Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras".

Junto a esta medida, foram publicados dois decretos: O Decreto nº 3.872 de 18 de Julho de 2001, que versa sobre o Comitê Gestor da Infra Estrutura de Chaves Públicas Brasileiras (CG ICP-Brasil), sua Secretaria-Executiva e sua Comissão Técnica Executiva – COTEC, o qual foi revogado pelo Decreto nº 6.605/2008 e o Decreto nº 3.996 de 31 de outubro de 2001, que dispõe sobre a prestação de serviços de certificação digital no âmbito da APF.

Em 2002, o Governo Brasileiro publicou o Decreto nº 4.553 de 27 de dezembro de 2002, que:

> "Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências" (BRASIL, 2002).

Este decreto foi revogado pelo Decreto nº 7845, de 14 de novembro de 2012, que passou a regulamentar "procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento".

O Decreto nº 4.829, de 03 de setembro de 2003, apresenta a "Criação do Comitê Gestor da Internet no Brasil (CGI.br), sobre o modelo de governança da Internet no Brasil, e dá outras providências". Conforme o inciso IV do artigo 1º compete ao CGI.br: "promover estudos e recomendar procedimentos, normas e padrões técnicos e operacionais, para a segurança das redes e serviços de Internet, bem assim para a sua crescente e adequada utilização pela sociedade" (BRASIL, 2003).

Em 2008, o Ministro Chefe do Gabinete de Segurança Institucional da Presidência da República, considerando "a necessidade de incrementar a segurança das redes e banco de dados governamentais", bem como "o dever do Estado de proteção das informações pessoais dos cidadãos", dentre outros, publicou a Instrução Normativa GSI/PR n° 01/2008, a qual regulamenta o processo de Gestão de Segurança da Informação e Comunicações na Administração Pública Federal.

Na tentativa constante de precaver o uso indevido das informações que está sob sua guarda através de instrumentos normativos, o Governo Brasileiro publica em 18 de Novembro de 2011 a Lei nº 12.527 (Lei de Acesso à Informação), que passou a vigorar a partir de Maio de 2012, a qual "dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios [...]".

> A Lei 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 (BRASIL, 2011).

O inciso XXXIII do artigo 5º da Constituição Federal afirma que "todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de

responsabilidade [...]". No entanto, este acesso sofre algumas restrições a depender do grau de sigilo da informação solicitada, levando-se em conta a segurança da sociedade e do Estado. O inciso II do § 3º do art. 37 versa sobre "o acesso dos usuários a registros administrativos e as informações sobre atos de governo, observando o disposto no art. 5º, X e XXXIII". Já o § 2º do art. 216 da Constituição Federal afirma que "[...] cabe à administração pública, na forma da lei, a gestão da documentação governamental e as providências para franquear sua consulta a quantos dela necessitem".

Em 14 de Agosto de 2018, foi sancionada a Lei Nº 13.709, a Lei Geral de Proteção dos Dados Pessoais (LGPD), a qual regula a política de proteção dos dados pessoais e privacidade para as organizações públicas e privadas que coletam, trata, guardam, processam, comercializam, dentre outros, os dados de milhões de brasileiros (BRASIL, 2018).

Com vigência prevista para 15 de Agosto de 2020, a LGPD regulamenta qualquer atividade que envolva dados pessoais, inclusive nos meios digitais, fazendo com que as instituições devam se adequar ao modo de proteção dos dados impostos pela legislação brasileira.

Neste sentido, a UFPB vem desde 2016 buscando realizar uma Política de Segurança Institucional, a qual ainda se encontra em debate, com o objetivo de abranger uma cultura de segurança institucional com foco na "salvaguarda e proteção das pessoas, do material, das áreas e instalações e da informação".

O art. 7º afirma que cabe a segurança da informação a compreensão sobre o conjunto de medidas que devem ser aplicadas para "proteger os dados e informações sensíveis ou sigilosas, cujo acesso ou divulgação não autorizados possa acarretar prejuízos de qualquer natureza à UFPB[...]".

3 PERCURSO METODOLÓGICO DESTA PESQUISA

De acordo com Prodanov e Freitas (2013), “a pesquisa cientifica é a realização de um estudo planejado, sendo o método de abordagem do problema que caracteriza o aspecto científico da investigação”. Logo, a pesquisa possui o objetivo de procurar respostas para um problema, para uma indagação, a qual se utiliza de métodos científicos para obtenção dos resultados esperados.

Para Gil (2008), a pesquisa pode ser definida como “o processo formal e sistemático de desenvolvimento do método cientifico”. Portanto, a pesquisa é um instrumento que envolve um conjunto de ações que visam encontrar soluções para um determinado problema e que se desenvolve através de meios racionais e sistemáticos.

Desta forma, esta pesquisa possui uma abordagem qualitativa, do tipo exploratória, possuindo como meio de informação para compor sua base teórica, a pesquisa documental e bibliográfica. O processo de coleta de dados foi realizado através de questionários, o qual abordou o público alvo com questões pertinentes ao nível de conhecimento sobre a gestão de segurança da informação.

A pesquisa exploratória, como define Gil (2008), possui “o objetivo de proporcionar visão geral, do tipo aproximativo, acerca de determinado fato”. Segundo o autor, este tipo de pesquisa se caracteriza por ser mais flexível, o que permite analisar o tema sobre diversos aspectos, envolvendo levantamentos bibliográficos, documental, entrevista com pessoas que possuem algum tipo de experiência com a temática pesquisada e analisar exemplos que incentivem a compreensão.

Na construção da base teórica, foram utilizadas as técnicas de pesquisa documental e bibliográfica. De acordo com Marcone e Lakatos (2013) “a característica da pesquisa documental é que a fonte de coleta de dados está restrita a documentos, escritos ou não, constituindo o que se denomina de fontes primárias”.

A pesquisa bibliográfica por sua vez, envolve todas as publicações já realizadas sobre o tema de estudo, constituindo-se de fontes secundárias como livros, revistas, artigos científicos, dissertações, teses, internet, dentre outros, que possuem o objetivo de aproximar o pesquisador com o material já publicado sobre o tema da pesquisa.

Percebe-se desta forma que a principal diferença entre estes dois tipos de pesquisas consiste na origem das fontes, pois, enquanto que a pesquisa bibliográfica possui como alicerce os estudos já publicados por diversos autores sobre a temática em

contexto, a pesquisa documental utiliza-se de materiais que ainda não passaram por um processo de análise ou que podem ser utilizados de acordo com os objetivos da pesquisa.

3.1 CAMPO EMPÍRICO

O campo de pesquisa deste estudo foi o CCAE, Campus IV da UFPB, em específicos nos setores administrativos, como a Direção de Centro, Gerência Administrativa, Gerência de Tecnologia da Informação e Comunicação, Biblioteca, Coordenações e Departamentos de Cursos e Sub Prefeitura Universitária. Estes fizeram parte da análise dos dados coletados.

O CCAE encontra-se localizado no Litoral Norte do Estado da Paraíba, o qual surgiu através da política pública de interiorização da educação superior, criada pelo Governo Federal através do programa Expandir. Em 2005 a UFPB elaborou o projeto de criação do Campus IV, sendo aprovado pelo Ministério da Educação e Cultura (MEC) em 2006 e posteriormente criado pelo Conselho Universitário (CONSUNI) através da resolução 05/2006 (BATISTA, et al, 2017).

Segundo Nascimento (2013), houve grandes dificuldades na implantação deste Campus, fator este relacionado principalmente pela sua localização, pois não foi possível se chegar a um consenso sobre em qual cidade o campus deveria ser instalado, como também a não definição de uma área geográfica que abrangesse a divisa entre os municípios envolvidos. Desta forma, após diversos embates políticos, ficou decidido que o Campus IV deveria existir em duas unidades localizadas na cidade de Mamanguape e Rio Tinto.

Administrativamente presente nas duas cidades, o CCAE, único centro existente no Campus IV, oferece doze cursos de graduação, três mestrados e duas especializações. Seu quadro de servidores conta atualmente com 60 técnicos administrativos em educação e 168 docentes distribuídos entre os diversos cursos existentes.

De acordo com o Regimento Interno (2017), fazem parte da estrutura básica administrativa do CCAE, os seguintes órgãos:

I. **Órgãos Deliberativos:**
   a) Conselho de Centro;
   b) Colegiados Departamentais;
   c) Colegiados de Cursos.

II. **Órgãos Executivos:**
   a) Diretoria do Centro;
   b) Chefias de Departamentos;
   c) Coordenações dos Cursos de Graduação;
   d) Coordenações de Cursos de Pós-Graduação lato sensu;
   e) Coordenações de Cursos de Pós-Graduação stricto sensu.

III. **Órgãos de Apoio Administrativo:**
   a) Secretaria geral;
   b) Gerência Administrativa;
   c) Sub prefeitura do centro;
   d) Gerência de Tecnologia da Informação e Comunicação;
   e) Gerência de Integração;
   f) Secretarias dos cursos;
   g) Secretarias dos departamentos.

IV. **Órgãos de Apoio didáticos científicos:**
   a) Coordenação de Assuntos Educacionais;
   b) Coordenação de Assistência Estudantil;
   c) Os setores de Multimídia e Laboratórios de uso geral;
   d) Bibliotecas setoriais

V. **Órgãos de Assessoria:**
   a) Assessoria de Ensino e de Graduação;
   b) Assessoria de Pesquisa e de Pós-Graduação;
   c) Assessoria de Extensão.

3.2 OBJETO DE ESTUDO

O presente estudo objetiva investigar como ocorre o processo de gestão da segurança da informação nas atividades desenvolvidas no CCAE, procurando identificar

os riscos, ameaças e vulnerabilidades existentes e na definição de um sistema de gestão da segurança da informação, que venha garantir a segurança dos dados institucionais.

SUJEITOS DA PESQUISA

Os sujeitos desta pesquisa foram 21 técnicos administrativos em educação em exercício no CCAE pertencentes a diversos setores diretamente envolvidos no processo de gestão, processamento, armazenamento, recuperação e uso da informação. A coleta de dados ocorreu por meio de um questionário com perguntas fechadas de múltipla escolha. Os dados coletados foram tratados e tabulados, fazendo uso de uma estatística simples, e em seguida analisados por meio da análise de conteúdo. Esta pesquisa está registrada no Comitê de Ética do Centro de Ciências da Saúde da UFPB sob o número 34192020.0.0000.5188

3.3 TÉCNICAS DE COLETA DE DADOS

O processo de coleta de dados se realizou de acordo com as orientações definidas no método *Facilitated Risk Analysis And Assessment Process* (FRAAP) ou Processo Facilitado de Análise e Avaliação de riscos, de forma adaptada aos objetivos desta pesquisa.

O FRAAP é uma metodologia formal desenvolvida através de métodos qualitativos de análise de riscos, o qual define os procedimentos que deverão ser realizados no processo de coleta e análise de dados. Na análise qualitativa dos riscos, ocorre uma revisão sistemática das potenciais ameaças, fazendo com que seja estabelecido probabilidades de ocorrências e perdas. Este método possui o objetivo de garantir que os riscos relacionados à segurança da informação em ambientes corporativos sejam identificados, documentados e quais controles deverão ser estabelecidos como forma de reduzir os riscos a níveis aceitáveis (PELTIER, 2005).

O FRAAP divide-se em três fases distintas, denominadas de Pré-FRAAP, sessão FRAAP e Pós-FRAAP. Na fase Pré-FRAAP, ocorre à preparação do material que servirá como guia na identificação das ameaças existentes no ambiente organizacional.

Na sessão FRAAP, a equipe de especialistas internos da organização, realizará uma reunião com ênfase na identificação das ameaças a confidencialidade, integridade e

disponibilidade da informação. Por último, a sessão Pós-FRAAP, apresenta uma série de documentos que contém a identificação das ameaças, priorizando-as em nível de risco e estabelecendo os controles que necessitam ser estabelecidos para elevar os riscos a níveis aceitáveis.

Para que a análise de risco seja realizada, três etapas deverão ser cumpridas, dentre elas: identificação das ameaças, probabilidade de ocorrência e o impacto gerado.

Algumas adaptações foram realizadas no modelo proposto para serem aplicadas ao ambiente deste estudo, onde o processo de identificação das ameaças foi realizado através de um questionário, de forma individual, contendo 25 perguntas, que estão relacionadas aos grupos de ameaças: acesso físico, estações de trabalho expostas, política de *softwares*, fraqueza no uso de senhas ou compartilhamento, capacitação de funcionários, classificação e tratamento da informação, vírus de computador, cópia de segurança *(backup)*, falha na rede elétrica, ausência de câmeras de segurança, cabeamento de rede exposto e ameaças externas e do meio ambiente.

O questionário é uma técnica composta por um conjunto de questões que são direcionadas a pessoas com o objetivo de buscar informações sobre determinados temas e que possui como vantagem a possibilidade de alcance de números elevados de participantes, a garantia do anonimato das respostas e baixo custo (GIL, 2008).

O roteiro do questionário está estruturado de tal forma que, a primeira parte encontra-se relacionada ao processo de identificação dos participantes, seguido de três categorias que estão relacionadas intrinsecamente aos elementos inerentes a segurança da informação: pessoas, processos e tecnologia.

Desta forma, foi possível o participante indicar as ameaças que já foram vivenciadas em seu ambiente de trabalho, dentre aquelas apresentadas no questionário, não sendo, portanto, realizado uma reunião para esta identificação como o método sugere na sessão FRAAP.

O processo de probabilidade de ocorrências das ameaças foi definido de acordo com a frequência com que estas aconteceram no ambiente organizacional conforme o relato dos participantes, onde foram classificadas em Alta, Média e Baixa, atribuindo-se para o nível alto, o percentual acima de 50%, nível médio, para os que ficarem entre o intervalo de 30% a 50% e baixo para os resultados inferiores a 30%, tomando-se como referência, o quadro de definições de probabilidades FRAAP conforme descrito no quadro 2.

Quadro 2 – Definições de probabilidade FRAAP

Termo	Definição
Probabilidade	Probabilidade que um evento irá ocorrer ou que um valor de perda específica pode ser alcançado no caso se o evento ocorrer.
Alta	Muito provável que a ameaça ocorrerá no próximo ano. (acima de 50%)
Média	Possível que a ameaça possa ocorrer no próximo ano. (de 30% até 50%)
Baixa	Altamente improvável que a ameaça ocorrerá no próximo ano. (até 30%)

Fonte: Peltier (2005)

No segundo momento, foi estabelecido qual o impacto que o ocorrido acarretou aos processos de trabalho, os classificando de acordo com as definições de impacto FRAAP, conforme o quadro 3 abaixo:

Quadro 3 – Definições de impacto FRAAP

Termo	Definição
Impacto	Uma medida da magnitude da perda ou danos no valor de um ativo da informação.
Alto	Missão inteira ou negócios são impactados.
Médio	Perda limitada a uma única unidade de negócio ou objetivo.
Baixo	Negócios são pouco afetados.

Fonte: Peltier (2005)

Depois de realizadas as classificações, foi estruturada uma tabela a qual atribuirá tanto para probabilidade, como para impacto, os valores de 1 a 3, correspondendo a 1 Baixo, 2 Médio e 3 Alto. A coluna do Nível de Risco corresponderá à soma dos valores definidos na classificação das ameaças para probabilidade e impacto, como orienta a estrutura do FRAAP para ameaças, de acordo com o quadro 4.

Quadro 4 – Estrutura de Ameaças FRAAP

Ameaça	Probabilidade 1= Baixa 2= Média 3= Alta	Impacto 1= Baixo 2= Médio 3= Alto	Nível de risco	Seleção de controles
Acesso físico				
Estações de trabalho expostas				
Fraqueza no uso de senhas ou compartilhamento				
Capacitação de funcionários				
Classificação e tratamento da informação				
Política de softwares				
Vírus de computador				
Cópias de segurança *(Backup)*				
Ausência de câmeras de segurança				
Falha na rede elétrica				
Cabeamento de rede exposto				
Ameaças externas e do meio ambiente				

Fonte: Peltier (2005)

Em seguida, com os resultados obtidos no quadro 4, foi possível montar uma matriz de risco de acordo com os índices de cada ameaça, conforme estabelece o quadro 5:

Quadro 5 - Matriz do Nível de Risco

	IMPACTO		
Probabilidade	Alto	Médio	Baixo
Alta	A (6)	B (5)	C (4)
Média	B (5)	B (4)	C (3)
Baixa	C (4)	C (3)	D (2)
A- Ação corretiva precisa ser implementada; B- Ação corretiva deve ser implementada; C- Requer monitoramento; D- Nenhuma ação é necessária no momento.			

Fonte: Peltier (2005)

Após realizar a montagem da matriz de risco, o FRAAP sugere uma lista de controles baseado no Anexo A da ABNT NBR ISO (27001), apresentado no Apêndice B (Lista de controles FRAAP), que poderão ser estabelecidos na organização como forma de diminuir os riscos existentes. Os controles são necessários para salvaguardar os sistemas de informação e proporcionar garantias de funcionamento de acordo com os padrões definidos administrativamente.

Os mecanismos de controle são formas de garantir a segurança nos sistemas de informação, porém ao utilizar todas as opções disponíveis, podem-se obter custos elevados, tornando o sistema economicamente e operacionalmente inviável. Segundo Peltier (2005), uma boa estratégia é definir controles que não custem mais que o ativo que se deseja proteger, ou caso contrário, o retorno do investimento aplicado deverá ser baixo.

3.4 ANÁLISE E TRATAMENTO DOS DADOS

O processo de análise e tratamento dos dados coletados se realizou através do Processo Facilitado de Análise e Avaliação de Risco (FRAAP), juntamente com o questionário e a análise de conteúdo, com o objetivo de apresentar os resultados obtidos que se relacionam aos objetivos específicos dessa dissertação.

Segundo Bardin (2016), a análise de conteúdo refere-se ao processo de interpretação dos dados, constituindo-se como a principal etapa de um projeto de pesquisa. A autora ressalta ainda que este processo se utiliza de indicadores (quantitativos ou não), para se chegar a uma conclusão sobre os dados que foram coletados.

A análise de conteúdo, de acordo com Gil (2008), proporciona que seja realizado o tratamento dos dados, a inferência e a interpretação, com o objetivo de que os dados sejam tornados válidos e significativos, recorrendo-se para este fim a utilização de "procedimentos estatísticos que possibilitam estabelecer quadros, diagramas e figuras que sintetizam e põem em relevo as informações obtidas".

Desta forma, o questionário instrumento desta pesquisa, foi realizado de forma estruturada conforme apêndice A, tendo início no dia 25 de junho de 2020, após aprovação concedida pelo Comitê de Ética do Centro de Ciências da Saúde da UFPB, visando coletar informações dos participantes sobre segurança da informação e

observando-se a preservação do anonimato para que não ocorresse intimidação dos sujeitos.

Foram selecionados 21 servidores técnicos administrativos em educação ocupantes de diversos cargos como, Assistentes Administrativos, Analista de Tecnologia da Informação, Técnicos de Informática, Bibliotecários, Administrador, Contador, Psicólogo, Técnicos de laboratório e Secretário Executivo, todos lotados no CCAE e pertencentes a setores diversos.

No processo de apuração dos dados, as respostas de múltipla escolha, foram ajustadas de forma a possuir um caráter dicotômico, devendo-se considerar como respostas “Sim”, as alternativas “Sempre” “Ás vezes” e “Raramente” das questões 7, 8, 9, 11, 12, 14, 15, 16, 18, 19. Para a questão 24, a alternativa “Não Sei Informar” será considera como resposta “Não”.

As questões de caráter fechado ou dicotômico são aquelas que apresentam alternativas fixas de respostas, como: sim/não; concordo/não concordo; gosto/não gosto (PRODANOV e FREITAS, 2013).

Nesta pesquisa, a realização do questionário com este tipo de questão, se deve ao fato de que, as pesquisas que realizam análise de riscos, necessitam de respostas dicotômicas ao investigar questões de fato, bem como problemas claro, facilitando a tabulação das respostas obtidas.

O quadro 6, apresenta como foi realizado o tratamento das respostas utilizadas como parte do processo de análise de riscos, que envolve o processo de gestão de segurança da informação.

Quadro 6 – Tratamento dos dados coletados

Identificação							
Nº	Perguntas	Resposta		Resultado		Percentual	
		Detalhada	Agrupada	Det.	Agr.	Det.	Agr.
1	Sexo	Masculino Feminino			13 8		61,9% 38,1%
2	Qual sua faixa etária?	18 á 29 anos 30 á 41 anos 42 á 53 anos 54 á 64 anos Acima de 64 anos		3 17 1 0 0		14,3% 81% 4,8% 0% 0%	
3	Qual seu cargo?	Resposta Aberta					
4	Qual seu tempo de ocupação no cargo?	Menos de 1 ano 1 á 7 anos 7 á 12 anos 12 á 19 anos 19 á 26 anos		7 10 3 1 0		33,3% 47,6% 14,3% 4,8% 0%	

		Acima de 26 anos		0		0%	
Módulo I – Pessoas							
5	Qual seu nível de conhecimento sobre segurança da informação?	Alto	Alto	1		4,8%	
		Médio Baixo	Baixo	10 10	20	47,6% 47,6%	95,2%
6	Você conhece a política de segurança da informação da UFPB?	Sim Não		7 14		33,3% 66,7%	
7	O Centro exige autorização de acesso ao setor por pessoas que não fazem parte da instituição?	Sempre Às vezes Raramente	Sim	7 7 3	17	33.3% 33.3% 14,3%	80,9%
		Nunca	Não	4		19%	
8	O Centro requer identificação pessoal pelo uso de crachás aos servidores?	Sempre Às vezes Raramente	Sim	3 3 3	9	14,3% 14,3% 14,3%	42,9%
		Nunca	Não	12		57,1%	
9	Ao deixar a estação de trabalho você realiza o seu bloqueio?	Sempre Às vezes Raramente	Sim	17 1 2	20	81% 4,8% 9,5%	95,2%
		Nunca	Não	1		4,8%	
10	Para senhas de acesso, qual o nível de complexidade das suas senhas?	Alto	Alto	11		52,4%	
		Médio Baixo	Baixo	7 3	10	33.3% 14,3%	47,6%
11	Você compartilha sua senha de acesso com terceiros?	Sempre Às vezes Raramente	Sim	0 3 2	5	0% 14,3% 9,5%	23,8%
		Nunca	Não	16		76,2%	
12	Você utiliza programas que não são destinados à sua função na instituição?	Sempre Às vezes Raramente	Sim	0 10 3	13	0% 47,6% 14,3%	61,9%
		Nunca	Não	8		38,1%	
13	Você já participou de alguma capacitação sobre Segurança da Informação na instituição?	Sim Não		5 16		23,8% 76,2%	
Módulo II – Processos							
14	É realizado processos de classificação e tratamento das informações de acordo com seu grau de importância?	Nunca Às vezes Raramente	Não	3 5 7	15	14,3% 23,8% 33,3%	71,4%
		Sempre	Sim	6		28,6%	
15	É necessário armazenar as documentações do setor de forma impressa?	Sim Às vezes	Sim	3 11	14	14,3% 52,4%	66,7%
		Não	Não	7		33,3%	

16	É realizado o gerenciamento de mídias removíveis como forma de prevenir que as informações sejam divulgadas sem autorização, modificadas, removidas ou destruídas?	Sempre Às vezes Raramente	Sim	3 10 4	17	14,3% 47,6% 19%	81%
		Nunca	Não	4		19%	
17	O Centro possui controles de proteção física contra desastres naturais, ataques maliciosos e acidentes?	Sim Não		1 20		1% 99%	
18	É possível recuperar as informações inerentes ao setor em lixeiras ou outros tipos de descartes?	Sempre Às vezes Raramente	Sim	4 7 6	17	19% 33,3% 28,6%	81%
		Nunca	Não	4		19%	
19	Falhas na rede elétrica comprometem os processos organizacionais?	Sempre Às vezes Raramente	Sim	8 11 2	21	38,1% 52,4% 9,5%	100%
		Nunca	Não	0		0%	
Módulo III – Tecnologia							
20	Com que frequência é realizada a atualização do antivírus?	Todos os dias. Uma vez por semana. Duas ou mais vezes por semana. Uma vez por mês. Não atualizo.	Sim	1 5 0 3	8	4,8% 23,8% 0% 14,3%	42,9%
			Não	12		57,1%	
21	É realizado restrições para instalação de softwares?	Sim Não		21 0		100% 0%	
22	É realizado algum procedimento de backup dos dados pertencentes ao setor?	Sim Não		13 8		61,9% 38,1%	
23	A organização dispõe de câmeras de segurança como parte de sua política de segurança institucional?	Sim Não		8 13		38,1% 61,9%	
24	Existe cabeamento de rede exposto que pode provocar riscos a rede de comunicação de dados do Centro?	Sim	Sim	16		76,2%	
		Não Não Sei Informar	Não	2 3	5	9,5% 14,3%	23,8%
25	Você faz uso do e-mail institucional como forma de comunicação oficial?	Sim Não		19 2		90,5% 9,5%	

Fonte: Elaborado pelo autor em pesquisa direta (2020)

Observa-se no quadro 6 que para efeito de análise das respostas coletadas, a coluna referente as respostas é composta por duas partes, onde a primeira identifica as questões presentes no formulário de forma detalhada, do mesmo modo que foi enviada aos participantes e a segunda, realiza o agrupamento destas, conferindo o caráter dicotômico no processo de análise.

As colunas seguintes apresentam os valores dos resultados que foram coletados, de forma detalhada e agrupada, bem como o percentual que estes representaram no processo de análise dos dados, contribuindo desta forma para o processo de análise de risco.

O questionário foi dividido em duas partes, onde na primeira foi realizado o processo de identificação dos participantes, objetivando conhecer o perfil dos 21 sujeitos através de quatro perguntas relacionadas ao sexo, faixa etária, o cargo que ocupa na instituição e qual o tempo de ocupação do cargo.

No segundo momento, o questionário encontra-se divido em 3 módulos, através de três categorias denominadas de pessoas, processos e tecnologia. O modulo I, referente a categoria pessoas, é composto pelas questões de 5 a 13 e aborda a temática relacionada ao conhecimento pessoal dos participantes sobre segurança da informação.

O módulo II, composto pelas questões de 14 a 19, apresenta perguntas relacionadas aos processos organizacionais que fazem parte da segurança da informação. Por fim, o módulo III, é composto por perguntas que envolvem os métodos tecnológicos que são aplicadas no ambiente organizacional como forma de minimizar os riscos relacionados à segurança da informação.

3.4.1 APRESENTAÇÃO E ANÁLISE DOS DADOS

Dos 21 entrevistados, apurou-se que 13 (61,9%) pertence ao sexo masculino, enquanto 8 (38,1%) são do sexo feminino. Em relação a faixa etária, 17 (81%) afirmou ter entre 30 e 40 anos de idade, enquanto 3 (14,3%) afirmaram possuir de 18 a 29 anos e 1 (4,8%) de 41 a 50 anos de idade. Nenhum dos participantes declarou possuir mais de 41anos.

Tabela 1 - Sexo dos participantes

IDADE	SEXO		TOTAL
	MASCULINO	FEMININO	
18 a 29 anos	3	0	3
30 a 40 anos	10	7	17
41 a 50 anos	0	1	1
51 a 58 anos	0	0	0
TOTAL GERAL	13	8	21

Fonte: Dados dos questionários respondidos pelos participantes

Em relação aos cargos ocupados, participaram da pesquisa os ocupantes dos seguintes cargos: um administrador, um analista de tecnologia da informação, seis assistente administrativo, um bibliotecário, um contador, um psicólogo, um secretário executivo, um técnico em topografia, um técnico de tecnologia da informação e sete técnicos de informática. O gráfico 1 apresenta esse resultado:

Gráfico 1 – Cargos dos entrevistados

Fonte: Elaboração própria (2020)

Quanto ao tempo de ocupação no cargo, 10 (47,6%) afirmaram possuir entre um e setes anos de ocupação, enquanto 7 (33,3%) possuem menos de um ano, 3 (14,3%) entre sete e doze anos e 1 (4,8%) entre doze e dezenove anos conforme apresentado na tabela 2.

Tabela 2 - Tempo de ocupação no cargo

EXPERIÊNCIA	MASCULINO	FEMININO
Menos de 1 ano	5	2
1 a 7 anos	7	3
7 a 12 anos	1	2
12 a 19 anos	0	1
19 a 26 anos	0	0
> 26	0	0
TOTAL GERAL	13	8

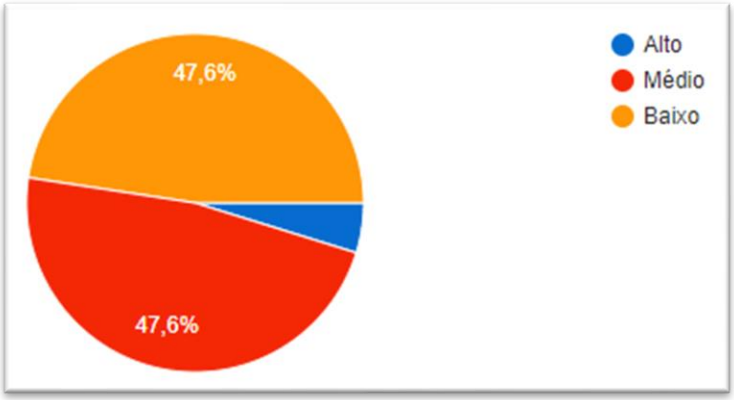
Fonte: Dados dos questionários respondidos pelos sujeitos

Observa-se um número expressivo de servidores que fazem parte da instituição com menos de um ano de exercício no cargo, fator este que ocorre devido à grande rotatividade de servidores neste centro.

3.4.2 MÓDULO I – PESSOAS

O módulo I inicia-se com a questão 5, a qual procurou identificar o nível de conhecimento sobre segurança da informação dos participantes, onde 10 (47,6%) afirmaram possuir um nível baixo e 10 (47,6%) médio sobre o tema e apenas 1 (4,8%) afirmou possuir alto conhecimento sobre boas práticas em segurança da informação, como pode-se observar no gráfico 2:

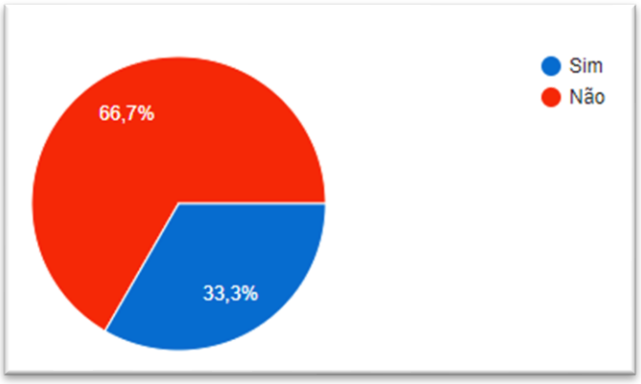
Gráfico 2 – Nível de conhecimento sobre segurança da informação



Fonte: Elaboração própria (2020)

A questão 6, se enquadra no mesmo nível de importância da anterior, ao questionar o conhecimento dos participantes sobre a PSI da UFPB, onde 14 (66,7%) afirmaram não possuir conhecimento sobre esta política e apenas 7 (33,3%) afirmaram possuir o referido conhecimento, como apresentado no gráfico 3.

Gráfico 3 – Conhecimento sobre Política de Segurança da Informação da UFPB



Fonte: Elaboração própria (2020)

A política de segurança é um documento formal elaborado pela alta direção e que deve servir como um guia aos usuários ao relatar as regras da organização referente a este recurso, possuindo como objetivo assegurar que toda informação da organização e dos seus colaboradores esteja protegida contra eventuais danos, perdas, destruição ou mal uso (FONTES, 2006).

O Art. 2º da PSI da UFPB torna clara essa ideia ao afirmar que:

> "A PSI consiste em um quadro de referência contendo princípios que norteiam a gestão da segurança da informação e que devem ser observados por professores, alunos, servidores e demais usuários que interagem com os ativos de TI da UFPB" (UFPB, 2014).

O Guia de Referência de Segurança da Informação da Presidência da República, afirma que é necessário que os colaboradores entendam a importância da segurança da informação para a organização e para o desenvolvimento das suas atividades cotidianas, devendo conhecer os danos que as falhas de segurança podem ocasionar, bem como quais são as potenciais ameaças existentes e quais as formas de se proteger (BRASIL, 2010).

A questão 7, procurou investigar se o Centro adota algum tipo de controle de acesso aos setores por pessoas que não pertencem ao seu quadro funcional, onde 7 (33,3%) afirmaram que sempre ou as vezes essa exigência é realizada, 3 (14,3%) responderam que raramente este procedimento é exigido e 4 (19%) indicaram que isto nunca acontece, o que ao ser permitido pode gerar ameaças as informações inerentes ao setor.

Ao questionar se o Centro realiza o método de identificação pessoal através do uso de crachás aos servidores, questão 8, 12 (57,1%) afirmaram que este procedimento nunca acontece, fator este que eleva o risco ao ambiente organizacional por pessoas não pertencentes ao setor pela não realização de controle de acesso físico, enquanto que apenas 3 (14,3%) indicaram que raramente, as vezes e sempre esse prerrogativa é exigida.

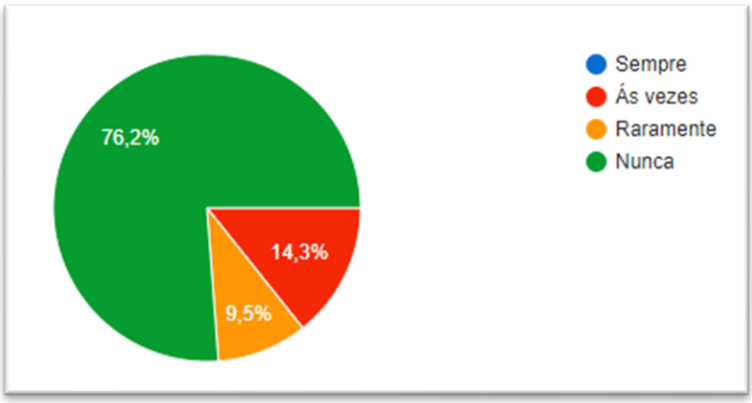
A questão 9, referente ao bloqueio da estação de trabalho quando da ausência do servidor, a grande maioria dos participantes 17 (81%) indicaram que realizam esta prática, porém 4 (19,1%) ainda afirmaram que as vezes, raramente ou nunca adotam este prática, o que apresenta um alto grau de vulnerabilidade pois deixa a estação de trabalho completamente livre ao acesso por pessoas indesejadas.

Quando perguntado sobre o nível de complexidade das senhas de acesso aos sistemas institucionais, questão 10, 11 (52,4%) dos participantes indicaram possuir senhas de alta complexidade, enquanto que 7 (33,3%) afirmaram que possuem senhas de média complexidade e 3 (14,3%) indicaram a baixa complexidade no nível das senhas.

A cartilha de boas práticas em segurança da informação elaborada pelo Tribunal de contas da união (2012) apresenta uma série de orientação aos usuários em relação a criação de senhas de acesso e enfatiza que é de fundamental importância que os usuários tenham conhecimento sobre a política de senhas definidas pela instituição para que este controle funcione de forma desejável.

A questão 11, procurou investigar se os sujeitos realizam a prática de compartilhamento de suas senhas de acesso pessoal com terceiros, onde a maioria 16 (76,2%) foram categóricos ao afirmar que nunca realizam este tipo de compartilhamento, enquanto que 3 (14,3%) relataram que as vezes realizam esta prática e 2 (9,5%) raramente o fazem, conforme podemos observar no gráfico 4:

Gráfico 4 – Compartilhamento de senhas com terceiros



Fonte: Elaboração própria (2020)

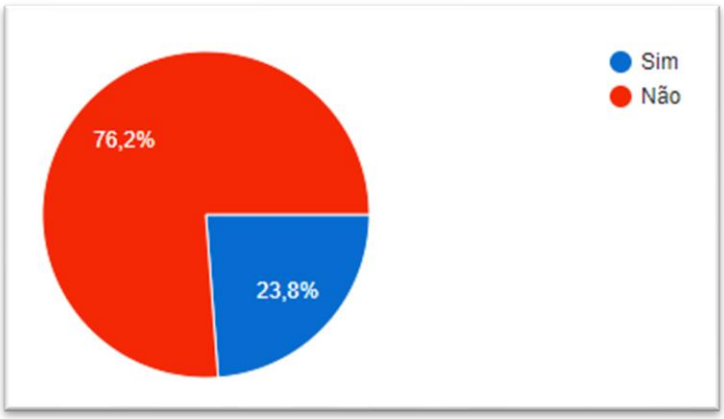
Embora a grande parte afirme não realizar o compartilhamento de senhas, 5 participantes ainda adotam esta prática, o que torna um fator preocupante, pois isto elava consideravelmente o risco de vulnerabilidade e exposição a ameaças que podem comprometer a confidencialidade e a integridade dos processos organizacionais.

A questão 12, procurou investigar se o servidor utiliza algum tipo de programa que não é inerente ao desenvolvimento de suas atividades na instituição, 10 (47,6%) afirmaram que as vezes fazem uso de softwares sem fim institucional, número este bastante expressivo e que alerta para a necessidade de um trabalho de conscientização, enquanto que 8 (38,1%) nunca realizam tal prática e 3 (14,3%) afirmam que raramente adotam o referido procedimento.

No tocante as restrições de instalações de softwares, a ABNT NBR ISO (27002), enfatiza que o não estabelecimento de regras, que definiam critérios de instalação de software por parte dos usuários, pode acarretar a introdução de vulnerabilidades, ocasionando o vazamento de informações, a perda da integridade ou a violação de direitos de propriedade intelectual.

Por fim, a questão 13, última questão do módulo I, indagou os participantes quanto a realização de capacitação sobre segurança da informação oferecida pela instituição, onde 16 (76,2%) afirmaram nunca ter realizado nenhum tipo de atividade de capacitação sobre o tema em questão e 5 (23,8%) confirmaram já ter participado de capacitação sobre este tema, conforme podemos observar no gráfico 5:

Gráfico 5 – Capacitação sobre segurança da informação



Fonte: Elaboração própria (2020)

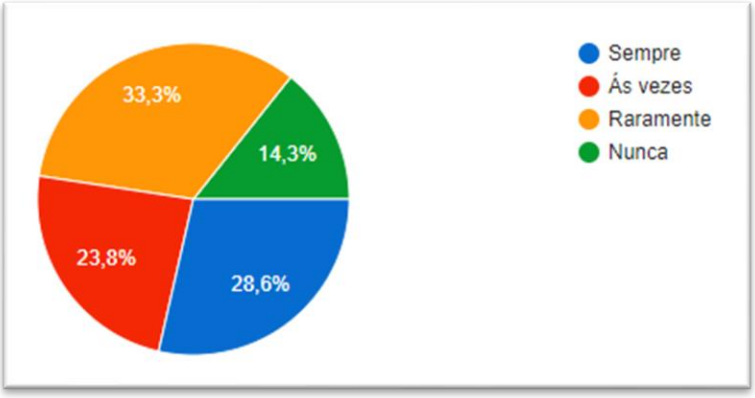
Como já mencionado nesta dissertação, os usuários constituem o elo mais fraco da corrente no processo de gestão de segurança da informação, portanto é evidente a importância da oferta de capacitação aos colaboradores da instituição, pois isto implica em orientar quais as boas práticas que deverão ser seguidas no ambiente organizacional de acordo com as normas da instituição e como mitigar os riscos a informação.

3.4.3 MÓDULO II – PROCESSOS

As questões presentes no módulo II dizem respeito aos “Processos” que são realizados no ambiente de trabalho envolvendo a classificação, tratamento, armazenamento, descarte e gerenciamento dos dados.

Desta forma, a primeira questão deste módulo, questão 14 do questionário, indagou aos participantes quanto a classificação e tratamento da informação baseado em seu grau de importância, onde 7 (33,3%) afirmaram que raramente esta prática é realizada, 5 (23,8%) as vezes adotam tal medida e 3 (14,3%) nunca a realizam, de tal forma que, agrupando estas respostas em caráter dicotômico como negativa ao questionamento (nunca, às vezes e raramente), temos que 71,4% dos participantes não realizam nenhuma ação na classificação e tratamento dos dados, enquanto que apenas 6 (28,6%) responderam que sempre realizam esta medida, como visto no gráfico 6.

Gráfico 6 – Classificação e tratamento da informação



Fonte: Elaboração própria (2020)

Nota-se que talvez não existe um procedimento formal de como deve ocorrer o tratamento da informação nos ambientes organizacionais, de tal forma que ao classificar as informações é possível que seja estabelecido um nível adequado de proteção de acordo com seu grau de importância (ABNT ISO 27002, 2013).

Na questão 15, foi questionado se os participantes necessitam realizar o armazenamento de documentações do setor de forma impressa, 11 (52,4%) responderam que as vezes realizam tal prática, 3 (14,3%) afirmaram que sim, que isto é sempre necessário e 7 (33,3%) informaram a não necessidade deste procedimento. Observa-se um alto número daqueles que gerenciam informações administrativas de forma impressa, mesmo a instituição tendo adotado práticas para erradicar os processos administrativos impressos, o que eleva o nível de ameaças que podem comprometer a integridade e sigilo das informações inerentes ao setor.

A questão 16, trata sobre o gerenciamento de mídias removíveis como forma de prevenir a captura de informações indesejáveis, onde 10 (47,6%) afirmaram que as vezes realizam tal prática, 4 (19%) raramente o fazem, 3 (14,3%) sempre praticam este ato e 4 (19%) disseram que nunca realizam nenhum tipo de gerenciamento. Observa-se que ainda existe aqueles que não adotam nenhuma prática de segurança relativa ao tema da questão, revelando desta forma a necessidade de uma política especifica ou controle que venha a disciplinar tal prática.

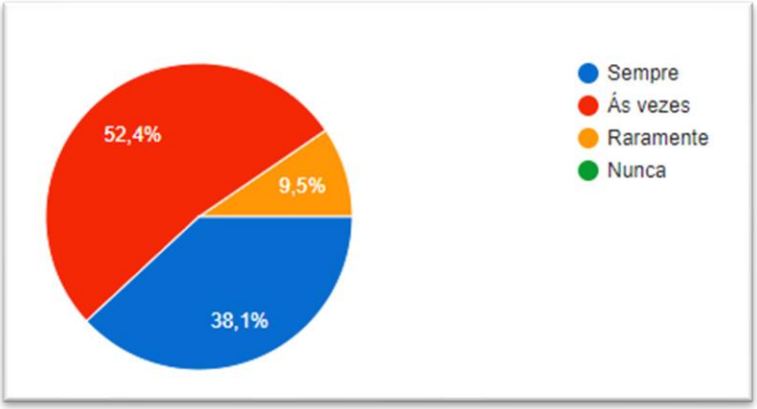
Na questão 17, ao investigar se o centro possui controles de proteção física contra desastres naturais, ataques maliciosos e acidentes, 20 (99%) foram categóricos ao relatar a não existência deste tipo de controle e apenas 1 (1%) apontou a sua existência.

Isto revela a necessidade de conhecer as potencias ameaças físicas e o nível de risco que pode pôr em risco a gestão da informação do centro em estudo e estabelecer mecanismo de controle para serem implementados como forma de atenuar as possíveis ameaças.

Sobre a possibilidade de recuperar as informações inerentes ao setor em meios não apropriados ao descarte de informações, questão 18, ao agrupar as alternativas sempre, as vezes e raramente de forma positiva, 17 (81%) afirmaram a possibilidade real que isto possa acontecer, enquanto que 4 (19%) disseram que isto nunca é possível. Este fato alerta sobre a possibilidade que terceiros possam recuperar e utilizar as informações inerentes aos setores de forma indevida, resultando assim em um elevado nível de risco.

Por último, a questão 19, investigou qual o comprometimento que falhas na rede elétrica podem ocasionar aos processos organizacionais. Para 11 (52,4%) dos participantes, às vezes, falhas do tipo podem ocasionar algum tipo de prejuízo, 8 (38,1%) afirmaram que isto sempre compromete e 2 (9,5%) relataram raramente ter algum tipo de prejuízo. Nenhum dos participantes afirmou que as falhas em sistemas elétricos nunca comprometem os processos organizacionais como podemos observar no gráfico 7:

Gráfico 7 – Falhas na rede elétrica



Fonte: Elaboração própria (2020)

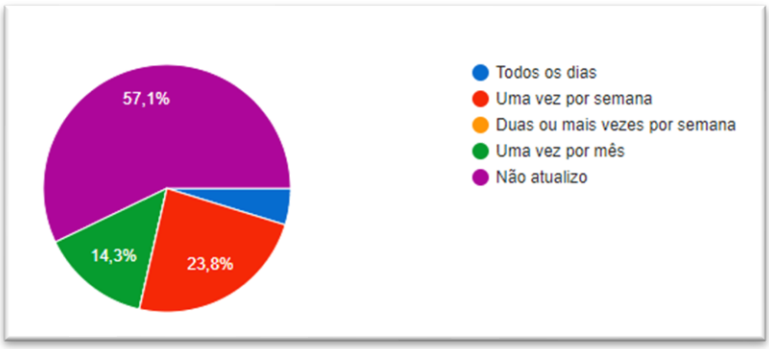
Desta forma, fica evidente que a existência de instalações elétricas precárias, podem comprometer significativamente os processos organizacionais, acarretando forte impacto nas atividades administrativas que envolvem a gestão da informação.

3.4.4 MÓDULO III – TECNOLOGIA

O módulo III apresenta questões que tratam sobre procedimentos e ferramentas de tecnologia que fazem partem do cotidiano administrativo da organização, servindo como mecanismos de combate e prevenção a possíveis ameaças no cumprimento de estratégias de segurança e que ajudam a reforçar o elo mais fraco da corrente, as pessoas.

A questão 20 presente neste módulo, tratou de investigar a periodicidade na qual os participantes realizam a atualização do antivírus presente na estação de trabalho, quanto a isso, a maioria 12 (57,1%) não realiza nenhuma atualização nesse tipo de ferramenta de segurança, 5 (23,8%) atualiza uma vez por semana, 3 (14,3%) uma vez por mês e apenas 1 participante afirmou que todos os dias é realizado a atualização do antivírus, como observa-se no gráfico 8:

Gráfico 8 – Atualização do antivírus



Fonte: Elaboração própria (2020)

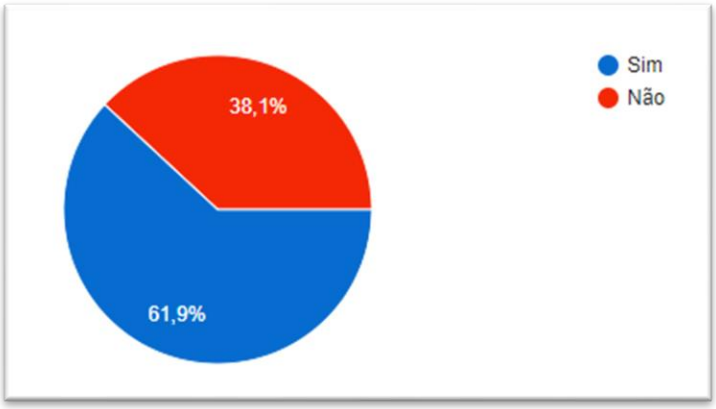
Desta forma fica evidente que existe a necessidade de estabelecer normas que regulamentem a periodicidade desta ação, pois ao não ser realizada os equipamentos e sistemas ficam expostos a ataques maliciosos o que pode comprometer a integridade, disponibilidade e confidencialidade da informação institucional.

Na questão 21, foi investigado junto ao participantes se ocorre algum tipo de restrição quanto a instalação de softwares nas estações de trabalho, onde todos os participantes 21 (100%) afirmaram a existência desta política de controle, o que corrobora com o que estabelece a ABNT NBR ISO (27002) ao recomendar o

estabelecimento e implementação de regras que versem sobre a instalação de softwares pelos usuários.

Quanto a cópias de segurança, a questões 22 questionou se é feito algum tipo de *backup* dos dados pertencentes ao setor, onde 13 (61,9%) afirmaram realizar este procedimento e 8 (38,1%) disseram que não existe nenhum tipo de ação neste sentido, como observado no gráfico 9:

Gráfico 9 – Procedimento de Backup



Fonte: Elaboração própria (2020)

Fica evidente um alto número daqueles que não fazem procedimentos de backup, elevando-se assim o risco de que, suas informações e softwares essenciais, não poderão ser recuperados de um desastre ou falhas, podendo ocorrer de forma definitiva a perda dos dados. A ABNT NBR ISO (27002) estabelece que copias de segurança do sistema e das informações, sejam realizadas e testadas com regularidade de acordo com o que prevê a política de cópias de segurança.

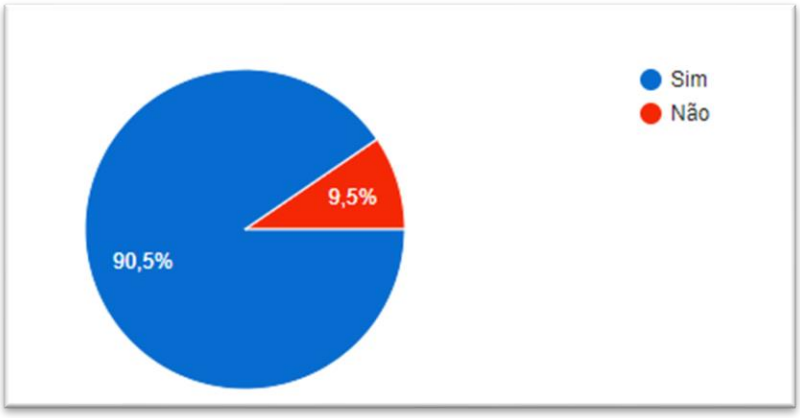
Quando questionado sobre a existência de câmeras de segurança no ambiente organizacional como forma de oferecer um mecanismo tecnológico de segurança física que diminua eventuais ameaças (questão 23), 8 (38,1%) afirmaram que a organização adota este mecanismo, enquanto que 13 (61,9%) relataram sua inexistência.

Na questão 24, indagou-se sobre a presença de cabeamento de rede exposto na infraestrutura de comunicação de dados, onde 16 (76,2%) relataram a existência deste fato, 2 (9,5%) afirmaram que não existe e 3 (14,3%) não souberam informar. A existência deste tipo de falha, põe em risco a integridade e disponibilidade dos sistemas e serviços presente na unidade organizacional, a ABNT NBR ISO (27002) enfatiza que

a proteção do cabeamento de rede deve ser realizada como forma de se evitar a interceptação, interferência ou danos.

Por fim, a questão 25 investigou se os sujeitos fazem uso do e-mail institucional como mecanismo de comunicação oficial da instituição, e obteve como resultado que, 19 (90,5%) dos participantes utilizam esta ferramenta e 2 (9,5%) não o fazem, como se pode observar no gráfico 10:

Gráfico 10 – Utilização do e-mail institucional



Fonte: Elaboração própria (2020)

Mesmo que a grande maioria afirme utilizar o e-mail institucional, ainda existe aqueles que não o fazem, fato este que pode colocar em risco a comunicação oficial existente na instituição, pois esta ferramenta atua como um instrumento importante na garantia de uma comunicação ágil, direta e segura, transmitindo ao público externo uma imagem de credibilidade.

3.5 ANÁLISE DE RISCO

Dado o processo de coleta e análise dos dados, o próximo passo foi realizar a análise de risco de acordo com as informações obtidas através do questionário e compiladas no Quadro 7. De forma a atender o objetivo desta pesquisa, o método FRAAP foi adaptado, como já mencionado anteriormente, de modo que as questões contidas no questionário estão interligadas a 12 grupos de ameaças, as quais tiveram suas respostas analisadas para em seguida estabelecer a probabilidade de ocorrência, os

possíveis impactos que podem ocasionar nos processos de trabalho, o nível de risco e quais medidas de controle poderão ser implementadas.

Com os percentuais estabelecidos no quadro 6 (tratamento dos dados coletados), na etapa seguinte, foi utilizado o quadro 3 (definições de probabilidade FRAAP), como referência para estabelecer qual a probabilidade de ocorrência das ameaças listadas, onde considera-se que, as ameaças que apresentaram o percentual acima de 50% são de nível alto, as que se encaixaram no intervalo de 30% a 50% foram consideradas como de nível médio e por fim, aquelas que ficaram abaixo de 30% foram classificadas como de baixa probabilidade de ocorrência.

Na etapa seguinte, foi estabelecido através do conhecimento empírico do pesquisador, qual o nível de impacto que as ameaças em análise podem acarretar no ambiente foco desta pesquisa, tomando-se como referência o quadro 4 (definições de impacto FRAAP), classificando como alto, quando o impacto ocasionado compromete todo o negócio, médio, quando ocorre uma perda limitada a uma unidade de negócio e baixo quando negócios são pouco afetados.

Após definir os níveis de probabilidade e impacto, o próximo passo foi realizar a soma dos valores que foram atribuídos para se estabelecer o nível de risco, os classificando em escalas que variam de acordo com a matriz de risco definida no quadro 6 (Matriz do nível de risco), onde os valores compreendidos entre 5-6 classificam o nível de risco como alto, 4 como risco médio e entre 2-3 são de nível baixo, como podemos observar no quadro 7, que apresenta os resultados da análise que foi realizada.

Quadro 7 – Análise de risco

Grupo de Ameaças	Perguntas	Probabilidade	Impacto	Nível de risco
		1 = Baixa 2 = Média 3 = Alta	1 = Baixo 2 = Médio 3 = Alto	Alto = 5-6 Médio = 4 Baixo = 2-3
1. Capacitação de funcionários	Qual seu nível de conhecimento sobre segurança da informação?	3	3	6 (Alto)
	Você conhece a Política de Segurança da Informação da UFPB?	3	3	6 (Alto)
	Você já participou de alguma capacitação sobre Segurança da Informação na instituição?	3	2	5 (Alto)
2. Acesso físico	O Centro exige autorização de acesso ao setor por pessoas que não fazem parte da instituição?	1	2	3 (Baixo)
	O Centro requer identificação pessoal pelo uso de crachás aos	3	3	6 (Alto)

	servidores?			
3.Estações de trabalho exposta	Ao deixar a estação de trabalho você realiza o seu bloqueio?	1	2	3 (Baixo)
4. Fraqueza no uso de senhas ou compartilhamento	Para senhas de acesso, qual o nível de complexidade das suas senhas?	2	3	5 (Alto)
	Você compartilha sua senha de acesso com terceiros?	1	3	4 (Médio)
5. Política de Softwares	Você utiliza programas que não são destinados à sua função na instituição?	3	3	6 (Alto)
	É realizado restrições para instalação de softwares?	1	1	2 (Baixo)
6. Classificação e tratamento da informação	É realizado processos de classificação e tratamento das informações de acordo com seu grau de importância?	3	3	6 (Alto)
	É necessário armazenar as documentações do setor de forma impressa?	3	2	5 (Alto)
	É realizado o gerenciamento de mídias removíveis como forma de prevenir que as informações sejam divulgadas sem autorização, modificadas, removidas ou destruídas?	1	2	3 (Baixo)
	É possível recuperar as informações inerentes ao setor em lixeiras ou outros tipos de descartes?	3	3	6 (Alto)
	Você faz uso do e-mail institucional como forma de comunicação oficial?	1	1	2 (Baixo)
7. Falha na rede elétrica	Falhas na rede elétrica comprometem os processos organizacionais?	3	3	6 (Alto)
8. Vírus de computador	Com que frequência é realizada a atualização do antivírus?	3	3	6 (Alto)
9. Cópias de segurança	É realizado algum procedimento de backup dos dados pertencentes ao setor?	2	3	5 (Alto)
10. Ausência de câmeras de segurança	A organização dispõe de câmeras de segurança como parte de sua política de segurança institucional?	3	3	6 (Alto)
11. Cabeamento de rede exposto	Existe cabeamento de rede exposto que pode provocar riscos a rede de comunicação de dados do Centro?	3	3	6 (Alto)
12. Ameaça externas e do meio ambiente	O Centro possui controles de proteção física contra desastres naturais, ataques maliciosos e acidentes?	3	3	6 (Alto)

Fonte: Dados da pesquisa (2020)

A primeira coluna do Quadro 7 apresenta doze grupos de ameaças que se interligam com as questões referenciadas no questionário e se relacionam com as principais ameaças existentes no ambiente da organização.

Os valores presentes na última coluna, correspondem ao nível de risco que foi encontrado com base na matriz de risco apresentada através do Quadro 5, a qual estabelece quais ações deverão ser realizadas para aplicação dos controles, onde: A – uma ação corretiva precisa ser implementada; B – uma ação corretiva deve ser implementada; C – requer monitoramento; D – nenhuma ação é necessária.

Dos grupos em análise, pode-se observar que a maioria apresentou pelo menos uma ameaça com alto nível de risco, dentre eles: capacitação de funcionários, acesso físico, fraqueza no uso de senha, política de softwares, classificação e tratamento da informação, falha na rede elétrica, vírus de computador, cópias de segurança, ausência de câmeras de segurança, cabeamento de rede exposto e ameaças externas e do meio ambiente. Todavia, apenas o grupo estações de trabalho exposta não possui ameaças que representem alto risco.

Desta forma, o quadro 8, apresenta sugestões de controles que podem ser implementados como forma de realizar ações que possam mitigar os riscos para as ameaças que foram consideradas de alto nível de risco.

Quadro 8 – Controles para riscos de alto nível

Grupo de ameaça	Ações
Capacitação de funcionários	- Implementação de programa de conscientização aos usuários atualizado e que deverá ser realizado ao menos uma vez por ano em conformidade com as políticas e procedimentos da instituição (PELTIER, 2005).
Acesso físico	- Convém que as áreas seguras sejam protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso permitido (ABNT NBR ISO 27002, 2013).
Fraqueza no uso de senha	- Convém que sistemas para gerenciamento de senhas sejam interativos e assegurem senhas de qualidade (ABNT NBR ISO 27002, 2013).
Política de softwares	- Convém que procedimentos para controlar a instalação de software em sistemas operacionais sejam implementados (ABNT NBR ISO 27002, 2013).
Classificação e tratamento da informação	- Elaboração, pela equipe gestora, de políticas e procedimentos para o apropriado tratamento e armazenamento das informações sigilosas (PELTIER, 2005). - Propiciar treinamento para usuários do sistema a fim de

	integrar esses procedimentos nas rotinas dos servidores, para que eles compreendam a manipulação dos dados e aplicações com diferentes níveis de classificação (PELTIER, 2005). - Convém que a informação seja classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada (ABNT NBR ISO 27002, 2013).
Falha na rede elétrica	- Requisitos de tempo para manutenção deverão ser monitorados e pedidos de ajustamento devem ser comunicados a gerência se a experiência garantir (PELTIER, 2005). - Convém que os equipamentos sejam protegidos contra falta de energia elétrica e outras interrupções causadas por falhas das utilidades (ABNT NBR ISO 27002, 2013).
Vírus de computador	- Instalação do padrão corporativo de software antiviral em todos os setores, incorporar nas políticas e normas da instituição técnicas de prevenção de vírus, bem como um programa de conscientização entre os envolvidos (PELTIER. 2005).
Cópias de segurança	- Convém que cópias de segurança das informações, softwares e das imagens do sistema, sejam efetuadas e testadas regularmente conforme a política de gestão de cópias de segurança definida (ABNT NBR ISO 27002, 2013).
Ausência de Câmeras de segurança	- Convém que seja projetada e aplicada segurança física para escritórios, salas e instalações (ABNT NBR ISO 27002, 2013).
Cabeamento de rede exposto	- Convém que o cabeamento de energia e telecomunicações que transporta dado ou dá suporte aos serviços de informações seja protegido contra interceptação, interferência ou danos (ABNT NBR ISO 27002, 2013).
Ameaças externas e do meio ambiente	- Convém que seja projetada e aplicada proteção física contra desastres naturais, ataques maliciosos ou acidentes (ABNT NBR ISO 27002, 2013).

Fonte: Dados da pesquisa (2020)

O quadro acima apresenta as ações que ao serem implementadas podem servir para mitigar os riscos inerentes a segurança da informação e na busca de melhorias que venham a estabelecer a proteção da informação e dos ativos existentes no ambiente organizacional.

Desta forma, observa-se que é de fundamental importância a oferta de capacitações periódicas que possuam o intuito de oferecer conscientização, treinamento e orientação acerca de boas práticas de segurança da informação que devem ser seguidas com como forma de diminuir a probabilidade de ocorrência das ameaças existentes, os impactos que estas podem ocasionar e o nível de risco que apresentam a organização.

No próximo capítulo apresenta-se o produto desta dissertação de mestrado: a proposta metodológica para implementação de um Sistema de Gestão de Segurança da Informação (SGSI) baseado nas normas ABNT NBR ISO 27001 e ABNT NBR ISO 27002. O modelo proposto possibilita a classificação da informação, identificação dos riscos, seleção de controles e a construção de um plano de ação para elaboração do SGSI.

4. METODOLOGIA PARA IMPLANTAÇÃO DE UM SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO (SGSI) BASEADO NAS NORMAS ABNT NBR ISO 27001 E ABNT NBR ISO 27002

O objetivo deste capitulo é apresentar uma metodologia para implementação de um Sistema de Gestão de Segurança da Informação (SGSI) baseado nas normas ABNT NBR ISO 27001 e ABNT NBR ISO 27002 de modo que simplifique as etapas de construção desse sistema, onde através do modelo proposto, espera-se que seja possível realizar o processo de classificação da informação, identificação dos riscos, seleção de controles e a construção de um plano de ação para elaboração do SGSI.

Segundo a ABNT NBR ISO 9000, um sistema de gestão "é um sistema que compreende as atividades pelas quais a organização identifica seus objetivos e determina os processos e recursos necessários para alcançar os resultados desejados". Assim, quando se pretende elaborar um sistema de gestão de segurança da informação, é necessário definir o que queremos de segurança, quais são os objetivos que se pretende alcançar e quais os resultados desejados, evidenciando-se que, sempre se deve realizar um alinhamento com a natureza da organização.

Como afirma Fontes (2006), para que sejam oferecidas garantias de proteção da informação no dia-a-dia de uma organização, se faz necessário que um conjunto de procedimentos que compreendam os conceitos, regulamentos e boas práticas em segurança, sejam seguidos por todos os usuários. Vale ressaltar que, a gestão da segurança da informação, deve ser vista dentro da organização como um processo de gestão (não um processo tecnológico) que objetiva implementar as orientações definidas nas normas com o intuito de mitigar os riscos a informação organizacional.

Neste sentido, as normas ABNT NBR ISO 27001 e ABNT NBR ISO 27002, apresentam um conjunto de requisitos que norteiam os procedimentos para estabelecer, operar, monitorar, analisar criticamente, manter e melhorar um SGSI. As técnicas presentes nestas normas são genéricas, podendo ser aplicadas a qualquer tipo de organização, independente da sua natureza ou porte, porém é preciso definir uma metodologia para aplicar os conceitos existentes.

4.1 ASPECTOS DA NORMA ABNT NBR ISO 27001

A norma ABNT NBR ISO 27001 apresenta em seu escopo que seu objetivo é "estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um SGSI".

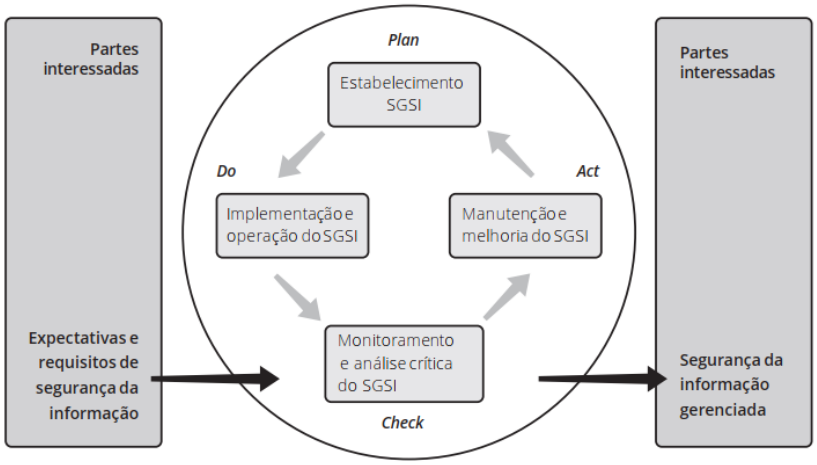
Um SGSI é análogo a um Sistema de Qualidade, desta forma é passível de certificação e esse processo ocorre a partir das evidências (documentos e práticas) que comprovem que a instituição está implantando, executando e registrando as diretrizes definidas nas normas, o que confere a credibilidade de que em todos os seus processos as informações são resguardadas, gerando consequentemente alta confiança perante a sociedade e ao mercado.

Esta norma adota um modelo denominado ciclo **"PDCA"** *(Plan-Do-Check-Act)*, o qual é utilizado como orientação para estruturar todos os processos que são definidos no SGSI. Este modelo teve sua origem em 1929 e até hoje atua como referência contínua dos sistemas de gestão do mundo, possibilitando assim, servir para as melhorias no campo da segurança da informação, bem como em outras áreas (MANOEL, 2014).

O PDCA é um método que define meios de se estabelecer um controle eficaz e confiável das atividades que são desenvolvidas na organização, possuindo o objetivo de tornar possível uma padronização nas informações relativas aos controles de qualidade e diminuir a probabilidade de erros nas análises ao tornar as informações mais entendíveis (FARIA, 2008).

Este método é composto por um conjunto de ações realizadas em sequência, representada pelas letras que compõe a sigla: **P** (*plan:* planejar), **D** (*do:* fazer, executar), **C** (*check:* verificar, controlar) e **A** (*act:* agir, atuar corretivamente), como se observa na figura 11.

Figura 11. Modelo PDCA



Fonte: ABNT (2006)

Assim, o quadro 9 define as etapas do ciclo PDCA aplicadas aos processos do SGSI de acordo com o que estabelece a norma ABNT NBR ISO 27001:

Quadro 9 – Etapas do modelo PDCA

Plan (planejar) (estabelecer o SGSI)	estabelecer a política, objetivos, processos e procedimentos do SGSI relevantes para a gestão de riscos e melhoria da segurança da informação, para produzir resultados de acordo com as políticas e objetivos globais de uma organização;
Do (fazer: implementar e operar o SGSI):	implementar e operar a política, controles, processos e procedimentos do SGSI;
Check (checar: monitorar e analisar criticamente o SGSI):	avaliar e, quando aplicável, medir o desempenho de um processo frente à política, objetivos e experiência prática do SGSI e apresentar os resultados para a análise crítica pela direção;
Act (agir: manter e melhorar o SGSI):	executar as ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e na análise crítica realizada pela direção ou em outra informação pertinente, para alcançar a melhoria contínua do SGSI.

Fonte: ABNT NBR ISO 27001 (2006)

4.2 ASPECTOS DA NORMA ABNT NBR ISO 27002

Esta norma faz parte de um do grupo de normas ISO/IEC 27000 que regulamenta todo o processo de gestão de segurança da informação. Seu objetivo principal é estabelecer diretrizes e princípios gerais para iniciar, implementar, manter e

melhorar o processo de gestão da segurança da informação em uma organização, apresentando um conjunto de controles que possuem a finalidade de gerenciar os riscos com a inclusão de políticas, procedimentos, práticas e diretrizes para implementação, de modo a atender os requisitos identificados por meio da análise/avaliação de riscos (ABNT, 2005).

Sua estrutura é composta por 11 seções de controles de segurança da informação, totalizando 39 categorias principais e uma seção introdutória que estabelece uma análise/avaliação e o tratamento de riscos. Cada seção versa sobre um tópico ou área diferente e encontra-se organizado da seguinte forma: Política de segurança da informação; Organizando a Segurança da Informação; Gestão de Ativos; Segurança em Recursos Humanos; Segurança Física e do Ambiente; Gestão das Operações e Comunicações; Controle de Acesso; Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação; Gestão de Incidentes de Segurança da Informação; Gestão da Continuidade do Negócio; Conformidade.

Assim como a ABNT NBR ISO 27001, esta norma apresenta requisitos genéricos, sendo desta forma possível de ser implementada em qualquer tipo de organização independente da sua área de atuação ou razão social (ABNT, 2006). Portanto, por ser de fácil adaptação, é esperado que a implementação de um SGSI seja realizada de acordo com as necessidades de cada organização, onde uma situação simples, requer um SGSI simples.

4.3 METODOLOGIA DE IMPLEMENTAÇÃO DE UM SGSI

O processo metodológico para implantação de um SGSI é baseado e orientado através das etapas do ciclo PDCA (Planejar, Fazer, Checar e Monitorar) e segue as orientações definidas nas normas ABNT NBR ISO 27001 e 27002. Vale salientar que elaborar uma metodologia para implementação de um projeto de segurança é uma tarefa de alta complexidade devido ao nível de detalhamento que é abordado em todos os tópicos, aspectos técnicos ou de caráter gerencial, portanto, não sendo a proposta deste método atender à necessidade especifica de uma organização, mas sim apresentar um modelo genérico que possa ser aplicado em qualquer tipo de ambiente.

As próximas seções abordam os módulos do ciclo PDCA com objetivo de definir as etapas metodológicas de implantação de um SGSI.

4.3.1 PLANEJAR

O ciclo PDCA se inicia com o módulo planejar *(Plan)*, onde deverá ocorrer o processo de estabelecimento do SGSI composto pela política, objetivos, processos e procedimentos que estão diretamente ligados com a segurança da informação e alinhados com as políticas e objetivos da organização.

A) Definição do Escopo

Para estabelecer o SGSI a norma ABNT NBR ISO 27001 orienta que incialmente se deve realizar a definição do escopo e estabelecer quais os limites que o SGSI deve abranger, observando-se as "características do negócio, a organização, sua localização, ativos e tecnologia, incluindo detalhes e justificativas para quaisquer exclusão do escopo" (ABNT, 2006).

A norma apresenta um alerta para o fato de que, a exclusão dos requisitos apresentados como fundamental a implantação do SGSI, não é aceitável caso a organização reivindique a conformidade com esta norma, a menos que seja comprovado pela pessoa responsável que tais exclusões não afetem a capacidade da organização, e/ou os requisitos de segurança determinados na avaliação de riscos.

B) Definir uma política de segurança da informação

Segundo Beal (2008), a PSI é parte fundamental de um sistema de gestão de segurança da informação eficaz, pois este documento deve conter o registro dos princípios e as diretrizes de segurança que devem ser seguidos por todos os colaboradores da organização e aplicados a todos os sistemas de informação e processos corporativos. A ABNT NBR ISO 27001 destaca que a PSI deve:

a) Incluir uma estrutura para definir objetivos e que estabeleça uma orientação global para ações que estejam envolvidas com a segurança da informação;
b) Considerar os requisitos de negócios e obrigações de segurança contratuais;
c) Realizar um alinhamento com a estratégia de riscos da organização na qual o SGSI irá ocorrer;
d) Estabelecer critérios para avaliação dos riscos;

e) Ser aprovada pela direção.

C) Criação do escopo

Para elaboração dos elementos que fazem parte do escopo da organização e que devem estar contidos no SGSI, sugere-se que seja realizado um inventário e a classificação dos ativos da informação. O quadro 10 apresenta uma forma de listar os ativos que fazem parte do SGSI bem como a indicação dos seus proprietários.

Quadro 10 – Inventário dos ativos da informação

Ativos	Proprietários
Documentos em papel	
Software	
Recursos Humanos	
Serviços ou Atividades	

Fonte: MENDES et al. (2013)

O processo de classificação dos ativos deve ser realizado com base na perda de sua confidencialidade, integridade e disponibilidade seguindo uma escala de 1 a 3, onde 1 representa um impacto pouco significativo, 2 um impacto mediano e 3 um dano que pode ser classificado como crítico, conforme o quadro 11.

Neste quadro a coluna valor deve ser composta pela média aritmética dos valores definidos em cada campo.

Quadro 11 – Classificação dos ativos da informação

Ativos	Confidencialidade	Integridade	Disponibilidade	Valor

Fonte: MENDES et al. (2013)

D) Análise de riscos

Para o processo de análise de riscos, pode-se utilizar o método FRAAP definido por Peltier (2005) como aplicado nesta pesquisa, realizando-se a identificação das

ameaças presentes no ambiente organizacional, o estabelecimento da probabilidade de ocorrência, conforme orienta o (Quadro 2 – Definições de probabilidade FRAAP), bem como o impacto que pode ser ocasionado, como visto no (Quadro 3 – Definições de impacto FRAAP), obtendo-se assim o nível de risco das ameaças presentes e a criação do quadro 12.

Quadro 12 - Análise de riscos

Ameaça	Probabilidade	Impacto	Nível de risco

Fonte: Peltier (2005)

E) Selecionar os objetivos de controle

Após a realização do processo de análise/avaliação de riscos, o próximo passo é selecionar o objetivo e a implementação dos controles que deverão ser aplicados, no qual esta seleção deverá considerar os requisitos contratuais, legais e regulamentares de aceitação dos riscos (ABNT. 2006). Nesta pesquisa foi sugerido a utilização dos controles definidos no Anexo A da norma ABNT ISO 27001.

Os objetivos de controle e os controles que são definidos no referido anexo, servem como guia para orientação dos requisitos identificados, mas como a própria norma orienta, estes não são exaustivos, podendo-se utilizar outros meios adicionais (ABNT, 2006).

F) Preparar uma declaração de aplicabilidade

A declaração de aplicabilidade deve apresentar um resumo das decisões tomadas quanto ao processo de análise de riscos, devendo conter três aspectos fundamentais:

a) Deve abordar o objetivo dos controles e quais foram os controles selecionados no tratamento dos riscos e a justificativa para esta seleção;
b) Apresentar os objetivos de controles que estão implementados na organização;
c) Detalhar quais os controles pertencentes ao SGSI que foram excluídos e a justificativa para tal exclusão.

O quadro 13 apresenta uma proposta de modelo de declaração de aplicabilidade que engloba os aspectos acima apresentados:

Quadro 13 – Declaração de aplicabilidade

DECLARAÇÃO DE APLICABILIDADE			
Versão			
Responsável pela declaração			
Responsável pela aprovação			
Última Revisão	___/___/___	Responsável:	
	___/___/___	Responsável:	
Controles	Controles já implantados	Controles em implantação	Controles não implantados/ Justificativa

Fonte: MENDES et al. (2013)

4.3.2 FAZER

Este módulo representa a segunda fase do ciclo PDCA, a qual compreende a elaboração e execução do plano de ação para implementar e executar o SGSI na prática, portanto deve ocorrer posteriormente a etapa de criação do planejamento do SGSI, devendo ser composto por três etapas, dentre elas (FARIA, 2008):

a) A formulação de um plano de tratamento de riscos que possua o objetivo de identificar a ação de gestão apropriada que deverá ser executada, recursos, responsabilidades e o estabelecimento de prioridades para a gestão dos riscos de segurança.

Para a formulação do plano de tratamento de riscos, deverá ser utilizado o plano de ação conhecido como 5W1H, o qual refere-se a uma ferramenta de qualidade estratégica que possui o objetivo de realizar um plano de ações para corrigir eventuais falhas e orientar quais ações deverão ser elaboradas e tomadas em um intervalo curto de tempo (HASS, 2010).

O 5W1H é uma sigla popular no mundo empresarial que se refere ao conteúdo que deve estar contido no plano de ação, onde deve conter **tudo o que deve ser realizado** ***(What ?)***, **quando** irá ser realizado ***(When ?)***, **quem** serão os responsáveis pelas ações ***(Who ?),*** os **porquês** de cada ação ***(Why ?),*** como estas deverão ser

realizadas ***(How ?)*** e **onde** ***(Where ?)*** serão feitas (HASS, 2010). O quadro 14 apresenta como deve ser preenchido o plano de tratamento de risco como orienta a técnica 5W1H.

Quadro 14 – Plano de tratamento de risco

PLANO DE TRATAMENTO DE RISCO						
Responsável:						
Data: ___/___/___						
Versão:						
Nº	O quê	Porque	Como	Quando	Quem	Onde
1 -						

Fonte: MENDES et al. (2013)

b) A implementação do plano de tratamento de riscos que compreenda o alcance dos objetivos de controle identificados, incluindo atribuições de papéis, responsabilidades e as considerações de financiamentos, para tanto, deve-se implementar os controles anteriormente selecionados durante o processo de análise de riscos. Em seguida, deve ocorrer a mensuração do desempenho alcançado pelo plano de tratamento de risco, definindo como medir a eficácia obtida pelos controles que foram selecionados, isso irá permitir avaliar o quanto os controles alcançaram os objetivos de controles que foram estabelecidos (ABNT, 2006).
c) O estabelecimento de programas de capacitação, a gerência das operações e dos recursos para o SGSI (ABNT, 2006).

4.3.3 CHECAR

A terceira fase do ciclo PDCA corresponde ao processo de checar, monitorar e analisar criticamente o SGSI, definindo ações que poderão ser realizadas para identificar não conformidades presentes no sistema. O processo de realização da análise crítica e a busca por não conformidades irão revelar a necessidade de implantação de novos controles e de aplicação de melhorias pontuais que poderão ser implementadas.

Neste sentido, como etapa inicial deste módulo, deverá ser realizado a análise crítica da eficácia do SGSI que deve levar em consideração, o alinhamento com a

política, os objetivos do sistema e a análise dos controles de segurança, observando-se os resultados obtidos com a "auditoria de segurança da informação, incidentes de segurança da informação, resultados da eficácia das medições, sugestões e realimentação de todas as partes interessadas" (MENDES et al., 2013).

Desta forma, uma ferramenta de qualidade que pode auxiliar nesse processo é o Diagrama de Pareto, criado pelo economista Vilfredo Pareto em 1987, cujo objetivo era estudar e descrever a desigualdade no processo de distribuição de renda no país. Com a aplicação deste método, é possível descobrir o nível de relevância das ocorrências ou não conformidades e desta forma, priorizar as ações que deverão ser aplicadas destacando os elementos de um grupo de acordo com a sua importância (FORLOGIC, 2016).

A representação do Diagrama de Pareto basicamente ocorre através de dois conjuntos de dados, composto por um gráfico de barras constituídos por elementos a serem analisados (ocorrências, não conformidades, defeitos, etc) que destacam os problemas mais recorrentes, até avançar aos menos recorrentes e por um gráfico em linha que representa a porcentagem acumulada da frequência das ocorrências (FORLOGIC, 2016).

Com a formação do Diagrama de Pareto é possível observar qual a relação entre a ação tomada e o benefício que ela proporciona e a partir da análise do gráfico determinar as ações que irão representar um melhor resultado para a organização (ELAINA, 2011). Os seguintes passos deverão ser realizados para a elaboração do diagrama:

a) Criar um quadro composto pelos aspectos que serão analisados, conforme o modelo a seguir (Quadro 15):

Quadro 15 – Identificação de não conformidades

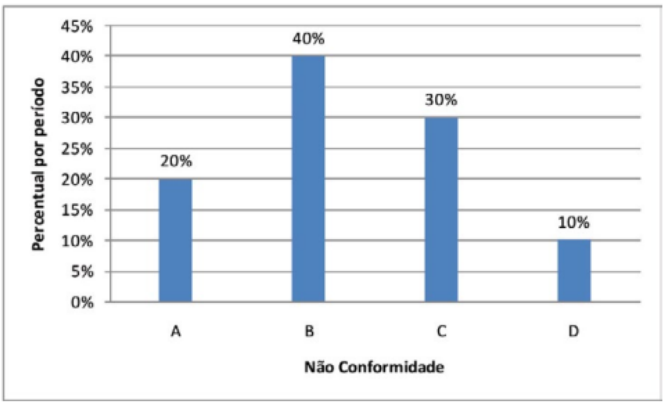
	A	**B**	**C**	**D**
Não Conformidade/ Período				
Janeiro				
...	...	...	...	...
Nº total de não conformidade				
Porcentagem				

Fonte: MENDES et al. (2013)

As colunas do quadro 15 representam as não conformidades que deverão ser analisadas, enquanto que as linhas devem fornecer a informação do número de eventos que foram detectados em determinado período, em seguida deve ser inserido o número total de não conformidade e sua porcentagem.

b) Construir um gráfico em barras logo após serem listados todos os eventos que foram diagnosticados em determinado período, como visto na figura 12.

Figura 12. Diagrama de Pareto



Fonte: MENDES et al. (2013)

Ao analisar o Diagrama de Pareto é possível detectar possíveis erros nos resultados de processamentos, identificar tentativas de violações e incidentes de segurança da informação bem sucedidos, bem como determinar se as ações que foram definidas como forma de prevenção de incidentes tiveram a eficácia esperada, adequando assim aos requisitos que estabelece a norma ABNT ISO 27001 no subitem 4.2.3 (Monitorar e analisar criticamente o SGSI).

4.3.4 AGIR

O módulo Agir compreende a última etapa do ciclo PDCA na formulação do SGSI (manter e melhorar o SGSI), onde o objetivo é a implantação de melhorias identificadas, executar ações preventivas e corretivas apropriadas, bem como fazer com que os resultados e ações alcançados sejam de conhecimento da alta direção e garantir

que as melhorias alcancem os objetivos que foram estabelecidos como forma de alcançar a melhoria contínua do SGSI (ABNT, 2006).

4.3.5 DOCUMENTAÇÃO

Para atender aos requisitos de implementação do SGSI, é preciso realizar a documentação de registros que incluam as decisões da direção e que torne possível o rastreamento das ações que foram definidas nas políticas e decisões da direção (ABNT, 2006).

Deve fazer parte da documentação do SGSI:

a) A política do SGSI;
b) O escopo do SGSI;
c) A descrição do método de análise de risco;
d) O plano de tratamento de riscos;
e) Alterações e registros posteriores, bem como os registros estabelecidos pela norma ABNT ISO/IEC 27001.

5. CONSIDERAÇÕES FINAIS

O desenvolvimento deste estudo permitiu realizar algumas considerações relevantes para problematizar a respeito das implicações que a segurança da informação representa para a UFPB e para o CCAE. Nessa perspectiva esta dissertação de mestrado, como produto, propõe uma abordagem metodológica para implementação de um sistema de gestão de segurança da informação (SGSI) baseado nas normas ABNT NBR ISO 27001 e ABNT NBR ISO 27002. A proposta metodológica apresentada para implementar o SGSI, contempla os requisitos fundamentais que as normas exigem no processo de certificação.

Outra contribuição desta pesquisa, foi identificar o nível de conhecimento dos colaboradores acerca dos procedimentos relacionados à segurança da informação através da aplicação de um questionário. Assim, os aspectos anteriormente discutidos evidenciam a importância de desenvolver novas abordagens metodológicas relacionados à segurança da informação que pressupõem uma transformação qualitativa do processo e não uma mera incorporação de novas tecnologias.

Na tentativa de sintetizar as reflexões e contribuições deste estudo, afirma-se que uma das suas contribuições mais significativas é o de apresentar uma abordagem metodológica para implementação de um sistema de gestão de segurança da informação (SGSI) baseado nas normas ABNT NBR ISO 27001 e ABNT NBR ISO 27002. Acredita-se que essa abordagem se apresenta como alternativa metodológica para o desenvolvimento de políticas para a segurança da informação.

Desta forma, o modelo apresentado serve de guia para que qualquer profissional possa implementar o SGSI em qualquer tipo de organização, contemplando os requisitos fundamentais que as normas exigem no processo de certificação.

Por fim, pode-se dizer que as contribuições do estudo e os temas que dele emergem, evidenciam a falta de critérios técnicos para se definir procedimentos de segurança da informação no âmbito institucional. Novas pesquisas poderão explorar a avaliação da metodologia apresentada, a elaboração de novas concepções sobre segurança da informação e como diversos ambientes lidam com a gestão da segurança da informação, apresentando novos métodos que busquem auxiliar na identificação das potenciais ameaças presentes no ambiente organizacional, novos métodos de análise de

risco, bem como propor uma nova metodologia para implementação de um SGSI que atenda aos requisitos definidos nas normas reguladoras.

REFERÊNCIAS

ASSOSIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO 27001. Tecnologia da informação – Técnicas de segurança – Sistemas de Gestão de Segurança da informação – Requisitos. Rio de Janeiro, 2006.

ASSOSIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO 27002. Tecnologia da informação – Técnicas de segurança – Código de prática para controles de segurança da informação. Rio de Janeiro, 2013.

ASSOSIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO 9000. Sistemas de Gestão da Qualidade – Fundamentos e vocabulário. Rio de Janeiro, 2015.

ANDRADE, A. R. de. **A informação como suporte para o planejamento e para a formulação de políticas no setor de transportes.** Tese (Doutorado na UFRJ). Rio de Janeiro, 2007.

BEAL, Adriana. **Segurança da informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações**. São Paulo: Atlas, 2005.

BRASIL. CERT.BR. **Incidentes Reportados ao CERT.br – Janeiro a Dezembro de 2018.** Brasília: Comitê Gestor da Internet no Brasil, 2018. Disponível em: <www.cert.br/stats/incidentes/2018-jan-dec/analise> Acesso em: 09 de Outubro de 2019.

Brasil. Presidência da República. Gabinete de Segurança Institucional. **Estratégia de segurança da informação e comunicações e de segurança cibernética da administração pública federal 2015-2018:** versão 1.0 / Gabinete de Segurança Institucional, Secretaria-Executiva, Departamento de Segurança da Informação e Comunicações. – Brasília: Presidência da República, 2015.

BRASIL. 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 e dá outras providências. **Diário Oficial da República Federativa do Brasil,** Brasília, DF, 14 jun. 2000. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/D3505.htm>. Acesso em: 25 de Nov. de 2019.

CAMPOS, André L. N. **Sistema de segurança da informação:** controlando os riscos. Florianópolis: Visual Books, 2006.

CARDOSO JÚNIOR, Walter Felix. **Inteligência empresarial estratégica**. Tubarão: Ed. Unisul, 2005.

CÔRTES, Pedro Luiz. **Administração de sistemas de informação**. São Paulo: Saraiva, 2008.

CHOO, Chun Wei. **A organização do conhecimento:** como as organizações usam a informação para criar significado, construir conhecimento e tomar decisões. São Paulo: SENAC, 2003.

CAVALCANTE, Luciane de F. Beckman. **Mediação da informação e comportamento informacional**, 2009. Disponível em: <http://www.ofaj.com.br/colunas.php?cod=465> Acessado em: 24 de Abril de 2020.
COELHO, F.E.S; ARAUJO, L.G.S; BEZERRA, E.K. **Gestão da segurança da informação.** 2. ed. Rede nacional de ensino e pesquisa, 2014.

DAVENPORT, T. **Ecologia da informação:** por que só a tecnologia não basta para o sucesso na era da informação. São Paulo: Futura, 1998.

FARIA, C. **PDCA (Plan, Do, Check, Action)**. Disponível em: http://www.infoescola.com/administracao/pdca-plan-do-check-action/. Acesso em: 30 jun. 2020.

FERREIRA, Antônio. A.; REIS, A. C. F., PEREIRA, M. I. **Gestão empresarial: de Taylor aos nossos dias:** evolução e tendências da moderna administração de empresas. São Paulo: Pioneira, 1997.

FONTES, Eduardo. **Segurança da informação: O usuário faz a diferença** / Edison Fontes. São Paulo: Saraiva, 2006.

Guia de Segurança – Red Hat Enterprise Linux 4: **Guia de Segurança.** Disponível em: <http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-pt_br-4/ch-sgs-ov.html> Acesso em: 07 de out. de 2019.

GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social.** São Paulo: Atlas, 2008.

HAAS, V. Sistema de qualidade: 5W1H(5W2H). 2010. Disponível em: http://www.ebah.com.br/content/ABAAABYqYAK/5w1h-5w2h#. Acesso em: 01 set. 2012.

HERNANDES, Raphael. No Brasil, empresa que falha ao proteger dados tem perdas menores. **Folha de São Paulo**, São Paulo, 23 de jul. de 2019. Disponível em: <https://www1.folha.uol.com.br/tec/2019/07/no-brasil-empresa-que-falha-ao-proteger-dados-tem-perdas-menores.shtml>. Acesso em: 12 de out. de 2019.

LAUDON, K. C.; LAUDON, J. P. **Gerenciamento de sistemas de informação.** 3. Ed. Rio de Janeiro: LTC, 2001.

MANOEL, Sergio da Silva. **Governança de segurança da informação:** como criar oportunidades para seu negócio. Rio de Janeiro: Brasport, 2014.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Metodologia do trabalho científico.** Procedimentos básicos, pesquisa bibliográfica, projeto e relatório, publicações e trabalhos. 7. ed. São Paulo: 2013.

MORIMOTO, Carlos Eduardo. **Redes - guia prático.** Porto Alegre: Sul Editores, 2010.

MORESI, E. **Delineando o valor do sistema de informação de uma organização.** Ciência da Informação, Brasília, v.29, n.1, 2000. Disponível em: <https://doi.org/10.1590/S0100-19652000000100002>. Acesso em: 20 de jan. de 2020.

NAKAMURA, Emilio Tissato; GEUS, Paulo Licio. **Segurança de Redes:** em ambientes cooperativos. São Paulo: Novatec, 2007.

Novo Dicionário Aurélio – **O Dicionário da Língua Portuguesa** – edição de 1999.

OLIVEIRA, D. P. R. **Sistemas de informações gerenciais:** estratégicas, táticas, operacionais. 14. ed. São Paulo: Atlas, 2011.

OLIVEIRA, Waldes. **Princípios Básicos da Segurança da Informação.** Tech Tem, 2019. Disponível em: <https://www.techtem.com.br/principios-basicos-da-seguranca-da-informacao/>. Acesso em: 02 de abril de 2020.

PELTIER, Thomas R. **Information security risk analisys.** 2. ed. United States: CRC Press, Taylor & Francis Group, 2005.

PRODANOV, C. C; FREITAS, E. C. **Metodologia do trabalho científico: métodos e técnicas da pesquisa e do trabalho acadêmico.** 2ª ed. Universidade Freevale - Novo Hamburgo, Rio Grande do Sul, 2013. Disponível em: <http://www.feevale.br/Comum/midias/8807f05a-14d0-4d5b-b1ad-1538f3aef538/E-book%20Metodologia%20do%20Trabalho%20Cientifico.pdf> Acessado em: 15 de jan. de 2020.

REGAZZI FILHO, Carlos L. **Normas técnicas:** conhecendo e aplicando na sua empresa. Brasília: CNI, 2000.

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

SILVA, J. L. C.; FREIRE, G. H. A. **Um olhar sobre a origem da ciência da informação: indícios embrionários para sua caracterização identitária. Encontros Bibli:** revista eletrônica de biblioteconomia e ciência da informação, v. 17, n. 33, p. 1-29, 2012.

SILVA, D. R. P. da; STEIN, L. M. **Segurança da informação: uma reflexão sobre o componente humano.** Ciência e Cognição – Revista Científica. Rio de Janeiro. v. 10. n. p. 46-53. MAR. 2007. Disponível em: <http://www.cienciasecognicao.org/revista/index.php/cec/article/view/628/410> Acesso em: 12 de dez. de 2019.

SILVA, Claudete Aurora. **Gestão da Segurança da Informação: um olhar a partir da ciência da informação.** Campinas, São Paulo, 2008.

TOIGO, Jon William. **Disaster recovery planning: preparing for the unthinkable**. 3rd ed. New jersey: Prentice Hall, PTR, 2003.

VIEIRA,T. M. **Quadro da legislação relacionada à segurança da informação. Departamento de segurança da informação e comunicação.** 2019. Disponível em: <http://dsic.planalto.gov.br/assuntos/editoria-c>. Acesso em: 22 de fev. de 2020.

WILSON, Ian. You must remember this. In: **Managing Information: As A Public Asset in the Public Interest**, Round Table series, Institute on Governance, Ottawa, 1999.

ZWASS, V. **Foundations of information Systems.** Boston: Irwin / McGraw-Hill, 1997.

APÊNDICE A – Questionário para análise dos aspectos de gestão da segurança da informação no Centro de Ciências Sociais e Aplicadas e Educação da Universidade Federal da Paraíba.

Este questionário foi aplicado com o objetivo levantar evidências no processo de análise de risco que envolve a gestão da segurança da informação no Centro de Ciências Sociais e Aplicadas da UFPB, através de 25 perguntas envolvendo as categorias: Pessoas, Processos e Tecnologia.

Como base para estrutura e elaboração, utilizou-se o método FRAAP (*Facilited Risk Analisys and Assessement Process*), bem como a norma ISO/IEC 27002:2013, que versa sobre as técnicas de segurança da informação e códigos de prática para controle de segurança da informação.

Item	**Pergunta**	**Resposta**
Identificação		
1	Sexo:	( ) Masculino ( ) Feminino
2	Qual sua faixa etária?	( ) 18 á 29 anos ( ) 30 á 41 anos ( ) 42 á 53 anos ( ) 54 á 64 anos ( ) Acima de 64 anos
3	Qual seu cargo na organização?	R.:_____
4	Qual seu tempo de ocupação no cargo	( ) Menos de 1 ano ( ) 1 á 7 anos ( ) 7 á 12 anos ( ) 12 á 19 anos ( ) 19 á 26 anos ( ) Acima de 26 anos
Módulo I – Pessoas		
5	Qual seu nível de conhecimento sobre segurança da informação?	( ) Alto ( ) Médio ( ) Baixo
6	Você conhece a Política de Segurança da Informação da UFPB?	( ) Sim ( ) Não
7	O Centro exige autorização de acesso ao setor por pessoas que não fazem parte da instituição?	( ) Sempre ( ) Ás vezes ( ) Raramente ( ) Nunca
8	O Centro requer identificação pessoal pelo uso de crachás aos servidores?	( ) Sempre ( ) Ás vezes

		( ) Raramente ( ) Nunca
9	Ao deixar a estação de trabalho você realiza o seu bloqueio?	( ) Sempre ( ) Ás vezes ( ) Raramente ( ) Nunca
10	Para senhas de acesso, qual o nível de complexidade das suas senhas?	( ) Alto ( ) Médio ( ) Baixo
11	Você compartilha sua senha de acesso com terceiros?	( ) Sempre ( ) Ás vezes ( ) Raramente ( ) Nunca
12	Você utiliza programas que não são destinados a sua função na instituição?	( ) Sempre ( ) Ás vezes ( ) Raramente ( ) Nunca
13	Você já participou de alguma capacitação sobre Segurança da Informação na instituição?	( ) Sim ( ) Não
Módulo II – Processos		
14	É realizado processos de classificação e tratamento das informações de acordo com seu grau de importância?	( ) Sempre ( ) Ás vezes ( ) Raramente ( ) Nunca
15	É necessário armazenar as documentações do setor de forma impressa?	( ) Sim ( ) Não ( ) Às vezes
16	É realizado o gerenciamento de mídias removíveis como forma de prevenir que as informações sejam divulgadas sem autorização, modificadas, removidas ou destruídas?	( ) Sempre ( ) Ás vezes ( ) Raramente ( ) Nunca
17	O Centro possui controles de proteção física contra desastres naturais, ataques maliciosos e acidentes?	( ) Sim ( ) Não
18	É possível recuperar as informações inerentes ao setor em lixeiras ou outros tipos de descartes?	( ) Sempre ( ) Ás vezes ( ) Raramente ( ) Nunca
19	Falhas na rede elétrica comprometem os processos organizacionais?	( ) Sempre ( ) Ás vezes ( ) Raramente ( ) Nunca
Módulo III – Tecnologia		
20	Com que frequência é realizada a atualização do antivírus?	( ) Todos os dias ( ) Uma vez por semana ( ) Duas ou mais vezes por semana ( ) Uma vez por mês ( ) Não atualizo

21	É realizado restrições para instalação de softwares?	( ) Sim ( ) Não
22	É realizado algum procedimento de backup dos dados pertencentes ao setor?	( ) Sim ( ) Não
23	A organização dispõe de câmeras de segurança como parte de sua política de segurança institucional?	( ) Sim ( ) Não
24	Existe cabeamento de rede exposto que pode provocar riscos a rede de comunicação de dados do Centro?	( ) Sim ( ) Não ( ) Não sei informar
25	Você faz uso do e-mail institucional como forma de comunicação oficial?	( ) Sim ( ) Não

APÊNDICE B – Lista de Controles FRAAP

Número do controle	Grupo	Descrição	Definição
1	Operação de Controles	*Backup* (Cópia de Segurança)	Requisitos de *backup* serão determinados e comunicados para os setores, incluindo envio de uma notificação eletrônica ao administrador do sistema afirmando que os *backups* foram concluídos. As operações serão solicitadas para testar os procedimentos de *backup*.
2	Operação de Controles	Plano de Recuperação	Desenvolver, documentar, testar os procedimentos de recuperação destinados a assegurar que a aplicação e a informação possam ser recuperadas, usando-se os *backups* criados, em caso de perda.
3	Operação de Controles	Análise de Risco	Realizar uma análise de risco para determinar o nível de exposição para identificar ameaças e identificar garantias possíveis de controles.
4	Operação de Controles	Antivírus	1) Assegurar que o administrador da rede local instala o padrão corporativo de software antiviral em todas as estações de trabalho. 2) Incluir nas políticas e normas da organização técnicas de prevenção de vírus, bem como um programa de conscientização entre os envolvidos.
5	Operação de Controles	Manutenção	Monitorar o tempo necessário na manutenção e se necessário, elaborar um pedido de ajuste a administração.
6	Operação de Controles	Contrato de Nível de Serviço	Adquirir e/ou manter acordos de nível de serviços com prestadores para garantir o estado operacional contínuo das aplicações.
7	Operação de Controles	Gestão da Mudança	Controles de migração de produção, como processo de busca e remoção, para garantir proteção aos dados armazenados.
8	Operação de Controles	Análise de impacto nos negócios	Uma análise de impacto formal de negócios será conduzida para determinar a criticidade relativa do ativo com outros ativos da organização.
9	Operação de Controles	Treinamento	Implementar um programa de conscientização atualizado e apresentar aos funcionários pelo menos uma vez por ano.
10	Operação de Controles	Plano de Recuperação	Implementar um mecanismo para limitar o acesso a informações confidenciais a redes específicas ou locais físicos.
11	Operação	Análise de	Implementar mecanismos de autenticação de

	de Controles	Risco	usuários (como *firewall*, senhas de acesso) para limitar permissões de acesso.
12	Operação de Controles	Aplicação de Controles	Projetar e implementar controles de aplicativos (verificação de edição de entrada de dados, campos de validação, indicadores de alarme, capacidades de expiração de senha) para garantir a integridade, confidencialidade e disponibilidade das informações da aplicação.
13	Operação de Controles	Teste de Aceitação	Desenvolver os procedimentos de teste a serem seguidos durante o desenvolvimento e durante modificações no aplicativo existente que incluem participação e aceitação.
14	Operação de Controles	Treinamento	Implementar programas de usuário (avaliação de desempenho) destinados a incentivar a conformidade com as políticas e procedimentos para garantir a utilização adequada das aplicações.
15	Aplicação de Controles	Treinamento	Os desenvolvedores de aplicativos devem fornecer apoio e documento de orientação à equipe de operações relativo à execução dos mecanismos para assegurar que a transferência de informações entre as aplicações seja segura.
16	Aplicação de Controles	Estratégias de Correção	A equipe de desenvolvimento deve desenvolver estratégias de correção tais como procedimentos reformulados, lógica de aplicação, dentre outros.
17	Controles de Segurança	Política	Desenvolver políticas e procedimentos para limitar o acesso de operações, concedendo privilégios aos que realmente precisam para o negócio.
18	Controles de Segurança	Treinamento	Treinamento do usuário irá incluir documentação sobre o uso correto das aplicações. Será destacada a importância de manter o sigilo das contas de usuário, senhas e informação competitiva.
19	Controles de Segurança	Inspeção	Incluir mecanismos de monitoração, relatórios e identificar atividades necessárias para avaliação por auditoria independente, incluindo revisões periódicas de IDs de usuários para que executem suas tarefas realmente necessárias ao negócio da instituição.
20	Controles de Segurança	Classificação de ativos	O ativo em análise será classificado de acordo com as políticas, normas e procedimentos de classificação de ativos da organização.
21	Controles de	Controle de acesso	Deverá ser implementado mecanismos de proteção do banco de dados contra acessos

	Segurança		não autorizados.
22	Controles de Segurança	Apoio da Gestão	Solicitar apoio da gestão para assegurar a cooperação e coordenação nas várias unidades de negócio.
23	Controles de Segurança	Licenças	Manter atualizados os acordos de licenças com terceiros e guardá-los em local seguro.
24	Controles de Segurança	Mecanismo de segurança	Implementar mecanismo de controle para evitar acesso não autorizado a informação, o qual deverá ser capaz de detectar, registrar e relatar tentativas de violação a segurança da informação.
25	Controles de Segurança	Controle de Acesso	Implementar mecanismos de criptografia para impedir o acesso não autorizado protegendo a integridade e confidencialidade das informações.
26	Controles de Segurança	Controle de Acesso	Consultar o núcleo de tecnologia para facilitar a implementação física dos controles de segurança projetados para proteger informação, software, hardware e sistemas.
27	Controles de Segurança	Segurança Física	Conduzir uma análise de risco para determinar o nível de exposição às ameaças identificadas e encontrar os possíveis controles.
29	Sistemas de Controle	Monitor de Logs do Sistema	Desenvolver registros de sistema, documentar e testar procedimentos de recuperação e assegurar que a aplicação e as informações possam ser recuperadas em caso de perda.

Fonte: Peltier (2005)

ANEXO A – APROVAÇÃO DO COMITÊ DE ÉTICA DO CENTRO DE CIÊNCIAS DA SAÚDE

UFPB - CENTRO DE CIÊNCIAS DA SAÚDE DA UNIVERSIDADE FEDERAL DA PARAÍBA

PARECER CONSUBSTANCIADO DO CEP

DADOS DO PROJETO DE PESQUISA

Título da Pesquisa: SEGURANÇA DA INFORMAÇÃO: UMA METODOLOGIA PARA IMPLANTAÇÃO DE UM SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Pesquisador: DIEGO CHAVES REINALDO DE SOUZA

Área Temática:

Versão: 1

CAAE: 34192020.0.0000.5188

Instituição Proponente: CENTRO DE EDUCAÇÃO

Patrocinador Principal: Financiamento Próprio

DADOS DO PARECER

Número do Parecer: 4.174.657

Apresentação do Projeto:

Projeto em Nível de Mestrado do Programa de Pós-Graduação em Políticas Públicas, Gestão e Avaliação da Educação Superior/CE/UFPB. Esta pesquisa possui uma abordagem qualitativa, do tipo exploratória, possuindo como meio de informação para compor sua base teórica, a pesquisa documental e bibliográfica. O processo de coleta de dados será realizado através de questionários on-line através do Google formulário, o qual abordará o público alvo com questões pertinentes ao nível de conhecimento sobre a gestão de segurança da informação.

Objetivo da Pesquisa:

Analisar o modelo de gestão de segurança da informação do Centro de Ciências Aplicadas e Educação da UFPB.

Avaliação dos Riscos e Benefícios:

Riscos:O presente estudo não apresenta riscos à saúde dos participantes, no entanto poderá ocorrer desconforto psicológico quando das respostas aos questionamentos, para que isso não venha ocorrer, o questionário será realizado de forma privada sem a presença de pessoas alheias ao estudo.Benefícios:Espera-se obter respostas aos problemas inerentes à segurança da informação em um ambiente organizacional, o qual possui infraestrutura tecnológica que lida com sistemas informacionais e uma quantidade expressiva de colaboradores que, ao não atuarem de acordo com as normas e padrões recomendados de segurança, podem colocar a instituição a

Endereço: UNIVERSITARIO S/N
Bairro: CASTELO BRANCO **CEP:** 58.051-900
UF: PB **Município:** JOAO PESSOA
Telefone: (83)3216-7791 **Fax:** (83)3216-7791 **E-mail:** comitedeetica@ccs.ufpb.br

UFPB - CENTRO DE CIÊNCIAS DA SAÚDE DA UNIVERSIDADE FEDERAL DA PARAÍBA

Continuação do Parecer: 4.174.657

mercê de potenciais riscos.

Comentários e Considerações sobre a Pesquisa:

Em consonância com os objetivos, referencial teórico, metodologia e referências.

Considerações sobre os Termos de apresentação obrigatória:

Apresenta a documentação de praxe.

Recomendações:

Divulgar resultados.

Conclusões ou Pendências e Lista de Inadequações:

APROVADO.

Considerações Finais a critério do CEP:

Certifico que o Comitê de Ética em Pesquisa do Centro de Ciências da Saúde da Universidade Federal da Paraíba – CEP/CCS aprovou a execução do referido projeto de pesquisa. Outrossim, informo que a autorização para posterior publicação fica condicionada à submissão do Relatório Final na Plataforma Brasil, via Notificação, para fins de apreciação e aprovação por este egrégio Comitê.

Este parecer foi elaborado baseado nos documentos abaixo relacionados:

Tipo Documento	Arquivo	Postagem	Autor	Situação
Informações Básicas do Projeto	PB_INFORMAÇÕES_BÁSICAS_DO_PROJETO_1546838.pdf	25/06/2020 14:37:53		Aceito
Orçamento	8_Orcamento.pdf	25/06/2020 14:33:44	DIEGO CHAVES REINALDO DE SOUZA	Aceito
Cronograma	7_Cronograma.pdf	25/06/2020 14:32:39	DIEGO CHAVES REINALDO DE SOUZA	Aceito
Outros	6_Questionario.pdf	25/06/2020 14:31:27	DIEGO CHAVES REINALDO DE SOUZA	Aceito
Projeto Detalhado / Brochura Investigador	5_Projeto.pdf	25/06/2020 14:30:11	DIEGO CHAVES REINALDO DE SOUZA	Aceito
Outros	4_Ata_de_aprovacao.pdf	25/06/2020 14:29:42	DIEGO CHAVES REINALDO DE	Aceito

Endereço: UNIVERSITARIO S/N
Bairro: CASTELO BRANCO CEP: 58.051-900
UF: PB Município: JOAO PESSOA
Telefone: (83)3216-7791 Fax: (83)3216-7791 E-mail: comitedeetica@ccs.ufpb.br

UFPB - CENTRO DE CIÊNCIAS DA SAÚDE DA UNIVERSIDADE FEDERAL DA PARAÍBA

Continuação do Parecer: 4.174.057

Outros	4_Ata_de_aprovacao.pdf	25/06/2020 14:29:42	SOUZA	Aceito
TCLE / Termos de Assentimento / Justificativa de Ausência	3_TCLE.pdf	25/06/2020 14:23:41	DIEGO CHAVES REINALDO DE SOUZA	Aceito
TCLE / Termos de Assentimento / Justificativa de Ausência	2_Termo_de_anuencia.pdf	25/06/2020 14:22:37	DIEGO CHAVES REINALDO DE SOUZA	Aceito
Folha de Rosto	1_Folha_de_rosto.pdf	25/06/2020 14:20:18	DIEGO CHAVES REINALDO DE SOUZA	Aceito

Situação do Parecer:
Aprovado

Necessita Apreciação da CONEP:
Não

JOAO PESSOA, 27 de Julho de 2020

Assinado por:
Eliane Marques Duarte de Sousa
(Coordenador(a))

Endereço: UNIVERSITARIO S/N
Bairro: CASTELO BRANCO **CEP:** 58.051-900
UF: PB **Município:** JOAO PESSOA
Telefone: (83)3216-7791 **Fax:** (83)3216-7791 **E-mail:** comitedeetica@ccs.ufpb.br

ANEXO B – TERMO DE ANUÊNCIA

SERVIÇO PÚBLICO FEDERAL
UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIÊNCIAS APLICADAS E EDUCAÇÃO

TERMO DE ANUÊNCIA

Declaramos para os devidos fins que estamos de acordo com a execução da pesquisa intitulada: **SEGURANÇA DA INFORMAÇÃO:** UMA METODOLOGIA PARA IMPLANTAÇÃO DE UM SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO, a ser desenvolvida pelo aluno **DIEGO CHAVES REINALDO DE SOUZA**, do **PROGRAMA DE PÓS-GRADUAÇÃO EM POLÍTICAS PÚBLICAS, GESTÃO E AVALIAÇÃO DA EDUCAÇÃO SUPERIOR DO CENTRO DE EDUCAÇÃO,** da Universidade Federal da Paraíba, sob orientação do Prof. **Dr. MARIANO CASTRO NETO**, nesta instituição.

Esta instituição está ciente de suas co-responsabilidades como instituição co-participante do presente projeto de pesquisa, e de seu compromisso em verificar seu desenvolvimento para que se possa cumprir os requisitos da Resolução 466/12 do Conselho Nacional de Saúde e suas complementares, como também, no resguardo da segurança e bem-estar dos participantes da pesquisa nela recrutados, dispondo de infraestrutura necessária para garantia de tal segurança e bem-estar.

Igualmente informamos que para ter acesso à coleta de dados nesta instituição, fica condicionada à apresentação à direção da mesma, da Certidão de Aprovação do presente projeto pelo Comitê de Ética em Pesquisa do Centro de Ciências da Saúde da Universidade Federal da Paraíba. Tudo como preconiza a Resolução 466/12 do Conselho Nacional de Saúde.

João Pessoa-PB, 25 de junho de 2020.

Erivaldo Pereira do Nascimento
Vice-Diretor do CCAE/UFPB
Siape 1543794

Erivaldo Pereira do Nascimento CPF 85309630406

ANEXO C – TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO – TCLE

ORIENTAÇÕES SOBRE TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO - TCLE

IV – DO PROCESSO DE CONSENTIMENTO LIVRE E ESCLARECIDO

O respeito devido à dignidade humana exige que toda pesquisa se processe com consentimento livre e esclarecido dos participantes, indivíduos ou grupos que, por si e/ou por seus representantes legais, manifestem a sua anuência à participação na pesquisa. Entende-se por Processo de Consentimento Livre e Esclarecido todas as etapas a serem necessariamente observadas para que o convidado a participar de uma pesquisa possa se manifestar, de forma autônoma, consciente, livre e esclarecida.

IV.1 - A etapa inicial do Processo de Consentimento Livre e Esclarecido é a do esclarecimento ao convidado a participar da pesquisa, ocasião em que o pesquisador, ou pessoa por ele delegada e sob sua responsabilidade, deverá:

a) buscar o momento, condição e local mais adequados para que o esclarecimento seja efetuado, considerando, para isso, as peculiaridades do convidado a participar da pesquisa e sua privacidade;

b) prestar informações em linguagem clara e acessível, utilizando-se das estratégias mais apropriadas à cultura, faixa etária, condição socioeconômica e autonomia dos convidados a participar da pesquisa; e

c) conceder o tempo adequado para que o convidado a participar da pesquisa possa refletir, consultando, se necessário, seus familiares ou outras pessoas que possam ajudá-los na tomada de decisão livre e esclarecida.

IV.2 - Superada a etapa inicial de esclarecimento, o pesquisador responsável, ou pessoa por ele delegada, deverá apresentar, ao convidado para participar da pesquisa, ou a seu representante legal, o Termo de Consentimento Livre e Esclarecido para que seja lido e compreendido, antes da concessão do seu consentimento livre e esclarecido.

IV.3 - O Termo de Consentimento Livre e Esclarecido deverá conter, obrigatoriamente:

a) justificativa, os objetivos e os procedimentos que serão utilizados na pesquisa, com o detalhamento dos métodos a serem utilizados, informando a possibilidade de inclusão em grupo controle ou experimental, quando aplicável;

b) explicitação dos possíveis desconfortos e riscos decorrentes da participação na pesquisa, além dos benefícios esperados dessa participação e apresentação das providências e cautelas a serem empregadas para evitar e/ou reduzir efeitos e condições adversas que possam causar dano, considerando características e contexto do participante da pesquisa;

c) esclarecimento sobre a forma de acompanhamento e assistência a que terão direito os participantes da pesquisa, inclusive considerando benefícios e acompanhamentos posteriores ao encerramento e/ ou a interrupção da pesquisa;

d) garantia de plena liberdade ao participante da pesquisa, de recusar-se a participar ou retirar seu consentimento, em qualquer fase da pesquisa, sem penalização alguma;

e) garantia de manutenção do sigilo e da privacidade dos participantes da pesquisa durante todas as fases da pesquisa;

f) garantia de que o participante da pesquisa receberá uma via do Termo de Consentimento Livre e Esclarecido;

g) explicitação da garantia de ressarcimento e como serão cobertas as despesas tidas

pelos participantes da pesquisa e dela decorrentes; e

h) explicitação da garantia de indenização diante de eventuais danos decorrentes da pesquisa.

IV.4 - O Termo de Consentimento Livre e Esclarecido nas pesquisas que utilizam metodologias experimentais na área biomédica, envolvendo seres humanos, além do previsto no item IV.3 supra, deve observar, obrigatoriamente, o seguinte:

a) explicitar, quando pertinente, os métodos terapêuticos alternativos existentes;

b) esclarecer, quando pertinente, sobre a possibilidade de inclusão do participante em grupo controle ou placebo, explicitando, claramente, o significado dessa possibilidade; e

c) não exigir do participante da pesquisa, sob qualquer argumento, renúncia ao direito à indenização por dano.

O Termo de Consentimento Livre e Esclarecido não deve conter ressalva que afaste essa responsabilidade ou que implique ao participante da pesquisa abrir mão de seus direitos, incluindo o direito de procurar obter indenização por danos eventuais.

IV.5 - O Termo de Consentimento Livre e Esclarecido deverá, ainda:

a) conter declaração do pesquisador responsável que expresse o cumprimento das exigências contidas nos itens IV. 3 e IV.4, este último se pertinente;

b) ser adaptado, pelo pesquisador responsável, nas pesquisas com cooperação estrangeira concebidas em âmbito internacional, às normas éticas e à cultura local, sempre com linguagem clara e acessível a todos e, em especial, aos participantes da pesquisa, tomando o especial cuidado para que seja de fácil leitura e compreensão;

c) ser aprovado pelo CEP perante o qual o projeto foi apresentado e pela CONEP, quando pertinente; e

d) ser elaborado em duas vias, rubricadas em todas as suas páginas e assinadas, ao seu término, pelo convidado a participar da pesquisa, ou por seu representante legal, assim como pelo pesquisador responsável, ou pela (s) pessoa (s) por ele delegada (s), devendo as páginas de assinaturas estar na mesma folha. Em ambas as vias deverão constar o endereço e contato telefônico ou outro, dos responsáveis pela pesquisa e do CEP local e da CONEP, quando pertinente.

IV.6 - Nos casos de restrição da liberdade ou do esclarecimento necessários para o adequado consentimento, deve-se, também, observar:

a) em pesquisas cujos convidados sejam crianças, adolescentes, pessoas com transtorno ou doença mental ou em situação de substancial diminuição em sua capacidade de decisão, deverá haver justificativa clara de sua escolha, especificada no protocolo e aprovada pelo CEP, e pela CONEP, quando pertinente. Nestes casos deverão ser cumpridas as etapas do esclarecimento e do consentimento livre e esclarecido, por meio dos representantes legais dos convidados a participar da pesquisa, preservado o direito de informação destes, no limite de sua capacidade;

b) a liberdade do consentimento deverá ser particularmente garantida para aqueles participantes de pesquisa que, embora plenamente capazes, estejam expostos a condicionamentos específicos, ou à influência de autoridade, caracterizando situações passíveis de limitação da autonomia, como estudantes, militares, empregados, presidiários e internos em centros de readaptação, em casas-abrigo, asilos, associações religiosas e semelhantes, assegurando-lhes inteira liberdade de participar, ou não, da pesquisa, sem quaisquer represálias;

c) as pesquisas em pessoas com o diagnóstico de morte encefálica deverão atender aos seguintes requisitos:

c.1) documento comprobatório da morte encefálica;

c.2) consentimento explícito, diretiva antecipada da vontade da pessoa, ou consentimento dos familiares e/ou do representante legal;

c.3) respeito à dignidade do ser humano;

c.4) inexistência de ônus econômico-financeiro adicional à família;

c.5) inexistência de prejuízo para outros pacientes aguardando internação ou tratamento; e

c.6) possibilidade de obter conhecimento científico relevante, ou novo, que não possa ser obtido de outra maneira;

d) que haja um canal de comunicação oficial do governo, que esclareça as dúvidas de forma acessível aos envolvidos nos projetos de pesquisa, igualmente, para os casos de diagnóstico com morte encefálica; e

e) em comunidades cuja cultura grupal reconheça a autoridade do líder ou do coletivo sobre o indivíduo, a obtenção da autorização para a pesquisa deve respeitar tal particularidade, sem prejuízo do consentimento individual, quando possível e desejável. Quando a legislação brasileira dispuser sobre competência de órgãos governamentais, a exemplo da Fundação Nacional do Índio – FUNAI, no caso de comunidades indígenas, na tutela de tais comunidades, tais instâncias devem autorizar a pesquisa antecipadamente.

IV.7 - Na pesquisa que dependa de restrição de informações aos seus participantes, tal fato deverá ser devidamente explicitado e justificado pelo pesquisador responsável ao Sistema CEP/CONEP. Os dados obtidos a partir dos participantes da pesquisa não poderão ser usados para outros fins além dos previstos no protocolo e/ou no consentimento livre e esclarecido.

IV.8 - Nos casos em que seja inviável a obtenção do Termo de Consentimento Livre e Esclarecido ou que esta obtenção signifique riscos substanciais à privacidade e confidencialidade dos dados do participante ou aos vínculos de confiança entre pesquisador e pesquisado, a dispensa do TCLE deve ser justificadamente solicitada pelo pesquisador responsável ao Sistema CEP/CONEP, para apreciação, sem prejuízo do posterior processo de esclarecimento.

APÊNDICE A

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO
(Elaborado de acordo com a Resolução 466/13 e 510/17 do CNS)

O(A) Sr.(a) está sendo convidado (a) a participar da pesquisa intitulada: **SEGURANÇA DA INFORMAÇÃO: UMA METODOLOGIA PARA IMPLANTAÇÃO DE UM SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO,** desenvolvida por **DIEGO CHAVES REINALDO DE SOUZA**, aluno regularmente matriculado no **MESTRADO PROFISSIONAL EM POLÍTICAS PÚBLICAS, GESTÃO E AVALIAÇÃO DA EDUCAÇÃO SUPERIOR** do **CENTRO DE EDUCAÇÃO** da Universidade Federal da Paraíba, sob a orientação do professor **MARIANO CASTRO NETO**.

Os objetivos da pesquisa é analisar o modelo de gestão de segurança da informação do Centro de Ciências Aplicadas e Educação da UFPB, identificando as ameaças e os riscos a segurança da informação, bem como o nível de conhecimento dos colaboradores acerca dos procedimentos de segurança da informação.

Justifica-se o presente estudo na perspectiva de fornecer uma análise dos riscos à segurança da informação, bem como, compreender o nível de conhecimento dos colaboradores sobre o referido tema. A literatura sobre o tema é escassa e pouco divulgada, fato que despertou real interesse em estudá-lo e divulgá-lo.

A participação do(a) sr.(a) na presente pesquisa é de fundamental importância, mas será voluntária, não lhe cabendo qualquer obrigação de fornecer as informações e/ou colaborar com as atividades solicitadas pelos pesquisadores se não concordar com isso, bem como, participando ou não, nenhum valor lhe será cobrado, como também não lhe será devido qualquer valor.

Caso decida não participar do estudo ou resolver a qualquer momento dele desistir, nenhum prejuízo lhe será atribuído, sendo importante o esclarecimento de que os riscos da sua participação são considerados mínimos, limitados à possibilidade de eventual desconforto psicológico ao responder o questionário que lhe será apresentado, para que isso não venha a ocorrer, será escolhido um local privado sem a interferência de pessoas alheias ao estudo, enquanto que, em contrapartida, os benefícios obtidos com este trabalho serão importantíssimos e traduzidos em esclarecimentos para a população estudada.

Em todas as etapas da pesquisa serão fielmente obedecidos os Critérios da Ética em Pesquisa com Seres Humanos, conforme Resoluções n.° 466/2012 e 510/17, ambas do Conselho Nacional de Saúde, que disciplina as pesquisas envolvendo seres humanos no Brasil.

Solicita-se, ainda, a sua autorização para apresentar os resultados deste estudo em eventos científicos ou divulgá-los em revistas científicas, assegurando-se que o seu nome será mantido no mais absoluto sigilo por ocasião da publicação dos resultados.

Caso a participação de vossa senhoria implique em algum tipo de despesas, as mesma serão ressarcidas pelo pesquisador responsável, o mesmo ocorrendo caso ocorra algum dano.

Os pesquisadores estarão a sua disposição para qualquer esclarecimento que considere necessário em qualquer etapa da pesquisa.

Eu, _____, declaro que fui devidamente esclarecido (a) quanto aos objetivos, justificativa, riscos e benefícios da pesquisa, e dou o meu consentimento para dela participar e para a publicação dos resultados, assim como o uso de minha imagem nos slides destinados à apresentação do trabalho final. Estou ciente de que receberei uma cópia deste documento, assinada por mim e pelo pesquisador responsável, como trata-se de um documento em duas páginas, a primeira deverá ser rubricada tanto pelo pesquisador responsável quanto por mim, assim como as demais assinada por ambos.

João Pessoa-PB, ____ de _____ de 2020.

Diego Chaves Reinaldo de Souza

Diego Chaves Reinaldo de Souza
Pesquisador responsável

_____
Participante da Pesquisa

Pesquisador Responsável: Diego Chaves Reinaldo de Souza
Endereço do Pesquisador Responsável: Luiz José Batista Nr. 21 Apt. 202 – Bairro: Jardim Cidade Universitária – João Pessoa-PB - CEP: 58.052-294 - Fones: 988184121 - E-mail: diegoreinaldo@gmail.com
E-mail do Comitê de Ética em Pesquisa do Centro de Ciências da Saúde da Universidade Federal da Paraíba: eticaccs@ccs.ufpb.br – fone: (83) 3216-7791 – Fax: (83) 3216-7791
Endereço: Cidade Universitária – Campus I – Conj. Castelo Branco – CCS/UFPB – João Pessoa-PB - CEP 58.051-900

OBSERVAÇÃO: No caso do pesquisado ser analfabeto, deverá ser colocado o quadrículo para colocação da impressão datiloscópica, assim como deverá ser inserido o espaço para colocação da assinatura de uma testemunha.

Diego Chaves Reinaldo de Souza

DIEGO CHAVES REINALDO DE SOUZA
Pesquisador responsável

_____
Testemunha