UNIVERSIDADE FEDERAL DA PARAÍBA

CENTRO DE CIÊNCIAS SOCIAIS APLICADAS

CENTRO DE EDUCAÇÃO

MESTRADO PROFISSIONAL EM GESTÃO NAS ORGANIZAÇÕES APRENDENTES

BRUNO ALEXANDRE BEZERRA DE AQUINO SIQUEIRA CAMPOS

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO NA ADMINISTRAÇÃO PÚBLICA: UMA ABORDAGEM SOCIOTÉCNICA

LINHA DE PESQUISA: GESTÃO DE PROJETOS EDUCATIVOS E TECNOLOGIAS EMERGENTES

JOÃO PESSOA - PB

AGOSTO/2019

BRUNO ALEXANDRE BEZERRA DE AQUINO SIQUEIRA CAMPOS

TÍTULO: POLÍTICA DE SEGURANÇA DA INFORMAÇÃO NA ADMINISTRAÇÃO PÚBLICA FEDERAL: UMA ABORDAGEM SOCIOTÉCNICA

Dissertação apresentada ao Mestrado Profissional em Gestão nas Organizações Aprendentes da Universidade Federal da Paraíba (UFPB), linha de pesquisa: **GESTÃO DE PROJETOS EDUCATIVOS E TECNOLOGIAS EMERGENTES** como requisito institucional para obtenção do Título de MESTRE.

Orientador: Prof. Drº. Pedro Jácome de Moura Jr.

JOÃO PESSOA - PB

AGOSTO/2019

Catalogação na publicação
Seção de Catalogação e Classificação

C198p Campos, Bruno Alexandre Bezerra de Aquino Siqueira.
Política de Segurança da Informação na Administração Pública Federal: Uma abordagem sociotécnica / Bruno Alexandre Bezerra de Aquino Siqueira Campos. - João Pessoa, 2019.
139 f.

Dissertação (Mestrado) - UFPB/CCSA - CE.

1. Política de Segurança da Informação. 2. Abordagem Sociotécnica. 3. Administração Pública Federal. I. Título

UFPB/BC

BRUNO ALEXANDRE BEZERRA DE AQUINO SIQUEIRA CAMPOS

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO NA ADMINISTRAÇÃO PÚBLICA FEDERAL: UMA ABORDAGEM SOCIOTÉCNICA

Projeto de Dissertação apresentado ao curso de Mestrado Profissional em Gestão de Organização Aprendentes – MPGOA da Universidade Federal da Paraíba, linha de pesquisa Gestão de Projetos Educativos e Tecnologias Emergentes.

Apresentado em: 10 / 06 / 2019

Banca Examinadora:

Prof. Dr. Pedro Jácome de Moura Jr. – Orientador – MPGOA/UFPB

Prof. Dr. Guilherme de Ataíde Dias – Examinador Interno – MPGOA/UFPB

Universidade Federal da Paraíba (UFPB)

Prof. Dr. Brivaldo André Marinho da Silva – Examinador Externo – CCSA/UFPB

Universidade Federal da Paraíba (UFPB)

AGRADECIMENTOS

A Deus, por ter me abençoado nessa conquista.

A minha mãe, que sempre me apoiou nos momentos de dificuldade e acreditou que eu conseguiria concluir essa etapa da minha vida.

A minha noiva, Danielle Nóbrega, pelo incentivo e compreensão nos momentos em que tive que abdicar para dar continuidade a pesquisa.

A meu orientador, Pedro Jácome de Moura Jr, por sempre estar disponível em ajudar e orientar da melhor forma possível.

Aos colegas do MPGOA, que sempre me incentivaram ao longo de toda pesquisa.

Aos meus chefes Zenildo Cézar e Hermes Pessoa, por terem me liberado por determinado período das atividades laborais para que eu pudesse concluir a pesquisa.

Aos membros da banca, Guilherme Ataíde e Brivaldo Marinho, pelas contribuições.

A todos que torceram por mim.

RESUMO

O presente estudo teve como objetivo analisar à luz da Abordagem Sociotécnica o cumprimento às orientações e aos requisitos de segurança da informação contidos na Política de Segurança da Informação (PSI) pelos servidores da Universidade Federal da Paraíba (UFPB). Metodologicamente, esta pesquisa tem abordagem quanti-qualitativa classificada como dos tipos exploratória e descritiva. A coleta dos dados foi realizada pessoalmente por meio de entrevista semiestruturada adaptada aos requisitos e orientações de segurança da informação da PSI/UFPB com 24 servidores da área administrativa, TI, docentes e Diretores do CCHLA, CCS, CCAE, CT, CI e CCSA. Por sua vez, a análise dos dados foi orientada por meio da Análise de Conteúdo, que previamente foram definidas categorias sociotécnicas*: pessoas, estrutura, tecnologia e tarefas* que foram relacionadas com as 18 categorias identificadas da PSI. Sucessivamente, as 18 subcategorias da PSI foram analisadas individualmente a partir das suas respectivas categorias sociotécnicas, onde foram identificadas vulnerabilidades que podem ser aproveitadas por ameaças nos procedimentos de segurança da informação implantados pelos servidores. Esse fato deve-se a ausência de conhecimento da PSI/UFPB, assim como, cursos e treinamentos na área de segurança da informação. Como resultado da pesquisa, foi desenvolvido uma Proposta de Boas Práticas de Segurança da Informação baseada em norma como a NBR ISO 27002:2013, *Guia de Boas Práticas do Tribunal de Contas da União* (2012) e sites que abordam a segurança da informação.

Palavras-Chaves: Política de Segurança da Informação. Abordagem Sociotécnica. Administração Pública Federal.

ABSTRACT

This study aimed to analyze in light of the Socio-technical Approach the compliance with the guidelines and information security requirements contained in the Information Security Policy (PSI) by the servers of the Federal University of Paraíba (UFPB). Methodologically, this research has a quanti-qualitative approach classified as exploratory and descriptive types. Data collection was performed personally through semi-structured interviews adapted to the information security requirements and guidelines of the PSI/UFPB with 24 servers from the administrative area, IT, teachers and Directors of CCHLA, CCS, CCAE, CT, CI and CCSA. In turn, the data analysis was guided by Content Analysis, which previously were defined socio-technical categories: people, structure, technology and tasks that were related to the 20 identified categories of PSI. Subsequently, the 20 subcategories of the PSI were analyzed individually from their respective socio-technical categories, where vulnerabilities were identified that can be taken advantage of by threats in the information security procedures implemented by the servers. This fact is due to the lack of knowledge of the PSI/UFPB, as well as courses and training in the area of information security. As a result of the research, it was developed a Proposal for Good Practices of Information Security based on standard such as NBR ISO 27002:2013, Good Practices Guide of the Court of Auditors of the Union (2012) and sites that address information security.

Keywords: Information Security Policy, Sociotechnical Approach, Federal Public Administration.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE QUADROS

LISTAS DE SIGLAS E ABREVIATURAS

MCC	MARSH & McLENNAN COMPANIES
APF	ADMINISTRAÇÃO PÚBLICA FEDERAL
ABIN	AGÊNCIA NACIONAL DE INTELIGÊNCIA
DSIC	DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO
GSI/PR	GABINETE DE SEGURANÇA INSTITUCIONAL PARANÁ
SIC	SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES
DOU	DIÁRIO OFICIAL DA UNIÃO
PNSI	POLÍTICA NACIONAL DE SEGURANÇA DA INFORMAÇÃO
PJ	PESSOA JURÍDICA
IFES	INSTITUTOS FEDERAIS DE ENSINO
Ufs	UNIVERSIDADES FEDERAIS
SI	SITEMA DE INFORMAÇÃO
PSI	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO
MAPA	MINISTÉRIO DA AGRICULTURA, PECUÁRIA E ABASTECIMENTO
TI	TECNOLOGIA DA INFORMAÇÃO
CGU	CONTROLADORIA GERAL DA UNIÃO
STI	SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO
GSEGI	GERÊNCIA DE SEGURANÇA DA INFORMAÇÃO
GSI	GERENCIAMENTO DE SEGURANÇA DA INFORMAÇÃO
SDI	SISTEMAS DE DETECÇÃO DE INTRUSÃO
TEM	MINISTÉRIO DO TRABALHO E EMPREGO
SUS	SISTEMA ÚNICO DE SAÚDE
IDS	SISTEMA DE IDENTIFICAÇÃO DE INTRUSÃO
RNP	REDE NACIONAL DE PESQUISA
PROGEP	PRÓ - REITORIA DE GESTÃO DE PESSOAS
AGP	AGENTE DE GESTÃO DE PESSOAS

CENTROS

CCSA	CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
CI	CENTRO DE INFORMÁTICA
CCS	CENTRO DE CIÊNCIAS DA SAÚDE
CT	CENTRO DE TECNOLOGIA
CCAE	CENTRO DE CIÊNCIAS SOCIAIS APLICADAS E EDUCAÇÃO
CCHLA	CENTRO DE CIÊNCIAS HUMANAS, LETRAS E ARTES

Sumário

1. INTRODUÇÃO

A informação é um recurso importante para diversos setores e atividades do Estado brasileiro tornando-se aspecto essencial para a gestão governamental, onde órgãos e entidades da Administração Pública Federal (APF) manipulam enorme volume de informações para realizar tomada de decisões estratégicas. Portanto, independente do formato, físico ou digital, a informação é um ativo primordial para as instituições públicas, e consequentemente, deve estar protegida de acesso de terceiros não autorizados (Governo Digital, 2019).

A partir disso, surge a preocupação com segurança da informação, a qual demanda o desenvolvimento de pesquisas sobre o impacto de incidentes de segurança nas organizações. Os resultados dessas pesquisas estimaram que o custo médio de um incidente (ataque) em uma organização cujo porte seja de mil empregados é em torno de meio milhão de dólares. Estima-se também que o tempo para recuperação das atividades após ataques é uma variável que afeta os custos, na qual, estima-se que o tempo médio de recuperação seja de 23 horas, durante as quais a organização convive com indisponibilidade de serviços (KASPERSKY, 2016).

No cenário nacional, um estudo realizado pela Norton em 2016, relatou que 42 milhões de brasileiros foram vítimas de cibercrimes, causando prejuízo de 37,1 bilhões de reais e o tempo médio gasto para lidar com esse problema gira em torno de 17 horas. O resultado de todas essas ações de cibercrimes afeta a reputação das organizações, causando prejuízos em termos de confiança e credibilidade para os clientes da organização (THORNTON, 2016).

A *Marsh & McLennan Companies* – MCC relata que, em escala mundial, os prejuízos financeiros causados por ataques cibernéticos às organizações é estimado em torno de 6,5 trilhões de reais até 2019. O estudo também aponta que as empresas vêm se preocupando com esse tema e enfatizando a importância da segurança da informação por meio de contratações de seguros contra os ataques. Os valores investidos acumulam mais de 6,2 bilhões de reais, podendo chegar à 62 bilhões de reais em 2025.

As organizações governamentais também enfrentam os mesmos problemas e desafios que as organizações privadas: a complexidade em enfrentar os diversos tipos de ameaças, dificuldade em detectar incidentes de forma proativa e consequentemente reduzir o tempo de reação aos ataques (ZANI, 2014).

Visando evitar incidentes de segurança da informação na esfera federal, desde a década de 90, o Governo Federal vem investindo e desenvolvendo Leis, Normas, Decretos e Políticas que tratam esse tema com o objetivo de que os órgãos e entidades da Administração Pública apliquem em suas atividades.

Mas o que é Administração Pública e quem a compõe? Segundo a Constituição de 1988, a Administração Pública é subdividida em direta e indireta. A APF Direta composta por órgãos que estão diretamente ligados ao chefe do poder executivo como o Governo Federal, o Presidente da República, os Ministérios, Secretarias, Coordenadorias e Departamentos. A APF Indireta é composta por órgãos com personalidade jurídica (PJ) própria, mas que desempenham funções do Estado de maneira descentralizada e em todas as esferas – Federal, Estadual, Distrital e Municipal. Exemplos de APF Indireta: fundações públicas, agências executivas, reguladoras e a autarquia como os Institutos Federais de Ensino (IFES) onde estão incluídas as Universidades Federais (UFs). Estas são criadas por meio de uma lei para executar uma atividade específica, vinculadas a Presidência da República ou Ministérios, possui patrimônio próprio, mas sujeito a fiscalização do Estado. O corpo administrativo é composto por servidores públicos que precisam previamente serem aprovados em concursos públicos para exercerem a função.

Diante do entendimento do que é a APF, as autarquias federais foram obrigadas a desenvolver Políticas de Segurança da Informação e práticas de SI nos órgãos e entidades por causa das leis e decretos do Governo Federal. Alguns exemplos como o Instituto Federal da Paraíba (IFPB) que desenvolveu sua PSI em 2011, o Instituto Federal de Pernambuco (IFPE) fez a sua PSI em 2017, o Instituto Federal de São Paulo (IFSP) desenvolveu a sua PSI em 2014, Instituto Federal do Ceará (IFCE) desenvolveu a sua PSI em 2017, a Universidade Federal de Santa Catarina desenvolveu a sua PSI em 2015. Porém, não apenas as IFES desenvolveram suas políticas, mas também os ministérios como o Ministério da Agricultura, Pecuária e Abastecimento (MAPA) em 2018, o Ministério

da Defesa em 2014 e o Ministério da Saúde que substituiu a que havia sido criada em 2010 por uma nova implantada em 2017.

A Universidade Federal da Paraíba (UFPB) por sua parte, instituiu a PSI por meio da **resolução de nº 32/2014,** na qual, estabelece diretrizes de segurança da informação a serem observadas no âmbito da Universidade e que servem de base de segurança para os recursos de Tecnologia da Informação (TI) e informações geradas dentro da UFPB. A Política possui princípios que norteiam a prática de segurança da informação e que devem ser observados por professores, alunos, servidores e demais usuários que interagirem com os ativos, redes e recursos de TI da UFPB.

Segundo o painel de Gastos da TI da Controladoria Geral da União (CGU), a UFPB investiu R$ 30.570.394,00 em ativos de TI no período de 2014 a 2018. Segundo a Superintendência de Tecnologia da Informação (STI) da UFPB, o gasto com equipamentos de segurança e redes estima-se em torno de 2 milhões por ano visando maior desempenho e segurança nas atividades da autarquia.

Operacionalmente, a Gerência de Segurança da Informação (GSEGI) da STI contribui com a segurança dos *campis* da Universidade, no que concerne o GSEGI (2019) aponta,

> "proporcionar todas as condições e orientações necessárias para que o risco de incidentes de TI possa ser diminuído ao patamar de níveis satisfatórios, procurando, com as ações de segurança, seguir as boas práticas de mercado, bem como as sugeridas, e até mesmo exigidas, por órgãos reguladores, tais como TCU e CGU."

Entretanto, mesmo com as orientações da GSEGI, os investimentos em ativos de segurança da informação, desenvolvimento e publicação da PSI/UFPB pela STI, vários incidentes de segurança da informação ocorrem na UFPB. Segundo o GSEGI, foram descobertas ameaças na rede da UFPB *Ransomware, Phishing*[1]*, Defacement Web*[2], Engenharia Social[3], *Malwares*[4] e invasão de máquinas. Todas visam o desconhecimento e fraqueza das pessoas em relação à segurança da informação. Muitas delas são oriundas

1 Ameaça que tenta obter informações sigilosas por meio de mensagens de e-mail.

2 Ataque que altera o conteúdo da página.

3 Método de ataque para se obter informações não autorizadas.

4 Programa malicioso com o intuito de causar danos no computador.

da subutilização dos ativos de TI como a instalação de *softwares* infectados da Internet e a inserção de dispositivos caseiros infectados para dentro da rede da UFPB. Zani (2014) afirma que essa prática é algo que a tecnologia em si não consegue evitar. Os funcionários e terceirizados dos setores públicos, por exemplo, possuem alguns maus hábitos trazendo consigo dispositivos móveis (*smartphones, tablets* e *notebooks*) infectados por *malwares* para o ambiente de trabalho, facilitando a inserção não intencional do acesso de ameaças aos sistemas e a rede da Instituição.

A partir disso, observa-se que as estratégias de segurança da informação originalmente focadas em contramedidas especialmente dedicadas a tecnologias (MOON, 2018; GOODHUE; STRAUB, 1991; NANCE & STRAUB, 1988; STRAUB, 1990; STRAUB; WELKE, 1998), precisam ampliar o seu propósito de atuação objetivando visão mais abrangente (GOLES & WHITE 2007; DIETRICH, 2005; KAYWORTH & WHITTEN, 2010), o que sugere uma abordagem sociotécnica, com ênfase na importância da integração da segurança da informação como foco principal, abordando aspectos do negócio e incorporando o elemento humano, processual, estrutural e tecnológico no projeto de sistemas de segurança mais eficazes.

A partir do que foi relatado pelos autores, em um cenário em que as IFEs investem em tecnologias e políticas de segurança da informação visando à segurança da informação na execução de suas atividades institucionais, foi definido como questão de pesquisa: **À luz da perspectiva sociotécnica, como os servidores da UFPB cumprem as orientações e os requisitos de segurança da informação contidos na Política de Segurança da Informação nos processos de trabalhos e ativos de TI?**

1.1 OBJETIVOS

1.1.1. Objetivo Geral

Investigar à luz da perspectiva sociotécnica, como os servidores da UFPB cumprem as orientações e os requisitos de segurança da informação contidos na Política de Segurança da Informação nos processos de trabalho e ativos de TI.

1.1.2. Objetivos Específicos

a) Identificar práticas de segurança da informação na execução das atividades pelos servidores que estão em conformidade com as orientações e os requisitos de segurança da informação contidos na PSI/UFPB;

b) Identificar vulnerabilidades de segurança da informação na execução das atividades dentro da UFPB dentro dos Centros;

c) Propor melhorias para a aplicação das orientações de segurança da informação visando alcançar os requisitos de segurança da informação contidos na PSI/UFPB.

1.2. Justificativa

A UFPB apesar de ser um órgão público e possuir informações públicas, que devem ser acessadas pela população sem restrição, também possui informações confidenciais de membros da comunidade acadêmico, que devem estar disponíveis somente para eles, assim como, as informações que auxiliam nas tomadas de decisões administrativas e que devem estar restritas pelo corpo técnico administrativo responsável.

Porém, as informações confidenciais dos órgãos públicos são de interesse de terceiros (ZANI, 2014), tornando-se passível de sofrer violações de segurança da informação que podem acarretar prejuízos à imagem e a credibilidade da organização.

Entretanto, vários aspectos podem contribuir para a violação da informação nos setores públicos, dentre eles estão o investimento desacelerado em ativos de TI que trazem consigo o benefício de processar e disseminar o acesso à informação dentro e fora das organizações, em contrapartida, a segurança da informação é por muitas vezes esquecida e inserida em segundo plano, criando vulnerabilidades que podem ser aproveitadas por ameaças.

A partir desse cenário, a UFPB vem investindo em ativos de TI de segurança da informação, buscando assim, ações proativas para tentar evitar acessos indevidos às informações da Instituição. Esses recursos tecnológicos vêm sendo importantes e eficazes quanto ao acesso externo indevido nas informações da Universidade.

Não menos importante, a UFPB desenvolveu uma Política de Segurança da Informação que contém orientações sobre segurança da informação em relação aos ativos de TI e que todos os membros da comunidade acadêmica devem seguir. Porém, estes mecanismos não vêm sendo suficientes, visto que foi relatado pela equipe do GSEGI que várias ocorrências foram informadas pelos Centros da UFPB sobre o surgimento de ameaças aos ativos de TI.

Essas situações acontecem devido a algumas ameaças que conseguem obter acesso à rede e aos ativos da Universidade não por meio de vulnerabilidades expostas pelas tecnologias de segurança da informação, mas sim das ações não intencionais dos membros da comunidade acadêmica que não são seguem orientações de segurança da informação.

2. FUNDAMENTAÇÃO TEÓRICA

Este capítulo está organizado em seis seções destinadas a abordar a teoria que servirá como base para a compreensão do assunto estudado. A primeira aborda sobre a informação, descrevendo conceitos e a sua importância para as organizações. A segunda seção trata sobre a segurança da informação, definindo conceitos e princípios de segurança da informação. A terceira seção aborda sobre as leis, decretos e normas sobre segurança da informação desenvolvidas e divulgadas pelo Governo Federal para serem aplicadas nos órgãos da APF. A quarta seção aborda sobre os eventos de segurança da informação que ocorreram em sistemas dos órgãos da APF. A quinta seção aborda sobre conceitos e definições de Política de Segurança da Informação. A sexta seção define conceitos sobre ameaças que os servidores e tecnologias da APF estão susceptíveis a sofrerem.

2.1 Informação

A informação vem sendo estudada por diversos autores e exibida de diversas maneiras. Davenport (1998) admite a dificuldade de definir, pôr o termo “informação” de maneira isolada e renova que as tentativas de fazê-lo por meio da distinção entre dados e

conhecimento resulta nitidamente em imprecisão. Pensando nisso, ele elaborou uma tabela comparativa sobre o que seria dado, informação e conhecimento, como expõe a **Tabela 1**.

Tabela 1**:** Diferença entre Dados, Informação e Conhecimento.

Dados	Informação	Conhecimento
Simples observações sobre o estado do mundo	Dados adotados de relevância e propósito	Informação valiosa da mente humana
Facilmente Estruturados; Facilmente Obtidos por Máquinas; Frequentemente quantificados; Facilmente Transferíveis	Requer unidade de análise; Exige consenso em relação ao significado; Exige necessariamente a mediação humana	Incluí reflexão, síntese, contexto; De difícil estruturação; De difícil captura em máquinas; Frequentemente tácito; De difícil transferência

Fonte: DAVENPORT, T. H. (1998).

Adicionalmente ao que cita Davenport (1998), Drucker (1988) e Drummond (2008), citam que a informação é relevante quando faz sentido e possui significado para alguém dentro de um contexto no qual está habitado.

Segundo **NBR ISO/IEC 27002:2013**, a informação pode existir em formatos como físico (escrita em papel como cartas e jornais) ou digital (arquivos de computadores, filmes e e-mail). Fontes (2010), relata que a informação, independente do seu formato, é um ativo importante para as pessoas e organizações independente do seu porte e segmento de atuação no mercado, visto que, segundo Rios et. al (2017), estas dependem incessantemente das informações para realizar seus processos decisórios, visando o planejamento das atividades estratégicas e operacionais e consequentemente o crescimento corporativo.

Portanto, relata Dzazali e Hussein (2012), devido à importância da informação, as organizações públicas possuem o desafio de protegê-las baseando-se nas normas e diretrizes de segurança da informação provenientes de órgãos centrais do governo para que sejam implantadas nos ativos tecnologias da informação das entidades subordinadas, para que, segundo a **NBR ISO 27002:2013**, não seja disponibilizada e acessada por terceiros não autorizados.

2.2 Segurança da Informação

Preconiza Sen & Samanta (2014), a segurança da informação é a prática de proteger a informação de acesso não autorizado; divulgação; destruição e corrupção. É um conceito que engloba fatores tecnológicos, estratégicos, documentos como *Política de Segurança da Informação* (PSI) e grupos interdependentes que interagem constantemente sobre SI nas organizações.

A **Norma NBR ISO 27002:2013** por outro lado define segurança da informação como a preservação da confidencialidade, integridade e disponibilidade da informação; adicionalmente, outras propriedades tais como autenticidade, responsabilidade, não repúdio e confiabilidade podem estar envolvidas com o único objetivo que é garantir a continuidade do negócio, minimizando o risco, maximizando o retorno sobre os investimentos e as oportunidades de negócio.

A segurança da informação é essencial para salvaguarda da informação necessitando estar inserida em uma boa estratégia organizacional de segurança da informação na qual estão envolvidos aspectos humanos; processos de trabalho; tecnologias e leis que busquem desenvolver capacidades para prevenir, monitorar e mitigar incidentes iniciados por ameaças externas como *hackers* e *malwares*, assim como, ameaças internas desenvolvidas por falhas humanas e funcionários insatisfeitos (NAKAMURA, 2010).

Segundo Stallings (2006), a segurança da informação quando implantada nas organizações, apresenta-se como fator crítico de sucesso tornando-se algo necessário e independente da ocasião. A partir disso, surgirão aspectos intrínsecos como a necessidade de proteger os dados, recursos e ativos de TI.

Visando esse cenário, as organizações investem em tecnologias e profissionais de segurança da informação buscando reduzir o escopo de vulnerabilidades que podem ser aproveitadas por ameaças. Entretanto, o apoio tecnológico não é suficiente, sendo necessário que outros setores estejam envolvidos e motivados para contribuir com a segurança da informação organizacional. Por consequência, as organizações vêm selecionando funcionários buscando encontrar perfis que se encaixam com o objetivo organizacional que é potencializar a segurança da informação institucional, evitando assim

equívocos ao selecionar funcionários desmotivados ou que não tenham interesse quanto à segurança da informação (SCHLIENGER, 2002).

Anteriormente, as organizações adotavam perfil reativo em relação à segurança da informação, porque os diretores e executivos não tinham visão de boa estratégia de segurança da informação e não conseguiam enxergar sua importância, colocando-a em segundo plano: segmentando orçamento praticamente inexistente em relação a essa temática, considerando-a sem retorno financeiro, cara e supérflua. Logo, a real necessidade era reconhecida quando ocorria incidente de segurança da informação que causavam prejuízos financeiros, imagem e credibilidade imensuráveis para a organização (NAKAMURA, 2010).

A partir desse potencial escala de perda financeira e advinda de violações de segurança da informação, as organizações direcionam-se a proteger rigorosamente seus ativos de informação, investindo em segurança da informação (MOON et. al, 2018).

Segundo Nakamura (2010), investimento em segurança da informação tornou-se estratégico. As organizações estão reservando parte do seu orçamento para adquirir tecnologias e treinamentos visando à capacitação dos funcionários com o objetivo de implantar a segurança da informação com eficiência. Essa ação direcionará o negócio para o caminho seguro em conjunto com o alinhamento do negócio (KAYWORTH & WHITTEN, 2010).

A necessidade de segurança da informação é uma realidade que vem ultrapassando os limites da produtividade e funcionalidade. As ações de negócio exigem cada vez mais velocidade e eficiência atreladas à segurança da informação evitando prejuízos exponenciais que venham prejudicar oportunidades de negócios futuras (BOSWORTH et. al, 2014).

2.2.1. Princípios de segurança da informação

Segundo a Norma **NBR ISO 27002:2013**, a SI possui alguns princípios: a disponibilidade, integridade e confidencialidade da informação como apresenta a **Figura 1**.

Figura 1**:** Tríade Composta pelos Princípios da SI.

Fonte: ISO 27002:2013

Entretanto, o *não-repúdio, confiabilidade, responsabilidade e autenticidade* são considerados princípios implícitos de segurança da informação.

Confidencialidade: garante Fonte (2010), a informação deve estar disponível somente a quem tem permissão para acessar o seu conteúdo. Afirmam Goodrich e Tamassia (2013), garantir a confidencialidade é não permitir a divulgação não autorizada da informação. Logo, a **ISO NBR 27001:2013** conclui que, a confidencialidade é a propriedade de que informação não esteja disponível ou revelada a indivíduos e entidades não autorizados.

De acordo com os autores supracitados, para garantir a confidencialidade, pesquisadores de segurança da informação e projetistas de sistemas têm desenvolvido ferramentas que buscam proteger a informação para garantir que este princípio não seja corrompido:

a) **Encriptação:** modificar a informação por meio de uma chave de encriptação, de forma que a informação se torne acessível apenas por chave de decriptação. Exemplo: Criptografia;

b) **Controle de Acesso:** permissões atribuídas que limitam o acesso à informação confidencial apenas para pessoas ou sistemas autorizados. Exemplo: Papéis desempenhados na organização.

c) **Autenticação:** Identificação única de alguém. Exemplo: *Smartcard*, senha e impressão digital.

d) **Segurança Física:** implantação de barreiras físicas para bloquear o acesso a ativos de TI. Exemplo: Cadeado e chaves em portas e armários.

Integridade: segundo a **NBR ISO 27002:2013**, é a propriedade de salvaguarda da exatidão e completeza da informação, adicionalmente, Fontes (2010) declara que o princípio da integridade prevê que a informação seja modificável somente por pessoas autorizadas visando mantê-la correta e verdadeira. Conforme os autores Goodrich e Tamassia (2013), várias ferramentas foram projetadas e desenvolvidas para dar suporte a integridade como cópias de segurança, *backup* e etc.

Disponibilidade: segundo a **NBR ISO 27002:2013**, é a propriedade da informação estar acessível e funcional, a qualquer momento, por entidade autorizada, adicionalmente, comenta Fontes (2010), que este princípio auxilia a organização para alcançar os objetivos e missões da organização. No que concerne a Goodrich e Tamassia (2013), pode ser garantida por meio de redundância computacional como dispositivo *backup* de dados e redundância.

Expõe Goodrich & Tamassia (2013), a **autenticidade** é a capacidade de atribuir que algumas ações, políticas e permissões originárias de pessoas ou sistemas são legítimas. A autenticidade pode ser garantida por assinatura digital. Segundo a **NBR ISO 27002:2013**, **confiabilidade** é garantia de tolerância a falhas de um sistema de informação. Segundo Fonte (2010), **não-repúdio ou irretratabilidade** é qualquer ato legítimo realizado por pessoa ou sistema que não pode ser negado sua autoria. Pode ser aplicado por assinatura digital.

2.3. Leis, Decretos e Normas sobre a Gestão da segurança da informação nos órgãos da informação nos órgãos da Administração Pública Federal

No cenário onde as informações estão migrando para o ambiente virtual, existe a preocupação constante em relação a possíveis violações de segurança da informação que podem acarretar na divulgação imprópria da informação em meios de comunicação como blogs e sites de *hackers.* Alguns exemplos são os grupos *WIKILEAKS* (wikileaks.org) e o *Anonymous* que dispõem informações sigilosas sobre órgãos governamentais.

Diante dessa situação, a segurança da informação na APF é tema forte do Governo Brasileiro, estabelecido como agenda estratégica no setor público desde a **Lei 8.159/1991**, que afirma:

> “é dever do poder público a gestão documental e a proteção especial a documentos de arquivos, como instrumento de apoio à administração, à cultura, ao desenvolvimento científico e como elementos de prova e informação.”

Posteriormente surgiram vários dispositivos legais como normas, decretos, cartilhas e instruções normativas que tratam de sua aplicação na esfera federal, cuja observância é obrigatória (SOUZA, 2017) o que ratifica e acrescenta (ARAÚJO, 2012; VIEIRA, 2008), o Brasil não detém apenas uma Lei única para abordar a segurança da informação, mas no conjunto de sua legislação, várias podem ser implantadas em relação ao tema.

No ano de 1999, a agência brasileira de inteligência (ABIN), criada por meio da **Lei 9.883**, passou a ser responsável por desenvolver programas e ferramentas que garantem a transmissão segura de informações do Governo Federal.

Em 13 de junho de 2000, o **Decreto nº 3.505**, institui a PSI nos órgãos e entidades da APF. Este decreto, por exemplo, estimula o desenvolvimento da mentalidade de segurança por meio do uso de tecnologias de defesa, assim como a conscientização dos órgãos quanto às informações processadas e suas vulnerabilidades, uso de produtos em conformidades com as leis e promover a capacitação de recursos humanos quanto ao desenvolvimento de competência tecnológica em SI etc. Este Decreto institui o Comitê Gestor da Segurança da Informação (CGSI) que assessora a Secretaria Executiva do Conselho de Defesa Nacional, exercida pelo Gabinete Segurança Institucional da Presidência da República (GSI/PR), na consecução das diretrizes da Política de Segurança da Informação (PSI), nos órgãos e nas entidades da APF, bem como na avaliação e análise de assuntos relativos aos objetivos estabelecidos no referido Decreto.

Em 28 de junho de 2001, a medida provisória de n° 2.200 Institui a Infraestrutura de Chaves Públicas Brasileira – ICP Brasil, que trata assegurar a autenticidade, a integridade e validade jurídica de documentos em forma eletrônica que utilizem certificados digitais, assim como as transações eletrônicas.

Em 2007, o **Decreto n° 5.772**, de 08 de maio de 2006, cria dentro do GSI/PR, o Departamento de Segurança da Informação – DSIC. Este departamento detém a função dentre elas: realizar medidas para planejar, coordenar a segurança da informação e comunicações da APF; definir requisitos metodológicos para implementação da segurança

da informação e comunicações pelos órgãos e entidades da APF e operacionalizar e manter centro de tratamento e resposta a incidentes ocorridos nas redes de computadores da APF.

Em 2008, lançou a Instrução **Normativa GSI/PR n° 01/2008**, onde disciplina a Gestão de Segurança da Informação e Comunicações na APF direta e indireta, dá outras providências como sobre orientações e atribuições de competências em relação à segurança da informação para departamentos, comitês e gestores do governo federal.

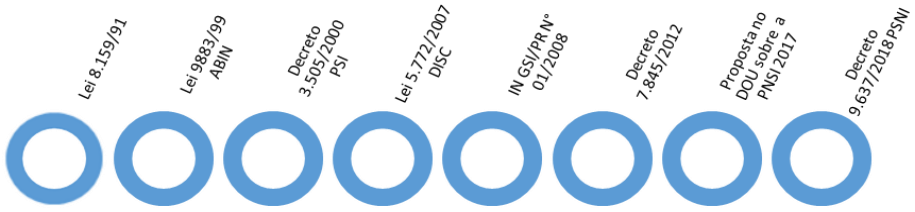
Em 2012, o **Decreto de nº 7.845**, onde regulamenta os procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento no âmbito do Poder Executivo Federal.

Em 2017, O **GSI/PR** publicou, no Diário Oficial da União (DOU), e instituiu, no âmbito de seu DSIC para elaborar proposta de Política Nacional de Segurança da Informação (PNSI) onde deverá reconhecer a informação como um bem econômico e de valor social, gerador de trabalho e renda e promotor de cidadania; abordar variáveis social, cultural, econômica e tecnológica; promover cooperação entre os entes públicos, setor empresarial e sociedade civil; abranger segurança das infraestruturas críticas nacionais e proteção das informações pessoais e biométricas.

Em 2018, o **Decreto n° 9.637** institui a Política Nacional de Segurança da Informação no âmbito da APF, com a finalidade de assegurar à disponibilidade, a integridade, a confidencialidade e a autenticidade da informação a nível nacional que abrange a segurança cibernética, a defesa cibernética, a segurança física e a proteção de dados organizacionais.

A **Figura 2** ilustra em ordem cronológica alguns documentos e ações do governo federal em termos de segurança da informação.

Figura 2**:** Ações do Governo Federal em Ordem Cronológica.



Fonte: Desenvolvida pelo autor (2019).

2.4. Eventos de Segurança da Informação na Administração Pública Federal

Mesmo com a preocupação do Governo Federal em criar Leis, Decretos e Instruções Normativas relacionadas à segurança da informação, os problemas em relação a vazamento de informações, ou quebra do sigilo em instituições públicas são ocorrem eventualmente.

Menciona Rohr (2011), a *Kaspersky Lab* divulgou sobre a subsistência de sites ilegais que disponibilizam informações pessoais como endereço, sexo, data de nascimento e nome da mãe de brasileiros. Os dados foram retirados de uma vulnerabilidade do sistema do próprio Ministério do Trabalho e Emprego (MTE).

Informa Tecnoblog (2011), o grupo hacktivista Anonymous *"divulgou um arquivo que possui logins e endereços de e-mail de diversos sites do governo brasileiro, como Ministério do Meio Ambiente e Ministério Público do Estado do Pará (MPPA).*"

Em abril de março de 2019, segundo a Justiça (2019), comunica

> "Receita Federal solicitou abertura de inquérito policial visando investigar o vazamento de dados para veículos da imprensa que contêm análises fiscais que envolvem autoridades e seus familiares, além de outras 130 pessoas."

Alude Padrão (2019) um banco de dados do Sistema Único de Saúde (SUS) foi *hackeado* e publicado em um site divulgando informações de 2,4 milhões de usuários como nome, CPF, endereço e data de nascimento. O ataque obteve êxito por meio de uma vulnerabilidade descoberta em um aplicativo do SUS chamado de CadSUS (Cadastro do Sistema Único de Saúde). O atacante havia tentado comunicação com o Ministério da

Saúde via e-mail dias antes, para notificar tal vulnerabilidade, porém não obteve retorno do órgão público e não houve correção no código do programa.

2.5. Política de Segurança da Informação

A política é uma regra geral, dentro de um ambiente organizacional, que define as ações e limites para alcançar os objetivos e metas organizacionais. É um documento que define as diretrizes e controles de segurança da informação que a organização deseja que sejam implantados na proteção da informação (RIOS et. al, 2017; ALBUQUERQUE Jr. & SANTOS, 2014).

Em segurança da informação, a **NBR ISO 27002:2013** define que, um documento de PSI deve ser aprovado pela Alta Direção e divulgado amplamente para que todos os funcionários e partes externas interessadas e relevantes tenham conhecimento, pois estes são componentes de um sistema sociotécnico complexo dentro das organizações (WEIDMAN & GROSSKLAGS, 2018).

A PSI deve ser clara e compreensível a quem deve ter conhecimento sobre este documento para orientar em relação às práticas de segurança da informação e agir concomitantemente de acordo com os requisitos do negócio, as leis, as regulamentações relevantes (**NBR ISO 27002:2013**) e a missão da organização (MONTEIRO, 2009).

A PSI é uma boa prática de segurança da informação para que as organizações desenvolvam suas ações de segurança da informação e implantem nos seus processos de trabalho. Entretanto, não é um documento estático, necessitando ser revisado e analisado criticamente a intervalos planejados ou quando mudanças significativas ocorrerem para assegurar sua contínua pertinência, adequação e eficácia (FONTES, 2010).

Expressam Martins e Eloff (2001), a PSI influenciará no comportamento dos empregados como ações do que é aceitável como quais medidas de segurança uma organização deve proceder para proteger seus bens físicos e os dados armazenados em componentes tecnológicos, adicionalmente, a **NBR ISO 27002:2013** conclui que, na ausência deste documento, as partes interessadas não saberão o que fazer e como comportar-se em situações de risco de segurança da informação.

Porém, além da PSI, é preciso que as partes interessadas sejam treinadas, educadas e conscientizadas em relação à segurança da informação para que implantem ações de segurança da informação nos processos de trabalho. (WEIDMAN & GROSSKLAGS, 2018).

Informa a **NBR ISO 27002:2013**, a PSI deverá conter:

a) uma definição de segurança da informação;

b) uma declaração do comprometimento da direção;

c) uma estrutura para estabelecer os objetivos de controle e os controles, incluindo a estrutura de análise/avaliação e gerenciamento de risco;

d) breve explanação das políticas, princípios, normas e padrões de segurança da informação (devem ser especificadas as consequências das violações na política de segurança da informação);

e) definição das responsabilidades gerais e específicas na gestão da segurança da informação;

f) referências à documentação que possam apoiar a política.

2.6. Ameaças

A **NBR ISO 27005:2011** define como:

> “ameaça é toda e qualquer evento que possa explorar vulnerabilidades; É a causa potencial de um incidente indesejado, que pode resultar em dano para os sistemas, pessoas ou a própria organização.”

A classificação de ameaças pode ser em: ameaças intencionais e ameaças da ação da natureza. São exemplos de ameaça intencionais: erros humanos; falhas de hardware; falhas de software e quanto às ações da natureza podem ser citadas terrorismo e vandalismo.

2.6.1. Engenharia Social

Engenharia social surgiu como uma ameaça séria às comunidades virtuais e sistemas de informação (KROMBHOLZ, 2014). É uma técnica por meio da qual uma pessoa procura persuadir outra a executar determinadas ações (CERT.BR, 2000), porque, segundo Bosworth et. al (2014), tem como objetivo explorar o elo mais fraco nos sistemas de segurança da informação: as pessoas.

Uma das vertentes do ataque de engenharia social é a sua aparência inofensiva e "legítima" buscando ludibriar alvos para que não tenham noção de que estão sendo atacados (ROUSE, 2006). É considerada uma prática de má-fé, usada costumeiramente por golpistas para tentar explorar a ganância, a vaidade, a boa-fé, abusando da ingenuidade e da confiança de outras pessoas, afim de obter informações sigilosas e importantes para aplicar golpes (CERT.BR, 2019) ou executar uma ação em nome da vítima (HUBER et. al, 2009).

Muitos fatores potencializam e incentivam a probabilidade de ocasioná-los. Um dos agravantes é a política de levar dispositivos pessoais infectados por *malwares* não intencional para o ambiente de trabalho. A redução de interação física entre os empregados e o estímulo do uso de mensagens de correios eletrônico torna-se armas contra a organização, pois é um meio de comunicação muito utilizado pelos "engenheiros sociais" para tentar obter informações pessoais do usuário por meio de "e-mails oficiais" dentro da própria organização ao se passar por outro colega de trabalho (KROMBHOLZ, 2014).

Conforme Bullé et. al (2017), ao obter informações pessoais dos funcionários como senhas dos sistemas, os "engenheiros sociais" conseguem burlar a tecnologia informação como *Firewall*, Sistema de Identificação de Intrusão (IDS) e outras ferramentas mesmo esses sistemas estejam sendo bem configurados.

As tecnologias tornam-se ineficazes contra essa ameaça, porque o objetivo dos ataques de engenharia social é burlar o sistema de informação a partir da fragilidade humana, influenciando e manipulando por meio de técnicas de persuasão, fazendo o usuário divulgar confidenciais (KROMBHOLZ, 2014).

O ataque pode ser realizado de forma isolada, como também a partir de *softwares* automatizados, por exemplo, uma aplicação que envia vários *e-mails* cujo conteúdo

solicitam informações do usuário (KROMBHOLZ, 2014). Depois de aberto o e-mail e enviado informações para o atacante, o resultado pode ser desastroso, acarretando danos a redes corporativas, roubo de informações de funcionários ou prejuízo financeiro (GUPTA & AGRAWAL, 2011).

Alude KROMBHOLZ (2014), esse ataque possui um conjunto de variações e cada uma possuindo sua especificidade, o que leva o funcionário de pequenas e grandes organizações a cometerem equívocos, tornando-as vítimas. Um dos motivos para que esses ataques aconteçam, é porque os funcionários acreditam que são bons em segurança da informação o suficiente para evitar esse tipo de ataque.

As dimensões buscadas pelos atacantes são: física, social e técnica. As formas de ataque são baseadas em: engenharia reversa social e abordagem sociotécnica.

Física:

Na qual o atacante procura obter dados pessoais como data de aniversário, número do seguro social por meio de objetos jogados no lixo (*dumpster diving*), manuais, memorando, senhas escritas em papel; roubar, extorquir e observar através dos ombros do usuário enquanto o mesmo estiver digitando ou vendo algo na tela do computador (*Shoulder surfing*).

Social:

Aspecto mais importante na engenharia social, o aspecto social (pessoal, mentalidade, maturidade, conhecimento). Utilizam técnicas sociopsicológicas para persuadir suas vítimas, desenvolvendo relacionamento com ela e buscando adquirir grau de intimidade. Tem como maior eficácia via telefone.

Técnica:

Dimensão na qual atacantes tem menos trabalho, porque utilizam os dados abertos e públicos na Internet e redes sociais das vítimas como e-mail, telefone e fotos. Outra forma é utilizar motores de pesquisa para capturar dados de forma automática e concatená-los por meio de ferramentas que agregam dados de diferentes fontes da Internet.

Formas de ataques:

Engenharia reversa social:

O atacante tenta se passar por alguém confiável para que futuras vítimas se aproximem dele solicitando ajuda para solucionar um problema que que o mesmo(atacante) criou, “forçando” o usuário a repassar informações pessoais como a senha, aproveitando-se da oportunidade para instalar sistemas maliciosos no ambiente.

Abordagem sociotécnica

É mais poderosa vertente desse ataque porque o usuário utiliza um *pen drive* infectado e lança-o em algum local público rotulado com alguma mensagem chamativa como “confidencial”. A partir disso, a vítima curiosa recolhe este dispositivo e espeta-o na sua máquina para verificar o conteúdo e acaba infectando o sistema.

2.6.2. Ataque de Força Bruta (*Brute Force Attack*)

Segundo Tasinaffo (2018), não é considerado uma técnica, porque consiste em tentar todas as possíveis senhas, até identificar a correta e, assim, conseguir acesso ao sistema e ativos de redes de computadores que exigem autenticação. Esse ataque costuma utilizar *wordlist* por ser uma modalidade bastante comum, na qual possui uma lista de senhas comuns, como data de aniversário ou conjunto de senhas personalizadas de acordo com cada usuário. Para automatizar essa ação, os atacantes utilizam ferramentas que facilitam trabalho como John The Ripper, Rainbow Crack, Aircrack-ng e Cain and Abel.

2.6.3. Cavalo de Troia

O Cavalo de Troia é um *malware* que se oculta em programas piratas que transparecem inofensivos para o usuário. Depois de instalados, eles permanecem ocultos e silenciosos, coletando informações e habilitando vulnerabilidades de segurança como os *backdoors* no computador. Outro fator importante é a queda de desempenho do *software*, visto que quando ele é craqueado, o código-fonte do *software* é alterado para ignorar tentativas de verificação de autenticidade gerando sobrecarga nas atividades da máquina (LEMMONIER, 2015).

2.6.4. E-mail *Spoofing*

O *spoofing*[5] é uma falsificação tecnológica que busca enganar uma pessoa fazendo-a acreditar que a origem de uma comunicação é verdadeira e confiável. No e-mail *spoofing,* o *hacker* pode enviar uma mensagem onde a origem aparenta vir de alguém que o usuário conheça cujo conteúdo solicita informações pessoais como dados bancários. Na prática, esse ataque funciona da seguinte forma, segundo o CERT.BR (2019),

> este ataque possui uma técnica que consiste em alterar campos do cabeçalho de um e-mail de forma a aparentar que ele foi enviado de uma determinada origem quando, na verdade, foi enviado de outra. Esse ataque é costumeiramente utilizado para propagação de códigos maliciosos, envio de spam e golpes de *phishing*. Atacantes utilizam-se de endereços de e-mail coletados de computadores infectados para enviar mensagens e tentar fazer com o que os seus destinatários acreditem que elas partiram de pessoas conhecidas."

2.6.5. Phishing

O *Phishing*[6] é um golpe originário de e-mail ou meio eletrônico, direcionado a uma pessoa ou organização específica. Além do objetivo que é roubar dados visando fins mal-intencionados, os *hackers* podem instalar *malware* no computador da vítima. Esse golpe é realizado por meio do envio de e-mails falsos ou direcionando o usuário a website falsos.

2.7 Abordagem Sociotécnica

A abordagem sociotécnica surgiu após o término da Segunda Guerra Mundial durante a reconstrução da indústria a partir de projetos de campo realizados pelo Instituto Tavistock de Relações Humanas (*Tavistock Institute of Human Relations*) nas Minas de Carvão em Londres na Inglaterra, em 1949 (TRIST, 1980).

A base da abordagem sociotecnica vem dos movimentos, correntes e escolas da administração originando-se a partir das ideias de Adam Smith e C. Babbage sobre os sistemas de trabalho nas fábricas e tem como finalidade estudar, descrever e inter-relacionar os aspectos organizacionais, técnicos, sociais e psicológicos. O estudo foi

5 Segundo Kaspersky (2019), empresa de segurança em TI.

6 Segundo Kaspersky (2019), empresa de segurança em TI

desenvolvido por E. Jaques, A. K. Rice, J.M.M. Hall, Bamforth, Fred Emery e Eric Trist no projeto conhecido como Glacier (GARCIA, 1980). Entretanto, Emery e Trist publicaram os primeiros trabalhos sobre a abordagem sociotécnicas (ROPOHL,1999).

A abordagem sociotécnica foi baseada e influenciada a partir de fontes de pesquisa de estudo como de J. Woodward com O impacto da tecnologia sobre a natureza, Trist e Bamforth com Método em galerias de extração de carvão, Karl Marx sobre a alienação humana, análises de Max Weber sobre burocracias, A Teoria do campo de Kurt Lewin e A Teoria geral do sistema de L. Von Bertalanffy (GARCIA, 1980).

Considerada mais uma filosofia do que uma metodologia, a abordagem sociotécnica consiste em um conjunto de princípios e processos humanísticos para contextos em que estão associados à tecnologia. Por isso, também ficou conhecida como o princípio da otimização conjunta dos sistemas social e técnico (CORREIA, 2013; MUMFORD, 2006). Assim como, preconiza que a obtenção do desempenho organizacional não decorre apenas do investimento em novas tecnologias, mas decorre da otimização conjunta dos subsistemas sociais e técnicos (LEAVITT, 1965 apud TORRES, 2009; TRIST, 1981).

A abordagem sociotécnica tem como objetivos: desvendar requisitos principais de qualquer sistema tecnológico; influenciar sobre o desempenho do sistema social; avaliar se a eficácia da produção depende da adaptação do sistema social em entender requisitos técnicos; e estabelecer um quadro de referência para análise e avaliação de processos produtivos (GARCIA, 1980).

A abordagem sociotécnica foi aplicada na Inglaterra, na década de 50, no momento em que vários problemas existiam no setor da mineração de carvão como conflitos entre trabalhadores e empregadores, baixa produtividade na indústria inglesa, necessidade das comunidades locais e grande evasão à procura de outras oportunidades de trabalho (TRIST, 1980).

As minas de carvão significavam para a Inglaterra um setor de importância estratégica, uma das principais fontes de energia da época, servia como ponto de reconstrução industrial inglesa e o desenvolvimento do país dependia do setor carvoeiro (MACHADO 2014; DUARTE, 1987).

Não obstante, preconiza Biazzi (1994), que o processo de mineração de carvão desde o surgimento, não havia sofrido modificações significativas; o trabalho era manual e exaustivo, não monitorado e com interdependência entre pequenos grupos. Anos depois, o investimento em máquinas foi realizado, surgiram novos métodos de extração carvão, trabalhadores foram segmentados em tarefas específicas a partir dos seus níveis de habilidades, remunerações diferenciadas a partir das funções, mas não houve aumento de produtividade e a rotatividade aumentou.

A primeira aplicação do experimento da abordagem sociotécnica foi realizado na mina de carvão *Haighmoor*, onde Trist implantou esquema de trabalho baseado em grupos autônomos, com troca internas de trabalhos, reguladas por no mínimo um supervisor. Entre os grupos havia cooperação, maior diversidade das tarefas para cada trabalhador, logo, características diversas foram desenvolvidas nos trabalhadores. O experimento deu certo e, como resultado, o número de incidentes diminuíram e a produtividade. A partir disso, surgiu o enfoque sociotécnico das organizações, um novo paradigma do trabalho (MACHADO, 2014; DUARTE, 1987).

O conceito foi expandido para outros países afora tendo evolução. Os primeiros foram os países escandinavos, que são os mais avançados na aplicação do método sociotécnico (GARCIA, 1980).

A Noruega deu o primeiro passo, criando lei que dava condições de trabalho aos trabalhadores de acordo com os princípios sociotécnicos de boas práticas de trabalho. A Suécia copiou o exemplo da Noruega e implantou uma Lei trabalhista que propunha melhor gestão pessoal e aumento de produtividade. A Volvo foi uma das empresas que implantou a abordagem sociotécnica para organizar os processos de trabalho. Na Dinamarca, utilizou-se a abordagem sociotécnica para equilibrar a produção e a satisfação do trabalho, com maior participação dos funcionários nos processos de decisão dos projetos.

A França e Itália focaram na humanização dos trabalhos. A Holanda é um dos países líderes na implantação dos princípios sociotécnicos para a restruturação do trabalho. A empresa Phillips foi uma das pioneiras dando importância igualmente a aspectos técnicos e sociais para ter um bom gerenciamento (MUNFORD, 2006).

Nos Estados Unidos, o conceito foi direcionado para outros setores como qualidade de vida em locais de trabalho, racionalização das tarefas e cargos, conteúdo de cargos e

conteúdo de papeis sociais. Na Índia teve grande importância numa fábrica têxtil e o projeto da Shell Inglesa (GARCIA, 1980).

2.7.1. Componentes Sociotécnicos

O sistema sociotécnico é composto por dois subsistemas: o técnico e o social. Para Trist & Murray (1993), ambos são independentes e interdependentes. A ação correlacionada de ambos transforma a matéria-prima em resultados. Quando utilizados separadamente, o desempenho do resultado diminui.

Afirmam Bostrom e Heinen (1977), que existem quatro variáveis num sistema de trabalho: *estrutura, pessoas, tecnologia* e *tarefas*. Essas variáveis foram atreladas nos subsistemas técnico (tecnologia e tarefas) e social (pessoas e estrutura). Sendo possível afirmar que as variáveis pertencentes a cada um desses subsistemas são igualmente relacionadas.

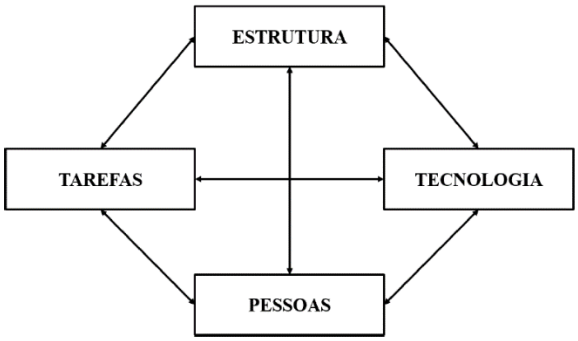
No que diz respeito à Correia (2013), o primeiro a utilizar essas quatro variáveis para designar o sistema de trabalho foi Leavitt em 1965. Para Leavitt, a variável Estrutura aborda sistemas de autoridade, estrutura hierárquica, sistemas de comunicação, organização do trabalho e fluxo de trabalho dentro da organização. Indicam Bellini & Strauss (2008) que, estão inclusas estruturas organizacionais formais e informais que possibilitam e dificultam a realização do trabalho.

A variável “Tecnologia” para Thakur (2013), cita que é responsável por dar assistência para as pessoas no alcance dos objetivos na organização. Referindo-se a equipamentos tecnológicos como hardware e software como instalação física e maquinário da organização que é requerido para a variável Tarefa. Esta engloba todas as tarefas e procedimentos criados para oferecer produtos e serviços na organização e vão além dos processos organizacionais como metas, objetivos do negócio e como as tarefas são executadas.

A variável “Pessoas” aborda sobre quem (os trabalhadores da organização) conduz as tarefas associadas com os objetivos. Considerando habilidade, nível de conhecimento, produtividade e eficiência (THAKUR, 2013).

O diagrama de Levitt é um modelo que é representado em forma de diagrama por um losango com setas duplas destacando a interdependência entre as quatro variáveis. Logo, a alteração e a priorização de uma das variáveis em relação às outras ocasionará mudanças nas outras e acarretará em perda no desempenho nos resultados. Sarker (2000) adaptou o *Diagrama de Levitt* com as variáveis sociotécnicas são expostas na **Figura 3.**

Figura 3**:** Diagrama de Levitt.

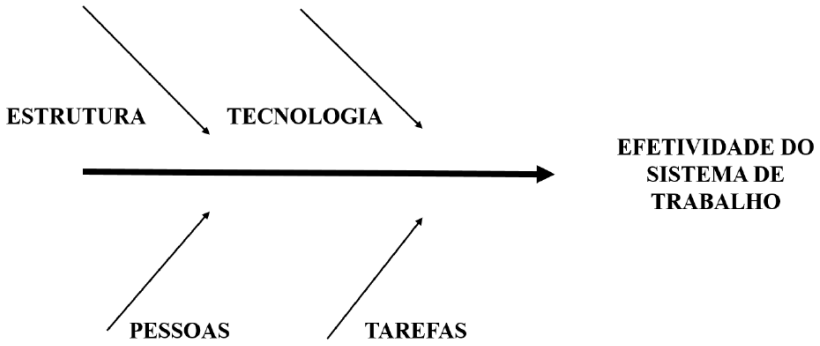


Fonte: Adaptado por Sarker (2000).

A **Figura 4** mostra as relações entre as quatro variáveis e suas interações, cada uma independente com seus valores locais e específicos, e ao mesmo tempo interativa e comunicativa, agindo de forma interdependente.

Este modelo também pode ser representado pelo *Diagrama de Ishikawa*, que se pode ver a seguir:

Figura 4**:** Diagrama de Ishikawa para Efetividade do Sistema de Trabalho.



Fonte: Adaptado por Bellini et. al (2012, p. 72).

O Diagrama de Ishikawa é uma ferramenta da qualidade que ajuda a levantar as causas-raízes de um problema, analisando todos os fatores que envolvem a execução do processo (FARIA, 2019). Nesse caso, ela foi adaptada com as variáveis sociotécnicas. As variáveis pessoas e tarefas, tecnologia e estrutura estão de lados invertidos da seta, mas ambas participam e influenciam diretamente nos resultados do processo.

2.7.2. Princípios Sociotécnicos

Cherns (1976) relata que durante anos estudou e praticou abordagem sociotécnica durante as aulas e consultorias. A partir das experiências adquiridas, descobriu muitas informações e problemas na criação e implantação de sistemas nas organizações. Um dos principais problemas era que os projetistas de sistemas se preocupavam apenas com a parte técnica, abstendo-se da dimensão social, portanto, muitos resultados não eram alcançados. Assim como não existia a participação das partes interessadas em todas as etapas do projeto do sistema. Logo, Cherns (1976) propôs que para um sistema ser produtivo, é preciso que a dimensão técnica e a dimensão social recebam as devidas prioridades igualmente e sejam integrados para trazer resultados.

Diante dessa situação, ele criou nove princípios norteadores conhecidos como princípios sociotécnicos baseado no trabalho de outros autores (EMERY & TRIST, 1972; HERBST, 1974), que tentam colocar em prática e implantar os preceitos levantados pela Abordagem Sociotécnica exemplificando como devem ser implantados sistemas sociotécnicos. Os princípios são os seguintes:

- **Compatibilidade**

Este princípio cita que o projeto do sistema sociotécnico deve ser compatível com os objetivos da organização, que para realizá-lo, é condição necessária dar oportunidades para participação dos empregados em todos os níveis da organização; buscar a competência; e aprender sobre a organização do trabalho. Pode ser usado também em projetos prevendo a dinamicidade em termos estruturais como adaptação as mudanças e incentivar criatividade individual. Um exemplo de como implantar esse princípio numa organização é começando por um local específico e gradativamente ir implantando em outros locais buscando a compatibilidade (CHERNS, 1976).

- **Especificação do Critério Mínimo:**

O objetivo desse princípio é preservar o espaço permanente para participação, experimentação, aprendizagem coletiva no cotidiano do trabalho; especificar o que é critério mínimo para tarefas, alocação de trabalho e papéis; e buscar o essencial. Nada do que seja além do essencial deve ser especificado. Surgem os aspectos positivo e negativo. O negativo é que o projeto não poder ir além do que é essencial; inflexível. O lado positivo é identificar o que é essencial. Organizações comentem erros aos especificar mais do que é necessário, trazendo complexidade para o projeto. Os resultados devem ser compatíveis com as necessidades implícitas e explícitas dos clientes (CHERNS, 1976).

- **Controle de Variância ou Critério Sociotécnico:**

Variância é entendida como um evento não esperado e que deve permanecer próximo ao ponto de origem o quanto possível. A solução para os problemas devem ser resolvidas pelos grupos que diretamente o enfrentam, não por seus supervisores. As pessoas envolvidas num sistema de trabalho devem inspecionar suas próprias tarefas e estarem aptas a aprender com os erros (CHERNS, 1976).

- **Multifuncionalidade:**

Este princípio busca evitar trabalhos rotineiros e repetitivos estimulando a polivalência dos trabalhadores, tornando-os altamente especializados e recebendo tarefas diversificadas. O resultado desse princípio tem como trazer a redundância de funções, e não de partes, reposição fácil, respostas dinâmicas e efetivas aos ambientes das organizações para promover a adaptação, aprendizado e flexibilidade para a mudança (CHERNS, 1976).

- **Princípios da Localização dos Limites ou Localização de Fronteiras:**

Os limites facilitam a troca e compartilhamento de experiências e conhecimentos entre os responsáveis. Eles devem ser criados onde as atividades de trabalho são trocadas de um grupo para o outro, mas também para limitar a comunicação entre departamentos. Cada departamento deverá organizar os recursos, atividades e as funções dentro da organização (CHERNS, 1976).

- **Fluxo de Informação**

O sistema de informação deve ser projetado para prover conhecimento inicialmente para o ponto onde a ação sobre o dado deve ser tomada. Geralmente não são projetados. Quando bem projetados e orientados pelo objetivo organizacional, os sistemas de informação tornam-se sofisticados e podem oferecer exatamente o que a equipe precisa em termos de informação para aprender e controlar as variâncias que ocorrem nas esferas das responsabilidades e competências antecipando-se a eventos que prejudicam a “performance” organizacional (CHERNS, 1976).

- **Apoio Congruente**

Os sistemas sociais de suporte devem ser designados para reforçar o comportamento que a estrutura organizacional é designada para elucidar. A ideia de gerenciamento deve ser compatível com ações de gerenciamento. Comportamento cooperativo entre empregados e gestores (CHERNS, 1976).

- **Valores Humanos e de Projeto**

Trabalho de alta qualidade requer funções com boa demanda; oportunidades de aprendizado; espaço para tomada de decisão; apoio social; associação entre trabalho e vida social; e encaminhamento para o futuro (CHERNS, 1976).

- **Princípio do Estado Incompleto**

O projeto da organização não deve ser definitivo, deve ser interativo, contínuo, composto por equipes multifuncionais constantemente operando, revisando o trabalho da organização, procurando revisões contínuas de objetivos estruturais (CHERNS, 1976).

Passados dez anos, e ter vivido experiências com aulas ministradas e palestras em locais onde a Abordagem Socioténica obteve certa notoriedade como nos Estados Unidos, Suécia e Noruega, Cherns em 1987 decidiu revisar os princípios criados e consequentemente escreveu um novo trabalho. Porém, a maioria dos princípios não houve alteração, apenas alterações nos nomes, além disso, acrescentou um décimo princípio:

- **A transição organizacional ou organização transitória:**

Definido em um contexto de mudança – como a implantação de um projeto sociotécnico –, depara-se com o sistema antigo em funcionamento, mas também a preparação para o novo. Esse período de transição entre o antigo e o novo sistema – por vezes mais complexo que ambos – requer planejamento e *design* (CHERNS, 1987).

2.7.3. Abordagem Sociotécnica na Segurança da Informação

Segundo Schneier (2000), a interação entre o homem e a máquina é considerada o ponto fraco da Segurança da Informação. Incidentes de segurança da informação são frequentemente causados por falha humana (CHAN et. al, 2005) em vez de falha técnica (SCHNEIER, 2000). Essas falhas podem trazer prejuízos imensuráveis à organização como perda financeira e reputação da organização (SCHLIENGER, 2002).

Em contrapartida, Adams (1999) cita que as falhas humanas ocorrem porque eles não são informados sobre os problemas de segurança da informação e que o departamento de segurança informação da organizacional e a Alta Direção são omissos ao não repassar informações sobre os procedimentos de segurança para os empregados.

É comum a Alta Direção ter a percepção apenas do objetivo do negócio e considerar a segurança da informação um aspecto somente técnico e que deve ser delegado aos Gestores de Segurança da Tecnologia da Informação (GSTI). Estes, por sinal, não costumam se envolver com os usuários finais para tentar entender como eles percebem a segurança da informação dentro da organização, assim como envolvê-los nas tomadas decisões. Os gestores de TI acreditam que o papel deles é trabalhar com tecnologia e apresentar ideias, abstendo-se de escutar usuários finais, embora reconheçam a importância dessa comunicação (ASHENDEN, 2008).

Porém, segundo Dhillon e Backhouse (2001), a segurança da informação é mais do que apenas fechaduras e chaves, devendo-se relacionar com o agrupamento social. Portanto, a segurança da informação não pode ser alcançada seguindo puramente uma estratégia focada na parte técnica, produtos e serviços de TI (KAYWORTH e WHITTEN, 2010).

É algo que precisa ser analisado e planejado estrategicamente, visando atender a necessidade de alcançar melhor compreensão dos aspectos sociais, e processuais da organização. Porém, Ashenden (2008) cita que gerenciar o fator humano na segurança da informação é um desafio das empresas, além de, segundo Adams e Sasse (1999), é um dos aspectos mais visados pelos *hackers* e esquecido pelos profissionais de segurança.

Logo, as organizações e os profissionais de TI precisam estar aptos para orientar, comunicar e influenciar diretamente no comportamento das pessoas envolvidas em termos de segurança, como mantê-los informados, conscientizados e treinados sobre a importância dos riscos de segurança (SCHLIENGER, 2002), visto que para alguns funcionários, a segurança é trabalhosa e desnecessária (ADAMS, 1999).

Destarte dessa situação Deursen et. al (2013) citam que abordagem sociotécnica surge com o intuito de designar a mesma importância da competência tecnológica e social, alinhando-os e integrando-os ao contexto organizacional para garantir o mínimo de segurança e implantar a abordagem sociotécnica na segurança da informação (KAYWORTH & WHITTEN, 2010). Ashenden (2008) incrementa ao informar que um bom gerenciamento de segurança da informação depende cada vez mais das pessoas atreladas aos processos e tecnologias.

Cada vez mais, a natureza sociotécnica (SIPONEN, 2006; BJORK, 2004) da segurança da informação vem à tona e a dimensão humana da prática de segurança da informação e do projeto tecnológico estão sendo reconhecidas (COLES-KEMP, 2009).

Além do ganho da segurança, a abordagem sociotécnica vem alcançando equilíbrio entre a necessidade de proteger os ativos de informação, necessidade de negócios, manter a conformidade perante as leis (*compliance*) e assegurar a cultura da segurança adequada para o ambiente organizacional (KAYWORTH AND WHITTEN, 2010).

3. METODOLOGIA

Essa seção contém os procedimentos metodológicos utilizados na pesquisa.

3.1. Natureza da Pesquisa, Instrumento de Coleta e Análise de Dados

O presente estudo propõe analisar à luz da perspectiva sociotécnica, como os servidores da UFPB cumprem as orientações e os requisitos de segurança da informação contidos na Política de Segurança da Informação nos processos de trabalho e ativos de TI.

Para chegar ao resultado desejado, o tipo de pesquisa teve caráter exploratório e descritivo. A pesquisa exploratória, como relata Gil (2007), consiste em proporcionar maior familiaridade com o problema, com vistas a torná-lo mais explícito ou a construir hipóteses, por exemplo, entrevistas com pessoas que tiveram experiências práticas com o problema pesquisado. A pesquisa descritiva exige do investigador uma série de informações sobre o que deseja pesquisar, além de descrever os fatos e fenômenos de determinada realidade (TRIVIÑOS, 1987).

A abordagem da pesquisa a ser utilizada será de cunho qualitativo-quantitativo. A pesquisa qualitativa conforme Gerhardt & Silveira (2009), não se preocupa com representatividade numérica, mas sim, com o aprofundamento da compreensão de um grupo social, de uma organização. Portanto, será utilizada entrevista semiestruturada, porque segundo Boni & Quaresma (2005), a entrevista tem o teor de uma conversa informal, perguntas são previamente definidas, que podem ser reordenadas com o decorrer da conversa. Ao desenrolar da entrevista, poderão ser feitas outras perguntas adicionais tornando-a mais longa, aprofundando cada vez mais sobre o assunto para esclarecer as questões e atingir o objetivo. Além disso, esse tipo de entrevista tem um índice de resposta mais abrangente, uma vez que é mais comum as pessoas aceitarem falar sobre determinados assuntos (SELTTIZ et. al, 1987).

Na pesquisa quantitativa, segundo Fonseca (2002), diferentemente da pesquisa qualitativa, os resultados podem ser quantificados. Para Gerhardt & Silveira (2009), recorre à linguagem matemática para descrever as causas de um fenômeno, as relações entre variáveis.

Para analisar as respostas das entrevistas, será feita Análise de Conteúdo, segundo Fonseca Jr. (2006), é uma metodologia quantitativa para estudos em comunicação e texto que parte da frequência de ocorrências e que alcançou popularidade a partir de Bardin (1977) para confirmar indicadores que permitam inferir sobre a realidade. É uma técnica de análise das comunicações, que analisará o que foi dito nas entrevistas ou observado pelo pesquisador. Na análise do material, busca-se classificá-los em temas ou categorias que auxiliam na compreensão do que está por trás dos discursos (SILVA & FOSSÁ, 2015). Em outras palavras, identificar indicadores para tornar mensurável o que deseja.

3.2. Objeto do Estudo

O presente estudo intenta a observação e análise da execução das atividades laborais nos Centros Acadêmicos da UFPB em termos de segurança da informação, se há o incentivo para implantar a segurança da informação nas atividades, conhecimento da Política de Segurança da Informação da UFPB, treinamento e conscientização da Alta Direção.

3.3. Sujeitos da Pesquisa

Consultando a GSEGI/STI, os centros de maiores ocorrência de eventos de Segurança da Informação, são: o Centro de Ciências Aplicadas e Sociais – CCSA, Centro de Ciências Humanas, Letras e Artes – CCHLA, Centro de Ciências Aplicadas em Educação – CCAE, Centro de Ciência da Saúde – CCS, Centro de Informação – CI e Centro de Tecnologia – CT.

4. APRESENTAÇÃO E DISCUSSÃO DE RESULTADOS

Os dados coletados por meio das entrevistas realizadas a partir de 14 de janeiro à 8 de fevereiro de 2019 foram analisados e inseridos nesta seção. Foram entrevistadas 24 pessoas de 6 Centros da UFPB; dentre os participantes: professores, diretores, técnicos-administrativos da área de TI e técnicos-administrativos que não são da área de TI, visto que de acordo com o artigo 2° da PSI/UFPB, cita-se expressamente que devem obedecer a essa Resolução Normativa.

As entrevistas, no total, duraram 10 horas, 54 minutos e 43 segundos, tendo em média 27 minutos por entrevista. Antes do rol de perguntas, foram levantados dados sociodemográficos dos entrevistados como apresenta na **Tabela 2**.

Tabela 2: Dados Sociodemográficos dos Entrevistados.

Sexo	**f**	**%**
Masculino	16	67%
Feminino	8	33%
Faixa Etária	**f**	**%**
31|---37	7	29%
37|---43	4	17%
43|---49	2	8%
49|---55	6	25%
55|---61	3	13%
61|---67	1	4%
67|---73	1	4%
Nível de Escolaridade	**f**	**%**
Superior Incompleto	1	4%
Superior Completo	6	25%
Mestrado	3	13%
Doutorado	12	50%
Especialização	2	8%
Cargos	**f**	**%**
TI	5	21%
Assessor em TI	1	4%
Assistente Administrativo	6	25%
Docente	6	25%
Diretor	5	21%
Vice-Diretor	1	4%
Tempo de Ocupação do Cargo / anos	**f**	**%**
2|----8	7	29%
8|----14	6	25%
14|---20	3	13%
20|---26	2	8%

26|---32	2	8%
32|---38	2	8%
38|---44	2	8%
Total	24	100%

Fonte: Desenvolvido pelo autor (2019).

Dos 24 entrevistados, a faixa etária mais frequente é entre 31 a 37 anos de idade com 29% dos respondentes. Quanto ao sexo dos entrevistados, foram 67% do sexo masculino e 33% do sexo feminino.

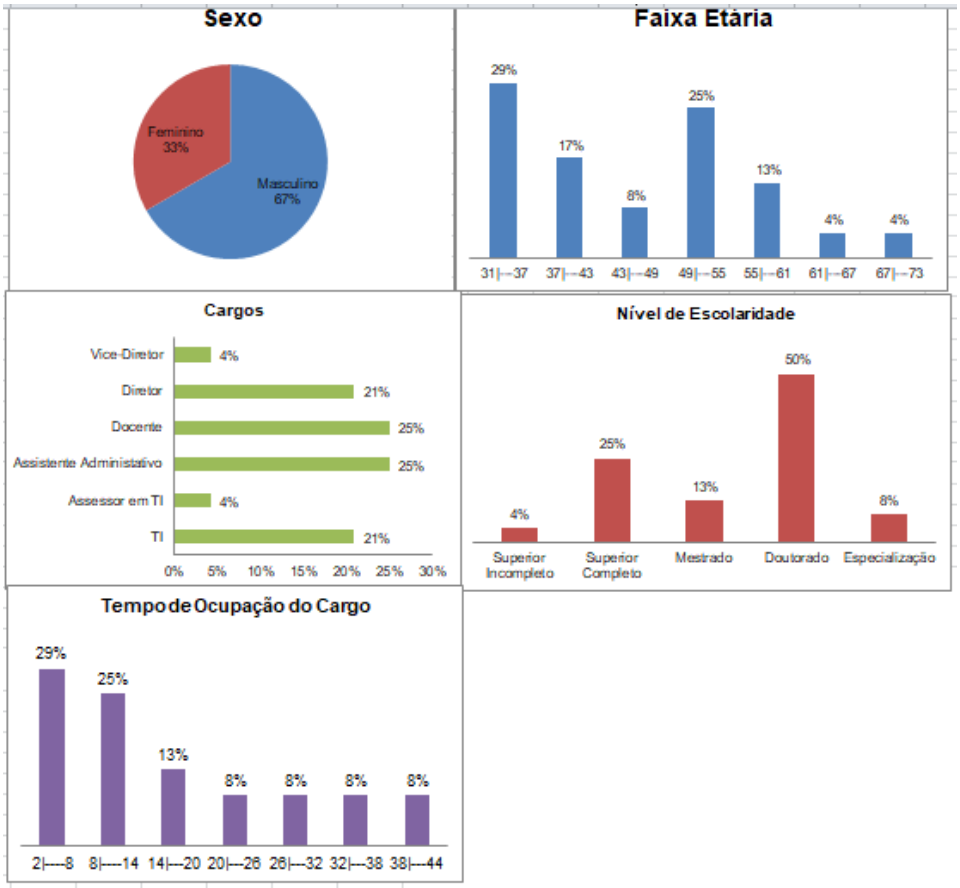
O nível de escolaridade consiste em entre superior completo com uma frequência percentual de 25% dos entrevistados; superior incompleto com 4% e pós-graduação (mestrado – 13%; doutorado – 50% e especialização – 8%).

Os cargos apontados pelos entrevistados foram: assistente administrativo e docente com a mesma frequência percentual de 25% cada; TI e Diretor com a mesma concentração percentual de 21% cada, ao passo que, assessor e vice-diretor com 4% dos entrevistados.

A faixa intervalar do tempo de serviço ou ocupação do cargo é entre 2 a 44 anos aproximadamente, na qual, a faixa intervalar centrada em 20 a 44 anos de ocupação de cargo representa 33% dos entrevistados, na medida em que, entre 2 a 20 anos de ocupação constitui 67% dos entrevistados.

As variáveis sociodemográficas podem ser conferidas também por meio de gráficos como apresenta os conjuntos de figuras contidas no **Quadro 1**.

Quadro 1**:** Conjuntos de Variáveis Sociodemográficas dos Entrevistados**.**



Fonte: Desenvolvido pelo autor (2019).

As entrevistas foram gravadas em formato **.mp3** e transcritas para um documento em formato texto gerando um arquivo com 127 páginas no tamanho 164KBs, o processo de transcrição das entrevistas para o documento texto durou cerca de 35 dias.

Foi utilizada a Análise de Conteúdo para realizar a observação das respostas transcritas dos entrevistados e isolar os pontos chaves que foram importantes para o estudo. Para Bardin (2011), cita:

> Análise de Conteúdo é um conjunto de técnicas de análise das comunicações visando a obter, por procedimentos sistemáticos e objetivos de descrição do conteúdo das mensagens, indicadores, quantitativos ou não, que permitem a inferência de conhecimentos relativos às condições de produção/recepção (variáveis inferidas) destas mensagens.

As entrevistas foram transcritas e organizadas em um documento em forma de tabelas. Sucessivamente foram criadas 8 colunas respectivamente: *Código Assertiva, Código Entrevistado, Código da Assertiva, Quem comunica, Natureza, Política de Segurança da Informação, Abordagem Sociotécnica, e Repetição.*

A coluna *Código da Assertiva* equivale a um número identificador de cada resposta do entrevistado ou pergunta do entrevistador em cada linha. Essa identificação serve para ordenar a sequência das falas como também com a função de apontador para, por exemplo, quando um entrevistado repetir alguma informação dita anteriormente, servir de referência para que este número seja citado na coluna *Repetição* onde ela foi citada.

A coluna *Código do Entrevistado* foi criada para identificar o entrevistado em cada resposta a cada pergunta. Cada entrevistado recebeu um código composto por BM + número, por exemplo, BM001.

A coluna *Código da Pergunta* serve para identificar a pergunta a qual o entrevistado está dando a resposta. Para identificar a pergunta foi utilizado o código Q + número, por exemplo, Q001 para a primeira pergunta.

A coluna *Assertiva* equivale a uma coluna que contém a pergunta do entrevistador e a resposta do entrevistado.

A coluna *quem comunica* é composta por dois valores: entrevistado e entrevistador. Serve para distinguir quem está se comunicando na entrevista.

A categoria “Natureza” foi utilizada para identificar o teor do contexto da assertiva, por exemplo, quando o entrevistado estava respondendo alguma pergunta definindo um conceito particular daquele assunto, foi atribuído um número identificador para conceito. Esse mesmo procedimento foi realizado para outras assertivas. A identificação das assertivas ficou assim: 1 - Conceito: Quando o entrevistado define algo de acordo com seu conhecimento; 2- Repetição: Informação dita anteriormente; 3 - Informação Irrelevante: Quando a resposta do entrevistado não entra no contexto. 4 - Opinião: Quando o entrevistado acha que algo deveria ser feito de tal forma. 5 - Exposição de fatos: Quando o entrevistado relata algo que seja realidade encontrada no seu ambiente de trabalho.

Como a análise será baseada em torno da Abordagem Sociotécnica, foi criada a categoria Abordagem Sociotécnica que tem como subcategorias previamente definidas os componentes sociotécnicos: Tarefas, Pessoas, Tecnologia e Estrutura.

O entrevistado ao responder **o que entende sobre segurança da informação,** citava algo que estava relacionado à execução de trabalho, por exemplo,

> “Proteger a informação da Universidade, questão de dados, questão de sistemas, fazer com que aquilo que a Universidade produza não seja passado para terceiros sem o consentimento legal da Universidade.”

Essa assertiva está relacionada à Tarefas, que segundo Thakur (2013) são tarefas e procedimentos criados para oferecer produtos e serviços na organização e vai além dos processos organizacional como metas, objetivos do negócio e como as tarefas são executadas.

O **Quadro 2** exibe como está relacionado à assertiva e a categoria Abordagem Sociotécnica com a subcategoria Tarefas no documento gerado para fazer a análise das entrevistas.

Quadro 2**:** Relação Assertiva e Categoria.

Assertiva	**AS**
“É proteger a informação da Universidade, questão de dados, questão de sistemas, fazer com que aquilo que a Universidade produza não seja passado para terceiros sem o consentimento legal da Universidade.”	**Tarefas**

Fonte: Desenvolvido pelo autor (2019).

A categoria Política de Segurança da Informação foi criada quando a assertiva do entrevistado estivesse retratando-se naturalmente ao tema Política de Segurança da Informação. Nesta categoria, dependendo do que o entrevistado respondia sobre a PSI/UFPB, como supracitado.

O núcleo da assertiva “*fazer com que aquilo que a Universidade produza não seja passado para terceiros sem o consentimento legal da Universidade”* define confidencialidade que Goodrich & Tamassia (2013) cita como evitar a revelação não autorizada de informação. Isto é, confidencialidade envolve a proteção de dados, propiciando acesso àqueles que estão autorizados e proibindo que outros não saibam a respeito do conteúdo. Logo essa assertiva está relacionada a *Tarefas* e a confidencialidade deve ser implantada nos processos de trabalho do servidor da UFPB.

O **Quadro 3** ilustra como foi realizado esse relacionamento na análise.

Quadro 3**:** Relação Assertiva e Categoria.

Assertiva	**AS**	**PSI**
"É proteger a informação da Universidade, questão de dados, questão de sistemas, fazer com que aquilo que a Universidade produza não seja passado para terceiros sem o consentimento legal da Universidade."	**Tarefas**	**Confidencialidade**

Fonte: Desenvolvido pelo autor (2019).

Por último, foi criada uma categoria denominada Repetição, na qual, possui o número da linha onde a informação foi repetida anteriormente pelo entrevistado em algum momento da entrevista.

Então, cada linha possui um identificador único, o identificador do entrevistado, o identificador da pergunta, assertiva, quem está comunicando, a natureza da fala, e repetição caso existisse, como ilustra o **Quadro 4.**

Quadro 4**:** Versão final da Análise de Conteúdo.

Cod. Assert	**Cod. Entrevistado**	**Cod. Perg**	**Assertiva**	**Quem Comunica**	**Nat**	**AS**	**PSI**	**Repetição**
1	BM001	Q001	"*Eu acho que segurança é ...*"	Entrevistado	1	Tarefas	Integri	Não

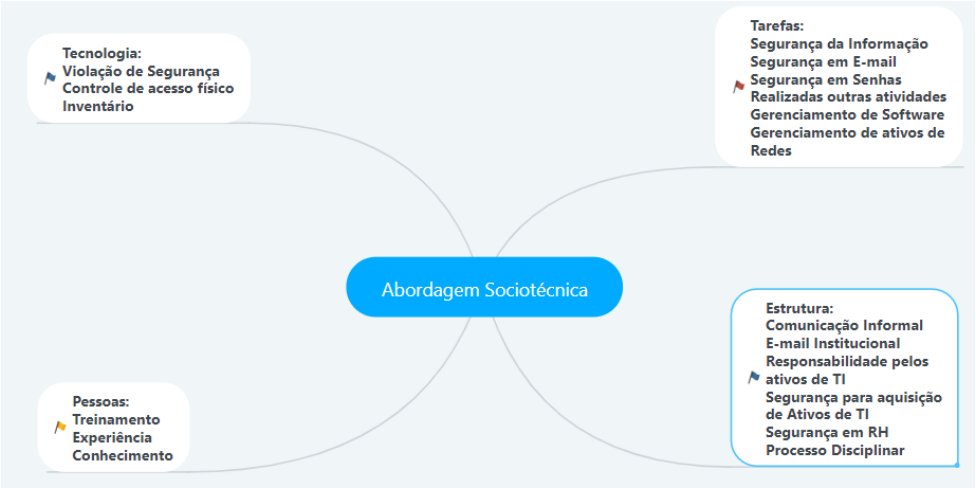
Fonte: Desenvolvido pelo autor (2019).

A partir disso, as assertivas dos candidatos a cada pergunta foram analisadas minunciosamente. No total, foram produzidas 1.001 de assertivas dos servidores. Para facilitar a Análise do Conteúdo, foi realizada filtragem na categoria Natureza a partir dos valores 1-Conceito, 4-Opinião e 5-Exposição de fatos, visto que o conteúdo dessas assertivas são importantes para a pesquisa e os valores 2-Repetição e 3-Informação

serviram apenas para acelerar a análise e evitar retrabalho. Consequentemente, o documento ficou com 973 linhas para serem analisadas.

Destarte disso, a **Figura 5** apresenta as subcategorias Sociotécnicas Estrutura, Pessoas, Tecnologias e Tarefas e as respectivas subcategorias da Política de Segurança da Informação identificadas a partir da Análise de Conteúdo das entrevistas dos servidores da UFPB.

Figura 5: Categorias Identificadas das Entrevistas Relacionadas com as Subcategorias Sociotécnicas.



Fonte: Desenvolvida pelo autor (2019).

4.1. Categoria Estrutura

Tabela 3: Relação Estrutura e PSI.

PSI	X	Palavras utilizadas pelo entrevistado
4.1.1 Comunicação Informal	5	Conversas do dia a dia, o que sabe de um e de outro
4.1.2 E-mail Institucional	24	Comunicação entre servidores via infraestrutura de e-mail da UFPB; Comunicação via e-mail com membros externos;
4.1.3 Responsabilidade pelos ativos de TI	24	Termo de responsabilidade; Formalização de recebimento de equipamentos; Responsabilidade por ativos;

4.1.4 Segurança para aquisição de ativos de TI	12	Avaliação dos ativos de TI; Elicitação de requisitos de segurança da informação funcional; Requisitos de TI;
4.1.5 Segurança em RH	16	Remoção dos privilégios quanto a saída dos servidores;
4.1.6 Processo Disciplinar	24	Penalidades aplicadas a servidores em caso de práticas

Fonte: Desenvolvida pelo próprio autor, 2019.

Legenda da Tabela 3:
PSI: categoria identificada durante entrevista;
X: quantidade de vezes citada;
Palavras utilizadas pelos entrevistados: Termos utilizados pelos entrevistados durante a entrevista que remeteram sobre a categoria;

A **Tabela 3** representa a subcategoria identificada, quantas vezes ela é mencionada pelos entrevistados e as palavras/frases utilizadas pelos entrevistados que transpuseram o mesmo sentido ou mesma ideia.

4.1.1. Comunicação Informal

Tabela 4: Recortes das Entrevistas Sobre Comunicação Informal em Segurança da Informação.

1- *"...então a gente só pega as informações que os outros dizem que eu acabei de dizer pra você para ter segurança."*

2- *"Infelizmente apenas conversas com os nossos servidores."*

3- *"O que eu fico sabendo de um e do outro."*

Fonte: Desenvolvido pelo autor (2019).

A subcategoria Comunicação Informal foi definida por meio de relatos de alguns entrevistados informando o que sabem sobre segurança da informação que é por meio de conversas informais no dia-a-dia com outros servidores, nada formalizado pela UFPB conforme os comentários 1, 2 e 3 na **Tabela 4.** Isso traz à tona o que Chiavenato (1987) cita que a conversa informal tanto pode prejudicar como contribuir nas atividades de trabalho.

Em contrapartida, Moreira (2017) afirma que, a Política de Segurança da Informação promove a homogeneização de atuação, de modo que todos saibam o que fazer e o que evitar, adequando-se mais a estrutura de organizações formais. Portanto, as práticas de segurança deveriam estar padronizadas e formalizadas por meio de uma PSI, evitando conversas informais sobre segurança da informação que talvez não sejam realmente corretas e importantes para o serviço. Entretanto, na subcategoria Conhecimento da PSI/UFPB foi identificado que apenas 17% dos entrevistados leram a Política e mesmo assim foi citado que os requisitos de segurança contidos na PSI/UFPB são abstratos aos servidores que não são da área dificultando o entendimento sobre o que a PSI/UFPB deseja que os servidores façam.

4.1.2. E-mail Institucional

Tabela 5**:** Recortes das entrevistas dos servidores sobre o uso do E-mail Institucional.

1- *" Eventualmente quando tenho que enviar para um fornecedor externo, pedindo informação."*
2- *"Quando vou fazer um ofício ou outro documento, procuro fazer pelo Institucional."*
3- *"Eu uso e-mail pessoal, porque o e-mail da instituição não funciona...mando e-mail do servidor de email da Instituição ele leva 2 ou 3 dias para a mensagem chegar, isso já com o sistema novo, o Zimbra...isso é problema de vários colegas...os que eu conheço não usam."*
4- *"O Zimbra é muito ruim, o que tem de SPAM, e você não pode organizar a informação para acessar as vezes está fora do ar e a gente precisa do e-mail todo dia."*
5- "...*mas dava muito problema, eu tive experiência com Yahoo e Hotmail, pense num negócio ruim! Hoje, eu uso do Gmail."*

Fonte: Desenvolvida pelo autor (2019).

O uso de e-mail institucional para comunicação interna possui algumas nuances, na qual, segundo o **Quadro 5,** na coluna **usam,** 62,5% dos entrevistados utilizam apenas o serviço de e-mail da Universidade para se comunicar durante as atividades laborais como entrar em contato com membro externo à Universidade ou oficializar uma comunicação interna conforme os comentários 1 e 2 na **Tabela 5**, enquanto que, na coluna **não usam**, 25% informaram que usam apenas outros serviços de e-mail como Gmail e Hotmail para realizar comunicação interna durante as atividades.

Dentre as justificativas conforme os comentários 3, 4 e 5 é que o servidor de e-mail da UFPB “não funciona”, “demora para enviar”, “recebe muito SPAM” e “não envia e-mail”. A partir dos das informações relatadas, percebe-se que apesar de ser a minoria, a ferramenta de serviço de e-mail da UFPB recebe críticas, gerando rejeição por parte de alguns servidores. Na coluna **ambos,** 12,5% citaram que usam ambos para se comunicarem internamente. Em relação aos Centros, apenas os servidores do CI informaram usar integralmente o e-mail institucional para realizar comunicações internas.

Quadro 5**:** Quantitativo do Uso do E-mail Institucional.

Usam	Não usam	Ambos	Centro
X			CCSA
	X		
X			
X			
X			CI
X			
X			
X			
	X		CCS
X			
	X		
X			
X			CT
		X	
		X	
	X		
X			CCAE
X			
X			
	X		
X			CCHLA
		X	
	X		

X			

Fonte: Desenvolvida pelo próprio autor (2019).

Porém o Art.5° da PSI/UFPB afirma que,

> "Requisitos de segurança em operações de sistemas de informação: define padrões, e princípios relacionados à operação dos sistemas de informação, tais como procedimentos operacionais, controles uso de correios eletrônicos..."

Embora a PSI/UFPB não detalhe em algum momento sobre que tipo de prática deve ser feita em relação à comunicação via e-mail dentro da UFPB, presume-se que as informações institucionais devem permanecer dentro da própria organização, visto que, possui um serviço para essa finalidade. Visando esse tema, o **Decreto** do Governo Federal de **nº 8.135** de 4 novembro de 2013 no Art.º 1, reforça a ideia de que comunicações internas devem ser feitas por infraestrutura do órgão que oferece o serviço, alude:

> "As comunicações de dados da administração pública federal direta, autárquica e fundacional deverão ser realizadas por redes de telecomunicações e serviços de tecnologia da informação fornecidos por órgãos ou entidades da administração pública federal, incluindo empresas públicas e sociedades de economia mista da União e suas subsidiárias."

4.1.3. Responsabilidades pelos ativos de TI

Tabela 6**:** Recortes das Entrevistas sobre Responsabilidades dos Ativos de TI.

1- "E*xiste um documento formal aqui que a gente possa entregar esse usuário o que existe é a documentação do equipamento em nível de tombamento para controle de equipamentos lá do patrimônio."*

2- *"Normalmente o responsável é o chefe da unidade, então a Direção de Centro é responsável por maior parte depois a gente transfere para departamentos e os departamentos colocam nos professores e funcionários."*

3- "*Tem o tombamento lá, o pessoal sabe que está na minha sala e ponto."*

4- *"Assina fisicamente junto ao almoxarifado, recebe a máquina junto com a especificação da configuração e assina o termo, somente."*

5- "O que normalmente tem é o termo de responsabilidade que aloca os equipamentos, não necessariamente para o servidor em si, mas para a pessoa responsável pelo setor o chefe da Unidade."

6- "Era apenas um documento que informava que eu tinha recebido, eles ficaram sendo responsabilidade do departamento, não com pessoa física..., mas não lembro de nada me responsabilizando sobre a Segurança da Informação."
7- "Não! Difícil por que várias pessoas trabalham utilizando aquele mesmo ativo como uma pessoa irá se responsabilizar sozinha? Como descobrir quem prejudicou?"

Fonte: Desenvolvida pelo autor (2019).

Segundo o artigo 3° da PSI/UFPB, ativos de TI são:

I. Ativo de Informação – qualquer recurso que faça parte dos sistemas de informação (SI) e meios para geração de documentos que tenham valor para a UFPB;

II. Ativo de Sistema – patrimônio composto por todos os dados e informações geradas e manipuladas durante a execução de Sis e processos da UFPB;

III. Ativo de Processamento – patrimônio composto por todos os elementos de hardware, software, serviço, infraestrutura e instalações físicas necessárias para a execução para a execução dos SIs e processos da UFPB, incluindo tanto aqueles produzidos internamente quanto os adquiridos externamente por esta Universidade;

Também, segundo a PSI/UFPB, no artigo 3° no inciso X cita Responsabilidade: "*obrigações e deveres da pessoa que ocupada determinada função em relação ao acervo de TI*". Como consta na **NBR ISO 27002:2013**,

> Política de Segurança da Informação deve atribuir responsabilidades, gerais e específicas, para o gerenciamento da segurança da informação para os papéis definidos e convém que as responsabilidades sejam complementadas, onde necessário, com orientações mais detalhadas para locais específicos e recursos de processamento da informação.

Segundo a PSI/UFPB, entende-se por recursos de processamento da Informação como o patrimônio composto por todos os elementos de hardware, software, serviço, infraestrutura.

Portanto, questionados sobre a existência de documento formal que notifica a responsabilidade dos servidores sobre os ativos de TI que eles executarão suas tarefas, no **Quadro 6** na coluna **existe,** 58% relataram que conforme os comentários de 1 à 6 na **Tabela 6** têm conhecimento sobre um documento formal que é o termo de responsabilidade, no qual consta que tal equipamento identificado por número de

patrimônio está localizado no devido setor e que o chefe do departamento ou servidor assinam e ficam responsáveis. Este documento não faz nenhuma menção sobre a responsabilidade em termos de segurança da informação, Política de Segurança da Informação ou penalidades cabíveis em caso de violação de segurança da informação dos ativos.

Outra situação relatada é que o termo de responsabilidade não é atualizado pela administração ou TI local (entende-se por TI local, a equipe de TI lotada nos demais Centros da UFPB). Quando um funcionário ausenta-se da empresa, segundo a **NBR ISO 27002:2013,** deve existir um documento formal denominado “termo de devolução” relacionando todos os ativos de TI que estavam na responsabilidade daquele funcionário e devolvidos à Instituição. Entretanto, essa ação não existe dentro dos Centros entrevistados. O novo servidor que ocupou a função vaga não assina novo termo de responsabilidade, logo, não terá responsabilidade formal sobre o ativo de TI que era usado anteriormente pelo servidor que saiu da Instituição.

Essa ação atinge o princípio da segurança da informação como o não-repúdio, por que caso venha ocorrer algum evento de segurança física (furto, depreciação etc.) daquele ativo de TI, como responsabilizar o servidor ou até mesmo quem o substituiu?

42% dos entrevistados afirmaram que nunca assinaram nenhum termo de responsabilidade. Dentre esse número, conforme o comentário 7 na **Tabela 6**, um dos entrevistados discordou desse procedimento: por que como uma pessoa irá se responsabilizar por algum equipamento que é usado por várias pessoas, como o próprio computador, que é um recurso de processamento de informação do setor onde existe uma conta em comum com outros servidores? Como avaliar quem foi que infringiu em termos lógicos (inserir *malware*, instalar programas não permitidos etc.) a Política de Segurança da UFPB? Nesse caso, segundo o Guia de Boas Práticas do TCU (p. 12) e o CERT.BR (2019), a situação ideal é criar usuários individuais para cada servidor naquele computador com permissão mínima de abrir programas como navegadores web e soluções de escritório como *Microsoft Office* e *BROffice*. Esse procedimento proporcionará maior privacidade dos usuários em termos de navegação, confidencialidade, integridade, Disponibilidade e não-repúdio dos seus arquivos, visto que teoricamente será o único responsável por aquela conta.

Quadro 6: Quantitativo de Servidores que Assinaram Termo de Responsabilidade.

Existe	Não existe	Centro
	X	CCSA
	X	
X		
	X	
	X	CI
	X	
X		
X		
	X	CCS
X		
X		
X		
	X	CT
X		
	X	
X		
X		CCAE
X		
X		
X		
X		CCHLA
X		
	X	
	X	

Fonte: Desenvolvido pelo próprio autor (2019).

4.1.4. Segurança na Aquisição de Ativos TI

Considerando o Art.5° da PSI/UFPB o Inciso VIII.

> *"Requisitos de segurança para aquisição de ativos de TI: define padrões e princípios relacionados à seleção, aquisição, instalação e gestão de contratos de fornecimento/provimentos de ativos de TI."*

Também, no Art. 20° da PSI/UFPB, cita *"os processos de aquisição de bens e serviços relacionados a ativos de TI na UFPB deverão estar em conformidade com esta PSI".*

Diretores e servidores da área de TI foram questionados **se a aquisição de bens e serviços relacionados a ativos de TI estavam em conformidade com a PSI/UFPB.** Nenhum dos entrevistados citou que consultou a PSI/UFPB em momento algum para realizar aquisição de ativos de TI. Em seguida, foi questionado se existia levantamento prévio dos requisitos funcionais de segurança em relação aos ativos de TI, ao passo que, segundo o **quadro 7,** na coluna **não,** 33% dos entrevistados informaram que não existe levantamento ou consulta em conjunto com a equipe de TI para elucidar requisitos de segurança da informação ou funcionais. Dentre os entrevistados informaram que geralmente quem faz as especificações é a PRA, e que isso vem gerando muitos problemas como a despadronização entre os equipamentos como impressoras de diversos fabricantes e a incompatibilidade entre os seus *tonners* gerando transtornos quanto ao levantamento das recargas dos tonners; como também seguem especificações de outros órgãos que detalham melhor o produto a ser comprado. Essa prática é vista com bons pelo entrevistado. Porém, segundo o Guia de Boas Práticas em Contratação de Soluções de Tecnologia da Informação (2012, p. 69), a TI do órgão deve ser consultada quanto à contratação de TI. Portanto, o **Quadro 7,** na coluna **sim,** 67% informaram que foram consultados pela Direção antes de adquirir ativos de TI. Desse grupo foi retirado que mesmo a Direção de Centro possuindo relacionamento com a TI para realizar esse processo, os departamentos e coordenações têm autonomia para adquirir seus próprios equipamentos sem consultar a TI, porém, foi identificado que esse processo pode trazer gastos excessivos e desnecessários para a UFPB como o que foi relatado por um servidor da TI numa situação onde dois *Nobreaks* seriam comprados por 38 mil reais em vez de adquirir um equipamento bem mais simples que custava 1 mil reais.

Para evitar esse tipo de problema, é preciso que o processo de aquisição de ativos de TI deva seguir um padrão pré-definido dentro da UFPB visando à contenção de gastos, conformidade com a PSI/UFPB, atuando de forma integrada com a STI e a TI local para levantar requisitos de segurança da informação como garantia, controle de acesso físico e lógico e redundância.

Quadro 7: Aquisição de Ativos de TI.

SIM	NÃO	Centro
X		**CCSA**
X		
	X	**CI**
	X	
	X	**CCS**
	X	
X		**CT**
X		
X		**CCAE**
X		
X		**CCHLA**
X		

Fonte: Desenvolvido pelo autor (2019).

4.1.5. Segurança em Recursos Humanos

Segundo a PSI da UFPB, no Art. 5° no VI retrata sobre:

> "Requisitos de Segurança em Recursos Humanos, onde define padrões e princípios relacionados a ações realizadas por ou eventos ocorridos com servidores (docentes e técnicos-administrativos), gestores, pessoal em cargos de chefia, estagiário, tais como procedimentos a realizar quando um servidor é exonerado, quando sofre relotação, quando está em licença e etc."

Entretanto, a **NBR ISO 27002:2013** possui um objetivo de controle denominado "Retirada de Direito de Acesso" com exemplo de algo que pode ser feito quando um funcionário é deslocado para outro setor ou é demitido da empresa, remete:

> "convém que os direitos de acesso de todos os funcionários, fornecedores e terceiros às informações e aos recursos de processamento da informação sejam

> retirados após o encerramento de suas atividades, contratos ou acordos, ou ajustado após a mudança destas atividades.”

Logo, foi questionado para os servidores **“Quando um servidor saí temporariamente/definitivamente, quais medidas são tomadas em relação as contas nos ativos de tecnologia da informação?”** Segundo o **quadro 8**, na coluna **não soube informar,** 36% dos servidores informaram não saber responder qualquer procedimento alteração/exclusão de permissão aos ativos de TI. Logo, na coluna **não existe,** 33% dos entrevistados informaram que não existe tal procedimento dentro da UFPB. Quando não acontece esse procedimento, vários problemas podem ocorrer como o acesso indevido de antigos membros da Instituição que podem alterar ou remover a informação infringindo os princípios da segurança da informação: confidencialidade, integridade e disponibilidade. Fato que já ocorreu dentro da UFPB. Segundo relato de um servidor, uma servidora foi removida e posteriormente retirou dados de uma pasta compartilhada do setor em que ela exercia a função, se não fosse o sistema de backup da TI, os dados teriam sidos perdidos.

No mais, na coluna **existe,** 31% informaram que existe sim procedimento para controlar as permissões dos usuários. Os entrevistados relataram que o Centro realiza tal atividade e que quando o servidor se ausenta do serviço ou sua lotação é alterada, é retirado do ponto eletrônico, conta de e-mail cancelada, o usuário no computador é modificado e os equipamentos são devolvidos.

Entre relação aos Centros, todos os servidores entrevistados do CCSA e CCS relataram não existir ou não saberem se tal procedimento é aplicado no ambiente de trabalho. Esse dado é preocupante, visto que segundo a **NBR ISO 27002:2013,** no objetivo de controle Encerramento ou Mudança da contratação, a organização deve definir responsabilidades para assegurar que a saída de servidores da organização seja feita de modo controlado, a devolução de todos os equipamentos e a retirada de todos os direitos de acesso sejam concluídas.

Por tanto, o Diretor de Centro como membro responsável por parte da UFPB deve possuir no mínimo o controle de permissões sobre os servidores ao entrar e sair das suas atividades, então orientar a TI e a administração local para retirar as permissões dos servidores quando não estiverem exercendo mais suas funções naquele setor.

A UFPB por meio da PSI/UFPB deve ser clara em relação a esses procedimentos. Porém, é um documento abstrato em relação aos procedimentos que devem ser feitos. É necessário que seja realizado um documento paralelo à PSI/UFPB para auxiliar como tais tópicos podem ser alcançados a partir de ações previstas nesse documento.

Quadro 8: Segurança em Recursos Humanos.

EXISTE	NÃO EXISTE	NÃO SOUBE INFORMAR	CENTRO
		X	CCSA
		X	
	X		
		X	
		X	CI
	X		
X			
X			
	X		CCS
	X		
	X		
	X		
		X	CT
		X	
X			
		X	
X			CCAE
		X	
	X		
X			
X			CCHLA

	X		

Fonte: Desenvolvido pelo autor (2019).

4.1.6. Processo Disciplinar

Segundo o Artº. 10 da PSI/UFPB "É dever de todo usuário dos ativos de TI da UFPB: [...] II. Cumprir a PSI/UFPB, sob pena das sanções disciplinares e legais cabíveis, prevista no art. 13 de Resolução. O Artº. 13 cita que:

> "Em caso de descumprimento de termos estabelecidos por esta Resolução, serão aplicadas as sanções e penalidades previstas na legislação em vigor, em especial no Código de Ética do Servidor Público Civil do Poder Executivo Federal, aprovado pelo Decreto n° 1.171/1994 e na Lei n°8.112/1990, que instituiu o Regime Jurídico dos Servidores Públicos Civis da União, das autarquias, inclusive as em regime especial e das fundações públicas federais."

Os entrevistados foram questionados sobre o conhecimento da PSI/ UFPB, considerando o **Quadro 9**, 46% dos entrevistados informaram saber da existência dela, entretanto apenas 17% a leram. Questionados sobre os processos disciplinares contidos na PSI/UFPB, os entrevistados questionaram como aplicar algo se os servidores não conhecem? Entretanto, segundo o **Decreto-Lei N°4.657**, de 4 de setembro de 1942 no Art.°3 *"Ninguém se escusa de cumprir a Lei, alegando que a não conhece."* Logo, independente ou não de conhecimento da PSI/UFPB, os servidores estão susceptíveis as suas penalidades.

Quadro 9**:** Conhecimento sobre a PSI/UFPB.

Sabe que Existe uma Psi	Leu a Política	Centro
X	X	
		CCSA
X		
		CI

X		
		CCS
X		
X	X	
		CT
X	X	
X		
X		**CCAE**
X		
X	X	**CCHLA**

Fonte: Desenvolvida pelo autor (2019).

Tabela 7: Síntese dos Achados na Categoria Estrutura.

Categoria Sociotécnica	Subcategorias da PSI	Síntese dos Achados
Estrutura	**Comunicação Informal**	• Conhecimento de alguns servidores sobre segurança da informação é por meio conversas informais como conversas e bate-papo do dia-a-dia.
	E-mail Institucional	• Mais da metade servidores utilizam e-mail institucional para comunicação interna; • Servidores utilizam para comunicação interna. • Servidores que não usam e-mai institucional reclamam do serviço oferecido pela UFPB: lentidão para enviar mensagens, limitação do serviço são uma das causas. • Governo Federal informa que mensagens institucionais devem permanecer dentro dos órgãos.
	Responsabilidade pelos ativos de TI	• A responsabilidade pelos ativos de TI é do servidor ou do chefe do departamento ou coordenação; • 58% assinaram termo de responsabilidade; • Os termos de responsabilidades não citam a PSI/UFPB ou segurança da informação; • A responsabilidade pelo ativo de TI não é atualizado quando o servidor ausenta-se do setor.
	Segurança para aquisição de ativos de TI	• Consultam a TI para realizar aquisição de ativos de TI, porém departamentos e coordenações possuem autonomia para realizar a compra de ativos de TI podendo ocasionar em gastos desnecessários para a UFPB.
	Segurança em Recursos Humanos	• Poucos servidores relataram a existência de procedimento formal para retirar permissões de acesso em serviços oferecidos pela TI ou devolução de ativos de TI de servidor removido, aposentado ou redistribuído do setor ou Centro que estava lotado.
	Processo Disciplinar	• A maioria dos servidores entrevistados não tem conhecimento de que estão passíveis de receberem um processo disciplinar caso cometam ação que viole a segurança da informação nos ativos de TI da Universidade.

Fonte: Desenvolvida pelo autor (2019).

4.2. Categoria Pessoas

Tabela 8: Subcategorias das Categorias Pessoas.

Política Segurança da Informação	X	Palavras utilizadas pelo entrevistado
4.2.1. Treinamento/Cursos	24	Palestras, cursos presenciais, cursos à distância; treinamento; educação;
4.2.2. Experiência	24	O que os outros falam; disciplinas de graduação; atuou como professor; pós-graduação; instruir como gerar senhas complexas;
4.2.3. Conhecimento da PSI/UFPB	24	Divulgação; Propagação da PSI; Comunicação sobre a PSI;

Legenda da Tabela 8:
PSI: categoria identificada durante entrevista;
X: quantidade de vezes citada;
Palavras utilizadas pelos entrevistados: Termos utilizados pelos entrevistados durante a entrevista que remeteram sobre a categoria;

4.2.1. Treinamento

Tabela 9: Recortes das Entrevistas dos Servidores sobre Treinamento.

1- "*Praticamente nada. Sou analfabeto no assunto."*

2- *"Eu reconheço que sou leigo quanto as Políticas e práticas de Segurança da Informação."*

3- "Para a formação de novos servidores, seria importante. Para ele entrar capacitado, eu acho difícil para você fazer com os antigos, mas para os novos é possível sim, porque é na entrada, eu acho que seria legal."

4- *"Os servidores antigos trazem muitos vícios, culturas, o que a gente precisa é que os novos venham com uma nova mentalidade e possam substituir essa mentalidade antiga. Essa cultura antiga. O que vemos é exatamente distinto. O novo incorporando o antigo."*

5- "...tem que preparar não só os novos como os velhos."

6- *"Principalmente os servidores antigos!"*

7- "A Universidade deve investir em treinamentos, em que os servidores sejam obrigados a participar fazer reciclagem por 1 ou 2 anos..."

8- "...por isso esse tipo de treinamento, para entender que isso não é frescura!"

9- "*Questões de cursos, cursos à distância, palestras, algumas coisas que motivem o servidor e despertem isso, porque a maioria sabe nem que existe."*

Fonte: Desenvolvida pelo autor (2019).

Cursos de segurança da informação na UFPB sob perspectivas dos servidores

Questionados sobre a participação de cursos de segurança da informação, segundo o **Quadro 10**, 88% dos entrevistados informaram não ter participado de nenhum curso de segurança da informação nem no ambiente institucional, nem em outras instituições, por outro lado, 12% dos entrevistados fizeram especialização e participaram de disciplinas da graduação. Todos os servidores que participaram de cursos são da área de TI.

Na UFPB, os cursos de segurança da informação são oferecidos por meio de duas formas: para os servidores de TI, todo ano são oferecidos cursos de segurança da informação por meio de um convênio que a UFPB tem com a Rede Nacional de Pesquisa (RNP). Para servidores de outras áreas de atuação e professores, no ano de 2017, 2018 e 2019, a PROGEP ofereceu curso de "Conscientização de Segurança da Informação", cada curso possui 40 vagas, cujo objetivo é orientar sobre os principais pontos de segurança da informação.

Porém, segundo o Quadro de Referência dos Servidores Técnicos-Administrativos em Educação - QRSTA da UFPB (2019), a UFPB possui 3.155 servidores ativos e segundo o Sistema Integrado de Gestão de Planejamento e de Recursos Humanos (SIGRH), possui 2.782 professores, além das constantes nomeações, aposentadorias e vacância em decorrência de aprovações em outros concursos públicos. Portanto, a oferta de curso é insuficiente para o enorme quantitativo de servidores e professores. Isso reflete no que foi apresentado durante a entrevista, onde se identificou que a média de tempo de serviço entre os servidores entrevistados é de 16 anos, e apenas três participaram de curso de segurança da informação, que não foram pela Universidade.

Porém, para que a PSI/UFPB seja eficaz, além de sua divulgação, é preciso que, segundo a NBR ISO 27002:2013, os servidores precisam ser educados e treinados, não bastando somente desenvolver um documento com diretrizes de segurança:

> "A organização deve fornecer a todos os funcionários da organização e, onde, pertinente, fornecedores e terceiros recebam treinamento apropriado em conscientização, quanto as suas responsabilidades e obrigações, bem como o treinamento do uso correto dos recursos de processamento da informação e informações sobre o processo disciplinar. Além disso, deve haver treinamento quando houver atualizações nas políticas e procedimentos organizacionais relevantes para as suas funções."

Adicionalmente para segundo Freitas & Araújo (2008, p.48), ressalta.

> "Para que a cultura da empresa seja mudada em relação à segurança da informação, é fundamental que os funcionários estejam preparados para a mudança, por meio de avisos, palestras de conscientização, elaboração de guias rápidos de consulta e treinamento direcionado."

Portanto, cursos e treinamentos são essenciais para aplicação de uma PSI dentro da Administração Pública Federal, principalmente em um ambiente como uma Universidade Pública, onde existe enorme quantitativo de servidores.

Relato dos servidores sobre a participação de cursos de segurança da informação.

Segundo a **Tabela 9,** nos comentários 1 e 2, os entrevistados enfatizam que não possuem conhecimento algum sobre práticas de segurança da informação. Comentários nesse sentido foram relatados por vários servidores durante as entrevistas. Esses comentários transmitem que treinamentos e cursos de segurança da informação são necessários para os servidores, embora o comentário 3 reconheça que os cursos seriam

importante apenas para os novos servidores que estão ingressando na UFPB, enquanto que os servidores antigos teriam certa resistência, porque segundo o comentário 4, estes trazem consigo práticas que só podem ser substituídas por inserção de nova mentalidade incorporada pelos novos servidores. Entretanto o comentário 5 discorda dessa vertente, e acredita que tanto os servidores antigos, principalmente eles, enfatiza o comentário 6, como os novos devem receber treinamento de segurança da informação. O que está de acordo com o que está contido na literatura, que todos os membros devem participar da segurança da informação organizacional. Adicionalmente, o comentário 7 afirma que além de oferecer os cursos, a UFPB deveria obrigar todos servidores a fazer reciclagem em relação à segurança da informação para mantê-los atualizados em relação a esse tema, visto que, segundo o comentário 8, a segurança da informação não é “frescura”. O comentário 9 cita que cursos à distância e palestras facilitariam o discernimento dos servidores sobre a importância da segurança da informação.

Quadro 10**:** Servidores que Informaram ter Participado de Curso/Treinamento de Segurança da Informação.

Sim	Centro
	CCSA
X	
	CI
	CCS
X	
	CT

X	**CCAE**
	CCHLA

Fonte: Desenvolvido pelo autor (2019).

4.2.2. Experiência

Tabela 10**:** Recortes das entrevistas dos servidores sobre experiência em Segurança da Informação.

1- "...meus conhecimentos nessa área são bem limitados, o que se espera geralmente nesse quesito, é que a equipe de TI já que a UFPB tem um setor específico para TI, realize os procedimentos necessários para dar a devida qualidade com relação as informações."
2- "Trabalhei em empresa privada, onde possuíam normas e regras que deveriam ser cumpridas dentro da empresa, trazendo isso para a Universidade."
3- "Sou gerente de segurança da informação onde trabalho."

Fonte: Desenvolvido pelo autor (2019).

Questionados sobre que tipo de experiência/competência os servidores possuíam para implantar processos de segurança da informação nas suas atividades dentro da UFPB, segundo o **Quadro 11**, relatou que 67% dos entrevistados afirmaram não ter experiência com práticas de segurança da informação para serem implantadas nos exercícios de trabalho. Desse número, o comentário 1 na **Tabela 10**, relata que quem deve se importar com a implantação de práticas de segurança da informação é o pessoal da TI e não o usuário final. Esse discurso vai de encontro ao que informa na PSI/UFPB no Art.º 2:

> "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 interagirem com os ativos de TI da UFPB".

Logo, esse discurso não condiz com o que propõe a PSI/UFPB, portanto, presume-se que esse tipo de raciocínio existe pela ausência de conhecimento de segurança da informação da própria PSI, visto que apenas 17% dos entrevistados a leram.

Por outro lado, 33% relataram que possuem experiências como o comentário 2, 3 e 4 na **Tabela 10**, que relataram ter trabalhado em empresa privada que possui normas de segurança da informação e que devem ser seguida, compartilhando esse tipo de experiência na Universidade, exercer função de segurança da informação ou ter conhecimento de atividades básicas como usar antivírus.

Quadro 11**:** Servidores que Informaram Possuir Alguma Experiência em SI.

Sim	Centro
X	**CCSA**
X	
	CI
X	
X	
X	
	CCS
X	
	CT
X	
X	**CCAE**
X	**CCHLA**

Fonte: Desenvolvido pelo autor (2019).

4.2.3. Conhecimento da PSI/UFPB

Tabela 11**:** Recortes das Entrevistas dos Servidores sobre Conhecimento da PSI.

1.*"Acho que só aqueles que se interessam conseguem chegar lá."*
2.*"Acredito que as pessoas só tenham conhecimento da Política se forem atrás."*
3. *"Eu acho que só se a pessoa estiver interessada em saber, vai pesquisar, e ter o conhecimento, mas não é amplamente divulgada"*
4. "*É muito vaga e generalista, não tem aquela especificidade falta complemento, falta exemplo… na Política tem "você deve manter a integridade dos seus arquivos" O que isso quer dizer?*
5. *Jogaram a norma para como se diz: "para inglês ver." Para formalizar e o TCU ver que criaram uma norma. "*
6. *"...na teoria é muito bonito isso, era algo que deveria funcionar"*

Fonte: Desenvolvida pelo autor (2019).

Segundo o art. 19.

> "PSI resultante nesta Resolução deverá ser publicada e amplamente promovida, garantindo que a comunidade universitária tenha conhecimento da mesma para adequado usufruto dos benefícios e assunção das responsabilidades sobre os ativos de TI da UFPB."

Os entrevistados responderam questões sobre o que sabem da PSI/UFPB. Conforme o **Quadro 12**, 46% dos entrevistados informaram ter conhecimento sobre a PSI/UFPB. 54% dos entrevistados relataram que não tem conhecimento sobre a norma. Conforme os comentários 1, 2 e 3 na **Tabela11**, expõem que o conhecimento sobre a PSI/UFPB só ocorre se o servidor estiver interessado nessa temática, o que vai de encontro ao que cita a literatura que a Alta Direção deve divulgar a PSI para toda organização tenha conhecimento sobre esta norma.

Indagados sobre o conhecimento do conteúdo da PSI, 17% informaram que leram. Dentre esse número, na **Tabela 11**, o comentário 4 enfatiza que o conhecimento da PSI/UFPB não garante que as ações dos servidores serão orientadas pela norma visto que é considerada vaga, generalista e não possui exemplos de como podem ser alcançados seus requisitos. O comentário 5 e 6 acrescentam que a PSI/UFPB só funciona na teoria e foi desenvolvida apenas para alinhar-se com o que recomenda os órgãos superiores como o Tribunal de Contas da União (TCU).

Quadro 12**:** Conhecimento sobre a PSI/UFPB.

Sabe que Existe uma Psi	Leu a Política	Centro
X	X	CCSA
X		
		CI
X		
		CCS
X		
X	X	
		CT
X	X	
X		
X		CCAE
X		
X	X	CCHLA

Fonte: Desenvolvida pelo autor (2019).

Tabela 12**:** Síntese dos Achados da Categoria Pessoas.

Categoria Sociotécnica	Subcategorias da PSI	Síntese dos achados
Pessoas	**Curso e Treinamento**	• 88% dos servidores não participaram de cursos de segurança da informação; • Apenas servidores da TI participaram durante a graduação; • Cursos oferecidos pela UFPB são insuficientes para o quantitativo de servidores e professores; • UFPB possui constante redistribuição e aposentadoria de servidores o que dificulta a disseminação da conscientização de segurança da informação na Instituição.
	Experiência	• 67% dos servidores relataram não ter nenhuma experiência com segurança da informação; • Alguns servidores relataram que a aplicação da segurança da informação é papel apenas da TI; • 33% dos entrevistados possuem experiência como professor de disciplina de segurança da informação e empresa privada que possui orientações em relação à segurança da informação.
	Conhecimento sobre a PSI/UFPB	• A PSI/UFPB tem como objetiva ser disseminada e seguida por toda a comunidade acadêmica; • 46% dos entrevistados informaram saber que existe uma PSI na UFPB; • 17% leram a PSI/UFPB;

Fonte: Desenvolvido pelo autor (2019).

4.3 Categoria Tecnologia

Tabela 13**:** Subcategoria – Tecnologia.

Política Segurança da Informação	X	Palavras Utilizadas pelo Entrevistado
4.3.1 Violação de Segurança	24	Furtos de computadores, datashow, mouses e switches; malwares; cartão clonado;
4.3.2 Controle de acesso físico ativos de TI	6	Hacks; Equipamentos mantidos à distância de terceiros;
4.3.3 Inventário	6	Inventário de hardware; Patrimônio; Quem acessa;

Fonte: Desenvolvida pelo autor (2019).

4.3.1. Violação de Segurança

Tabela 14**:** Recortes das Entrevistas Sobre Violação de Segurança da Informação.

1- *"...um terceirizado à noite que ele entrava no meu computador, e ficava assistindo filme, ele encheu meu computador de vírus... "*
2- *"Um professor uma vez num departamento colocou um pendrive num computador…o dispositivo encheu de vírus, porque a máquina estava infectada."*
3- "*...trouxe o pendrive dela dizendo que os dados dela sumiram e por coincidência a máquina dela estava totalmente infectada."*
4- *"Olha está aqui um link, mas era apenas um phishing com um arquivo executável e contaminou a máquina...o computador está com vírus porque não teve a preocupação, a pessoa tinha a consciência, mas na hora a pessoa vai e termina abrindo e infecta os computadores."*
5-*"Em 2017, já houve invasão de salas e roubo de equipamentos de TI. Como Data Show, computadores e cabos."*
6- *"Levaram um switch e computadores"*
7- "*Já houve roubo de memórias"*
8- *"...os alunos são vândalos mouses, e se brincar levam até as máquinas."*
9- "*De repente a impressora começou a imprimir vários de cunho pessoal, palavrões."*
10- *"Malwares? Não, porque eles não têm permissão para instalar programas."*
11- "*Dificilmente acontece, porque poucos têm acesso administrativo."*
12- *"Aconteceu invasão em computadores de professores que utilizavam em pesquisa"*
13- *"Nossas máquinas são invadidas regularmente!"*
14- "*Usei um cartão para realizar uma compra e ele foi clonado dentro da rede da Universidade."*

Fonte: Desenvolvida pelo autor (2019).

Sobre violação de segurança da informação dentro da UFPB, dos 24 entrevistados, apenas 46% relataram ter conhecimento de alguma violação de segurança da informação dentro da UFPB. Conforme a **Tabela 14**, a partir dos comentários 1, 2, 3 e 4 percebe-se que existem *malwares* nos computadores da UFPB. Um dos motivos para inserção desses códigos maliciosos nos computadores é a subutilização e descuido dos servidores ao acessarem conteúdos inapropriados para o ambiente do trabalho e consequentemente realizando *download* não intencional dessas ameaças. Esses códigos maliciosos podem ser expandidos e potencializados por meio da inserção de dispositivos removíveis como *pendrives* nas máquinas infectadas e compartilhadas em outras máquinas podendo acarretar diversos prejuízos como a integridade da informação como foi relatado pelo comentário 3.

Durante a entrevista foram encontradas possíveis soluções para evitar a inserção de *malwares* na rede da UFPB, uma delas surgiu por meio dos comentários 9 e 10, que afirmam que nos seus Centros não existem relatos sobre a inserção de *malwares,* porque os computadores dos servidores estão limitados para realizar tarefas básicas.

Outro tipo de violação de segurança da informação vem ocorrendo dentro da rede da UFPB são os furtos aos ativos de TI. A falha na segurança física dos ativos de TI é uma realidade dentro da Instituição. Conforme os comentários 5, 6, 7 e 8, os ativos de TI como computadores, *mouses, switches,* memória RAM (*Random Access Memory)* já foram retirados do ambiente institucional por terceiros.

A segurança lógica também é um dos alvos dos atacantes. Conforme os comentários 12 e 13, os computadores dos professores são alvos constantes de invasão. Na *categoria gerenciamento de ativos de rede* e *gerenciamento e software*, percebe-se que os professores possuem liberdade total para realizar suas tarefas nos computadores da Instituição, consequentemente, gerando vulnerabilidades para que ameaças possam aproveitar-se e ter acesso à rede da UFPB.

4.3.2. Controle de Acesso Físico Ativos de Redes

Tabela 15**:** Recortes das Entrevistas dos Servidores sobre o Controle de Acesso Físico.

1- *“e sempre tem um curioso que acha que entende mais, tenta resolver, agoniado querendo ajeitar, porque a Internet caiu e começa a mexer no cabeamento.”*

2- *"...tem algum problema na Internet às vezes o usuário acha que é um cabo mal conectado no setor dele aí ao em vez de ligar e pedir algum suporte vai lá e tenta ajeitar a Internet e acaba não colocando no lugar certo o cabo, às vezes o computador dá problema...depois foi um cara da telefonia que foi lá também mexer nos VOIPs que saiu trocando tudo de lugar e as coisas não funcionavam mais durante um tempo."*

Fonte: Desenvolvida pelo autor (2019).

Considerando o Art.º 5 A PSI/UFPB abrange os seguintes aspectos: [...] III. Requisitos de segurança de redes, **por cabos e fios**, tais como administração, design e configuração de redes, **segurança física** e redundância, conexão dos dispositivos, serviços e protocolos;

As questões referentes a este tópico foram realizadas apenas com os servidores da TI que gerenciam e configuram os ativos de TI que podem relatar com maior propriedade sobre o que de fato acontece dentro do Centro onde exercem suas atividades.

Questionados sobre como é gerenciada a segurança física todos ativos de redes da UFPB, 100% dos entrevistados informaram que a maioria dos comutadores de rede *(switches*) são implantados em ambientes como coordenações e departamentos com *hacks* protegendo contra acesso de terceiros não autorizados, entretanto é comum encontrá-los com algum problema seja ausência de trava de segurança ou ausência de chave gerando problema para a rede da UFPB, conforme o comentário 1 e 2 na **Tabela 15**, servidores, professores e qualquer interessado podem modificar as configurações das portas fisicamente do *switches,* porque acreditam entender do assunto e consequentemente acarretando em problemas para a rede deixando-a indisponível.

4.3.3. Inventário de TI

Quadro 13**:** Inventários por Centros.

Sim	Não	Como é feito	Centro
X		Manual	**CCSA**
X		Manual	**CI**
	X		**CCS**
X		Software	**CT**

X		Manual	**CCAE**
	X		**CCHLA**

Fonte: Desenvolvida pelo autor (2019).

Considerando o Art.º 5 no Inciso II. Requisitos de segurança no manuseio e tratamento de informação, que *"define padrões e princípios relacionados ao manuseio de informações, o que incluem inventários [...]"*; e também conforme PSI/UFPB, o Art.7° Parágrafo Único

> "Todos os ativos de TI da UFPB deverão ser inventariados e classificados de acordo com as instruções no Decreto N° 7.845 de novembro de 2012."

A própria PSI/UFPB define ativos de TI no Art. 3° também como

> "III- Ativos de Processamento – Patrimônio composto por todos os elementos de hardware, software, serviço, infraestrutura e instalações físicas necessárias para a execução dos SIs e processos da UFPB, incluindo tanto aqueles produzidos internamente quanto os adquiridos externamente por essa Universidade."

A partir desse trecho da PSI/UFPB, foi questionado aos servidores de TI, se o Centro onde realizam os trabalhos possui inventário de TI. Conforme o **Quadro 13**, 67% dos servidores entrevistados responderam que sim, por meio de controle de patrimônio ou sistema de Software. A maioria deles relatou que é realizado via controle de patrimônio, que funciona quando o ativo de TI é enviado para algum setor e algum chefe assina o termo de responsabilidade citado previamente na subcategor*ia Responsabilidade sobre os ativos de TI* identificando que aquele ativo está naquele setor. Esse controle registra apenas os ativos de TI em nível de *hardware.*

Contudo, a PSI/UFPB é transparente quando cita que ativos de TI abrangem *hardware* e *software*. Porém, o inventário realizado por meio de sistema de *software* possui escopo maior de opções, além de relatar onde o ativo de TI encontra-se, informa as configurações da máquina como nome, HD, processador, memória RAM e qualquer alteração que por ventura venha acontecer, o agente de *software* instalado naquela máquina reportará o ocorrido, por exemplo, caso o algum pente de memória RAM tenha sido retirado por qualquer pessoa, o sistema acusará, isso é uma ação proativa de segurança que visa anular as ocorrências relatadas na subcategoria *Violação de Segurança.*

Não menos importante, outra função é a de registrar os *softwares* que estão instalados naquele ativo de TI. Como relatado na subcategoria *Gestão de Software*, a existência de *softwares* piratas é realidade em todos os Centros da UFPB. Por tanto, o inventário de s*oftware* registra todos

os s*oftwares* instalados naquele ativo de TI, e que periodicamente vai sendo atualizado por meio do agente que reportará as alterações que foram realizadas pelo servidor em termos de *software* naquela máquina fazendo com que a equipe de TI possa agir proativamente excluindo os *softwares* não autorizados.

Tabela 16**:** Síntese dos Achados da Categoria Tecnologia.

Categoria Sociotécnica	Subcategorias da PSI	Síntese dos achados
Tecnologia	**Violação de Segurança**	• 46% dos entrevistados relataram ter conhecimento de algum caso de violação de segurança da informação; • Alguns entrevistados citaram a existência de *malwares* por causa dos controles implantados pela equipe de TI nos computadores; • Clonagem de cartão; • Furto de Computadores, memória RAM, mouse e pontos de acesso;
	Controle de acesso aos ativos de redes	• 100% dos servidores relataram que a maioria dos ativos de redes são instalados em *hacks* e mantidos à distância de difícil acesso pelos servidores ou terceiros; • Em alguns casos, as portas dos *hacks* ficam aberta porque as chaves de proteção foram perdidas;
	Inventário	• 67% dos servidores dos Centros fazem inventário; • Inventário de *software* ou Manual; • A maioria faz inventário manual via controle de patrimônio;

Fonte: Desenvolvido pelo autor (2019).

4.4 Subcategoria Tarefas

Tabela 17**:** Subcategorias – Tarefas.

Política Segurança da Informação	X	Palavras utilizadas pelo entrevistado
4.4.1 Segurança da Informação	38	Proteger a informação por terceiros não autorizados; evitar dados privados acessados por terceiros; preservar dados; resguardar dados; Evitar o vazamento de dados; Proteção da informação do usuário. Preservação dos dados; Informações íntegras; não violação dos dados; modificar ou alterar sem o consentimento;
4.4.2. Segurança em Senha	34	Números sequenciais; Data de aniversário; Senhas complexas;

4.4.3 Realizar outras atividades que não sejam do trabalho	24	Acessar banco, e-mail pessoal, pesquisar sobre o ambiente de trabalho
4.4.4 Gerenciamento de software	24	Quem instala os softwares; licença; software pirateado; software livre
4.4.5 Gerenciamento de ativos de redes	24	Configuração de Pontos de acesso; switch; roteador;
4.4.6 Segurança em E-mail	25	Senha difícil; deslogar quando sair; mudar sempre a senha;

Fonte: Desenvolvida pelo autor (2019).

4.4.1. Segurança da Informação

Tabela 18**:** Recortes das Entrevistas dos Servidores Sobre Segurança da Informação.

1- "*Proteger as informações pessoais dos servidores, alunos e professores contidas nos sistemas para que sejam não divulgadas por terceiros não autorizados e venham a prejudicar membros da comunidade acadêmica;*

2- "*Todo processo onde com essa dificuldade de surgirem tantos hackers de manter o sigilo são os métodos, metodologias e trabalhos que se desenvolvem para evitar o vazamento da notícia, então quanto mais segurança, melhor para nosso trabalho."*

3- "*Informações não podem estar acessíveis para o público de foram da comunidade acadêmica"*

4- "*...preservar esse tipo de informação e evitar que pessoas estranhas não possam fazer uso indevido delas."*

5- *"...fazer com o que a gente produza não seja utilizada por outras pessoas como se fosse dela."*

6- "*São todos os meios utilizados para preservar e resguardar a Instituição com o que diz respeito aos dados que tramitam aqui dentro principalmente da área de TI garantindo a confidencialidade das informações e preservando a segurança dos dados e as funções das tarefas do usuário basicamente isso."*

7- *"Eu percebo em todos setores que eu frequento e no meu próprio trabalho uma pilha de processos na mesa da Secretaria que vão ser processados alí as vezes a pessoa saí para o almoço, saí para outra atividade e aqueles documentos ficam"*

8- *"...muitas vezes documentos sendo largados em mesas com informações estratégicas."*

9- *"Costumo ver e-mail aberto, tela de computadores abertas logados em sistemas como e-mail do Zimbra da UFPB."*

10- *"Manter as informações íntegras."*

11- *"Informações e dados que a gente tem armazenados ou que trafegam pelas nossas máquinas na rede e não sejam violados ou corrompidos."*

12- *"Porém, os processos físicos têm protocolos que entram em algum lugar e eles desaparecem no meio da coisa."*

Fonte: Desenvolvida pelo autor (2019).

Questionados sobre o que entendiam sobre segurança da informação, alguns servidores definiram características do princípio de confidencialidade de segurança da informação como observa-se nos comentários 1 à 6 na **Tabela 18**, que em resumo são mecanismos para proteger as informações físicas (papel, processo) e lógicas (sistemas) produzidas pela UFPB para que terceiros não autorizados acessem e se beneficiem dessas informações.

Porém, a partir dos comentários 7, 8 e 9, percebe-se que existem falhas na realização das atividades dos servidores que comprometem a segurança da informação, principalmente o princípio da confidencialidade, por exemplo, manter documentos expostos na mesa, esquecer a tela de e-mail aberta e ausentar-se para realizar outra atividade. Nesses cenários, qualquer pessoa mal-intencionada pode tentar obter acesso a essas informações, extrair benefício ou fazer mau uso como divulgação pela Internet.

Por outro viés, por meios dos comentários 10 e 11, percebe-se que os entrevistados entendem segurança da informação com características do princípio da integridade, que seria proteger a informação de alteração ou exclusão não autorizada por parte de terceiros. Porém, conforme o comentário 12, procedimentos administrativos realizados pelos próprios servidores atingem esse princípio, que são as perdas dos processos dentro da Instituição.

4.4.2. Segurança em Senha

Tabela 19**:** Recortes das Entrevistas dos Servidores Sobre Segurança em Senha.

1- *"...mas a gente nunca tem uma orientação dizer: ó isso aqui tem que ter uma segurança maior por isso, por isso, não."*
2- *"Servidores compartilham senhas dos sistemas como o SIPAC."*
3- *"Tinha professores que me davam as senhas dele para fazer algo."*
4- *"...mas é comum na UFPB em virtude de ausência do quantitativo inadequado de servidores que se contrate muitos terceirizados e muitas vezes esses terceirizados acabam substituindo essas atividades que são de um servidor normal e não raro esses terceirizados utilizam dessas senhas, há casos também que a senha é exclusiva para um servidor e esse servidor por comodidade transfere para outro como uma chefia do setor, ele passa mediante "confiança" para que aquela pessoa execute aquela tarefa… Eu atuo como chefia do setor e o acesso das compras governamentais só me é permitido, mas dentro do setor, que é composto por 10 pessoas, atribuí todas as tarefas a minha pessoa fica bastante complicado é muita tarefa e às vezes a gente acaba delegando essas tarefas e como as pessoas não podem realizar essas tarefas sem a senha, eu repasso elas.*
5- "*Os sistemas deveriam forçar os servidores a mudar suas senhas"*
6 - *"O ponto eletrônico que é uma importante ferramenta pra gente, mas que gera senha padrão que é tal (informado pelo entrevistado, mas que não será disponibilizado) permitindo que qualquer outro servidor de posse de outro CPF fazer os registros de ponto."*
7- "*...mas a professora ficou com raiva, porque eu disse que não ia passar minha senha, mas é difícil o chefe entender isso, principalmente se forem professores mais antigos, tem professor novo que é a mesma coisa."*
8- "Os servidores mais antigos, professores, que têm senhas, antigamente tinha uma senha aqui que era data de nascimento e data que entrou na Universidade, o próprio STI dava para todos os professores, depois eles trocavam, tinha cara que tinha 20 anos com a mesma senha."
9- "*O básico é não mudar a senha padrão, tem senhas anotadas e você deixar tudo logado como e-mail, senha gravada em navegador."*
10- "*Nós temos conhecimento até pelo vazamento da senha de administrador no qual permite as pessoas mesmos instalarem o computador."*

Fonte: Desenvolvida pelo próprio autor (2019).

Considerando o art. 5 e o tópico IV - Requisito de segurança em operações de sistemas de informação - "*define padrões e princípios relacionados à operação de sistemas de informação tais como [...]responsabilidade sobre senhas[...].* A segurança em senha foi citada 38 vezes pelos entrevistados, possuindo vários vieses dentro da UFPB.

A partir do comentário 1 na **Tabela 19**, afirma não existe nenhum estímulo por parte da equipe de TI ou da UFPB sobre a importância de gerar senhas complexas, adicionalmente, um entrevistado da TI afirma que por ser uma informação básica, não acredita que seja necessário tal orientação. Porém, a segurança de senhas é um dos principais aspectos que devem ser observados por qualquer membro da organização, visto que por meio delas, as informações dos sistemas são acessadas via senha, que em caso de descoberta, pode trazer prejuízos imensuráveis para a organização.

Logo, 70% dos entrevistados informaram que apenas eles têm acesso as suas senhas. Porém, conforme o comentário 2 e 3, percebe-se que alguns servidores compartilham senhas dos sistemas como o Sistema Integrado Patrimônio, Administração e Contratos - SIPAC, onde é possível gerar e buscar processos, assim como verificar contratos e patrimônios da UFPB. Segundo relatos de alguns servidores, essa prática acontece visando agilizar demandas do serviço, conforme cita o comentário 4, porém essa prática é arriscada, visto que, caso ocorra alguma alteração indevida, a responsabilidade recairá para o dono do usuário, que terá que responder pela ação. Outra situação é quando os chefes solicitam a senha do servidor para realizar alguma atividade no computador e o pedido é negado gerando certo desconforto entre chefe e subordinado conforme o comentário 7. Percebe-se que os servidores não reconhecem a importância de manter em sigilo as suas senhas e os prejuízos que podem acarretar para sua carreira pública.

29% dos entrevistados informaram que usam senhas simples para facilitar a memorização, por exemplo, sequência numérica ou relacionado a alguma informação pessoal. Esse tipo de prática facilita a quebra de senhas por meio de ataques conhecidos como o ataque de dicionário, força bruta e dedução. Este número só não é maior, porque segundo relatos dos 25% entrevistados, informaram que suas senhas são complexas porque alguns dos sistemas atuais da UFPB restringem a inserção de senhas fáceis, exigindo do servidor certa complexidade como mínimo de caracteres, letras maiúsculas, minúsculas e números no momento de gerar a senha.

Em contrapartida, o sistema de ponto eletrônico da UFPB não exige complexidade de senhas e segundo relatos dos servidores, a senha padrão de primeiro acesso gerada pelo Agente de Gestão de Pessoa (AGP), que é responsável pelo ponto dos servidores, é mantida pelos servidores facilitando qualquer um ter acesso a seus dados de entrada/saída

da UFPB, conforme o comentário 6. O sistema do ponto eletrônico deveria forçar os servidores a mudar sua senha como enfatiza bem o comentário 5, visto que qualquer pessoa mal intencionada pode fazer registros de entrada e saída dos servidores.

A alteração de senhas periódica na UFPB por parte dos servidores é algo incomum. Inclusive, há relatos de que utilizam senha única para vários sistemas, logo, em caso de descoberta por uma pessoa má intencionada, pode acarretar prejuízos para os servidores e a Instituição.

Ainda são encontrados na UFPB cenários como: senhas anotadas em papéis coladas na mesa, senha de administrador do computador sob conhecimento de todos, servidores antigos como professores mantendo senhas como a data de entrada na UFPB e data de aniversário como relatam os comentários 8, 9 e 10.

4.4.3. Utiliza o Computador da Universidade para Outras Atividades

Considerando o Art.º10, aponta

> "É dever de todo usuário dos ativos de TI da UFPB: [...] III- Utilizar os SIs da UFPB e os recursos a eles relacionados apenas para fins previsto na Universidade."

Isto é, os ativos deveriam ser usados apenas para as atividades cotidiano institucional, entretanto, foi relatado que 80% dos entrevistados declararam que utilizam os recursos computacionais da UFPB para acessar banco, e-mail pessoal, fatura do cartão e até sites de filmes piratas.

O acesso a sites de filmes piratas trouxe *malwares* para o computador da UFPB depreciando o desempenho das atividades laborais do servidor e produtividade na Universidade e um servidor já teve seu cartão clonado acessando à rede da UFPB, segundo relato dos entrevistados, mas esses dados refletem muito o que informa na subcategoria *Conhecimento sobre a Política de Segurança da Informação*, na qual apenas 21% dos entrevistados têm conhecimento sobre a PSI; e a subcategoria *Treinamento e Cursos* onde apenas 12% dos entrevistados relataram ter feito algum curso de Segurança da Informação.

4.4.4. Gestão de Software

Quadro 14**:** Tipos de Softwares Utilizados Pelos Servidores.

Licenciado	Livre	Pirata	Resistência	Conhece quem usa	Não soube	Centro
	X		X			CCSA
X				X		
	X					
	X					
					X	CI
	X					
X	X					
	X					
					X	CCS
X						
	X					
					X	
		X				CT
					X	
X						
X						
	X	X	X			CCAE
X	X	X				
	X	X	X			
X	X					
X	X	X	X			CCHLA
					X	
					X	
X	X	X				

Fonte: Desenvolvida pelo autor (2019).

Considerando o Art.º5 da PSI/UFPB VII. Requisitos de segurança em Gestão de Software: define padrões e princípios relacionados a administração de softwares instalados nos computadores da UFPB, tais licenças, uso de “Software livre”, riscos relacionados ao desenvolvimento por parte do usuário, atualização de versão etc.” e também o Art.º 10

> “É dever de todo usuário dos ativos de TI da UFPB:[...] IV- Abster-se de instalar, utilizar, inspecionar, copiar, armazenar ou fornecer ativos de TI (incluindo, enfaticamente, programas de computador/software) em violação à legislação de propriedade intelectual vigente;”.

Legenda Quadro 14
Licenciado: Servidores usam software licenciado;
Livre: Servidores que informaram usar software livre;
Pirata: Servidores que informaram usar software pirata;
Resistência: Servidores relataram que têm resistência a software livre;
Conhece quem usa: Conhece quem usa software pirata.
Não soube: Não soube informar.

A partir disso, os servidores foram questionados sobre quem gerencia software dentro da UFPB. Segundo o **Quadro 14,** 96% dos servidores relataram que é a equipe de TI que instala os softwares por meio da conta Administrador do terminal.

4% revelaram que chama uma pessoa de confiança para instalar software no computador da UFPB. Percebe-se que a equipe de TI deveria ser chamada para solucionar este tipo de problema, porém, o servidor optou por um membro externo da UFPB, que poderia ter intenção de obter informação da Instituição como da própria servidora.

Durante as entrevistas foram relatados que os professores têm total liberdade para instalar softwares nos seus computadores, não cabendo a equipe de TI gerenciá-los, consequentemente foi relatado que os computadores deles já foram alvo de invasões dentro da UFPB.

42% dos entrevistados relataram usar softwares licenciados. Os entrevistados relaram que os softwares são licenciados porque foram bancados por projetos de pesquisa ou que eles já vêm instalados nas máquinas atuais como os Sistemas Operacionais, leitor de PDF, Antivírus e o software de escritório como pacote *Microsoft Office* que é utilizado instalado sem realizar o crack deixando-o ativo até o fim do prazo livre para o usuário não precise quebrar direitos legais.

Dos entrevistados, 54% relataram que usam softwares livres nas suas atividades. Software Livre seria o ideal, pois não haveria custos para UFPB, porém 17% relataram que a cultura dos servidores de usar o pacote Office gera certa resistência quanto o uso de soluções livres que é o caso do LibreOffice e BROFFICE.

25% dos servidores informaram que têm conhecimento de uso de softwares piratas onde trabalham como pacote Office, Autocad, Adobe e Photoshop. Porém, segundo a Microsoft (2018), ao optar por usar softwares ilegais, os riscos de vulnerabilidade e incidência de ataques cibernéticos são extremamente altos.

No cenário atual da UFPB, no processo de instalação desse tipo de *software*, existem dois vieses, o primeiro é que é solicitado a instalação desse *software* por professores, servidores e diretores, porém ninguém deseja assinar Termo de Compromisso sobre aquela ação, mesmo assim, a instalação é realizada porque o uso desse tipo de *software* é essencial por causa dos cursos existentes nos *Campi.* Em contrapartida, os *Campi*

possuem recursos financeiros para realizar a compra de licença desses *softwares*, porém o processo de compra formal pela UFPB nunca é concluído.

A outra situação é a ampla disseminação da senha de administrador em um dos Centros que permite a instalação desses *softwares* sem a autorização da TI local. A ausência de conhecimento sobre a PSI/UFPB potencializa essa prática dentro da UFPB. Os servidores não têm conhecimento das ações que estão realizando e o quanto pode ser prejudicial para a Instituição não apenas para dimensões legais por essa ação ser um crime, como também em relação à segurança dos dados, embora a PSI/UFPB cite apenas prejuízos de propriedade intelectual, os softwares pirateados podem acarretar danos à informação dos servidores como o cavalo de troia.

4.4.5. Gestão de Ativos de Redes

Tabela 20**:** Recortes sobre Gestão de Ativos de Redes.

1- *"...porque às vezes como a Instituição tem dificuldade em adquirir esse tipo de equipamento, então o servidor no ambiente dele traz um access point de casa e vai e espeta na rede."*
2- *"...às vezes acontece de um que se acha mais experiente e realizar a instalação "*
3- *"Os professores gostam de instalar access points no ambiente deles"*
4- *"Professor e Doutor estão pouco ligando para servidor. Ele chega e faz o que quer. Se o Diretor for falar, eles ignoram até o Diretor. É aquela coisa, minha vontade acima de todos."*
5- *"Quando vou olhar, equipamento configurado errado."*
6- *"...aí eles colocavam muito (switch e ponto de acesso) e ficavam não identificados, aí ficava um problema aqui, caia a Internet em todo setor."*
7- *"...identificar o local desses switches que é uma coisa bem trabalhosa."*
8- "*Teve mês de passar 20 dias sem conexão, por ter servidor DHCP que não conseguia encontrar distribuindo IP na rede "*
9- "*A rede caí, porque a configuração do equipamento entra em conflito com a configuração que é feita pela STI."*

10- *“...isso você gerava brecha para qualquer um chegar e baixar o que quisesse sem identificação...”*

Fonte: Desenvolvida pelo autor (2019).

Considerando o Art.º 5 A PSI/UFPB abrange os seguintes aspectos: [...] III. Requisitos de segurança de redes, por cabos e fios, tais como administração, design e configuração de redes, segurança física e redundância, conexão dos dispositivos, serviços e protocolos;

Diante dessa informação, os entrevistados foram questionados **se já haviam instalado equipamento de redes por conta própria na UFPB?** Conforme **o Quadro 15**, na coluna **“TI”**, em que, 92% dos entrevistados relataram que os ativos de rede da Universidade foram instalados pela equipe de local de TI ou a STI. Na coluna **Outros**, 36% dos entrevistados informaram que já encontraram ativos de redes que não foram instalados e configurados pela equipe de TI ou a STI, mas sim servidores ou professores que não são da área de TI.

A UFPB possui equipe de servidores da área de TI em todos os Centros entrevistados. Todo procedimento de instalação e configuração de ativos de redes segue um padrão definido pela STI e TI local para prevenir que violações de segurança da informação possam ocorrer dentro do ambiente acadêmico. Entretanto, esse procedimento não é obedecido costumeiramente.

Segundo a **Tabela 20,** um dos problemas encontrados nessa categoria foi que conforme o comentário 1, uma das justificativas da instalação dos ativos de redes dentro da Universidade por outros servidores, que não pertencem à área de TI, é porque os ativos de redes que a UFPB possui são insuficientes para abranger toda a área da Universidade.

O comentário 2 informa que a instalação dos ativos de TI parte dos servidores não autorizados por acreditarem possuir conhecimento suficiente para realizar estava atividade no seu setor, sem causar prejuízos à rede da UFPB.

O comentário 3, enfatiza que além dos servidores, os professores também costumam instalar ativos de redes no seu ambiente particular. Nesse viés, possui certo agravante, conforme o comentário 4, relata que existe certa imprudência por parte dos professores ao não obedecer aos servidores de TI, ignorando às regras de implantação dos ativos de TI e que até as ordens do Diretor de Centro são descartadas.

Entretanto, em alguns casos, esses ativos de redes implantados possuem configurações erradas que podem prejudicar o desempenho da rede. Conforme o comentário 5, o ativo só é identificado quando a falha aconteceu, visto que, o comentário 6 explica que um dos exemplos é quando a rede cai de todo o setor, os servidores entram em contato com a equipe de TI relatando o ocorrido, durante a análise da causa do problema, o ativo é descoberto. Segundo o comentário 7, dependendo do tamanho do Centro, esta atividade custa muito tempo da equipe da TI. O comentário 8 relatou que um setor do chegou a ficar mais de 20 dias sem Internet, porque não conseguiu identificar onde estava o ativo de TI que indisponibilizou à rede.

Uma dos problemas é causado, conforme o comentário 9, porque as configurações dos ativos de redes implantados pelos servidores nos ativos de redes entram em conflito com os ativos de redes implantados pela equipe de TI local ou a STI ocasionando a indisponibilidade da Internet, por exemplo, distribuindo endereços lógicos (IP) para os computadores na rede do Centro, gerando conflito com IPs configurados localmente pela equipe de TI. Segundo o pessoal da pesquisa, esse problema é recorrente nos Centros onde trabalham.

Outro problema é os ativos de redes que são implantados de fácil acesso por terceiros, conforme o comentário 10, que é o caso das redes sem fio, onde as senhas são divulgadas em quadro de aviso ou informada livremente pelos servidores. Esta ação pode permitir que qualquer pessoa que estiver em trânsito pela UFPB acesse conteúdos impróprios por meio da rede da Universidade tendo como agravante a impossibilidade de realizar auditoria sobre quem realizou esta atividade, visto que o ativo não possui a funcionalidade de identificar unicamente quem praticou tal ação.

Nesses casos, é importante solicitar a implantação da rede *UfpbSemFios* ou *Eduroam* que possui mecanismos de segurança e possibilitam apenas a comunidade acadêmica ter acesso à rede.

Quadro 15**:** Gestão de Ativos de Redes.

TI	Outros	Rede indisponível	Centro
X			CCSA
X			
X	X	X	
X	X		
X			CI
X	X	X	
X			
X			CCS
X			
X	X	X	
X	X		CT
X	X	X	
X			
X			
X	X	X	CCAE
X			
X			
X	X		
X	X	X	CCHLA
X			
X			
X			

Fonte: Desenvolvida pelo autor (2019).

Legenda do Quadro 15:
TI: Servidores relataram que é a equipe de TI que instalam e configuram os ativos de TI;
Outros: Servidores relataram que presenciaram outros servidores instalando e configurando ativos de TI por conta própria.
Rede indisponível: Servidores relataram que a instalação e configuração de ativos de TI por outros servidores foram causa de indisponibilidade da rede.

4.4.6. Segurança em E-mail

Considerando o Art.º5 da PSI/UFPB, tem-se que: “IV. Requisitos de segurança em operações de sistemas de informação: define padrões princípios relacionados à operação dos sistemas de informação, tais como procedimentos, operacionais, controles [...] uso de correio eletrônicos [...].

O e-mail é uma ferramenta ágil, prática e formal para realizar a troca de informações sigilosas e não sigilosas dentro do ambiente institucional, sendo considerada importante para a realização das atividades rotineiras e requer certa segurança, tanto no gerenciamento do serviço e-mail por parte da TI, como também por partes dos servidores ao trocar mensagens. Isso porque segundo um relatório do *Federal Bureau of Investigation* (FBI) sobre ataques a e-mails corporativos revela que as perdas globais acumuladas de outubro de 2013 a maio de 2018 atingiram U$12,5 bilhões (R$ 47,2 bilhões[7]). Os golpes realizados por meio de e-mail corporativos são constantes, e a maioria deles é baseado em engenharia social (pessoas) do que propriamente no conhecimento técnico dos atacantes (TI INSIDE, 2018).

Por isso, os entrevistados foram questionados **que práticas de segurança da informação são implantadas ao gerenciar suas contas de e-mail**. A equipe de TI não foi interrogada em relação a esse tema, por subentender que tem conhecimento básico para implantar práticas de segurança da informação em relação ao gerenciamento da sua conta de e-mail.

Considerando o **Quadro 16**, na coluna **senha complexa,** 17% dos entrevistados estão preocupados com senhas difíceis. Segundo o CERT.BR (2019), essa prática é muito importante porque, a final de contas, é a senha que dá acesso a sua conta.

44% relataram verificar quem é o remetente do e-mail na coluna **remetente.** Ou seja, caso o e-mail recebido tenha sido enviado por conta de e-mail legítima de outro servidor, eles confiariam em abri-lo e baixar os conteúdos em anexo. Nesse cenário, os entrevistados cairiam facilmente em ataque do tipo E-mail *Spoofing*, porque, se qualquer computador que estivesse infectado por *malware* que venha ter acesso à conta de e-mail de qualquer

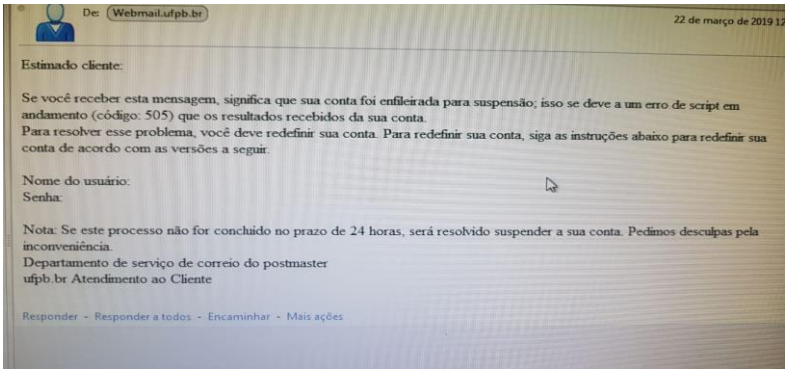
7 Cotação do dólar atual: 1$ = 3,78 R$ - Acessado às 16:41 – 29/07/2019

servidor, pode enviar e-mails solicitando informações pessoais de outro servidor se passando pelo proprietário da conta de e-mail.

11% verificam o conteúdo em anexo antes de realizar o download, segundo a coluna **anexo.** Esta é uma das boas práticas indicadas pelo CERT.BR (2019), que considera importante evitar fazer *download* de arquivos em anexo sem que esteja esperando previamente. Evitando assim o *download* de arquivos que podem conter de *malwares*.

11% dos entrevistados consideram o serviço de e-mail confiável. Porém, foi diagnosticado que servidores estavam recebendo e-mails cujo conteúdo solicitava o usuário e senha do servidor para redefinir sua conta que seria suspensa em caso de não envio das informações como consta na **Figura 6,** logo a seguir.

Figura 6**:** Atacante Usando Técnica de *Phishing* nos e-mails da UFPB.



Fonte: Desenvolvida pelo autor (2019).

Este tipo de ataque à conta de e-mails é conhecido como *Phishing*. Neste cenário, o atacante identificou-se como *webmail.ufpb.br*, algo que pode facilmente induzir servidores a informar seus dados por pensar ser e-mail da STI ou da própria TI local.

Entretanto, 6% não gravam senhas no navegador, 17% deslogam do navegador, 11% somente o usuário tem acesso ao e-mail e apenas 6% nunca pensou em segurança de e-mail.

De fato, todas essas práticas são relevantes para manter a segurança da informação nas contas de e-mail da UFPB para evitar possibilidade de ataque.

Quadro 16**:** Segurança em E-mail.

Senha complexa	Remetente	Anexo	Seguro	Não gravar senha no navegador	Deslogar do E-mail	Somente o usuário possui a senha	Nunca pensou	Centro
X								CCSA
X	X							
	X	X						CI
			X					
X	X							
	X							CCS
				X				
	X							
	X		X					CT
	X							
					X	X		
	X					X		CCAE
	X	X			X			
					X			
	X					X		CCHLA
							X	
	X							

Fonte: Desenvolvido pelo próprio autor (2019).

Categoria Sociotécnica	Subcategorias da PSI	Síntese dos Achados
Tarefas	**Segurança da Informação**	• Foi definida como procedimentos para proteger a informação de sistemas da UFPB contra acesso não autorizado por parte de terceiros; • Porém foi identificado que documentos e processos são mantidos expostos o que facilita o acesso de terceiros não autorizados; • Foi identificado que telas de computadores são mantidas desprotegidas quando servidores vão resolver atividades externas. • Foi definida pelos servidores como mecanismos para proteger informações de alterações indevidas por terceiros não autorizados;
	Segurança em Senha	70% dos entrevistados informaram que apenas eles possuem acesso à sua senha; • 4 entrevistados relataram que não existe estímulo por parte da equipe de TI para gerar senhas complexas; • 29% usam senhas fáceis para facilitar a memorização; • 25% usam senhas complexas porque sistemas exigem; • Ponto eletrônico não exige senhas complexa e ela não é alterada pelos servidores; • Senha única para vários sistemas; • Senhas anotadas em anote e cole na mesa; • Senha de administrador disseminada pelo campus; • Senhas geradas com data de entrada no serviço público e data de aniversário.
	Realizar outras atividades que não sejam do trabalho	• 80% dos entrevistados usam os ativos computacionais da UFPB para acessar outros conteúdos como banco, e-mail pessoal e fatura de cartão.
	Gerenciamento de Software	• 96% dos entrevistados relataram que a TI é quem gerencia os softwares; • 4% dos entrevistados relataram que contrata terceirizado de confiança para instalar software; • Professores têm total liberdade para instalar software; • Computadores dos professores foram alvos de invasões; • As equipes de TI informaram realizar estudo prévio do software antes de realizar instalação; • 42% dos entrevistados relataram usar software licenciado; • 54% dos entrevistados informaram usar software livre; • 17% dos entrevistados relataram existir certa resistência quanto o uso de software livre como o BrOffice; • 25% dos servidores relataram presenciar o uso de software pirata; • Processo de compra de licença de software é burocrático dentro da UFPB;
	Gerenciamento de ativos de redes	• 92% dos entrevistados relataram que os ativos de TI foram instalados pela equipe de TI; • 36% dos entrevistados informaram ter visto ativos de TI instalados por outros servidores; • Ativos de redes da UFPB são insuficientes para a necessidades dos servidores; • A rede da UFPB teve oscilações pós-instalação desses ativos; • Identificação desses ativos em centros maiores é um processo oneroso; • Alguns centros já desenvolveram normas para evitar esse tipo de prática na UFPB.

	Segurança em E-mail	• 17% dos entrevistados estão preocupados com senhas difíceis; • 44% revelaram verificar se quem enviou a mensagem realmente foi o remetente; • 11% checam se o conteúdo em anexo é malicioso; • 11% dos entrevista dos consideram o e-mail da UFPB seguro; • 6% não gravam senhas no navegador; • 17% deslogam do navegador; • 11% somente o usuário possui acesso a sua senha; • 6% nunca pensou em práticas de segurança de e-mail; • E-mails já foram enviados para as contas de e-mails dos servidores buscando informações; • Ataques de *Pishing* acontecem na Universidade;

Fonte: Desenvolvido pelo próprio autor (2019).

4.5. Proposta de Cartilha de Boas Práticas de Segurança da Informação

Considerando os dados levantados e analisados nas subcategorias sociotécnicas, foram identificadas falhas e ausências de procedimentos padrões de segurança da informação dos servidores dos seis Centros entrevistados da UFPB, que podem acarretar vulnerabilidades para os ativos de TI e informação da UFPB.

Alguns fatores influenciam este cenário: ausência de conhecimento e divulgação da PSI/UFPB; a PSI/UFPB é considerada abstrata pelos servidores que tiveram acesso; a PSI/UFPB não mostra como os servidores alcançarão os requisitos; poucos servidores receberam treinamento sobre segurança da informação e as informações sobre práticas de segurança são adquiridas por meio de comunicação informal;

Diante desses dados, segundo a Cartilha de Boas Práticas de Segurança da Informação do Tribunal de Contas da União (TCU) (2012),

> quando a instituição achar conveniente e necessário que a PSI seja mais abrangente e detalhada, sugere-se a criação de outros documentos que especifiquem práticas e procedimentos e que descrevam com mais detalhes as regras de uso da tecnologia da informação. Esses documentos costumam dispor sobre regras mais específicas, que detalham as responsabilidades dos usuários, gerentes e auditores e, normalmente, são atualizados com maior frequência.

Considerando o cenário de segurança da informação dentro da UFPB e o que cita a Cartilha de Boas Práticas de Segurança da Informação do TCU (2012), este tópico foi criado visando propor uma Cartilha de Boas Práticas de Segurança da Informação da UFPB, cuja finalidade é dar transparência aos requisitos de segurança da informação citados na PSI/UFPB, especificando com detalhes que práticas devem ser realizadas para alcançar tais requisitos.

Essa proposta não substitui o treinamento e curso de segurança da informação, mas orientarão os servidores a realizar atividades buscando a segurança da informação e consequentemente estar em conformidade com a PSI/UFPB.

Propostas de Cartilha de Boas Práticas de Segurança da Informação – UFPB.

No artigo 5° que a PSI/UFPB abrange os seguintes aspectos:

I. Requisitos de segurança criptográficos: define padrões e princípios sobre quando e como recursos criptográficos devem (ou não) ser utilizados sobre dados institucionais;

Figura 7: Uso de Recursos Criptográficos nos Processos de Trabalho.

Ação	O que deve ser feito	Referência
Utilizar recursos criptográficos nos processos de trabalho	Por meio da TI local ou STI, solicitar treinamento sobre o uso de ferramentas que implementam criptografia usando algoritmo simétrico ou assimétrico para realizar cifração ou decifração dos arquivos da UFPB para garantir a confidencialidade, integridade e autencidade das informações sigilosas. Exemplo: VeraCrypt, TrueCrypt, EncryptOnClick, Kruptos 2 Pro.	CERT.BR (2019) e ISO 27002:2013(p.43),Techtudo(2019)
	Utilizar programa para criptografar arquivo único contendo senhas. Exemplo: Keypass.	CERT.BR (2019), Keypass(2019)
	Ao navegar em sites, verificar se possuem *https://*	CERT.BR (2019)

Fonte: Desenvolvida pelo próprio autor (2019)

II. Requisitos de segurança no manuseio e tratamento de informação: define padrões e princípios relacionados ao manuseio de informações, o que incluem inventário, administração e propriedade sobre dados, eliminação e emoção de informação, informações disponíveis em mesas de trabalho etc.

Figura 8: Administração e Propriedade Sobre Dados e Inventário.

Ação	O que deve ser feito	Referência
Administração e propriedade sobre dados	A STI ou a TI local deve ser orientada pela administração para gerenciar as permissões leitura, escrita e execução de acesso aos arquivos contidos em pastas compartilhadas como Samba, e Drive da UFPB.	Adaptado da ISO 27002:2013 (p.39, c)
	A administração local deverá notificar a STI ou a TI local sobre remoções e aposentadorias para que retirem as permissões dos usuários.	Adaptado da ISO 27002:2013 (p.31, 32 e 34)
Inventário	Todos os ativos de TI precisam ser identificados, mantidos, organizados estruturalmente e cada um deles possuir um responsável formalmente identificado por sua propriedade seja por meio de soluções de software ou administrativo;	Adaptado da ISO 27002:2013 (p.23)
	É importante que os inventários de TI sejam realizados em solução de software, porque facilitarão a gerência de softwares e hardwares instalados nos computadores. Exemplo: OCS Inventory, Spiceworks e Lansweeper	Adaptado da ISO 27002:2013 (p.23)
Equipamento de usuário sem monitoração	Ao ausentar-se do seu computador, bloquear a conta que está em atividade e desligar o monitor;	Adaptado da CERT.BR (2019); ISO 27002:2013(p.55,a e c)
	Desconectar de serviços ou sistemas, quando não estiver mais usando.	Adaptado da ISO 27002:2013(p.55,b)
Política de mesa limpa e tela limpa	Ao ausentar-se de atividades, retirar documentos e inseri-los em armários com proteção de chaves, cofres e salas de arquivo que possuem chaves.	Advisera (2016), ISO 27002:2013(p.56, a)
	Retirar imediatamente documentos sigilosos da bandeja de impressora	Adaptado da ISO 27002:2013(p.56, d)

Fonte: Desenvolvida pelo próprio autor (2019).

III. Requisitos de segurança de redes e dispositivos móveis: define padrões e princípios relacionados à segurança de redes, por cabos e sem fio, tais como administração, design e configurações de redes, segurança física e redundância, conexão de dispositivos, serviços e protocolos.

Figura 9**:** Requisitos de Segurança de Redes e Dispositivos Móveis.

Controle	O que deve ser feito	Referência
GERENCIAMENTO DE ATIVOS DE REDES	Procurar sempre a TI local ou a STI para realizar qualquer procedimento em termos de ativos de redes. Exemplo: instalação e configuração pontos de acesso, switches, roteadores e passagem de cabos.	Adaptado da ISO 27002:2013 (p.31)
	Manter os ativos de redes (switches, pontos de acesso e roteadores) protegidos do acesso físico por terceiros. Exemplo: Mantê-los em hacks com chaves, distância física de fácil	Adaptado da 27002:2013 (p. 32, c)
	Não realizar qualquer alteração física nos ativos de redes como adição, alteração e remoção de cabos de redes ou energia sem o consentimento da equipe da TI;	Adaptado da 27002:2013
ACESSO À REDE DA UFPB	Recomenda-se o uso de rede sem fio implantadas pela TI local ou STI como Eduroam ou UfpbSemFios.	Adaptado da CERT.BR (2019), ISO 27002:2013(p.32)
GERENCIAMENTO DE DISPOSITIVOS MÓVEIS	Solicitar permissão a TI local ou STI para o uso de dispositivo móvel(notebook) pessoal na rede da UFPB	Adaptado da 27002:2013 (p.14)
SEGURANÇA DO CABEAMENTO	Manter distância do cabo de rede com o de energia para evitar interferência;	Adaptado da ISO 27002:2013(P.52, b)
	Manter cabeamento de transmissão de dados distantes da passagem de servidores;	Adaptado da ISO 27002:2013(P.52, a)

Fonte: Desenvolvida pelo próprio autor (2019).

IV. Requisitos de segurança em operações de sistemas de informação: define padrões e princípios relacionados à operação dos sistemas de informação, tais como procedimentos operacionais, controles, responsabilidades sobre senhas, contas de usuários, uso de correio eletrônico, relato de incidentes de segurança da informação e falhas de software;

Figura 10**:** Senhas, Uso dos Correios Eletrônicos, Contas de Usuários e Relatos de Incidentes.

Ação	O que deve ser feito	Referências
Senhas	Incluir no mínimo 6 caracteres com números, letras maiúsculas, minúsculas e caracteres especiais ($,%,@,! etc);	TCU(2012, p. 21) ; CERT.BR(2019); ISO 27002:2013(p. 38, d)
	Alterar a senha no primeiro acesso	TCU (2012, p. 20); ISO 27002:2013 (p.41, c)
	Verifique sempre se alguém está observando no momento de gerar sua senha;	CERT.BR (2019) ;
	Evitar gerar senha com sequência de teclado como: zxcvbn, asdfgh...	CERT.BR (2019) , TCU (2012, p. 20); ISO 27002:2013 (p.38, d)
	Deslogar de sistemas;	CERT.BR (2019) ; ISO 27002:2013(p. 40)
	Não inserir nenhuma data familiar (aniversário de qualquer familiar, nome, futebol, inserção no serviço público etc.);	CERT.BR (2019); TCU (2012, p. 20); ISO 27002:2013(p. 38, d)
	Não inserir nenhum nome ou combinação de nomes que estejam contidos no dicionário;	CERT.BR (2019) ; TCU (2012, p.20); ISO 27002:2013(p.38, d)
	Alterar a senha sempre que existir suspeita violação de segurança no sistema ou da própria senha	Adaptado da ISO 27002:2013(p.38, c)
	Caso seja necessário enviar senha pela rede da UFPB, criptografá-la antes	ISO 27002:2013(p. 40, j)
	Manter senha de grupo apenas com os membros participantes;	Adaptado da ISO 27002:2013(p.35, a)
	Modificar a senha regularmente;	CERT.BR (2019) ; TCU (2012, p.20); ISO 27002:2013(p.38)
	Não repetir senhas usadas anteriormente;	CERT.BR (2019);
	Não anotar senhas em papeis	TCU(2012, p. 20) ; ISO 27002:2013(p.38, b)
	Não usar a mesma senha para vários serviços;	CERT.BR (2019), TCU (2012, p. 20); ISO 27002:2013
	Não mostra a senha na tela quando estiver digitando-a	ISO 27002:2013(p. 41, g)
	Não compartilhar senhas com outros servidores ou qualquer outra pessoa.	Adaptado CERT.BR, 2019; TCU(2012, p.12); ISO 27002:2013(P.38, i)

Uso dos Correios Eletrônicos	Usar sempre o e-mail institucional para comunicações internas;	Decreto 8.135/2013
	Gerar senhas complexas vide tópico senhas;	CERT.BR (2019), TCU (2012, p.12), AVG (2016), Google (2019), ISO 27002:2013
	Nunca usar a mesma senha duas vezes ou parecidas.	AVG (2016)
	Não compartilhar senhas.	CERT.BR, 2019, TCU(2012, p.12);
	Verificar sempre o remetente do e-mail recebido, caso seja desconhecido, descartar.	CERT.BR, 2019
	Fazer download de arquivo em anexo apenas quando esteja previamente esperando de servidores conhecidos.	AVG (2016), Olhar Digital (2014), CERT.BR (2019)
	Não informar dados pessoais como cartão de crédito, nomes de usuário e senha via e-mail.	AVG (2016)
	Quando desejar enviar e-mail para vários destinatários sem que outros saibam, usar o opção CCO.	AVG (2016)
	Manter sempre o navegador web (Chrome, Firefox, Internet Explorer) atualizados;	GMAIL (2019)
	Ter cuidado com *links* recebidos via e-mail. É aconselhado digitar diretamente a URL no navegador.	CERT.BR (2019)
	Atualizar sempre os antivírus.	CERT.BR (2019)
Contas de Usuário	Apenas a TI ou a STI é responsável por gerenciar as contas dos usuários computadores, e-mails e sistemas de compartilhamento de arquivo em redes;	Adaptada da CERT.BR (2019) e ISO 27002:2013 (p.34)
	As contas dos servidores devem ser padronizadas, identificadas unicamente e possuir senha com permissão apenas para executar programas de uso cotidiano: navegadores de Internet, pacote de escritório (Office e LibreOffice), leitor de PDF e etc.	Adaptada da CERT.BR (2019), TCU (2012, p. 17)
	Um aviso deverá ser inserido nos computadores informando que o uso é somente permitido para os servidores.	ISO 27002:2013(p. 40, b)
	As contas dos usuários dos computadores, e-mails, compartilhamento de arquivos em redes devem ser revisadas periodicamente para que seja removida em caso de remoção ou aposentadoria.	Adaptada da ISO 27002:2013(p. 35 e 36)
Uso de equipamentos de TI	Evitar comer, beber e fumar perto dos ativos de TI	ISO 27002:2013(p.50, f)
Relato de incidentes de segurança da informação e falhas: malwares, tentativa de	Entrar em contato com a STI ou TI local via telefone ou sistema de chamados da UFPB;	PSI/UFPB

Fonte: Desenvolvida pelo próprio autor (2019)

V. Requisitos de segurança contratual e acordo de nível de serviço: define padrões e princípios relacionados à manutenção da segurança de ativos TI que são acessados ou fornecidos por terceiros;

Figura 11**:** Controle de Acesso de Terceiros aos Ativos de TI.

Ação	O que deve ser feito	Referência
Controle de acesso de terceiros aos ativos de TI	Uma lista formal deve ser desenvolvida e publicada contendo identificação de terceiros que podem acessar determinado ativo de TI da UFPB.	Adaptado 27002:2013(p.91).

Fonte: Desenvolvida pelo próprio autor (2019).

VI. Requisitos de segurança em recursos humanos: define padrões e princípios de segurança relacionados a ações realizadas por ou eventos ocorridos (docentes e técnicos-administrativos), gestores, pessoal em cargos de chefia, estagiários, tais como procedimentos a realizar quando os servidores quando sofre relotação, quando está em licença etc.:

Figura 12**:** Segurança em Recursos Humanos.

Ação	O que deve ser feito	Referência
Segurança em Recursos Humanos	Por meio do Termo de Confidencialidade, certificar que o servidor, estagiário, professor, Diretor ou terceirizado que o mesmo é responsável pelo ativo de TI onde exerce suas atividades podendo responder por qualquer evento de segurança como inserção de malware, furto, violação da confidencialidade, integridade e disponibilidade dos ativo des TI e informações.	Adaptada da ISO 27002:2013 (p.17)
	Por meio do Termo de Confidencialidade, citar que existe a PSI/UFPB certificando que o servidor, estagiário, professor, Diretor ou terceirizado deve seguir as orientações contidas nela e caso haja algum evento de segurança da informação como inserção de malware, furto, violação de integridade, confidencialidade e disponibilidade do ativo de TI e da informação deverá ser penalizado em relação as punições contidas na 8.112/1990.	Adaptada da ISO 27002:2013 (p.18 e 22)
	Servidor, estagiário, professor, Diretor ou terceirizado ao receber qualquer ativo de TI deve assinar Termo de Confidencialidade pela segurança da informação das informações e dos ativos de TI	Adaptado da ISO 27002:2013 (p. 18)
	O servidor, estagiário, professor ou terceirizado que perdeu o vínculo/removido para a outra unidade, deverá perder as permissões de acesso de arquivos em pastas compartilhadas privativas do setor, a conta de usuário no computador, exclusão da listas de e-mail do setor, exclusão da conta em sistema local do setor e etc.	Adaptado da ISO 27002:2013
	Ativos de TI que estejam em sua posse devem ser devolvidos por meio de Termo de Devolução devidamente formalizado pela administração local/Direção local;	Adaptado da ISO 27002:2013 (p.25)
	Convém que o Diretor de Centro solicite a todos professores, estagiários, servidores, alunos e terceirizados que pratiquem a segurança da informação de acordo com a PSI/UFPB e este Guia de Boas Práticas de Segurança da Informação	Adaptado da ISO 27002:2013 (p.19)

Fonte: Desenvolvida pelo próprio autor (2019).

VII. Requisitos de segurança em gestão de software: define padrões e princípios relacionados à administração de softwares instalados nos computadores da UFPB, tais como gerenciamento de licenças, uso de “softwares livres”, riscos relacionados ao desenvolvimento de software por parte de usuário, atualização de versão;

Figura 13**:** Segurança em Gestão de Software.

SEGURANÇA EM GESTÃO DE SOFTWARE	Realizar solicitação a equipe de TI local ou STI para instalar ou remover software mediante justificativa formal.	Adaptado da ISO 27002:2013(p.42, c, e e, p.84)
	Realizar solicitação a equipe de TI local ou a STI para atualizar os softwares instalados;	Adaptado da ISO 27002:2013(p.42, d, e 84), CERT.BR(2019)
	TI local ou STI deve criar lista de softwares para serem instalados no sistema.	Adaptado da ISO 27002:2013(p.61, b)
	Solicitar autorização da TI local ou STI para instalar programas que não estão inclusos na lista permitida	Adaptado ISO 27002:2013 (p. 42, d)
	Apenas Softwares Livres e Licenciados serão instalados nos ativos de TI.	CERT.BR (2019) e Adaptado ISO 27002:2013 (p. 61,
	A instalação de softwares piratas poderá acarretar em prejuízos legais para UFPB; Habilitar brechas para malwares serem implantados nos computadores locais acessando dados sigilosos daquele ativo de TI, difundir-se a partir da rede da UFPB; depreciar os requisitos não-funcionais daquele computador com o passar do tempo como processamento e velocidade na execução de tarefas.	SOFTLINEGROUP (2016)

Fonte: Desenvolvida pelo próprio autor (2019).

VIII. Requisitos de segurança para aquisição de ativos de TI: define padrões e princípios relacionados à seleção, aquisição, instalação e gestão de contratos de fornecimento/provimento de ativos de TI:

Qualquer aquisição de ativos de TI deve observar os requisitos de segurança e citar a PSI/UFPB previamente;

Figura 14**:** Segurança em Aquisição de Ativos de TI.

Ação	O que deve ser feito	Referência
Análise e especificação dos requisitos de segurança da informação	Reunir com a equipe de TI local ou consultar STI para levantar o máximo de informação possível sobre as necessidades e requisitos de segurança lógico(firewall UTM, antivírus, criptografia, redundancia de dados, IDS, VPN etc)	Adaptado da ISO 27002:2013(p.90-92)
	Reunir com a equipe de TI local ou consultar STI para levantar o máximo de informação possível sobre as necessidades e requisitos de segurança física(trancas de proteção, chaves e cadeados e etc.) para proteger acesso de terceiros.	
	Reunir com a equipe de TI local ou consultar STI para levantar o máximo de informação possível sobre as necessidades e requisitos de segurança contratual como garantia.	

Fonte: Desenvolvida pelo próprio autor (2019).

4.5. Política de Segurança da Informação na UFPB e os princípios sociotécnicos

Esse tópico foi criado com o intuito de relacionar os princípios sociotécnicos com a realidade da atuação da PSI/UFPB nos processos de trabalho identificados na Análise de Conteúdo e os resultados encontrados.

Estado incompleto: considerando a análise realizada, foi possível identificar que a implantação da PSI/UFPB não está em conformidade com o princípio sociotécnico do estado incompleto. Cherns (1976) cita que:

> o projeto da organização não deve ser definitivo, deve ser interativo, contínuo, composto por equipes multifuncionais constantemente operando, revisando o trabalho da organização, procurando revisões contínuas de objetivos estruturas.

Partindo desse princípio e adicionalmente no Art° 21 da PSI/UFPB cita que “a PSI será revisada anualmente pela GSEGI/STI, apreciada pelo CGTI e submetida à aprovação do CONSUNI”. Portanto, a PSI/UFPB, um documento sociotécnico, criada em 2014 e não atualizada desde então, deveria ser revisada de forma periódica e contínua, buscando alinhar-se com os objetivos organizacionais, atualizar-se quanto as necessidades da comunidade acadêmica em relação à segurança da informação. A não atualização da PSI/UFPB impossibilitou ampliar a gama de requisitos de segurança da informação que poderiam ser abrangidos por este documento, visando preencher lacunas que existem nela, por exemplo, um novo requisito poderia ser adicionado como “requisitos na navegação web” orientando como navegar, que tipo site deve ser evitado, que prejuízos podem ocorrer ao acessar sites de filmes pirateados para a rede da UFPB e etc.

A transição organizacional ou organização transitória: Caso a Proposta de Boas Práticas de Segurança da Informação seja aprovada, é preciso previamente preparar a comunidade acadêmica quanto a relevância deste documento por meio de divulgação nos meios de comunicação da UFPB como sites, e-mail e comunicados em quadro de aviso, pois os processos implantados de segurança da informação deverão ter como base o Guia de Boas Práticas de Segurança da Informação.

Compatibilidade: Esse princípio encaixa-se como a PSI/UFPB foi desenvolvida. Segundo relatos dos entrevistados, que têm conhecimento sobre a PSI/UFPB, este

documento quando foi criado, não buscou a compatibilidade em adequar-se à realidade e a dinamicidade das mudanças que venham ocorrer em cada Centro em termos de segurança da informação, por exemplo, dar oportunidade a comunidade acadêmica em relatar sobre o que entende sobre segurança da informação e como eles a praticam, a partir disso, oferecer treinamentos sobre segurança da informação buscando alcançar os requisitos de segurança da informação da PSI/UFPB.

5. CONSIDERAÇÕES FINAIS

Nos cenários onde inúmeras ameaças são desenvolvidas por *hackers* e consequentemente disseminadas pela rede mundial de computadores com o objetivo de infiltrar-se em redes privadas para obter informações privilegiadas das organizações, por outro lado, os órgãos públicos preparam toda sua equipe para desenvolver consciência em relação às práticas de segurança da informação para não gerar vulnerabilidades por meio dos ativos de tecnologia da informação, reduzindo o escopo de vulnerabilidades que poderão ser aproveitadas por essas ameaças.

Nesse sentido, este estudo buscou responder o seguinte questionamento: **à luz da perspectiva sociotécnica, como os servidores da UFPB cumprem as orientações e os requisitos de segurança da informação contidos na Política de Segurança da Informação nos processos de trabalho e ativos de TI?**

Para chegar a esse resultado, foi percebido que dentre outros aspectos que possibilitaram atingir os objetivos do trabalho, a efetiva participação dos servidores, professores e Diretores de Centro foram determinantes relatando informações sobre o conhecimento deles da PSI/UFPB e as práticas de segurança que eles executam nos processos de trabalho.

Dentre as atividades que compuseram o processo de identificação das práticas de segurança da informação implantado pelos servidores da UFPB, a Análise de Conteúdo das entrevistas foi à atividade mais crítica e complexa, pois gerou dedicação, concentração e tempo, uma vez que, foi preciso identificar as subcategorias da Política de Segurança da Informação a partir das entrevistas e relacioná-las com as subcategorias sociotécnicas previamente definidas: estrutura, pessoa, tarefas e tecnologia.

Em seguida, por meio das subcategorias da Política de Segurança da Informação identificadas, foi possível identificar que **os servidores implantam os requisitos contidos na Política de Segurança da Informação, porém as práticas contêm falhas que podem ser aproveitadas por vulnerabilidades.**

Para suprir a deficiência existente nas práticas de segurança da informação, ausência do conhecimento sobre a PSI/UFPB, abstração dos requisitos contidos na PSI/UFPB e a insuficiência de curso de segurança da informação da UFPB, **foi desenvolvida uma Proposta de Boas Práticas de Segurança da Informação para nortear os servidores em relação ao cumprimento dos requisitos de segurança das informações contidas na PSI/UFPB, assim como, melhorar a qualidade das práticas de segurança da informação na UFPB.**

5.1. Contribuições Teóricas

Durante o estudo, foram encontradas na literatura, pesquisas que tratam de forma genérica a relação da segurança da informação com a Abordagem Sociotécnica e a importância de investir não apenas no subsistema técnico, mas também ao subsistema social como um todo a projetar a segurança da informação de uma organização (LI; HORJOFF; MYLOPOULOS, 2016).

Porém, este estudo buscou aprofundar-se nessa temática analisando as individualmente as 4 variáveis de um sistema de trabalho que são técnicos (tecnologia e tarefas) e social (pessoas e estrutura) em relação à PSI de uma autarquia da APF algo que não foi encontrado na literatura.

Para tanto, foi possível identificar que a PSI é um documento sociotécnico e para desenvolvê-lo em um IFE é preciso previamente explorar e buscar entender como funcionam essas 4 variáveis em cada setor com a finalidade de assimilar como as atividades são realizadas. A partir disso, é possível reconhecer qual é o cenário atual da segurança da informação dentro do IFE, quais são os problemas que precisam ser tratados, priorizados e corrigidos visando o ponto principal que é a harmonia entre os aspectos sociotécnicos atrelados aos objetivos organizacionais em termos de segurança da informação e a eficiência no trabalho.

5.2. Contribuições Práticas

5.2.1. Complexidade da aplicação de uma Política de Segurança da Informação no IFE

Como em qualquer organização, a PSI precisa ser disseminada periodicamente, e por meio de treinamentos, avisos e publicação em sites da Instituição, conscientizar a comunidade acadêmica em relação à segurança da informação. O cenário de um IFE é complexo. A oferta de cursos de conscientização em segurança da informação como é o caso da UFPB é insuficiente para abranger o quantitativo de servidores. Outro fator agravante é a constante rotatividade de servidores em termos de aposentadoria, redistribuição e aprovação em outro concurso público. Para isso é preciso de mecanismos auxiliares à PSI, que sirvam de base para os servidores, nesse cenário o Guia de Boas Práticas de Segurança da Informação auxiliará a comunidade acadêmica a praticar ações de segurança da informação nas atividades.

5.2.2. Proposta de Boas Práticas de Segurança da Informação

Como resultado deste estudo, foi desenvolvida uma Proposta de Boas Práticas de Segurança da Informação, porque durante a pesquisa foram identificadas vulnerabilidades nas práticas de segurança da informação implantadas pelos servidores da UFPB e que acarretaram eventos de segurança da informação. Segundo relatos, a maioria não participou de cursos e treinamentos de segurança da informação, assim como, não possui experiência com essa área. A PROGEP oferece por ano cursos de segurança da informação contendo apenas 40 vagas, número ínfimo comparado com o quantitativo de servidores na UFPB. A partir desses dados, visando não substituir treinamento e cursos de segurança da informação, a proposta de Boas Práticas de Segurança da Informação foi elaborada a partir da norma **NBR ISO 27002:2013**, Guia de Boas Práticas de Segurança do TCU (2012) e outros portais de segurança da informação para auxiliar os servidores a cumprir as orientações e os requisitos de segurança da informação contidos na PSI/UFPB.

5.3 Limitações da Pesquisa

- Quantidade de Centros

A UFPB possui 16 Centros onde poderiam ser realizados a pesquisa ,entretanto, devido o tempo reduzido, a espera pela aprovação do Comitê de Ética da UFPB para realizar as entrevistas, dificuldade em encontrar servidores no campus no período de férias para realizar as entrevistas, o custoso trabalho para transcrever as entrevistas e a distância em relação aos *campi* do interior dificultaram escopo maior da pesquisa.

- Coleta de dados psicométrica

Os dados foram coletados por meio das respostas dos entrevistados, que não puderam ser validados por ausência de ferramenta que auxiliasse na validação dos dados.

5.4 Recomendações de Continuidade

Para investigações futuras, recomenda-se que tais pontos sejam abordados:

- Expandir a pesquisa para outros Centros da UFPB;
- Acompanhar via chamados de segurança da informação se a PSI e as Boas práticas são eficientes;
- Realizar a pesquisa com outro órgão federal e comparar resultados;

REFERÊNCIAS

ADAMS, A.; SASSE M. A., "Users are not the enemy,"Communications of the ACM, vol. 42 (12), pp. 41 – 46,1999.

ADVISERA. **Política de Mesa Limpa e Tela Limpa – O que a ISO 27001 requer?** 2016. Disponível em: https://advisera.com/27001academy/pt-br/blog/2016/03/17/politica-de-mesa-limpa-e-tela-limpa-o-que-a-iso-27001-requer/ Acesso em: 02 de Maio,2019 às 13:45.

AKHYARI, N.; RUZAINI, A.; RASHID, A. H. **Information Security Culture Guidelines to Improve Employee'S Security Behavior: A Review of Empirical Studies**. Journal of Fundamental and Applied Sciences. 2018

ANDRESS, M. **Manage People to Protect Data, InfoWorld**. vol. 22, Issue 46, 13 November, 2000.

ASHENDEN, D. **Information Security Management: A Human Challenge?** Journal Elsevier. 2008.

AVAST. **O que é Phishing?** Disponível em **https://www.avast.com/pt-br/c-phishing** Acesso em: 13 de Abril, 2019 às 08:08.

AVG. **Lista De Verificação de Segurança de E-Mail – 9+1 Dicas Para Ficar Seguro**. Disponível em: **https://www.avg.com/pt/signal/email-security-checklist** Acesso em: 02 de Maio, 2019 às 9:30.

BADDINI, P. **Conheça Os 6 Riscos de Utilizar Software Pirata na Sua Empresa**, **2017**. Disponível em: **https://www.techsoupbrasil.org.br/6-riscos-da-instalacao-de-um-software-pirata-para-sua-empresa-ou-organizacao** Acesso em 16 de Dezembro, 2018 às 11:55.

BARDIN, L. **Análise de Conteúdo**. Ed. 70, São Paulo, 2011.

BJORK, F. **Institutional Theory: A New Perspective For Research Into IS/IT Security In Organisations.** Proceedings Of The 37th Hawaii Internation Conference On System Sciences. Hawaii: IEEE, 2004.

BONI, V.; QUARESMA, S. J. **Aprendendo A Entrevistar: Como Fazer Entrevistas em Ciências Sociais**. Revista Eletrônica dos Pós-Graduandos em Sociologia Política da UFSC, 2005.

BOSWORTH, S.; KABAY, M.; WHYNE, E. **Computer Security Handbook (6th Ed.)**. New York: Wiley, 2014.

BULLÉ, J. H.; MONTOYA, L.; PIETERS W.; JUNGER M.; HARTEL, P. **On The Anatomy Of Social Engineering Attacks—A Literature-Based Dissection Of Successful Attacks**. WILEY. 2017

BOSTROM, R. P.; HEINEN, J. S. **MIS Problem And Failures: A Sócio-Technical Perspective. MIS Quartely**, v.1, n.3, p. 17-32, 1977.

BULGURCU, B.; CAVUSOGLU, H.; BENBASAT, I. **Roles Of Information Security Awareness And Perceived Fairness In Information Security Policy Compliance.** AMCIS 2009 Proceedings, 419.

CERT.BR – **Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança da Informação no Brasil**, 2018.Disponível em: https://www.cert.br/ Acesso em: 16 de Novembro, 2018 às 11:50.

CHAN, M.; WOON, I.; KANKANHALLI, A. **Perceptions Of Information Security At The Workplace: Linking Information Security Climate To Compliant Behavior,** 2005.

CHERNS, A. **The Principles Of Sociotechnical Design.** Human Relations, 29, 783-792, 1976.

CHIAVENATO, I**. Administração de Empresas: Uma Abordagem Contingencial.** 2. ed. São Paulo: McGraw-Hill, 1987.

_____ **Principles Of Sociotechnical Design Revisted**. Human relations, v. 40, n. 3, p. 153-161, 1987.

CHOO, C. W. **A Organização do Conhecimento: Como as Organizações Usam A Informação para Criar Significado, Construir Conhecimento e Tomar Decisões**. Editora Senac. Ed.1. 1998.

CNN tech. **Researchers Find Possible North Korea Link To Massive Cyberattack**. Disponível em: http://money.cnn.com/2017/05/15/technology/wannacry-hack-responsible-hackers/index.html Acesso em: 16 de Outubro, 2018 às 18:52.

CONOLLY, P.J. **Security Starts From Within**, InfoWorld,Volume 22, Issue 28, 10 July 2000.

CORREIA, R. R. **Estrutura de Equipes-Cliente em Projetos de Implantação de Sistemas de Informação no Setor Público: Evidências em Reuniões por Videoconferência entre Organizações Federais.**

DAVENPORT, T. H. **Ecologia da Informação: Por Que só a Tecnologia Não Basta Para o Sucesso na Era da Informação**. São Paulo: Futura, 1998a.

DAVENPORT, T. H.; PRUSAK, L. **Conhecimento Empresarial: Como as Organizações Gerenciam o Seu Capital Intelectual**. Rio de Janeiro: Campus, 1998.

DE ARAÚJO, W. J. **Leis, Decretos e Normas Sobre Gestão da Segurança da Informação Nos Órgãos da Administração Pública Federal**. 2012.

DEURSEN N. Van, BUCHANAN, N. J, DUFF, A. **Monitoring Information Security Risks Within Health Care**. Computer & Security. 2013.

DHILLON, G. **Violation Of Safeguards By Trusted Personnel And Understanding Related Information Security Concerns**, Computers & Security, Volume 20, Issue 2, 1 April 2001.

DHILLON. G.; BACKHOUSE. J. **Current Directions In IS Security Research: Towards Socio-Technical Perspectives'** Information Systems Journal 2001:11. Blackwell.

DRUCKER, P. F. **The Coming Of The New Organization**. Harvard Business Review, n. 66, p. 45- 53, jan/fev., 1988.

DRUCKER, P. **Sociedade Pós Capitalista**. São Paulo: Pioneira, p. XVI, 1993.

DUARTE, F.J.C.M. **O Enfoque Sócio-Técnico: Conceitos e Condições de Aplicação numa Fundição de Alumínio**. (Dissertação) UFRJ, 1987.

DRUMMOND, R. C. **Gestão do Conhecimento em Organizações: Proposta de Mapeamento Conceitual Integrativo**. 1a edição. Editora Saraiva 2008.

FARIA, C. **Diagrama de Causa e Efeito.** Disponível em: **https://www.infoescola.com/administracao_/diagrama-de-causa-e-efeito/** Acesso em: 06 de Maio, 2019 às 21:09.

FRAGA, J. S. **Segurança de Redes em Ambientes Corporativos**. Ed. 2. 2010

FRIAS, M. C. **Quase Metade do Software Utilizado no Brasil é Irregular, Aponta Entidade.** Disponível em: https://www1.folha.uol.com.br/colunas/mercadoaberto/2018/06/quase-metade-do-software-utilizado-no-brasil-e-irregular-aponta-entidade.shtml Acesso em: 10 de Abril, 2019 às 11:31.

FONSECA, J. J. S. **Metodologia da Pesquisa Científica**. Fortaleza: UEC, 2002.

FONSECA Jr., W.C. **Análise de Conteúdo**. In: DUARTE, J.; BARROS, A. (org.). **Métodos e Técnicas de Pesquisa em Comunicação**. 2ª Ed.São Paulo: Atlas, 2006, p.280-315.

FONTES, E. **Segurança da Informação: O Usuário Faz a Diferença**. Ed. 1. 2010.

FREITAS, F; ARAUJO, M. **Políticas de Segurança da Informação: Guia Prático Para Elaboração e Implementação.** 2ed. Rio de Janeiro: Ciência Moderna LTDA, 2008

GARCIA, R.M. **Abordagem Sociotécnica: Uma Rápida Avaliação**. Revista da Administração de Empresas. 1980.

GAUNT, N. **Practical Approaches To Creating A Security Culture**, International Journal of Medical informatics, Volume 60, Issue 2, 1 November 2000.

GETSCHKO, D. **Segurança de Redes em Ambientes Corporativos**. Ed. 2. 2010.

GIL, A. C. **Como Elaborar Projetos De Pesquisa**. 4. ed. São Paulo: Atlas, 2007.

GOOGLE. **Dicas de Segurança do Gmail.** Disponível em: https://support.google.com/mail/answer/7036019?co=GENIE.Platform%3DDesktop&hl=pt-BR Acesso em: 02 de Maio, 2019 às 9:41.

GOORDRICH, M.T.; TAMASSIA, R. **Introdução a Segurança de Computadores**. Bookman. 2013.

GOVERNO DIGITAL. **Segurança da Informação.** 2019. Disponível em: **https://www.governodigital.gov.br/transformacao/compras/orientacoes/seguranca-da-informacao**. Acessado em 17 de Fevereiro, 2019 às 15:32.

GSEGI. **Gerência de Segurança da Informação**. Disponível em: https://security.ufpb.br/gsegi. Acesso em: 25 de Abril, 2019 às 10:51.

GUPTA, M., AGRAWAL, S**. A Survey On Social Engineering And The Art Of Deception.** International Journal of Innovations in Engineering and Technology, 1(1), 31–35, 2011.

GREIG A.; RENAUD K.; FLOWERDAY S. **An Ethnographic Study To Assess The Enactment Of Information Security Culture In A Retail Store**. In IEEE World Congress on Internet Security, pp. 61-66, 2015.

HERATH, T.; RAO, H.R**. Protection Motivation And Deterrence: A Framework For Security Policy Compliance In Organisations.** Eur. J. Inf. Syst. 18, 106–125, 2009.

HERBST, P. G. **Sociotechnical Design**. London: Tavistock, 1974.

HU Q.; DINEV T.; HART P.; COOKE D. **Managing Employee Compliance With Information Security Policies: The Critical Role Of Top Management And Organizational Culture**. Decision Sciences, 43(4):615-660, 2012.

HUBER, M.; KOWALSKI, S.; NOHLBERG, M.; TJOA, S. **Towards Automating Social Engineering Using Social Networking Sites, Computational Science And Engineering**. CSE '09. International Conference on, Vancouver, BC, Canada, Vol. 3, pp. 117–124, 2009.

Hui Na Chua, Siew Fan Wong, Yeh Ching Low, Younghoon Chang. **Impact of Employees' Demographic Characteristics on the Awareness and Compliance of Information Security Policy in Organizations**. ELSEVIER 2018.

ISO 27002:2013. **Gestão de Segurança da Informação – Práticas de um Sistema de Segurança da Informação.**

ISO 27005:2011. **Gestão de Riscos de TI**.

JUSTIÇA E SEGURANÇA PÚBLICA. **Polícia Federal vai investigar vazamento de Dados da Receita Federal.** Disponível em: https://www.justica.gov.br/news/collective-nitf-content-1551383415.21 Acesso em: 27 de Abril, 2019 às 14:12.

KAYWORTH, T.; WHITTEN D. **Effective Information Security Requires A Balance Of Social And Technology Factors**. MIS QUARTERLY EXECUTIVE, v. 9,n. 3, p. 163-175, 2010.

KARPERSKY. **O Verdadeiro Custo dos Ciberataques Para as Empresas.** Disponível em: https://www.kaspersky.com.br/blog/cost-cyberattack-enterprise/6080/ Acesso em 21 de Outubro, 2018 08:37.

KASPERSKY. **O que é Spear Phishing?** Disponível em: https://www.kaspersky.com.br/resource-center/definitions/spear-phishing Acesso em 19 de Maio, 2019 às 15:30.

KNAPP, K. J.; MARSHALL, T. E.; MONTGOMERY, G. H.; RAINER, R. K.; Jr. **Do Information Security Professionals And Business Managers View Information Security Differently?** Information Security Journal, v. 16, n. 2, p. 100-108, 2007.

KROMBHOLZ, K.; HOBEL, H.; HUBER, M.; WEIPPL, E. **Advanced Social Engineering Attacks**. Elsevier, 2014.

LEMONNIER, J. **O Que é O Malware do Cavalo de Troia?** Disponível em: https://www.avg.com/pt/signal/what-is-a-trojan Acessado em 06 de Maio, 2019 às 10:48.

LI, Tong, HORJOFF, Jeniffer, MYLOPOULOS. John. **Holistic Security Requirements Analysis for Socio-Technical Systems.** Software & Systems Modeling. 2016

LUNDY, O. & Cowling, **Strategic Human Resource Management**, Routledge, London, 1996

MACHADO, A. C. M. MACHADO, D. P. E. S. A **Abordagem Sociotécnica Como uma Forma Alternativa de Organizar O Trabalho.**

MARSH & McLENNAN COMPANIES (MCC). Disponível em: http://securityreport.com.br/wp-content/uploads/2017/02/MMC-Cyber-Handbook-2016-11-2016.pdf Acesso em: 21 de Outubro, 2018 às 10:30.

MARTINS, A.; ELOFF, J. **Information Security Culture**. 2001.

MEDICE, R. **A importância da Segurança da Informação – Visão Corporativa.** 2013. Disponível em: https://www.profissionaisti.com.br/2013/07/a-importancia-da-seguranca-da-informacao-visao-corporativa/ Acesso em: 07 de Maio, 2019 às 09:54.

McEVOY, R.; KOWALSKI, S**. Beyond Training and Awareness: From Security Culture to Security Risk Management**. 2018.

MONTEIRO, I. **Proposta de Um Guia Para Elaboração de Políticas de Segurança da Informação e Comunicação em Órgãos da APF**. (Dissertação) - Universidade de Brasilia, 2009.

MOON, Y. J.; CHOIB, M.; ARMSTRONG, D. J. **The Impact Of Relational Leadership And Social Alignment On Information Security System Effectiveness In Korean Governmental Organizations,** 2018.

MOREIRA, E. **O que é Política de Segurança da Informação?** Disponível em: https://www.profissionaisti.com.br/2013/08/politica-de-seguranca-da-informacao-conceitos-caracteristicas-e-beneficios/ Acesso em 03 de Abril, 2019 às 11:17.

MUMFORD, E. **The Story Of Socio-Technical Design: Reflections On Its Successes, Failures And Potential.** Information Systems Journal, v. 16, n. 4, p.317–342, 2006.

NAKAMURA, E.; GEUS, P. L. **Segurança de Redes em Ambientes Corporativos**. Ed. 2. 2010

NORTON**. Relatório de Informações de Segurança Cibernética do Norton**. Disponível em: https://br.norton.com/cyber-security-insights-2015 Acesso em: 21 de Outubro, 2018 às 09:40.

OLHARDIGITAL. **7 Dicas Para Abrir Anexos De E-Mail Com Segurança**. 2014. Disponível em: https://olhardigital.com.br/fique_seguro/noticia/7-dicas-para-abrir-anexos-de-e-mail-com-seguranca/42027 Acesso em: 02 de Maio, 2019 às 10:42.

PDTI. **Plano Diretor de Tecnologia da Informação**. Disponível em: http://www.planejamento.gov.br/publicacoes/tecnologia-da-informacao/pdtic-mpdg-2017-2019-v1-4.pdf 22 de Maio, 2019 às 20:02.

PADRÃO, M. **Dados Pessoais de 2,4 Milhões de Usuários do SUS São Vazados na Internet**. 2019. Disponível em: https://noticias.uol.com.br/tecnologia/noticias/redacao/2019/04/11/dados-pessoais-de-24-milhoes-de-usuarios-do-sus-sao-vazados-na-internet.htm Acesso em: 27 de Abril, 2019 às 14:33.

RANSBOTHAM, S.; MITRA, S. **Choice And Chance: A Conceptual Model Of Paths To Information Security Compromise**. Inf. Syst. Res. 20, 121–139, 2009.

RICHARDSON R. **CSI Computer Crime And Security Survey**. 2011. Disponível em: http://www.kwell.net/doc/FBI2008.pdf Acesso em: 24 de Abril, 2018 às 11:41.

RIOS; TEIXEIRA FILHO; RIOS **Gestão de segurança da Informação: Práticas Utilizadas pelas Instituições Federais de Ensino Superior para Implantação de Política de Segurança da Informação**. 2017

ROPOHL, G. **Philosophy Of Socio-Technical Systems**. Society for Philosophy and Technology, v.4, n.3, 1999.

ROUSE, M. **What is social engineering?** (2006) Disponível em: https://www.researchgate.net/publication/308315268_Social_Engineering_An_Introducction. Acesso em 21 de Janeiro de 2019 às 10:21.

SAVOLA R.; ANTTILA, J.; SADEMIES A.; KAJAVA J.; HOLAPPA J. **Measurement Of Information Security In Processes And Products**. 2018.

SARKER, S. **Toward A Methodology For Managing Information Systems Implementation: A Social Constructivist Perspective**. Information Science, v3, n.4, p. 195-205, 2000.

SEN, S.; SAMANTA, S. **Information Security.** International Journal of Innovative Research in Technology, 1(11), 224–231, 2014.

SCHLIENGER, T.; TEUFEL S. **The Socio-Cultural Dimension in Information Security.** Information Security Culture Journal. p. 191-201, 2002.

SCHNEIER, B. **Secrets And Lies, Digital Security In A Networked World**, John Wiley & Sons, Inc, NY, 2000.

SELLTIZ, et al. **Métodos de Pesquisa nas Relações Sociais**. Tradução de Maria Martha Hubner de Oliveira. 2a edição. São Paulo: EPU, 1987.

SIPONEN, M. **Information Security Standards Focus On The Existence Of Process, Not Its Content.** Communications of the ACM, 49, 2006.

SOLMS, B. V.; SOLMS, R. **The 10 Deadly Sins Of Information security Management**. 2004.

STALLINGS, W. **Criptografia e Segurança de Redes. Princípios e Práticas**. Ed. 4. 2006.

SOUZA, J. G. **Análise de Tratamento de Segurança da Informação na Gestão de Riscos de Governança de Tecnologia da Informação de Uma Instituição Federal de Ensino Superior Público Federal**. 2017

TAYLOR, R. S. **Value-Added Processes In Information Systems**. Westport, CT, USA: Greenwood Publishing Group Inc., 1986.

TRIST, E.L.**The Evolution of Social-Technical Systems**, 1981.

TRIVIÑOS, A. N. S. Introdução à Pesquisa em Ciências Sociais: A Pesquisa Qualitativa em Educação. São Paulo: Atlas, 1987.

ULICH E., *Arbeitspsychologie.* Zurich: vdf, Hochschulverlag an der ETH Zurich, 2001. von Solms B., "Information Security - The Third Wave,"*Computers &Security,* vol. 19 (7), pp. 615 - 620, 2000.

ZANI, B. Desafios da Segurança da Informação no Setor Público, 2014. Disponível em: **https://canaltech.com.br/seguranca/Desafios-da-seguranca-da-informacao-no-setor-publico/** Acessado em 15 de Outubro, 2018 às 19:26.

APÊNDICE A – ROTEIRO DE ENTREVISTA

QUESTÃO	Referência
SEGURANÇA DA INFORMAÇÃO	
1.O que você entende por Segurança da Informação? Já fez algum curso?	**Dhillon, 2001**
2. Que tipo de competência você acredita ter para implantar práticas de Segurança da Informação?	**Desenvolvida pelo autor(2019)**
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	
3. O que você entende sobre Política de Segurança da Informação?	**Solms e Solms, 2004.**
4. Você está ciente de que existe uma Política de Segurança da Informação na UFPB?	**Desenvolvida pelo autor (2019).**
5.Qual é a importância da Política de Segurança da Informação da UFPB nos procedimentos do seu trabalho?	**Solms e Solms, 2004.**
ATIVOS	
6. Você sabe o que é um ativo de TI? Poderia citar exemplos?	**ISO 27002:2013**

RESPONSABILIDADE E DIREITO DE ACESSO	
7.Servidores ao entrar recebem ativos de TI para realizar suas atividades?	**ISO 27002:2013**
8. Se sim, existe algum procedimento, termos, conscientizando-o sobre a responsabilidade que terá quanto a segurança daquele ativo?	**ISO 27002:2013**
SIGILO DE DOCUMENTOS	
9.Em relação ao acesso e manuseio de documentação sigilosa da Universidade, que cuidados são tomados em relação ao acesso de terceiros não autorizado? Exemplo: Tela de computador aberta, documentos impressos em impressoras compartilhadas, documentos confidenciais na mesa, senhas escritas em papeis na mesa...	**ISO 27002:2013**
SEGURANÇA DE REDES E DISPOSITIVOS MÓVEIS	
10. Qual é o procedimento para a instalação de ativos de redes (switches e acess points) dentro da instituição?	**ISO 27002:2013**
11. Como os ativos de redes são mantidos em segurança?	**ISO 27002:2013 e Guia de Boas Práticas de Segurança da Informação do TCU (2012)**
12. Como é feita a instalação de cabeamento na instituição?	**ISO 27002:2013**

SEGURANÇA EM OPERAÇÕES DE SISTEMAS DE INFORMAÇÃO	
13. Existem procedimento para criar senhas dos usuários? Complexidade inserida, tamanho máximo e mínimo...	**CERT.BR – 2019**
14. Como é feito o controle dos computadores da Universidade?	**PSI/UFPB (2019)**
15.Como são atribuídas as permissões dos usuários assim que criadas as contas nos computadores da Universidade?	**Guia de Boas Práticas de Segurança da Informação do TCU (2012)**
16.Quais procedimentos de segurança da informação são realizados ao gerenciar sua conta de email?	**Krombholz, 2014**
17. Já ocorreu alguma violação de segurança da informação aos ativos de TI? Quais procedimentos são tomados??	**Nakamura (2010)**
18. A GSEGI é notificada?	**PSI/UFPB, 2019**
SEGURANÇA EM RECURSOS HUMANOS	
19. Quando um servidor saí temporário/definitivo quais medidas são tomadas em relação as contas nos ativos de tecnologia da informação?	**ISO 27002:2013; Guia de Boas Práticas de Segurança da Informação do TCU (2012)**
SEGURANÇA EM GESTÃO DE SOFTWARE	
20.Como é realizado o controle de instalação de softwares nos computadores da Universidade?	**Paulo Baddini, 2017**

21. Caso a funcionalidade de um software solicitada seja acessível apenas pela forma de pagamento prévio, qual procedimento é tomado?	**CERT.BR (2019)**
22. Softwares livres são considerados como opções?	**CERT.BR (2019)**
SEGURANÇA PARA AQUISIÇÃO DE ATIVOS DE TI	
23. A segurança da informação é avaliada antes da seleção, compra e contratos com terceiros?	**ISO 27002:2013; Guia de Boas Práticas de Segurança da Informação do TCU (2012)**
GERENCIAMENTO DE RISCOS E INCIDENTES	
24. No momento da instalação de ativos que riscos são considerados para a integridade deles?	**ISO 27002:2013; Guia de Boas Práticas de Segurança da Informação do TCU (2012)**
25.O que você entende por inventário de TI? Como é realizado o inventário de ativos de TI no Centro?	**ISO 27002:2013**
DOS DEVERES E DAS RESPONSABILIDADES	
26. Você costuma utilizar o seu computador para resolver outros problemas que não sejam do trabalho?	**Bruno Zani, 2015**
27. Softwares pirateados são instalados dentro da UFPB? Se sim, por quê?	**CERT.BR (2019)**
28. Violações de Segurança da Informação são notificadas ao GSEGI?	**PSI/UFPB (2019)**
29. Você tem conhecimento das penalidades e sanções contidas na Lei 8.112 são cabíveis em caso de não	**ISO 27002:2013**

cumprimento do que está contido na Política de Segurança da Informação da UFPB?	
30. O você acha das aplicações destas penalidades e sanções em caso de descuido que causam ataques a ativos da UFPB?	**Desenvolvida pelo autor (2019).**
QUESTÕES DEMOGRÁFICAS	
Idade, gênero, escolaridade, função/carga e data de ingresso na universidade	

APÊNDICE B – ROTEIRO DE ENTREVISTA DE JUSTIFICADO

Análise da Referência	**Texto retirado da Política de Segurança da Informação**
A efetividade da Segurança da Informação depende da competência das pessoas que estão a implantando.	
Geralmente os usuários finais não têm conhecimento sobre a Política de Segurança da Informação da organização, logo não têm ciência dos procedimentos e padrões de segurança contidos na própria. Todas as normas internacionais de práticas segurança da informação mostram que uma política de segurança da informação é o coração	Art.1° Fica estabelecida a Política de Segurança da Informação da UFPB contendo diretrizes de Segurança da Informação a serem observadas no âmbito desta Universidade

e base do sucesso do planejamento e implantação da segurança da informação. Considerado o ponto de partida para outras sub-políticas de segurança da informação dentro da organização, procedimentos e padrões base.	
Ativo de TI - são aplicativos, sistemas, ferramentas de desenvolvimento e utilitários; equipamentos computacionais, equipamentos de comunicação, mídias removíveis e outros equipamentos;	Art. 2° A PSI consiste em um quadro de referência contendo princípios de segurança da informação e que devem ser observados por todos ao interagirem com os **ativos de TI**
Os inventários de ativos ajudam a assegurar que a proteção efetiva ocorra, e podem igualmente ser exigidos para outras finalidades, tais como a saúde e segurança, razões de seguro ou financeicos.	Art. 7. Parágrafo único - Todos os ativos de TI da UFPB deverão ser inventariados e classificados com a instruções no Decreto N° 7.845 de 14 de Novembro de 2012
Convém que seja adotada uma política de mesa limpa de papéis e mídias de armazenamento removível e política de tela limpa para os recursos de processamento da informação.	Art. 5. Inciso II. Requisitos de Segurança no manuseio e tratamento de informação: define padrões e princípios relacionados ao manuseio da informação, o que inclui inventários, administração sobre os dados, eliminação e remoção da informação, informações disponíveis em mesas de trabalho, tela de computador, material impresso e etc
Uma senha forte/complexa ao ser elaborada deve ser criada usando	Art. 5 Inciso IV Requisito de Segurança em operações de sistemas

caracteres, número aleatórios, letras maiúsculas e minuscúlas, evitando inserir nomes, sobrenomes, apenas números sequenciais, sequencias no teclado	de informação: define padrões e princípios relacionados à operação dos sistemas de informação, tais como procedimentos operacionais, controles, **responsabilidades sobre senhas,** contas de usuários, uso de correios eletrônico, relato de incidentes de segurança da informação e falhas de software.
E-mails enviados por membros conhecidos ou não, onde possuem arquivos em anexo, ao baixá-los para a máquina e esse arquivo esteja infectado, pode causar problemas para a organização, o malware pode se expandir pela rede e derrubar sistemas e serviços, além de obter informações confidenciais.	Art. 5 Inciso IV Requisito de Segurança em operações de sistemas de informação: define padrões e princípios relacionados à operação dos sistemas de informação, tais como procedimentos operacionais, controles, responsabilidades sobre senhas, contas de usuários, **uso de correios eletrônico**, relato de incidentes de segurança da informação e falhas de software.
Qualquer ocorrência de violação de segurança da informação deve ser relatava para a equipe de segurança local ou para o responsável.	Art. 9º Os incidentes de segurança da informação identificados por quaisquer servidores, alunos ou professores deverão ser prontamente reportados ao responsável do setor onde incidente ocorreu, bem como à STI
Usar computadores da organização para atividades pessoais podem gerar ameaças paras as empresas e para os dispositivos de trabalho.	Art. 10° III. Utilizar os sistemas de informação da UFPB e os recursos a eles relacionados apenas para os fins previstos por esta Universidade.

A instalação de softwares sem os devidos direitos adquiridos pode acarretar em prejuízos legais, instabilidade do sistema por conter falhas por não serem atualizados pelo desenvolvedor, estas que podem diminuir a eficácia da segurança da informação e aumentando a vulnerabilidade, diminuir o desempenho, pois não estão sendo atualizados.	art. 10º IV. Abster-se de instalar, utilizar, inspecionar, copiar, armazenar ou fornecer ativos de TI (incluindo, enfaticamente, programas de computador/software) em violação à legislação de propriedade intelectual vigente;
Convém que exista um processo disciplinar formal, implantado e comunicado, para tomar ações contra funcionários que tenham cometido uma violação de segurança da informação. Convém que o processo disciplinar formal assegure um tratamento justo e correto aos funcionários que são suspeitos de cometer violações de segurança da informação	Art. 13º Em caso de descumprimento de termos estabelecidos por esta Resolução, serão aplciadas as sanções e penalidades previstas na legislação em vigor, em especial no Código de Ética do Servidor Público Civil do Poder Executivo Federal, aprovado pelo Decreto número 1.171/1994 e na Lei No 8.112/1990, que instituiu o Regime Jurídico dos Servidores Públicos Civis da União, das autarquias, inclusive as em regime especial, e das fundações públicas federais

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

UFPB - CENTRO DE CIÊNCIAS MÉDICAS DA UNIVERSIDADE FEDERAL DA PARAÍBA / CCM

Plataforma Brasil

PARECER CONSUBSTANCIADO DO CEP

DADOS DO PROJETO DE PESQUISA

Título da Pesquisa: Política de Segurança na Informação na Administração Pública Federal: Uma abordagem sociotécnica

Pesquisador: BRUNO ALEXANDRE BEZERRA DE AQUINO SIQUEIRA CAMPOS

Área Temática:

Versão: 1

CAAE: 04950818.7.0000.8069

Instituição Proponente: UFPB - Centro de Ciências Médicas/CCM

Patrocinador Principal: Financiamento Próprio

DADOS DO PARECER

Número do Parecer: 3.104.015

Apresentação do Projeto:

Trata-se de uma pesquisa acadêmica para fins de Dissertação de Mestrado Profissional em Gestão nas Organizações Aprendentes da Universidade Federal da Paraíba (UFPB), linha de pesquisa: GESTÃO DE PROJETOS EDUCATIVOS ETECNOLOGIAS EMERGENTES, de BRUNO ALEXANDRE BEZERRA DE AQUINO SIQUEIRA CAMPOS, tendo como Orientador o Profº. Drº. Pedro Jácome de Moura Jr. Pesquisa do tipo exploratória e descritiva. A abordagem da pesquisa a ser utilizada será de que cunho qualitativo-quantitativo sobre as práticas de Segurança da Informação contidas na Política de Segurança da Informação da Universidade Federal da Paraíba(UFPB) que são implantadas nos processos de trabalho e nos ativos de tecnologia pelos membros participantes da Comunidade Acadêmica da UFPB à luz da Abordagem Sociotécnica.

Objetivo da Pesquisa:

Objetivo Primário:

-Identificar o nível de aplicação da Política de Segurança da Informação nos processos de trabalho da UFPB.

Objetivos Secundários:

• Coletar informações a partir de entrevistas de modo objetivo e subjetivo sobre as práticas de Segurança da Informação a partir da Política de

Segurança da Informação;

Endereço: Centro de Ciências Médicas, 3º andar, Sala 14 - Cidade Universitária Campus 1
Bairro: CASTELO BRANCO **CEP:** 58.051-900
UF: PB **Município:** JOAO PESSOA
Telefone: (83)3216-7617 **E-mail:** comitedeetica@ccm.ufpb.br

UFPB - CENTRO DE CIÊNCIAS MÉDICAS DA UNIVERSIDADE FEDERAL DA PARAÍBA / CCM

Continuação do Parecer: 3.104.015

• Nivelar os centros em relação ao conhecimento de prática de PSI nas suas atividades;
• Realizar estudo comparativo sobre o nivelamento entre os centros acadêmicos em termos de práticas sobre a Políticas de Segurança da
Informação da UFPB;
• Propor melhorias para a aplicação da práticas de Política Segurança da Informação dentro da universidade;
• Realizar estudo comparativo entre os centros acadêmicos em termos de práticas da Políticas de Segurança da Informação da UFPB
• Realizar a divulgação da Política de Segurança da Informação
• Propor maior visibilidade, importância e reconhecimento sobre o papel PSI
• Propor maior visibilidade e conhecimento sobre a importância da PSI no processo de trabalho;
• Propor melhorias para a aplicação da práticas de Política Segurança da Informação dentro da universidade
• realizar estudo comparativo a partir do nivelamento das práticas de Segurança contidas na PSI entre os centros acadêmicos.

Avaliação dos Riscos e Benefícios:

A pesquisa não possui riscos presumíveis relevantes, sendo sua execução apta a gerar benefícios no âmbito dos processos de trabalho e nos ativos de tecnologia pelos membros participantes da Comunidade Acadêmica da UFPB.

Comentários e Considerações sobre a Pesquisa:

A análise das entrevistas serão realizadas com text mining para identificar padrões das amplas entrevistas. Depois serão pontuadas e realizadas a análise quantitativa quanto as práticas implantadas.

Considerações sobre os Termos de apresentação obrigatória:

Foram todos apresentados permitindo tecer julgamentos concernentes aos aspectos éticos envolvidos, conforme recomenda a Resolução 466-12, CNS, MS.

Recomendações:

No desenvolvimento da pesquisa observar a metodologia apresentada e aprovada pelo CEP/CCM.

Conclusões ou Pendências e Lista de Inadequações:

Aprovado por não haver óbices éticos.

Considerações Finais a critério do CEP:

O protocolo de pesquisa foi APROVADO ad referendum.

Endereço: Centro de Ciências Médicas, 3º andar, Sala 14 - Cidade Universitária Campus 1
Bairro: CASTELO BRANCO **CEP:** 58.051-900
UF: PB **Município:** JOAO PESSOA
Telefone: (83)3216-7617 **E-mail:** comitedeetica@ccm.ufpb.br

UFPB - CENTRO DE CIÊNCIAS MÉDICAS DA UNIVERSIDADE FEDERAL DA PARAÍBA / CCM

Continuação do Parecer: 3.104.015

Este parecer foi elaborado baseado nos documentos abaixo relacionados:

Tipo Documento	Arquivo	Postagem	Autor	Situação
Informações Básicas do Projeto	PB_INFORMAÇÕES_BÁSICAS_DO_PROJETO_1279509.pdf	20/12/2018 11:31:00		Aceito
Projeto Detalhado / Brochura Investigador	DISSERTACAO1.pdf	20/12/2018 11:30:43	BRUNO ALEXANDRE BEZERRA DE AQUINO SIQUEIRA	Aceito
Outros	entrevista.pdf	20/12/2018 11:29:53	BRUNO ALEXANDRE BEZERRA DE AQUINO SIQUEIRA	Aceito
TCLE / Termos de Assentimento / Justificativa de Ausência	Termo_de_anuencia.pdf	20/12/2018 11:29:26	BRUNO ALEXANDRE BEZERRA DE AQUINO SIQUEIRA	Aceito
Folha de Rosto	CCF18122018_0004.pdf	20/12/2018 11:28:59	BRUNO ALEXANDRE BEZERRA DE AQUINO SIQUEIRA	Aceito
TCLE / Termos de Assentimento / Justificativa de Ausência	TCLE.pdf	20/12/2018 11:28:20	BRUNO ALEXANDRE BEZERRA DE AQUINO SIQUEIRA	Aceito

Situação do Parecer:
Aprovado

Necessita Apreciação da CONEP:
Não

JOAO PESSOA, 28 de Dezembro de 2018

Assinado por:
Iaponira Cortez Costa de Oliveira
(Coordenador(a))

Endereço: Centro de Ciências Médicas, 3º andar, Sala 14 - Cidade Universitária Campus 1
Bairro: CASTELO BRANCO **CEP:** 58.051-900
UF: PB **Município:** JOAO PESSOA
Telefone: (83)3216-7617 **E-mail:** comitedeetica@ccm.ufpb.br

ANEXO B – TERMO DE ANUÊNCIA

SERVIÇO PÚBLICO FEDERAL
UNIVERSIDADE FEDERAL DA PARAÍBA
SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

TERMO DE ANUÊNCIA

Declaramos para os devidos fins que estamos de acordo com a execução da pesquisa intitulada **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO NA ADMINISTRAÇÃO PÚBLICA FEDERAL: UMA ABORDAGEM SOCIOTECNICA** a ser desenvolvida pela aluno **BRUNO ALEXANDRE BEZRRA DE AQUINO SIQUEIRA CAMPOS**, do curso de **PROGRAMA DE PÓS-GRADUAÇÃO EM GESTÃO NAS ORGANIZAÇÕES APRENDENTES** do **CENTRO DE EDUCAÇÃO - CE** da Universidade Federal da Paraíba, sob orientação da Prof. **DR. PEDRO JÁCOME DE MOURA JR.** , 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, 19 de Dezembro de 2018.

Assinatura do Responsável
Nome Completo do Responsável
CPF/CNPJ
Carimbo

Francisco Ramalho de Albuquerque
PRO-REITOR DE GESTÃO DE PESSOAS
Mat. 331387

Cidade Universitária - João Pessoa – PB CEP 58051-900 Fone (83) 3216-7390 Fax: (83) 3216-7133
www.sti.ufpb.br

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

O(A) Sr.(a) está sendo convidado (a) a participar da pesquisa intitulada: **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO NA ADMINISTRAÇÃO PÚBLICA FEDERAL: UMA ABORDAGEM SOCIOTÉCNICA,** desenvolvida por **BRUNO ALEXANDRE BEZERRA DE AQUINO SIQUEIRA CAMPOS,** aluno regularmente matriculado no Programa de Pós-Graduação em Gestão nas Organizações Aprendentes da Universidade Federal da Paraíba, sob a orientação do professor Dr. Pedro Jácome de Moura Jr.

Os objetivos da pesquisa são identificar o nível de aplicação da Política de Segurança da Informação(PSI) nos processos de trabalho da UFPB; coletar informações a partir de entrevistas de modo objetivo e subjetivo sobre as práticas de Segurança da Informação a partir da Política de Segurança da Informação; nivelar cada centro em relação ao conhecimento de prática de PSI nas suas atividades; propor maior divulgação, visibilidade e conhecimento sobre a importância da PSI no processo de trabalho; realizar estudo comparativo a partir do nivelamento das práticas de Segurança contidas na PSI entre os centros acadêmicos; propor melhorias para a aplicação da práticas de Segurança da Informação contidas na Política de Segurança da Informação dentro da UFPB;

Justifica-se o presente estudo por se tratar da Segurança da Informação que é um assunto importante e vem chamando atenção das organizações privadas e públicas, logo elas vêm investindo em tecnologia da informação e desenvolvendo documentos como a Política de Segurança da Informação para orientar e direcionar os trabalhadores/servidores para que possam desenvolver suas atividades observando sempre a Segurança da Informação junto com a produtividade, visto que os usuários finais são considerados o elo mais fraco em termos de Segurança da Informação na interação homem-máquina. 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, 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 Resolução nº. 466/2012 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.

João Pessoa-PB, ____ de Janeiro de 2019.

_____
Bruno Alexandre Bezerra de Aquino Siqueira Campos
Pesquisador responsável

_____
Participante da Pesquisa

Pesquisador Responsável: Bruno Alexandre Bezerra de Aquino Siqueira Campos
Endereço do Pesquisador Responsável: Rua Carlos Ulisses de Carvalho, 60, apto 403 – Bairro Brisamar – João Pessoa-PB - CEP: 58.033-

130- Fones: 98881-2280/99929-7277 - E-mail: brunoalexandrebasc@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.

_____
Bruno Alexandre Bezerra de Aquino Siqueira Campos
Pesquisador responsável

_____
Testemunha