UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO

SUENY GOMES LÉDA ARAÚJO

A DIMENSÃO HUMANA NO PROCESSO DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO: um estudo aplicado à Pró-Reitoria de Gestão de Pessoas da Universidade Federal da Paraíba

João Pessoa
2016

SUENY GOMES LÉDA ARAÚJO

A DIMENSÃO HUMANA NO PROCESSO DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO: um estudo aplicado à Pró-Reitoria de Gestão de Pessoas da Universidade Federal da Paraíba

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Informação do Centro de Ciências Sociais Aplicadas da Universidade Federal da Paraíba como requisito parcial à obtenção do título de Mestre em Ciência da Informação. Área de concentração: Informação, conhecimento e sociedade. Linha de pesquisa: Ética, Gestão e Políticas de Informação.

Orientador: Prof. Dr. Wagner Junqueira de Araújo

João Pessoa

2016

A663d Araújo, Sueny Gomes Léda.
A dimensão humana no processo de gestão da segurança da informação: um estudo aplicado à Pró-Reitoria de Gestão de Pessoas da Universidade Federal da Paraíba / Sueny Gomes Léda Araújo.- João Pessoa, 2016.
154f. : il.
Orientador: Wagner Junqueira de Araújo
Dissertação (Mestrado) - UFPB/CCSA
1. Ciência da informação. 2. Gestão de segurança da informação. 3. Política de segurança da informação.
4. Segurança da informação - dimensão humana. 5. Normas de segurança da informação.

UFPB/BC CDU: 02(043)

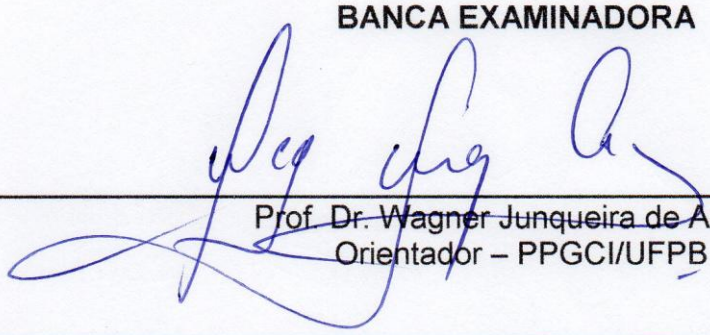
SUENY GOMES LÉDA ARAÚJO

A DIMENSÃO HUMANA NO PROCESSO DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO: um estudo aplicado à Pró-Reitoria de Gestão de Pessoas da Universidade Federal da Paraíba

Aprovada com distinção em: 21/03/2016.

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Informação do Centro de Ciências Sociais Aplicadas da Universidade Federal da Paraíba como requisito parcial à obtenção do título de Mestre em Ciência da Informação.

BANCA EXAMINADORA



Prof. Dr. Wagner Junqueira de Araújo
Orientador – PPGCI/UFPB

Profa. Dra. Emeide Nóbrega Duarte
Membro interno - PPGCI/UFPB

Profa. Dra. Maria das Graças Vieira
Membro externo – MPGOA/UFPB

Prof. Dr. Marckson Roberto Ferreira de Sousa
Membro interno (suplente) - PPGCI/UFPB

Prof. Dr. Ed Porto Bezerra
Membro externo (suplente) – PPGI/UFPB

Dedico

Ao meu marido, Fabiano, pelo amor,
carinho e compreensão no decorrer desta pesquisa; e
Aos meus filhos, José Roberto e Maria Fernanda,
o amor de vocês me dá forças
para ser uma pessoa melhor a cada dia.

AGRADECIMENTOS

Tentarei manifestar minha gratidão a todos que incentivaram e contribuíram com o desenvolvimento desta pesquisa.

Inicialmente agradeço ao meu **Deus** por ter me abençoado em cada momento deste mestrado, desde o processo seletivo às últimas linhas desta pesquisa. Sem Ele, nada disso seria possível. Toda honra e toda glória rendo a Ti, Senhor.

Agradeço aos meus amados pais, **José Antonio Silva Araújo** e **Solane Gomes Léda Araújo** que, apesar da distância, sempre apoiaram minhas escolhas e suportaram os momentos de ausência com amor e paciência.

Agradeço aos meus filhos, **José Roberto** e **Maria Fernanda** pelo amor incondicional, pelo sorriso nos momentos difíceis, e por me mostrar que perto deles tudo se torna muito pequeno.

Agradeço ao meu amor, marido, companheiro e cúmplice, **Fabiano de Moura Ribeiro**, pelo apoio sem restrição em todos os momentos desta pesquisa.

Agradeço ao meu orientador, **Prof. Dr. Wagner Junqueira de Araújo**, pela orientação, atenção e paciência no desenvolvimento desta pesquisa.

Agradeço aos docentes **Profa. Dra. Maria das Graças Vieira**, **Profa. Dra. Emeide Nóbrega Duarte**, **Prof. Dr. Marckson Roberto Ferreira de Sousa**, e Prof**. Dr. Ed Porto Bezerra** por participarem da Banca Examinadora e pelas valorosas contribuições.

Agradeço aos preciosos frutos deste mestrado, as amigas **Chistiane** (Chis) e **Rafaela** (Rafa) por transformarem os momentos de angústia em superação, e por não permitir que essa escrita fosse um processo tão solitário. Seus conselhos e sugestões não só enriqueceram esta pesquisa, mas a vida desta pesquisadora. A vocês, meu muito obrigada!

Agradeço a **Profa. Dra. Elizabeth Cristina**, que colaborou de forma tão carinhosa com as últimas etapas desta pesquisa.

Agradeço às amigas **Josilene Ribeiro** e **Aliceana Menezes** pelo exemplo de amor e dedicação à pesquisa, além da eterna disposição em ajudar sempre.

Agradeço ao amigo **Clodemir Costa do Nascimento**, pois seus sábios e excelentes conselhos foram sempre muito bem recebidos.

Agradeço à amiga **Clarissa Sá**, pela ajuda e ombro amigo em todos os momentos dessa caminhada.

Agradeço aos amigos **Isac Newton**, **André Luiz**, **Ana Roberta**, **Ana Cláudia Cavalcante, Suzana Lira e Josivan Ferreira** pelo incentivo e apoio incondicional no início dessa caminhada.

Agradeço ao amigo **Thiago Antonio Cavalcante**, por me liberar das minhas atividades laborais e me possibilitar ficar dedicada exclusivamente a esta pesquisa.

Agradeço à amiga **Márcia Sandra**, por sempre me fornecer as informações necessárias à conclusão desta pesquisa.

Agradeço à equipe da Divisão de Educação e Capacitação Profissional (DECP) representada pela Diretora **Renata Batista** por aceitar as sugestões desta pesquisa de forma tão receptiva.

Agradeço à **Fátima França** e a **Nice** por me proporcionar um ambiente de estudo tão agradável.

Agradeço a todos os **Diretores da Progep** por responderem nossa pesquisa de forma tão receptiva e atenciosa.

“Eu não sou quem eu gostaria de ser; eu não sou quem eu poderia ser, ainda, eu não sou quem eu deveria ser. Mas graças a Deus eu não sou mais quem eu era!”

Martin Luther King Jr.

RESUMO

A informação apresenta-se como um importante ativo para as instituições, necessitando ser protegida de forma adequada contra destruição indevida, indisponibilidade temporária , adulteração ou divulgação não autorizada . Várias formas de ameaças físicas, virtuais e humanas, comprometem a segurança das informações. Apesar de a tecnologia ser responsável por fornecer parte da solução para esses problemas, muitas das vulnerabilidades dos sistemas de informação podem ser atribuídas às ações do homem. Nesse sentido, torna-se salutar estudar a dimensão humana nesses processos. Preocupado com a segurança da informação nas Instituições Públicas Federais, o governo publicou uma série de leis, decretos, normas e relatórios que orientam a implementação de ações de gestão de segurança da informação nas instituições públicas. Assim, o presente estudo teve por objetivo analisar a dimensão humana no processo de gestão de segurança da informação na Pró-Reitoria de Gestão de Pessoas (Progep) da Universidade Federal da Paraíba (UFPB) sob a ótica das normas do governo federal. Esta pesquisa caracteriza-se como pesquisa descritiva, com abordagem quali-quantitativa e, quanto ao método de investigação, estudo de caso. Para tanto, foi utilizada a pesquisa documental, observação participante e entrevista, como instrumentos de coleta de dados. A partir da triangulação dos três instrumentos de coleta, para a análise dos dados, foi aplicada a análise de conteúdo. A amostra desta pesquisa foi constituída pelos nove diretores que compõem a Pró-Reitoria de Gestão de Pessoas. Os resultados possibilitaram identificar a necessidade da UFPB em elaborar uma política de classificação da informação, uma vez que sua inexistência impossibilita a gestão da segurança da informação. Quanto à conscientização em segurança da informação, observou-se a inexistência de ações que poderiam contribuir no processo de conscientização dos servidores, como: menção à segurança da informação no momento de ingresso/posse de colaboradores e servidores; elaboração do termo de responsabilidade e confidencialidade; processo disciplinar formal para a violação da segurança da informação; e ações como manuais informativos, campanhas, palestras e reuniões. Na utilização dos controles de segurança da informação, observaram-se iniciativas de implantação de determinados controles, entretanto, os procedimentos acabaram sendo realizados de forma equivocada, sem a observância das orientações normativas. Com base no exposto, os resultados desta pesquisa podem auxiliar a minimizar a incidência de ameaças à segurança da informação na Progep/UFPB, bem como contribuir com a criação de uma cultura de segurança em instituições federais.

Palavras-chave: Segurança da Informação. Política de Segurança da Informação. Dimensão Humana da Segurança da Informação. Normas de Segurança da Informação.

ABSTRACT

The information is presented as an important asset for institutions and needs to be protected adequately against undue destruction, temporary unavailability, adulteration or unauthorized disclosure. Various forms of physical, virtual and human threats jeopardize the security of information. Although the technology is responsible for providing part of the solution to these problems, many of the vulnerabilities of information systems can be attributed to man's actions. In this sense, it is salutary to study the human dimension in these processes. Concerned about the security of information in Federal Public Institutions the government published a series of laws, decrees, rules and reports that guides the implementation of information security management actions in public institutions. Thus, this study aimed to analyze the human dimension in the information security management process in the Dean of Personnel Management (Progep) of the Federal University of Paraíba (UFPB) from the perspective of the rules of the federal government. This research is characterized as descriptive research with qualitative and quantitative approach and case study as the method of investigation. Therefore, the documentary research was used, participant observation and interview as data collection techniques. From the triangulation of the three collection methods for data analysis was applied to content analysis. The sample was made up of nine directors who compose the Dean of Personnel Management. The results allowed identifying the need of UFPB on elaborate a policy of information classification, since its absence turns impossible the management of information security. As for information security awareness, it was noted the absence of actions that could contribute in the awareness of the public employee process, such as information security mentioned at the time of entry / ownership of public employees and collaborators; preparation of the responsibility and confidentiality term; formal disciplinary proceedings for breach of information security; and actions as informative manuals, campaigns, lectures and meetings. In the use of information security controls, there were initiatives of implementation of certain controls, however, the procedures were eventually made in error, without compliance of the regulatory guidelines. Based on the above, the results of this research can help minimize the impact of threats to information security in Progep / UFPB and, as well, contribute to the creation of a safety culture in federal institutions.

Keywords: Information Security. Information Security Policy. Human Dimension of the Information Security. Standards of Information Security.

LISTA DE FIGURAS

LISTA DE QUADROS

SUMÁRIO

1 INTRODUÇÃO

A atual sociedade é caracterizada pela explosão informacional em decorrência da disseminação e do uso das tecnologias de informação e comunicação. Nesse sentido, embora o conhecimento e a sua comunicação sejam fenômenos basilares de toda sociedade humana, considera-se que o surgimento da tecnologia da informação e seus impactos globais, caracterizam a sociedade contemporânea como sociedade da informação (CAPURRO; HJØRLAND, 2007, p. 149).

Na dinâmica dessa sociedade, a informação se constitui como o elemento essencial para o seu desenvolvimento, responsável pelas transformações tecnológicas, administrativas e organizacionais. Tendo em vista sua importância como insumo, a informação requer cuidados específicos que considerem sua origem, criação, tratamento, disponibilização e uso, visto que ao longo do seu ciclo de vida, diversos fatores podem emergir, dentre eles, a necessidade da manutenção da segurança dos ativos informacionais, uma vez que o seu excedente representa um dos aspectos mais problemáticos, tanto em termos de uso e de circulação quanto com relação ao seu volume físico.

Os ativos informacionais correspondem a quaisquer elementos que assegurem os processos de negócio de uma determinada organização, instituição ou áreas de negócios diversos, sendo de relevância para o seu desenvolvimento, requerendo um gerenciamento preciso que possa coordenar toda a complexidade que gira em torno do ciclo de vida das informações necessárias aos negócios. Como importante constituinte da expansão organizacional, a gestão dos ativos informacionais precisa considerar, como um dos procedimentos essenciais, sua segurança. No campo da segurança da informação, a manutenção desses ativos envolve um amplo conjunto que contempla distintos componentes como o tecnológico - sistemas, *hardware* e *software* -, processos e pessoas.

Nos últimos anos, a segurança da informação tornou-se um assunto relevante no meio organizacional, pois, à medida que a tecnologia avança, mais dados e informações passam a ser armazenados em grande escala e levados a qualquer lugar do planeta de forma rápida e eficiente. Com a inovação da tecnologia digital e o advento da *internet*, o mundo vem passando por transformações contínuas, cuja globalização se fundamenta na conexão em rede, que contribui com o crescimento

das transações eletrônicas que incluem correspondências particulares, operações comerciais, bancárias, entre outras (FERREIRA, 2013, p. 59).

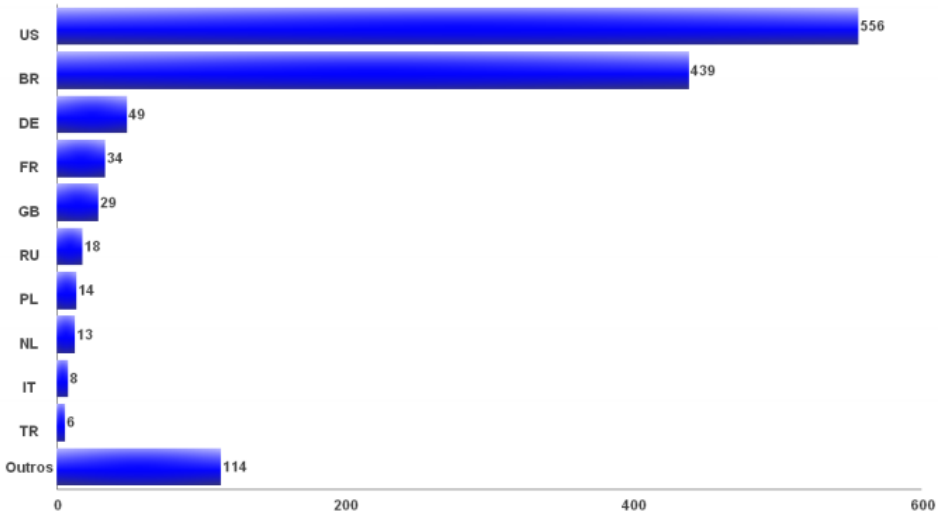
Os avanços tecnológicos resultam de uma evolução constante dos sistemas de informação possibilitando às instituições grandes benefícios, como mobilidade e maior capacidade de gestão. Entretanto, o inevitável aumento da competitividade e da descentralização da informação, ocasionado pelas transformações das tecnologias, suscita a necessidade de gestão da segurança da informação.

De acordo com a Estratégia de Segurança da Informação e Comunicação e Segurança Cibernética da Administração Pública Federal 2015-2018 (BRASIL, 2015, p. 16), os ativos de informação guardam relação direta com riscos de Segurança da Informação e Comunicação e de Segurança Cibernética uma vez que a dependência tecnológica das instituições governamentais é cada vez maior. Observa-se que diversos órgãos e entidades, conforme divulgado na mídia foram alvos de ações maliciosas, com destaque para ações de engenharia social[1], desfigurações de sites e vazamento de informações, causando prejuízos ao Estado e refletindo negativamente na sociedade.

De acordo com as estatísticas do Centro de Tratamento de Incidentes de Segurança de Rede de Computadores da Administração Pública Federal - CTIR Gov, órgão responsável pelo atendimento aos incidentes em redes de computadores da Administração Pública Federal (APF), o Brasil é o segundo país com maior número de notificação de incidentes (BRASIL, 2016, p. 4) conforme demonstra a Figura 1.

[1] Alguém que usa a fraude, a influência e a persuasão contra as empresas, em geral visando suas informações (MITNICK; SIMON, 2003, p. xiii).

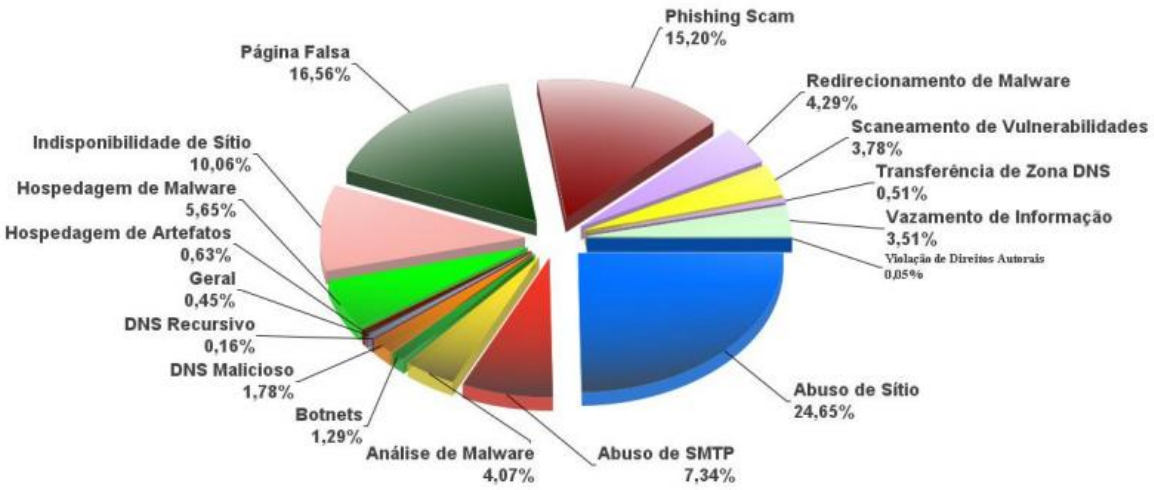
Figura 1 - Países destinatários das notificações de incidentes



Fonte: Centro de Tratamento de Incidentes de Segurança de Rede de Computadores da Administração Pública Federal (BRASIL, 2016, p. 4).

A Figura 2 apresenta os percentuais por categoria de incidentes. Destacam-se como as maiores ocorrências, as categorias de abuso de sítio (24,65%), página falsa (16,56%), *phishingscam*[2] (15,20%), e indisponibilidade de sítio (10,06%) respectivamente.

Figura 2 - Distribuição de incidentes por categoria



Fonte: Centro de Tratamento de Incidentes de Segurança de Rede de Computadores da Administração Pública Federal (BRASIL, 2016, p. 2).

[2] Tática de engenharia social, que consiste na tentativa de fraude pela internet, utilizando "iscas", isto é, artifícios para atrair a atenção de uma pessoa e fazê-la realizar alguma ação.

Nesse contexto, ressaltam-se os esforços do governo em fortalecer as ações de segurança da informação, o que inclui uma série de leis e decretos, além de um arcabouço de normas publicadas pelo Gabinete de Segurança Institucional da Presidência da República, nos últimos oito anos. Entretanto, segundo o Acórdão nº 3117/2014 - TCU – Plenário, os órgãos e entidades da Administração Pública Federal ainda se apresentam em um patamar abaixo do desejado para os órgãos e entidades federais, uma vez que ainda são insuficientes as ações de segurança da informação, de modo que possam agregar valor aos resultados da instituição (TCU, 2014, p. 2).

Assim, muitas são as informações (digitais ou armazenadas em ambiente convencional) que fazem parte da rotina de trabalho das instituições, e esse universo informacional está sujeito a várias formas de ameaças físicas, virtuais e humanas, que comprometem seriamente a segurança das informações. Compete à tecnologia da informação fornecer parte da solução para esse problema, não sendo, contudo, capaz de resolvê-lo em sua plenitude, uma vez que grande parte das vulnerabilidades dos sistemas de informação pode ser atribuída às ações humanas.

Nesse sentido, no governo federal publicou recentemente um documento denominado de Estratégia de Segurança da Informação e Comunicação e Segurança Cibernética da Administração Pública Federal 2015-2018, onde em seus objetivos estratégicos o governo demonstra seu interesse relacionado à segurança da informação nas instituições federais. Esse documento abrange a relevância tanto dos recursos computacionais, de infraestrutura, como os recursos humanos para uma efetiva segurança da informação e comunicação. Percebe-se, nos objetivos estratégicos do documento a ênfase dada pelo governo na aprendizagem, capacitação e inovação em segurança da informação, preocupando-se em fornecer condições para que os funcionários envolvidos promovam as melhorias necessárias nas instituições, nas estruturas e nos processos de gestão da informação, possibilitando resultados efetivos para a sociedade e a melhoria do próprio Estado (BRASIL, 2015, p. 40).

Diante desse contexto, buscou-se com esta pesquisa abordar sobre a segurança da informação concentrando-se na dimensão humana[3], dada à relevância

[3] São várias as terminologias utilizadas por diversos autores para designar a parte humana da segurança da informação, como: aspectos, dimensão, elemento, fator, dentre outras. Entretanto, para esta pesquisa, recorreu-se à terminologia dimensão, entendendo ser mais valorosa para área.

do tema no contexto da segurança da informação na Administração Pública Federal, cujos propósitos de sua efetuação foram norteados pela curiosidade de responder ao seguinte questionamento: como a dimensão humana é considerada no processo de gestão da segurança da informação na Pró-Reitoria de Gestão de Pessoas (Progep) da Universidade Federal da Paraíba (UFPB) de modo a atender as normas do governo federal?

Para tanto, fez-se necessário atingir o objetivo geral de analisar a dimensão humana no processo de gestão de segurança da informação na Progep da UFPB, sob a ótica das normas do governo federal, para o qual foi preciso alcançar os seguintes objetivos específicos:

a) Elencar as orientações legais aplicadas à gestão de segurança da informação na Progep/UFPB;
b) Identificar os processos informacionais prioritários na Progep/UFPB que devam ser foco de gestão de segurança da informação;
c) Verificar como a dimensão humana é abordada nas ações de gestão de segurança da informação implementadas pela Progep/UFPB; e
d) Propor um programa de capacitação em segurança da informação para a Progep/UFPB.

Como órgão responsável pelo planejamento e acompanhamento das estratégias e políticas de gestão de pessoas da universidade, a Progep possui como algumas de suas competências: propor políticas de gestão de pessoas para os servidores da UFPB; propor programas de educação e capacitação profissional; e estabelecer um sistema de gerenciamento e controle de processos de gestão de pessoas (UFPB, 2012, p. 2). Desse modo, a Progep representou-se como um importante campo de pesquisa, o que compreendeu um ambiente prolífico para o início de uma cultura de segurança da informação em toda instituição.

A pesquisa foi desenvolvida com base em uma metodologia científica no campo das ciências sociais que procurou obter conhecimentos no contexto da realidade institucional da UFPB, de modo a pesquisar as ações que contribuem com a gestão de segurança das informações que tramitam na Progep. Para tanto, a pesquisa se caracterizou como descritiva, por ter visado identificar os processos informacionais prioritários que são foco de gestão de segurança da informação, bem

como por ter verificado a abordagem da dimensão humana nas ações de gestão de segurança da informação desenvolvidas pela Progep/UFPB. Referente à abordagem que foi aplicada, esta pesquisa se definiu como quali-quantitativa, visto que necessitou abordar o tema sob a integração dessas duas abordagens.

Por ter se tratado de uma pesquisa em uma instituição pública federal, o método adotado foi o estudo de caso, que representou uma importante estratégia por ter permitido estabelecer o questionamento foco desta pesquisa frente aos fenômenos da gestão de segurança da informação que se encontram inseridos no contexto da Progep/UFPB, e os aspectos das ações humanas relacionados nesse processo.

Diante dessa perspectiva, a necessidade de compreender a dimensão humana no processo de gestão da segurança da informação no âmbito de uma instituição pública, especificamente a Progep/UFPB, foi o principal motivador pessoal que condicionou ao desenvolvimento desta pesquisa, em particular pelo fato de sua autora ser servidora pública federal e ter almejado a realização de uma pesquisa que pudesse contribuir de forma prática e oferecesse alguma melhoria para as instituições de forma geral. Essa condição representou também a sua relevância perante o levantamento realizado sobre a situação da gestão de segurança da informação da Progep/UFPB, podendo vir a refletir sobre os procedimentos administrativos em relação às demais instâncias da instituição.

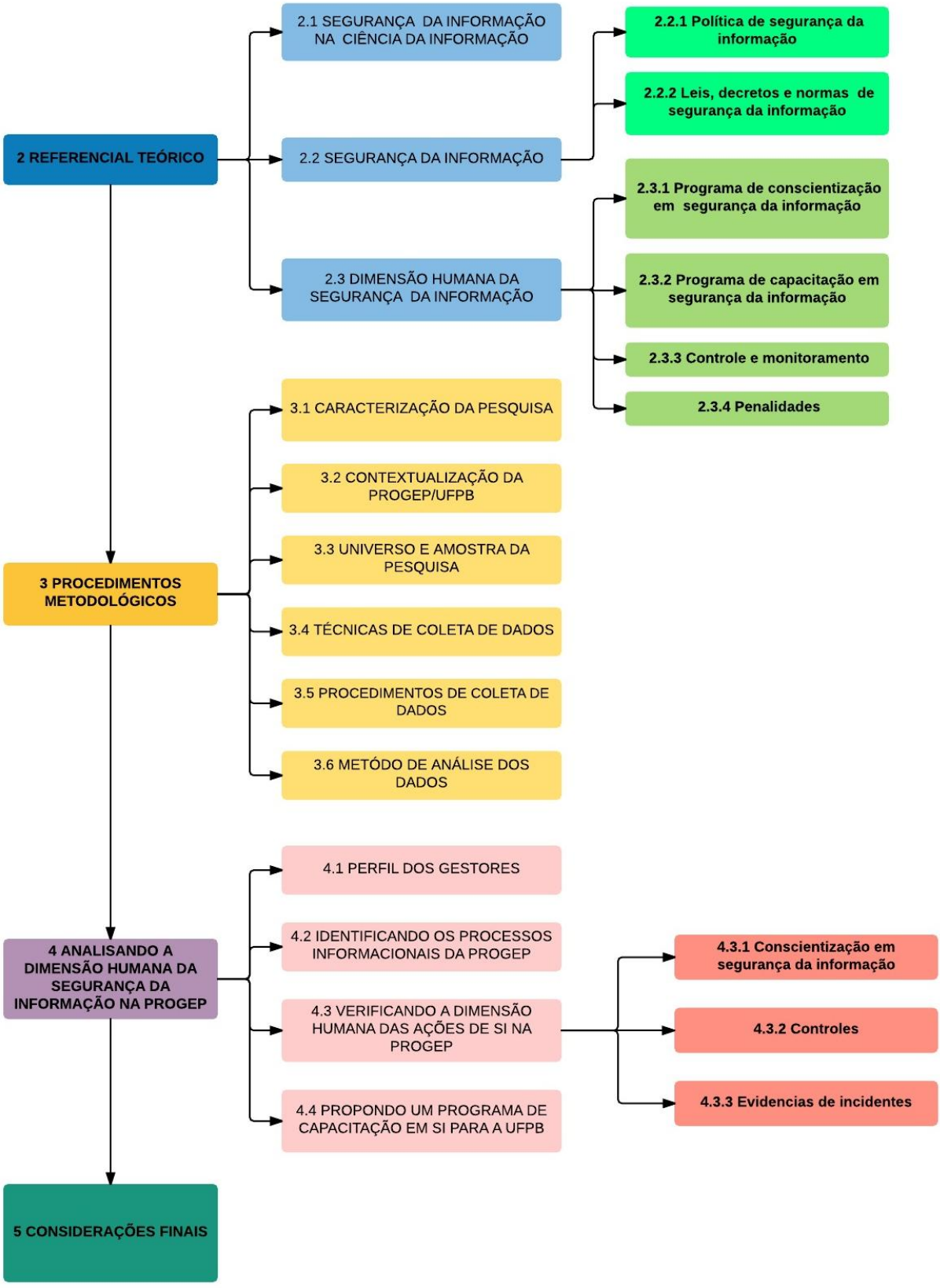
Para o âmbito acadêmico, o desenvolvimento desta pesquisa contribuiu com a ampliação da abordagem da segurança da informação no campo das ciências sociais, visto que por representar um conceito muito amplo, a segurança da informação tem sido estudada por múltiplas áreas, tanto nas ciências exatas (estudando tecnologias mais seguras), como nas ciências sociais (estudando os processos e pessoas).

Dentre as áreas das ciências sociais preocupadas com essa temática de pesquisa, inclui-se a ciência da informação. Nesse contexto, adotou-se uma divisão da ciência da informação em seis subáreas, a saber: os fluxos da informação científica; a representação e a recuperação da informação; os estudos de usuários; a gestão do conhecimento; a economia política da informação; e os estudos métricos da informação. Dentro da subárea de gestão do conhecimento, encontra-se inserida a temática segurança da informação, centrando seus estudos na parte de processos e de pessoas (ARAÚJO, C. A. A, 2014, p. 64).

Tendo em vista a importância da dimensão humana para a efetivação da gestão de segurança da informação em contextos organizacionais, foi possível com a pesquisa compreender os aspectos que consideraram tanto o campo da ciência da informação, quanto às políticas que norteiam a segurança da informação, direcionando-os aos aspectos humanos referentes aos programas de conscientização e capacitação para efetivação da segurança da informação perante as necessidades organizacionais de assegurar suas informações.

Todos os dados e resultados obtidos encontram-se estruturados com base em cinco seções, que iniciou com esta seção introdutória, seguido pelo referencial teórico, procedimentos metodológicos, analisando a dimensão humana da segurança da informação na Progep/UFPB, e finalizando, com as considerações, conforme ilustrado na Figura 3.

Figura 3 - Estrutura da pesquisa



Fonte: Elaborado pela autora (2016).

2 REFERENCIAL TEÓRICO

Esta seção tem como objetivo apresentar desde como a temática Segurança da Informação (SI) é abordada pela Ciência da Informação (CI), perpassando pelos conceitos, princípios, políticas e pela dimensão humana da segurança da informação.

2.1 SEGURANÇA DA INFORMAÇÃO NA CIÊNCIA DA INFORMAÇÃO

Ciência da Informação é uma ciência relativamente nova que surge na primeira década do Século XX, depois da segunda revolução científica. Ela nasce como uma área interdisciplinar que objetiva estudar as propriedades e o comportamento da informação. Borko (1968, p. 3, tradução nossa) realiza uma síntese das três definições de Ciência da Informação, feitas por Taylor (1966):

> A Ciência da Informação é a disciplina que investiga as propriedades e o comportamento da informação, as forças que governam o fluxo da informação e os meios de processá-las para ótimo acesso e uso. Está preocupada com esse corpo de conhecimentos relativos à origem, coleta, organização, armazenamento, recuperação, interpretação, transmissão, transformação e utilização de informações.

Para Saracevic (1996, p. 47) a Ciência da Informação é um campo dedicado tanto às questões científicas como à prática profissional, voltando-se aos problemas da efetiva comunicação de seus registros entre os seres humanos, no contexto social, institucional ou individual do uso e das necessidades de informação. Nesse sentido, Silva e Freire (2012, p. 3) ressaltam a necessidade de uma área para tratar problemas relativos à informação:

> É pertinente ressaltar que o ser humano, no decorrer da história, vem tentando arregimentar formas de classificar, registrar, organizar e difundir a informação em suas mais diversas áreas. Porém, havia a necessidade premente de uma área específica para tratar de problemas relativos à informação, enquanto fenômeno social.
> Isto quer dizer que, na história da humanidade, sempre foi preciso pensar a possibilidade de uma ciência para organizar o conhecimento e propor procedimentos de organização e

> disseminação da informação, principalmente a partir da explosão informacional do século XX.

Com base no exposto, pode-se observar que a Ciência da Informação está intimamente relacionada ao ciclo de vida informacional, desde sua origem até o seu descarte. Nesse caminho, muitos problemas relacionados à informação podem emergir e um deles pode ser inerente à Segurança da Informação que, nos últimos anos, tornou-se um assunto importante no meio organizacional, pois, à medida que a tecnologia avança, mais dados e informações passam a ser armazenados em grande escala e levados a qualquer lugar do planeta (FERREIRA, 2013, p. 59).

Para entender como a Ciência da Informação aborda a temática Segurança da Informação, fez-se um levantamento[4] das publicações nos anais do Encontro Nacional de Pesquisa em Ciência da Informação (Enancib), no período entre 2007 e 2015. Promovido pela Associação Nacional de Pesquisa e Pós-Graduação em Ciência da Informação (Ancib), o Enancib é considerado uma referência na área de Ciência da Informação no Brasil. Atualmente, em sua décima sexta edição, o evento consolida-se como importante espaço de discussão científica, congregando conjunto de pesquisadores de diversos programas de pós-graduação nacionais.

O evento proporciona, ainda, identificar os principais temas de interesse e as lacunas de pesquisa a serem preenchidas no campo da CI. Em sua organização, atualmente, o Enancib compõe-se de 11 (onze) Grupos de Trabalho - GTs, classificados por categorias, apresentados no Quadro 1.

Quadro 1 - Grupo temático do Enancib

GT	CATEGORIA
GT01	Estudos Históricos e Epistemológicos da Ciência da Informação
GT02	Organização e Representação do Conhecimento
GT03	Mediação, Circulação e Apropriação da Informação
GT04	Gestão da Informação e do Conhecimento nas Organizações
GT05	Política e Economia da Informação
GT06	Informação, Educação e Trabalho
GT07	Produção e Comunicação da Informação em CT&I
GT08	Informação e Tecnologia

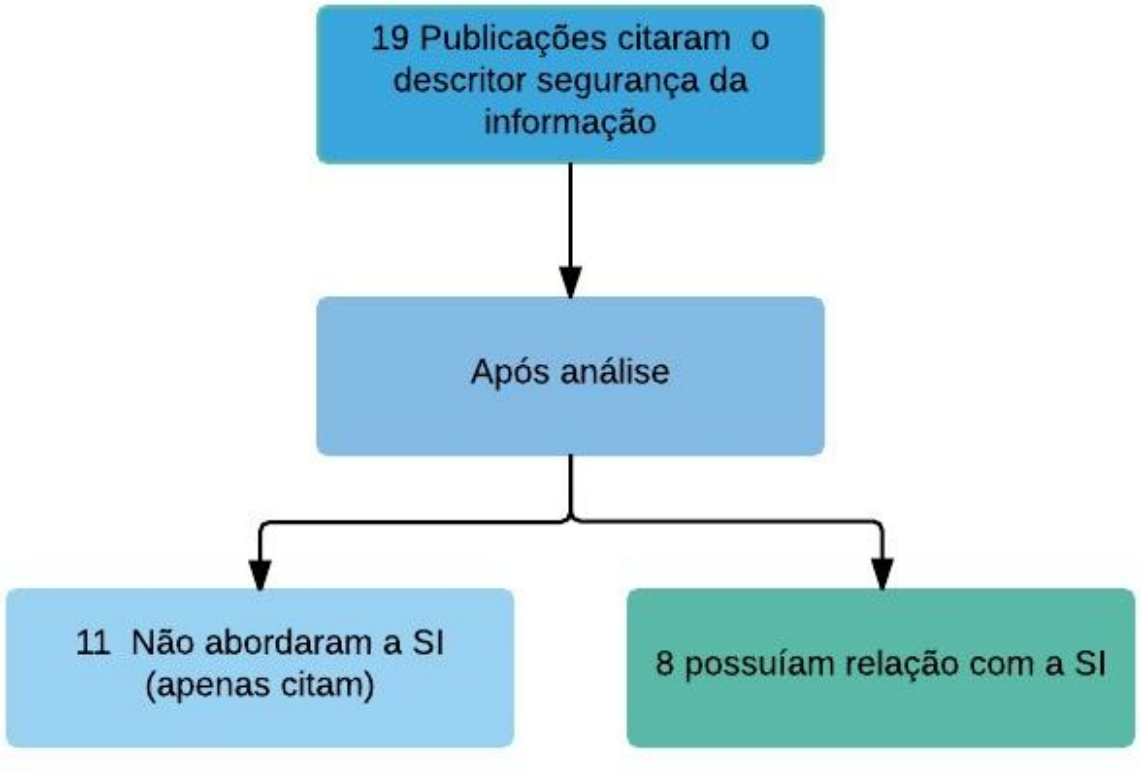
[4] Realizado durante a disciplina de Gestão da Informação e do Conhecimento nas Organizações, ministrada pelas professoras Dra. Emeide Nóbrega Duarte e Dra. Alzira Karla Araújo da Silva.

GT09	Museu, Patrimônio e Informação
GT10	Informação e Memória
GT11	Informação e Saúde

Fonte: Adaptado de página da Associação Nacional de Pesquisa e Pós-Graduação em Ciência da Informação (ANCIB, 2014).

A pesquisa foi realizada buscando o descritor segurança da informação no título, resumo e palavras-chave das publicações nos 11 (onze) grupos de trabalho do Enancib. Nesse primeiro momento, foram recuperadas 19 publicações que possivelmente abordariam a temática. No entanto, após análise, apenas oito referiam-se efetivamente à segurança da informação, conforme se observa na Figura 4.

Figura 4 - Fluxograma dos resultados da pesquisa



Fonte: Dados da Pesquisas (2015).

Em meio às oito publicações que abordam Segurança da Informação, verifica-se que a temática perpassa por quatro Grupos de Trabalho distintos, com 62,5% das publicações localizadas no GT4, Gestão da Informação e do

Conhecimento nas Organizações, e apenas 12,5% das publicações localizadas no GT8, Informação e Tecnologia, onde se acreditava haver maior incidência de publicações, devido à forte relação da segurança da informação com a área tecnológica, conforme Quadro 2.

Quadro 2 – Apresentação das Publicações

TÍTULO DO ARTIGO	ANO	GT	INSTITUIÇÃO	AUTORES DAS PESQUISAS
Percepções de segurança e ameaças em ambientes de tecnologias da informação	2007	GT- 4	UNESP/UFPB	Miguel Maurício Isoni e Silvana Aparecida Borsetti Gregório Vidotti
Segurança da informação: nova disciplina na ciência da informação?	2010	GT- 1	UNB	Jorge Henrique Cabral Fernandes
A segurança do conhecimento nas práticas da gestão da segurança da informação e da gestão do conhecimento.	2010	GT – 4	UFPB/UNB	Wagner Junqueira Araújo e Suely Angélica do Amaral
Brasil informacional: a segurança cibernética como desafio à segurança nacional	2011	GT- 5	-	Rafael Oliveira de Ávila e Rafael Pinto da Silva
Análise de informações pessoais na web: métrica para identificar o grau de exposição da informação	2013	GT – 4	UFPB	Narjara Bárbara Xavier da Silva, Wagner Junqueira de Araújo e Patrícia Morais de Azevedo
Análise de risco no sistema de concessão de diárias e passagens (SCDP): estudo de caso sob a ótica da segurança da informação no departamento contábil da UFPB	2013	GT – 4	UFPB	Josivan de Oliveira Ferreira e Wagner Junqueira de Araújo
Modelo para o descarte seguro da informação em suporte digital	2014	GT- 8	UFPB	Silvio Lucas da Silva e Wagner Junqueira de Araújo
Aspectos humanos da segurança da informação	2015	GT-4	UFPB	Sueny Gomes Léda Araujo, Rafaela Romaniuc Batista e Wagner Junqueira de Araújo

Fonte: Dados da pesquisa (2015).

Com relação à instituição de origem dos autores e co-autores que publicaram sobre segurança da informação no Enancib, percebe-se que a Universidade Federal da Paraíba (UFPB) representa a Instituição de Ensino Superior com maior número de publicações sobre a temática segurança da informação. Tratando-se da forma como a temática segurança da informação vem sendo abordada no Enancib, apresenta-se uma breve descrição das publicações recuperadas:

Isoni e Vidotti (2007) tratam da concordância ou discordância de questões que caracterizam a origem dos ataques e as ameaças à segurança da informação que podem ocasionar a interrupção do fluxo de informação.

Fernandes (2010) em sua publicação defende a vinculação da segurança da informação à ciência da informação, entendendo a informação como um produto de natureza social, de modo a tornar necessário enfatizar os estudos dos aspectos humanos na segurança da informação.

Araujo e Amaral (2010) identificam a relevância do conhecimento como um ativo organizacional e, com isso, constata-se a necessidade de proteger esses ativos. Contudo, identificou-se na literatura de Ciência da Informação uma lacuna a ser pesquisada, ao abordar a segurança do conhecimento.

Ávila e Silva (2011), em seu aporte teórico, traçam um paralelo da questão conceitual da Segurança Cibernética com o conceito de Segurança da Informação.

Ferreira e Araújo (2013) analisam, sob a ótica da gestão da segurança da informação, o Sistema de Concessão de Diárias e Passagens/SCDP - do Departamento Contábil da Universidade Federal da Paraíba. Os autores investigam a garantia de confidencialidade, da integridade e da disponibilidade da informação, por meio de uma análise de risco nos elementos e nos documentos que integram o sistema.

Silva, Araújo e Azevedo (2013) abordaram os sites de redes sociais que desenvolve o fenômeno conhecido como “hipermobilidade estética dos internautas” que amplia a exposição de informações pessoais na *Web*, aumentando também os riscos associados às pessoas, principalmente em relação à aplicação de técnicas de engenharia social.

Silva e Araújo (2014) apresentam em seu estudo a elaboração de uma proposta de modelo para o descarte seguro da informação em suporte digital (considerando os requisitos de gestão da segurança da informação), avaliando que alguns procedimentos de descarte inviabilizam o uso posterior da mídia informática.

Araújo, Batista e Araújo (2015) realizam uma pesquisa para identificar quais ações de segurança da informação relacionadas aos aspectos humanos são utilizadas pela Pró-Reitoria de Gestão de Pessoas da Universidade Federal da Paraíba.

Percebe-se, no âmbito do Enancib, que as publicações que abordaram a temática segurança da informação, mantiveram-se presentes em cinco das nove edições do evento pesquisadas. Ressalta-se que os interesses particulares da Ciência da Informação abrangem desde a problemática conceitual do termo segurança da informação, perpassando pelo modo como a Ciência da Informação deveria abarcar a temática, chegando às aplicações empíricas, concretizadas nos estudos de caso, demonstrando que as pesquisas em segurança da informação ainda são pulverizadas, não possuem um tema central. No levantamento, percebe-se também a existência de apenas uma de pesquisa que possuem como objeto de estudo a dimensão humana.

2.2 SEGURANÇA DA INFORMAÇÃO

Independente de segmento de mercado ou de porte, as instituições sempre usufruíram da informação, objetivando melhor produtividade, redução de custos, aumento de agilidade, competitividade e apoio mais eficiente aos processos de tomada de decisão (SÊMOLA, 2014, p. 1). Assim, a informação se apresenta como um ativo, como qualquer outro ativo importante para os negócios de uma organização, consequentemente, necessita ser protegida de forma adequada contra destruição, indisponibilidade temporária, adulteração ou divulgação não autorizada (ABNT NBR ISO/IEC 27002, 2013, p. x; BEAL, 2008, p. xi).

Para Beal (2008, p. xi) ativo de informação é “qualquer dado ou informação a que esteja associado um valor para o negócio”. Para a autora, representam ativos de informação, as informações relevantes mantidas na mente dos tomadores de decisão, em bases de dados, arquivos de computador, documentos e planos registrados em papel, entre outros. Corroborando essa definição, para a ISO/IEC 27000 (2014, p. v, tradução nossa), ativos de informação incluem informação financeira, propriedade intelectual, informação de funcionário, ou a informação que lhes foi confiada pelos clientes ou por terceiros.

Relativo à proteção desses ativos, são necessárias ações continuadas alicerçadas por conceitos sólidos e amplamente reconhecidas, desenvolvidas por áreas especializadas apoiadas nas normas e padrões de segurança. Nesse sentido, o Governo Federal Brasileiro define segurança da informação como:

> [...] proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenadas, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento. (BRASIL, 2000[5]).

Marciano e Marques (2006) apresenta um conceito social para a segurança da informação, buscando abranger: os usuários, o ambiente de atuação da segurança e o objetivo dessa atuação. Assim, o autor define segurança da informação como:

> [...] um fenômeno social no qual os usuários (aí incluídos os gestores) dos sistemas de informação têm razoável conhecimento acerca do uso destes sistemas, incluindo os ônus decorrentes expressos por meio de regras, bem como sobre os papéis que devem desempenhar no exercício deste uso. (MARCIANO; MARQUES, 2006, p. 95).

Para a *Information Systems Auditand Control Association* (ISACA, 2012, p. 19, tradução nossa) a segurança da informação garante que, dentro da empresa, as informações são protegidas contra a divulgação para usuários não autorizados - **confidencialidade**, modificação indevida - **integridade** e o não acesso quando requerido - **disponibilidade**.

Sêmola (2014, p. 43) expõe o conceito de segurança da informação como "uma área do conhecimento dedicada à proteção de ativos da informação contra acesso não autorizado, alterações indevidas ou sua indisponibilidade". Percebe-se que o autor insere a segurança da informação como área do conhecimento. Nesse sentido, da mesma forma que a ISACA, Sêmola (2014) emprega os princípios confidencialidade, integridade e disponibilidade como meio para alcançar a segurança da informação.

[5] Documento eletrônico não paginado.

Para proteção desses ativos, as organizações necessitam assumir uma posição proativa diante das vulnerabilidades das quais os ativos estão expostos, entendendo-se que as vulnerabilidades são fragilidades presentes ou associadas a ativos que manipulam ou processam a informação que, ao serem exploradas por ameaças[6], as vulnerabilidades permitem a ocorrência de incidente na proteção, afetando negativamente um ou mais princípios da segurança da informação (SÊMOLA, 2014, p. 46).

Dessa forma, além dos princípios de segurança da informação explicitados nas definições do ISACA (2012) e de Sêmola (2014), que são: **confidencialidade, integridade** e **disponibilidade,** a ISO/IEC 27000 (2014, p. 4, tradução nossa) acrescenta outras propriedades que devem ser consideradas, a saber:

- **Autenticidade** - propriedade de que uma entidade é o que a mesma diz ser;
- **Responsabilidade** - propriedade na qual o responsável pela informação deve prestar contas da mesma;
- **Não repúdio** - capacidade de comprovar a ocorrência de uma reivindicação de um evento ou ação e suas entidades originárias;
- **Confiabilidade** - propriedade de que o comportamento e o resultado acham-se consistentes com a intenção.

O Gabinete de Segurança Institucional da Presidência da República, por meio da Instrução Normativa GSIPR n. 1, de 13 de junho de 2008 define Gestão de Segurança da Informação e Comunicações (GSIC) como:

> [...] ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação e comunicações. (BRASIL, 2008[7]).

[6] Agentes ou condições que causam incidentes que comprometem as informações e seus ativos por meio da exploração de vulnerabilidades (SÊMOLA, 2014, p. 45).
[7] Documento eletrônico não paginado.

Nesse sentido, Fontes (2012, p. 23) esclarece que a segurança da informação não é uma ação isolada, mas um processo que deve considerar a informação tanto no ambiente tecnológico quanto no ambiente convencional. Geralmente, as organizações abrangem apenas as informações que estão no ambiente computacional. Entretanto, tanto o ambiente convencional, quando do uso do papel, quanto o ambiente pessoal, com as informações na mente das pessoas, precisam ser contemplados no processo de segurança da informação. O autor conclui que se deve considerar a segurança da informação independente do ambiente onde se encontra, embora a maior parte das informações esteja localizada no ambiente tecnológico, sua utilização acontece pelas pessoas inseridas no ambiente convencional. Além da preocupação com o ambiente, torna-se necessário preocupar-se com a fase em que se encontra a informação dentro do ciclo de vida informacional.

De acordo com ABNT NBR ISO/IEC 27002 (2013, p. xii), a “informação tem um ciclo de vida natural, desde a sua criação e origem, armazenagem, processamento, uso e transmissão, até a sua eventual destruição ou obsolescência”. Para a norma, o valor e os riscos aos ativos podem variar durante o tempo de vida da informação, porém a segurança da informação permanece importante em todos os estágios.

Conforme a Norma Complementar 20/IN01/DSIC/GSIPR do Gabinete de Segurança Institucional da Presidência da República, o ciclo de vida da informação está agrupado nas seguintes fases:

> **Produção e Recepção:** refere-se ao estágio em que as informações são produzidas ou recebidas pelos agentes públicos, independentemente de seu formato ou suporte.
> **Registro e Armazenamento:** diz respeito à fase em que as informações são registradas e armazenadas em quaisquer suportes ou formatos.
> **Uso e Disseminação:** trata-se do estágio em que as informações estão sendo utilizadas e compartilhadas pelos órgãos e entidades da Administração Pública Federal, envolvendo ações como o seu uso, transporte, transmissão e divulgação.
> **Destinação:** refere-se ao estágio final do ciclo de vida da informação, no qual devem ser tomadas as medidas necessárias à sua destinação, tais como guarda permanente ou eliminação. (BRASIL, 2014, p. 4, grifo nosso).

No âmbito da Administração Pública Federal (APF), os órgãos produzem e tratam informações diariamente na rotina de trabalho de seus agentes públicos[8], ocupando relevância fundamental para a gestão da máquina pública e o processo de tomada de decisões quanto às políticas públicas federais. Referente ao tratamento das informações, ao longo de seu ciclo de vida, este deverá ser realizado de modo ético e responsável pelos agentes públicos dos órgãos e entidades da APF e com respeito à legislação vigente (BRASIL, 2014, p. 2-3).

Com relação às fases do ciclo de vida da informação, essas são vivenciadas quando os ativos físicos, tecnológicos e humanos utilizam a informação, expondo-a a ameaças que colocam em risco suas propriedades. Nesse sentido, independente da fase do ciclo em que a informação se encontra, é necessário que esteja protegida. Entretanto, Araújo (2009, p. 43) esclarece que nem todas as informações devem ser protegidas, apesar de ser um ativo importante para organização, pois o custo e o esforço demandado tornariam o processo inexequível de ser efetivado. De acordo com a ABNT NBR ISO/IEC 27002 (2013, p. 18), “a informação deve ser classificada de acordo com seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada”. Esse processo de classificação colabora para definir quais ativos de informação devem ser protegidos, e os níveis de proteção que devem se aplicados. O Quadro 3 discrimina os tipos de informação.

Quadro 3 - Tipos de informação

TIPO DE INFORMAÇÃO	DISCRIMINAÇÃO
1 Sigilosa classificada em grau de sigilo	1.1 Reservada - Prazo máximo de restrição de acesso de 5 anos
	1.2 Secreta – Prazo máximo de restrição de acesso de 15 anos
	1.3 Ultrassecreta – Prazo máximo de restrição de acesso de 25 anos
2 Sigilosa protegida por legislação específica (as hipóteses legais de restrição de acesso à informação elencadas neste item não são exaustivas)	**2.1 Sigilos Decorrentes de Direitos de Personalidade**
	2.1.1 Sigilo Fiscal

[8] Todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da APF.

	2.1.2 Sigilo Bancário
	2.1.3 Sigilo Comercial
	2.1.4 Sigilo Empresarial
	2.1.5 Sigilo Contábil
	2.2 Sigilos de Processos e Procedimentos
	2.2.1 Acesso a Documento Preparatório
	2.2.2 Sigilo do Procedimento Administrativo Disciplinar em Curso
	2.2.3 Sigilo do Inquérito Policial
	2.2.4 Segredo de Justiça no Processo Civil
	2.2.5 Segredo de Justiça no Processo Penal
	2.3 Informação de Natureza Patrimonial
	2.3.1 Segredo Industrial
	2.3.2 Direito Autoral e Propriedade Intelectual de Programa de Computador
	2.3.3 Propriedade Industrial
3 Ostensiva	3.1 Transparência Passiva
	3.2 Transparência Ativa
4 Pessoal	4.1. Pessoal – Prazo máximo de restrição de acesso de 100 anos, independente de classificação de sigilo e quando se referir à intimidade, vida privada, honra e imagem das pessoas

Fonte: Adaptado da Norma Complementar 20/IN01/DSIC/GSIPR (BRASIL, 2014, p. 12).

Com a classificação é possível identificar quais informações necessitam de maior proteção, de modo a evitar possíveis ameaças. Sêmola (2014. p. 45) classifica as ameaças que podem comprometer a segurança das informações, por meio da exploração de vulnerabilidades, em três grupos: naturais – decorrentes de fenômenos da natureza (incêndios naturais, enchentes, terremotos etc.); involuntárias – ameaças inconscientes (acidentes, erros etc.); e voluntárias – ameaças propositais causadas pelo elemento humano (hackers, espiões, criadores e disseminadores de vírus, entre outros). Segundo o autor, existem vários tipos de vulnerabilidades que sozinhas não causam incidentes, necessitando de um agente

causador ou condição favorável. Sêmola (2014) e Beal (2008) destacam alguns desses tipos de vulnerabilidades no Quadro 4.

Quadro 4 – Tipos de vulnerabilidades

TIPOS	EXEMPLOS
Físicas	Instalações prediais que não atendem às boas práticas ou às normas e regulamentações vigentes; falta de extintores; detectores de fumaça e de outros recursos para combater o incêndio em ambientes com ativos ou informações estratégicas, controle de acesso deficiente em locais contendo informações confidenciais ou sensíveis, materiais estocados dentro do data center, fitas de backup armazenadas em armários sem proteção , dentro de caixas de papelão, excesso de poeira, cabeamento de rede desorganizado e desprotegido etc.
Naturais	Ambientes com equipamentos eletrônicos próximos a locais suscetíveis a desastres naturais, como incêndios, enchentes, terremotos, tempestades e outros, como falta de energia, aumento de poeira, aumento de umidade e de temperatura etc.
Hardware	Computadores são suscetíveis a poeira, umidade, sujeira e acesso indevido a recursos inadequadamente protegidos, podendo ainda sofrer com componentes deficientes ou mal configurados, com falhas ou flutuações no suprimento energético ou aumento excessivo na temperatura do ambiente.
Software	Erros na codificação, instalação ou configuração de sistemas e aplicativos podem acarretar acessos indevidos , vazamento de informações , perda de dados e de trilhas de auditoria ou indisponibilidade do recurso quando necessário, senhas de administrador vindas de fábrica que não são alteradas na instalação do software etc.
Mídias	Discos, fitas, relatórios e impressos podem ser perdidos ou danificados; falhas de energia podem causar panes em equipamentos, podendo danificar trilhas lógicas de dados; discos rígidos usualmente têm vida útil; a radiação eletromagnética pode afetar diversos tipos de mídias magnéticas.
Comunicação	A comunicação telefônica é vulnerável a escutas (acesso indevido) ou a problemas na infraestrutura física ou lógica que a impeçam de ser estabelecida.
Humanas	Falta de treinamento ou de conscientização das pessoas, falta de avaliação psicológica adequada ou verificação de antecedentes que identifiquem objetivos escusos ou problemas anteriores, ou mesmo má-fé ou o descontentamento de um funcionário, entre outros, podem levar ao compartilhamento indevido de informações confidenciais, a não execução de rotinas de segurança ou a erros, omissões etc., que ponham em risco as informações.

Fonte: Adaptado para quadro de (SÊMOLA 2014, p. 46-47; BEAL 2008, p. 18).

Com relação às vulnerabilidades expostas por Sêmola (2014) e Beal (2008), percebe-se que, em sua maioria, são decorrentes do não atendimento às práticas e/ou normas e regulamentações vigentes que orientam sobre os referidos assuntos,

como a falta de treinamento e conscientização abordada pela ABNT NBR ISO/IEC 27002 (2013, p. 13), que profere:

> Convém que todos os funcionários da organização e, onde pertinente, partes externas recebam treinamento, educação e conscientização apropriados, e as atualizações regulares das políticas e procedimentos organizacionais referentes para as suas funções.

Neste contexto, a ABNT NBR ISO/IEC 27002 (20013, p. x) ressalta a necessidade da segurança da informação ser gerenciada por todos os tipos de organização, incluindo o setor privado e o público, organizações comerciais e sem fins lucrativos. Fontes (2006, p. 74) ressalta que mesmo as instituições governamentais, assim como as organizações sem fins lucrativos, almejam permanecer no mercado a que se propuseram. Essas organizações também oferecem retorno aos seus acionistas, mas de uma forma diferente: retribuição social aos cidadãos, serviços prestados à população, melhoria de vida e ações que fortalecem a cidadania. Para tanto, devem integrar os seguintes controles de segurança da informação:

> A segurança da informação é alcançada pela implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de *software* e *hardware*. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, quando necessário, para assegurar que os objetivos do negócio e a segurança da informação da organização sejam atendidos. (ABNT NBR ISO/IEC 27002, 2013, p. x).

Fontes (2012, p. 29) afirma que, para garantir que a segurança das informações esteja em um nível aceitável, torna-se necessário que a organização possua uma Política de Segurança da Informação cujo processo de proteção da informação seja planejado e ocorra de forma efetiva. Essa política (ou conjunto de políticas) determinará as diretrizes, os limites e os direcionamentos que a organização espera dos controles que serão implantados na proteção da informação.

2.2.1 Políticas de segurança da informação

Por políticas entende-se um conjunto de intenções, diretrizes, limites e direcionamentos formalmente expressos pela direção de uma instituição (FONTES, 2012, p. 29). Já uma Política de Segurança da Informação (PSI) pode ser considerada “um conjunto de regras e padrões sobre o que deve ser feito para assegurar que as informações recebam a proteção conveniente que possibilite garantir a sua confidencialidade, integridade e disponibilidade.” (BARMAN, 2002, p. 4). Observa-se que o conceito de PSI, expresso por Barman, propõe práticas gerais para garantir que os princípios básicos da segurança da informação sejam atingidos.

Em um entendimento mais social sobre política de segurança da informação, Marciano (2006, p. 119) a define como “uma linha de conduta coletiva, resultante da interação entre atores dentro de um quadro de cooperação-integração reciprocamente reconhecido”. Desse modo, a política de segurança se apresenta como um fenômeno social, considerando-se que o elemento humano dialoga com a informação, como objetos e atores que carecem ser gerenciados e protegidos.

Para o instituto *SysAdmin, Audit, Networking and Security* (SANS), a política de segurança da informação é entendida como a atitude da organização frente à informação, e anuncia, interna e externamente, que a informação é um ativo, a propriedade da organização, e deve ser protegida contra acesso não autorizado, modificação, divulgação e destruição (SANS, 2007, p. 2, tradução nossa). Beal (2011) elenca alguns objetivos da política da segurança da informação, quais sejam:

> **Identifica**r, em todos os níveis da organização, quem é o responsável e presta contas pela informação, bem como as linhas hierárquicas para essas funções;
> **Classifica**r as informações analisando o valor que elas representam para a instituição e o custo delas;
> **Estabelecer** o padrão mínimo de segurança para aplicação em todos os sistemas corporativos e orientar a encontrar, mediante análise de risco, os pontos que merecem medição extra de proteção;
> **Reconhecer** que a proteção efetiva deverá estar sempre presente em todo o desenvolvimento do sistema ao invés de ser adicionada num momento posterior;
> **Implementar** a segurança da informação nos procedimentos operacionais, estabelecendo controles de acesso e auditoria interna;
> **Determinar** a política de segurança de pessoal e treinamento;
> **Atentar** para os procedimentos de controle de material proprietário e de licenças de uso de software e fazer as adaptações necessárias para garantir adequação à legislação aplicável;

> **Criar** uma política quanto ao relatório e investigação de incidentes de segurança, bem como requisitos de planejamento para continuidade do serviço;
> **Estabelecer** uma política de segurança da informação que responda às mudanças da organização de acordo com as suas necessidades, pois, desse modo, ela não ficará estática. (BEAL, 2011, p. 55, grifo nosso).

Fontes (2006, p. 88) entende como objetivo da PSI explicar aos colaboradores, que acessam e utilizam a informação, qual a filosofia e quais as regras para o manuseio, armazenamento, transporte e descarte dessa informação. Para o autor, essas regras de segurança da informação são implantadas no intuito de proteger os recursos de informação, utilizados estratégica e operacionalmente para o funcionamento da organização e para o atendimento dos objetivos da organização. Compreendendo o alto valor da informação para o desenvolvimento das organizações, o autor direciona a atenção à responsabilidade dos gestores da organização, no que tange à garantia da existência e a continuidade do processo de segurança da informação. Para tanto, torna-se primordial que seja desenvolvida e implementada uma política de segurança da informação para que todas as ações de proteção dos recursos de informação sejam bem direcionadas e adequadas à organização (FONTES, 2012, p. 23-25).

Seguindo as orientações dos órgãos internacionais, o Governo Federal Brasileiro instituiu o Decreto nº 3.505, de 13 de junho de 2000, que estabelece diretrizes relativas à política de segurança da informação nas entidades da Administração Pública Federal. Como pressupostos básicos da política de segurança, o decreto destaca as seguintes diretrizes:

> I - assegurar a garantia ao direito individual e coletivo das pessoas, à inviolabilidade da sua intimidade e ao sigilo da correspondência e das comunicações, nos termos previstos na Constituição;
> II - proteção de assuntos que mereçam tratamento especial;
> III - capacitação dos segmentos das tecnologias sensíveis;
> IV - uso soberano de mecanismos de segurança da informação, com o domínio de tecnologias sensíveis e duais;
> V- criação, desenvolvimento e manutenção de mentalidade de segurança da informação;
> VI - capacitação científico-tecnológica do País para uso da criptografia na segurança e defesa do Estado;

> VII - conscientização dos órgãos e das entidades da Administração Pública Federal sobre a importância das informações processadas e sobre o risco da sua vulnerabilidade. (BRASIL, 2000[9]).

Entende-se que esses pressupostos normalizam a PSI no sentindo de orientar, proteger e conscientizar os colaboradores quanto à importância da segurança da informação na administração pública federal. A partir do Decreto nº 3.505, foi criado o Comitê Gestor da Segurança da Informação, composto por representantes de todos os ministérios, além de representantes de outros órgãos do governo com atribuição de assessorar a Secretaria-Executiva do Conselho de Defesa Nacional na consecução das diretrizes da Política de Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal (BRASIL, 2000[10]).

Atendendo as exigências do referido Decreto, a Universidade Federal da Paraíba elaborou em 2014 sua Política de Segurança da Informação, que 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 da UFPB". (UFPB, 2014a[10]). No Art. 4º, a PSI da UFPB apresenta seus objetivos, que consistem em:

> I – Definir o escopo da segurança da informação da UFPB;
> II – Orientar as ações de segurança com intuito de reduzir riscos e garantir a confidencialidade, integridade e disponibilidade dos ativos da UFPB;
> III - Incentivar o uso de soluções integradas de segurança;
> IV – Servir de referência para auditoria, apuração e avaliação de responsabilidade (UFPB, 2014[10]a).

Entretanto, para a existência do processo de segurança da informação nas instituições, é fundamental que a PSI e as demais políticas dela derivada (específicas por tema) sejam publicadas e comunicadas a todos os colaboradores, de forma que sejam entendidas, acessíveis e relevantes aos colaboradores pertinentes, bem como sejam implementados e estruturados os controles de segurança, considerando as necessidades de grupos ou tópicos específicos (ABNT NBR ISO/IEC 27002, 2013, p. 3). Exemplos de tópicos específicos dessas políticas e seus respectivos controles são observados no Quadro 5.

[9] Documento eletrônico não paginado.
[10] Documento eletrônico não paginado.

Quadro 5 - Políticas de segurança por temas específicos

TEMA DA POLÍTICA	CONTROLE
Controle de acesso	Convém que uma política de controle de acesso seja estabelecida, documentada e analisada criticamente, baseada nos requisitos de segurança da informação e dos negócios.
Classificação e tratamento da informação	Convém que a informação seja classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada.
Segurança física do ambiente	Convém que perímetros de segurança sejam definidos e usados para proteger tanto as áreas que contenham as instalações de processamento da informação como as informações críticas ou sensíveis.
Uso aceitável dos ativos	Convém que regras para o uso aceitável das informações, dos ativos associados com a informação e dos recursos de processamento da informação, sejam identificadas, documentadas e implementadas.
Mesa limpa e tela limpa	Convém que seja adotada uma política de mesa limpa de papéis e mídias de armazenamento removíveis e uma política de tela limpa para os recursos de processamento da informação.
Transferência de informação (usuários finais)	Convém que políticas, procedimentos e controles de transferências formais, sejam estabelecidos para proteger a transferência de informações, por meio do uso de todos os tipos de recursos de comunicação.
Dispositivos móveis e trabalho remoto	Convém que uma política e medidas que apoiam a segurança da informação seja adotada para gerenciar os riscos decorrentes do uso de dispositivos móveis.
Restrições sobre o uso e instalações de software	Convém que sejam estabelecidas e implementadas regras definindo critérios para a instalação de *software* pelos usuários.
Backup	Convém que cópias de segurança das informações, softwares e das imagens do sistema, sejam efetuadas e testadas regularmente conforme a política de geração de cópias de segurança definida.
Transferência da informação	Convém que políticas, procedimentos e controles de transferências formais, sejam estabelecidos para proteger a transferência de informações, por meio do uso de todos os tipos de recursos de comunicação.
Proteção contra *malware*	Convém que sejam implementados controles de detecção, prevenção e recuperação para proteger contra códigos maliciosos, combinado com um adequado programa de conscientização do usuário.
Gerenciamento de vulnerabilidades técnicas	Convém que informações sobre vulnerabilidades técnicas dos sistemas de informação em uso, sejam obtidas em tempo hábil, com a exposição da organização a estas vulnerabilidades avaliadas e tomadas as medidas apropriadas

	para lidar com os riscos associados.
Controles criptográficos	Convém que seja desenvolvida e implementada uma política para o uso de controles criptográficos para a proteção da informação.
Segurança nas comunicações	Convém que as redes sejam gerenciadas e controladas para proteger as informações nos sistemas e aplicações.
Proteção e privacidade da informação de identificação pessoal	Convém que a privacidade e proteção das informações de identificação pessoal sejam asseguradas conforme requerido por legislação e regulamentação pertinente, quando aplicável.
Relacionamento na cadeia de suprimentos	Convém que a organização identifique e exija os controles de segurança da informação para tratar, especificamente, do acesso do fornecedor as informações da organização, através de uma política.

Fonte: Adaptado para quadro da (ABNT NBR ISO/IEC 27002 2013, p. 3-77).

Como forma de divulgar o conhecimento referente às políticas de segurança da informação, o SANS *Institute* desenvolveu algumas políticas e as disponibilizou em seu *site* na *internet*, de modo que sejam utilizadas livremente, parcial ou integralmente, por qualquer instituição. Destaca-se, dentre as políticas criadas pelo SANS *Institute*, a Política de mesa limpa, conforme o Quadro 6.

Quadro 6 - Política de mesa limpa

POLÍTICA DE MESA LIMPA	
Visão Geral	A política de mesa limpa pode ser uma ferramenta importante para garantir que todas as informações sensíveis / confidenciais sejam removidas do espaço de trabalho do funcionário e trancadas, quando os itens não estão em uso, ou quando o funcionário deixa sua estação de trabalho. É uma das principais estratégias quando se tenta reduzir o risco de violações de segurança no local de trabalho. Esta política pode também aumentar a consciência do funcionário sobre a proteção de informações confidenciais.
Finalidade	O objetivo dessa política é estabelecer os requisitos mínimos para a manutenção de uma "mesa limpa" - onde a informação sensível/crítica sobre funcionários, propriedade intelectual, clientes e fornecedores seja protegida.
Âmbito	Esta política se aplica a todos empregados e afiliados.
Política	Os funcionários são obrigados a garantir que todas as informações sensíveis/ confidenciais em formato impresso ou eletrônico sejam protegidas na sua área de trabalho, no final do dia, e quando eles se ausentam por período prolongado.
	Estações de trabalho de computador devem ser bloqueadas quando desocupados.
	Estações de trabalho de computador devem ser desligadas completamente no

	final do expediente.
	Informações confidenciais devem ser removidas da mesa e trancadas em armários ou gaveta no final do expediente.
	Armários contendo informações confidenciais ou restritas devem ser mantidos fechados, quando as mesmas não estiverem em uso.
	Laptops devem ser bloqueados com um cabo de bloqueio ou trancados em gavetas.
	As senhas não podem ser deixadas em notas postadas sobre ou sob um computador, nem pode ser deixado escrito em um local acessível.
	As impressões contendo informações sensíveis ou restritas devem ser imediatamente removidas da impressora.
	Para eliminação, os documentos sensíveis ou restritos, devem ser triturados nos escaninhos oficiais.
	Trancar dispositivos de computação portáteis, como laptops e *tablets*.
	Dispositivos de armazenamento em massa, tais como CD-ROM, DVD ou USB devem ser tratados como sensíveis e guardados em gavetas trancadas.

Fonte: Adaptado para quadro (SANS, 2014 p. 1-2, tradução nossa).

Diante do exposto, percebe-se a relevância da segurança da informação para as instituições, bem como dentro das políticas de Estado. Para Fontes (2012, p. 38), tanto as políticas como os demais regulamentos de segurança precisam ter uma organização que facilite sua compreensão.

2.2.2 Leis, Decretos e Normas de segurança da informação

Entende-se que são muitas as variáveis envolvidas com a segurança da informação, e crescentes à medida que vão surgindo novas tecnologias, novos modelos de negócios e inovações no relacionamento comercial. Decorrente disso, em 1995, a comunidade britânica, liderada pela Inglaterra, por meio da *Britsh Standard Institute* (BSI), criou a norma BS 7799. Nesse momento, a norma BS 7799 continha duas partes: a primeira parte, composta de práticas para o gerenciamento da segurança da informação; a segunda parte continha os requisitos de auditoria para certificação de Sistemas de Gestão de Segurança da informação (SGSI). Diante da relevância do assunto, tornou-se fundamental que essa norma fosse publicada por um órgão de reconhecimento internacional. Assim, em 2000, a *International Organization for Standartization* (ISO) construiu a sua versão da norma

para tratar da segurança da informação, denominando-a ISO 17799, baseada na norma BS 7799-1. Em 2005, a norma ISO17799-1 foi revisada e renomeada para ISO 27002:2005, norma estrutural da gestão da segurança da informação, levando ao desenvolvimento da família de normas associadas à gestão de segurança da informação. No mesmo ano, foi lançada a segunda parte da norma, ISO 27001, baseada na norma BS 7799-2, que define o sistema de gestão da informação e a possibilidade de certificação das empresas pelo estabelecimento desse tipo de sistema (SÊMOLA, 2014, p. 69-70; FONTES, 2012, p. 40-41).

No Brasil, essas normas são adotadas pela Associação Brasileira de Normas Técnicas (ABNT) que é o Foro Nacional de Normalização. Na ABNT, as normas são submetidas ao Comitê Brasileiro de Computadores e Processamento de Dados e pela Comissão de Estudos de Técnicas de Segurança, sendo publicadas no Brasil como ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002. Em novembro de 2013 a ABNT lançou revisões dessas duas normas. O Quadro 7 elenca as normas mais relevantes da série 27000, família de normas sobre gestão de segurança da informação e gestão de riscos, traduzidas pela ABNT.

Quadro 7 - Normas da ABNT de Segurança da Informação

NORMA	ASSUNTO
ABNT NBR ISO/IEC 27001:2013	Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos.
ABNT NBR ISO/IEC 27002:2013	Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação.
ABNT NBR ISO/IEC 27003:2011	Tecnologia da informação — Técnicas de segurança — Diretrizes para implantação de um sistema de gestão da segurança da informação.
ABNT NBR ISO/IEC 27004:2010	Tecnologia da informação — Técnicas de segurança — Gestão da segurança da informação — Medição.
ABNT NBR ISO/IEC 27005:2011	Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação.
ABNT NBR ISO/IEC 27007:2012	Diretrizes para auditoria de sistemas de gestão da segurança da informação.
ABNT NBR ISO/IEC 27011:2009	Tecnologia da informação —Técnicas de segurança — Diretrizes para gestão da segurança da informação para organizações de telecomunicações baseadas na ABNT NBR ISO/IEC 27002.

ABNT NBR ISO/IEC 27014:2013	Tecnologia da Informação — Técnicas de Segurança — Governança de segurança da informação.
ABNT NBR ISO/IEC 27031:2015	Tecnologia da informação — Técnicas de segurança — Diretrizes para a prontidão para a continuidade dos negócios da tecnologia da informação e comunicação.
ABNT NBR ISO/IEC 27037:2013	Tecnologia da informação — Técnicas de segurança — Diretrizes para identificação, coleta, aquisição e preservação de evidência digital.
ABNT NBR ISO/IEC 27038:2014	Tecnologia da informação — Técnicas de segurança — Especificação para redação digital.

Fonte: Adaptado para quadro do (CATÁLOGO da ABNT, 2014)

Além das normas elencadas no quadro acima, torna-se relevante fazer referência a ISO 27000:2014, ainda não traduzida pela Associação Brasileira de Normas Técnicas, que aborda: a tecnologia da informação, técnicas de segurança, sistemas de gestão de segurança da informação, descrições e vocabulário.

As normas ABNT NBR ISO/IEC 27001 e 27002, atualizadas em novembro de 2013, trazem uma abordagem mais flexível e simplificada de seus conteúdos, a fim de possibilitar uma gestão de segurança mais efetiva. Essas normas tratam de aspectos bem abrangentes da segurança da informação, como a 27002 que reúne os tópicos que devem ser analisados, as melhores práticas e, didaticamente, aponta “o que” deve ser feito, sem os detalhes relacionados ao “como”. Apesar de abrangente, essas normas representam um importante instrumento sinalizador de direção para as instituições preocupadas com a operação do seu negócio e a proteção das informações que as sustentam. A ABNT NBR ISO/IEC 27002:2013 possui 18 seções, sendo as quatro primeiras consideradas introdutórias e as demais organizadas em 35 objetivos de controles que se estendem a 114 controles sugeridos. Essa norma serve como apoio à implantação de Sistemas de Gestão da Segurança da Informação (SGSI), conforme descrito na ABNT NBR ISO/IEC 27001:2013 (SÊMOLA, 2014, p. 70-71).

Além das normas que garantem certificação internacional às organizações, o Governo Federal instituiu a política de segurança da informação nos órgãos e entidades da administração pública federal por meio do Decreto Presidencial n. 3.505, de 13 de junho de 2000. Coube, ainda, ao Comitê Gestor de Segurança da Informação, criar grupos de trabalho para estudar as diretrizes apontadas no referido

Decreto e buscar soluções para sua efetiva aplicação (BRASIL, 2000[11]). Entretanto, essa aplicação se mostrou complexa, tornando necessária a publicação de novas normas para discipliná-lo.

A Instrução Normativa (IN) GSI/PR nº 1, de 13 de junho de 2008, do Gabinete de Segurança Institucional da Presidência da República, disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal (APF), direta e indireta, determinando, no seu Art. 5º, que aos órgãos e entidades da Administração Pública Federal, direta e indireta, em seu âmbito de atuação, compete:

> I - coordenar as ações de segurança da informação e comunicações;
> II - aplicar as ações corretivas e disciplinares cabíveis nos casos de quebra de segurança;
> III - propor programa orçamentário específico para as ações de segurança da informação e comunicações;
> IV - nomear Gestor de Segurança da Informação e Comunicações;
> V - instituir e implementar equipe de tratamento e resposta a incidente em redes computacionais;
> VI - instituir Comitê de Segurança da Informação e Comunicações;
> VII - aprovar Política de Segurança da Informação e Comunicações e demais normas de segurança da informação e comunicações;
> VIII - remeter os resultados consolidados dos trabalhos de auditoria de Gestão de Segurança da Informação e Comunicações para o Gabinete de Segurança Institucional da Presidência da República. (BRASIL, 2008[12]).

Entende-se que várias são as competências da APF no que se refere à segurança da informação. Assim, a Instrução Normativa GSI/PR nº 1 de 2008 gerou várias normas complementares (NC), que demonstram a diversidade de áreas de atuação da gestão de segurança da informação e comunicação, abreviadas no Quadro 8.

Quadro 8 - Normas complementares à Instrução Normativa 01/GSI/PR

NC	DESCRIÇÃO
01/IN01/2008	Atividade de Normatização.
02/IN01/2008	Metodologia de Gestão de Segurança da Informação e Comunicações.
03/IN01/2009	Diretrizes para a Elaboração de Política de Segurança da Informação e

[11] Documento eletrônico não paginado.
[12] Documento eletrônico não paginado.

	Comunicações.
04/IN01/2013	Diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC.
05/IN01/2009	Disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR.
06/IN01/2009	Estabelece Diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações.
07/IN01/2010	Estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações.
08/IN01/2010	Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais.
09/IN01/2013	Estabelece orientações específicas para o uso de recursos criptográficos em Segurança da Informação e Comunicações.
10/IN01/2012	Estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a SIC.
11/IN01/2012	Estabelece diretrizes para avaliação de conformidade nos aspectos relativos à Segurança da Informação e Comunicações.
12/IN01/2012	Estabelece diretrizes e orientações básicas para o uso de dispositivos móveis nos aspectos referentes à SIC.
13/IN01/2012	Estabelece diretrizes para a Gestão de Mudanças nos aspectos relativos à Segurança da Informação e Comunicações.
14/IN01/2012	Estabelece diretrizes para a utilização de tecnologias de Computação em Nuvem, nos aspectos relacionados à SIC.
15/IN01/2012	Estabelece diretrizes de Segurança da Informação e Comunicações para o uso de redes sociais.
16/IN01/2012	Estabelece as Diretrizes para o Desenvolvimento e Obtenção de *Software* Seguro.
17/IN01/2013	Estabelece Diretrizes nos contextos de atuação e adequações para Profissionais da Área de Segurança da Informação e Comunicações.
18/IN01/2013	Estabelece as Diretrizes para as Atividades de Ensino em Segurança da Informação e Comunicações.
19/IN01/2014	Estabelece Padrões Mínimos de Segurança da Informação e Comunicações para os Sistemas Estruturantes da APF.
20/IN01/2014	Estabelece as Diretrizes de Segurança da Informação e Comunicações para Instituição do Processo de Tratamento da Informação.
21/IN01/2014	Estabelece as Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da Administração Pública Federal, direta e indireta.

Fonte: Adaptado para quadro das Normas Complementares à IN Nº 01 GSI/PR/2008 - Segurança da Informação e Comunicações (BRASIL, 2015[13]).

Além das Normas Complementares já expostas no quadro acima, o Governo Federal editou as seguintes leis e decretos relacionados à segurança da informação:

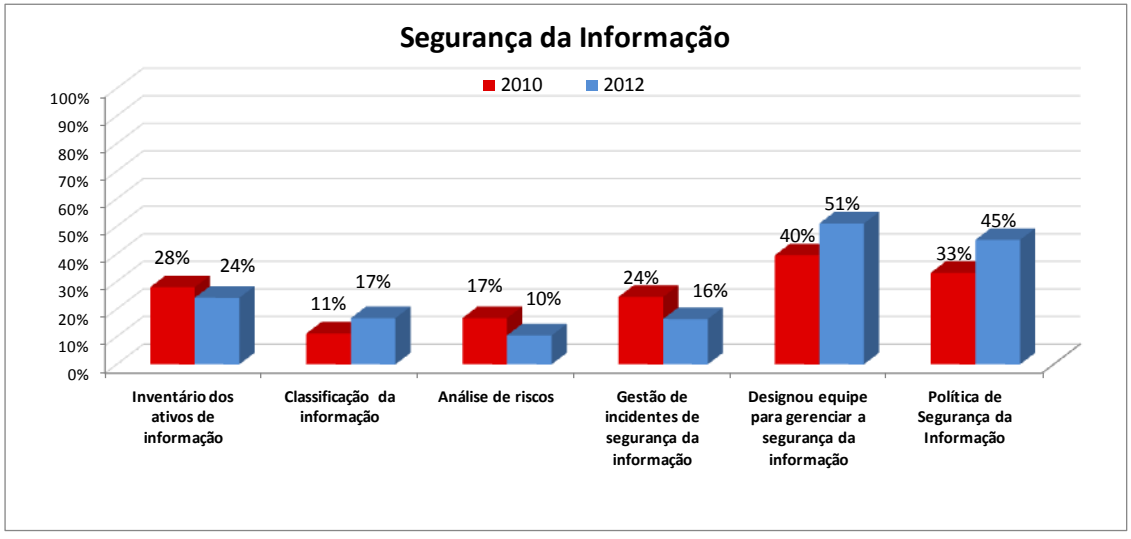
[13] Documento eletrônico não paginado.

- Lei 9.983/2000 - Altera o Código Penal acrescentando os seguintes dispositivos: apropriação indébita previdenciária; inserção de dados falsos em sistema de informações; modificação ou alteração não autorizada de sistema de informações; e sonegação de contribuição previdenciária.
- Decreto Nº 3.505/2000 - Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.
- Lei nº 10.683, de 28 de maio de 2003, em seu art. 6º, estabelece ao Gabinete de Segurança Institucional da Presidência da República (GSI/PR) a competência de coordenar as atividades de inteligência federal e de segurança da informação do governo, entre outras.
- Decreto nº 4.829, de 03 de setembro de 2003, que dispõe sobre a criação do Comitê Gestor da Internet no Brasil - CGI.br, sobre o modelo de governança da Internet no Brasil, e estabelece a coordenação do mesmo a ser exercida pelo, então, Ministério da Ciência e Tecnologia – MCT.
- Decreto nº 5.772, de 08 de maio de 2006, dispõe sobre a reestruturação do GSI/PR, com inserção de novas atribuições relacionadas à Segurança da Informação no rol de competências da secretaria executiva. Fica, então, criado o Departamento de Segurança da Informação e Comunicações (DSIC), com a missão de planejar e coordenar as atividades de Segurança da Informação e Comunicações (SIC) na APF.
- Lei 12.527/2011 - Dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações.
- Decreto Nº 7.845/2012 - Regulamenta os procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento.
- Lei nº 12.737, de 30 de novembro de 2012, a qual dispõe sobre a tipificação criminal de delitos informáticos.

- Lei nº 12.735, de 30 de novembro de 2012, a qual tipifica as condutas realizadas mediante uso de sistema eletrônico, digital ou semelhante, que sejam praticadas contra sistemas informatizados e similares.
- Lei Nº 12.965, de 23 de abril de 2014 - estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.
- Acórdão Nº 3117/2014 TCU - Plenário de 12 de novembro de 2014, divulga o resultado do levantamento da governança de TI, realizado no processo do TCU nº 003.732/2014. Avaliação da governança de tecnologia da informação na administração pública federal.

Observa-se que, desde o Decreto nº 3.505 de 2000, diversas leis, normas e ações e normatizações foram editadas, a fim de auxiliar, com critérios homogêneos, uma gestão consistente de segurança da informação na APF. Um panorama dessa situação apresenta-se no Relatório de Avaliação da Governança de Tecnologia da Informação na Administração Pública Federal, realizado pelo Tribunal de Contas da União (TCU), em 2012, com 350 instituições públicas federais, conforme Figura 5.

Figura 5 - Gráfico comparativo da situação de segurança da informação na APF



Fonte: Relatório do Tribunal de Contas da União (TCU, 2012, p. 16).

Ainda de acordo com o TCU (2012, p. 17), com relação aos resultados obtidos, verifica-se que, apesar da evolução quanto ao número de instituições públicas que possuem uma política de segurança da informação, a situação ainda é preocupante, considerando que a ausência dessa política pode implicar em:

procedimentos não padronizados relativos à segurança; deficiência nos controles de segurança; dificuldade de responsabilização em incidentes de segurança; risco de acessos não autorizados e de vazamento de dados e informações; entre outros. Observa-se, também, ligeira evolução no percentual de instituições que possuem processo de classificação das informações. Entretanto, esse percentual ainda é baixo, considerando o advento da Lei nº 12.527/2011, que regula o acesso a informações mantidas pelo Estado, a julgar pela ausência de classificação, que pode implicar em tratamento inadequado da informação e na divulgação ostensiva de informações não públicas.

Diante do exposto, segundo Vianna (2015, p. 19), percebe-se que a área de segurança da informação, na APF, chama a atenção pelos altos índices de não conformidade[14], e as instituições não somente permanecem expostas a ameaças diversas e não mapeadas, como também não atuam com agilidade necessária para saná-las. Concernente às recomendações emitidas pelo TCU, percebe-se que na APF, de modo geral, ainda existem muitas lacunas no processo de gestão da segurança da informação que precisam ser preenchidas. Assim, destaca-se a importância das contribuições de mais pesquisas, que devem ser realizadas pelas organizações e instituições acadêmicas, na tentativa de auxiliar o preenchimento dessas lacunas.

2.3 DIMENSÃO HUMANA DA SEGURANÇA DA INFORMAÇÃO

A tecnologia da informação tornou-se parte integrante da vida contemporânea. Hoje, o uso da informação permeia todos os aspectos de negócios e vidas privadas. A maioria das organizações precisa de sistemas de informação para sobreviver e prosperar e, portanto, precisa proteger seus ativos de informação. Nesse sentido, Mitnick e Simon (2003, p. 3) alertam que:

> [...] a empresa pode adquirir as melhores tecnologias de segurança [...], pode ter treinado seu pessoal muito bem [...]. Mesmo assim essa empresa ainda estará vulnerável, embora os indivíduos possam seguir as melhores práticas de segurança [...] e vigiar muito bem a configuração adequada do sistema e a aplicação das correções de segurança, ainda assim, estarão vulneráveis.

[14] Cumprimento das legislações, normas e procedimentos.

Nesse contexto, com a vasta tecnologia existente, seria, portanto, trivial a obtenção de níveis adequados de segurança. No entanto, muitas organizações, que têm uma abundância de controles técnicos, experimentam um número desproporcional de infrações relacionadas com a segurança. A razão fundamental é que a segurança da informação é, sobretudo, um problema de pessoas e não um problema tecnológico. Apesar do fato de que uma quantidade considerável de tecnologia ser projetada para ser executada sem a interferência humana, mesmo assim, em algum momento, as pessoas precisam interagir com ela, como na instalação, configuração e manutenção dessa tecnologia, algo que deixa uma ampla oportunidade para o erro humano, ou que pode resultar em exposições que podem permitir uma oportunidade àqueles que têm a intenção de atacar (SCHULTZ, 2005, p. 425, tradução nossa).

Desse modo, a segurança da informação deve contemplar de forma abrangente esse "fator humano". Para isso, faz-se necessário um olhar holístico para todos que compõem a instituição, desde o zelador ao superintendente, passando por secretárias, telefonistas e assistentes. De acordo com a Pesquisa Global de Segurança da Informação, realizada pela PWS, em 2014 muitos dos incidentes são originados por funcionários e ex-funcionários, conforme Figura 6.

Figura 6 - Origem provável dos incidentes

Fonte: Pesquisa Global de Segurança da Informação (PWS, 2014, p. 13).

Isso ocorre porque, apesar do desenvolvimento contínuo de tecnologias de segurança, deixando ainda mais difícil a exploração de vulnerabilidades técnicas, os

atacantes se voltarão cada vez mais para a exploração do elemento humano por meio de técnicas de engenharia social. Por engenharia social entende-se:

> Um conjunto de procedimentos e ações que são utilizados para adquirir informações de uma organização ou de uma pessoa por meio de contatos falsos sem o uso da força, do arrombamento físico ou de qualquer brutalidade. É a velha conversa do malandro [...] (FONTES, 2006, p.135).

De um modo geral, os engenheiros sociais possuem grande habilidade em lidar com as pessoas. Eles são educados, simpáticos e agradam com facilidade, ou seja, possuem as características necessárias para estabelecer a afinidade e conquistar a confiança das pessoas. Nesse sentido, segundo Marcelo e Pereira (2005, p. 4), o engenheiro social sabe explorar algumas das facetas do ser humano, tais como vaidade, humildade e egocentrismo, visando, com isso, obter informações a respeito de alguém ou de uma empresa.

Nesse contexto, Mitnick e Simon (2003, p. 4) acreditam que à medida que os especialistas contribuem para o desenvolvimento de novas tecnologias de segurança, tornando a exploração de vulnerabilidades técnicas mais difíceis, os atacantes se voltarão cada vez mais para a exploração do elemento humano. Desse modo, não se pode confiar que produtos de segurança, funcionando de forma isolada, possam garantir uma segurança efetiva. Acreditar nisso pode levar a falsa ideia de segurança, ou seja, viver em um mundo de fantasia onde mais cedo ou mais tarde poderão ser vítimas de um incidente de segurança. Além disso, a segurança não pode ser vista como um produto, mas deve ser tratada como um processo, tornando-se não apenas um problema para a tecnologia, mas, sobretudo, para pessoas e para gestão institucional.

Corroborando essa ideia, Frangopoulos, Eloff e Venter (2013, p. 53-54 tradução nossa) declaram que grandes vulnerabilidades de sistemas de informação podem ser atribuídas ao seu elemento humano, ou seja, os colaboradores. Quando esses colaboradores vêm a ser o alvo, o comprometimento da segurança da informação torna-se iminente, independentemente de medidas técnicas que reforçam a segurança da informação, bem como a segurança física.

Isso porque, diferentemente das máquinas que são determinísticas, os seres humanos não são muito previsíveis. Ao contrário, podem representar uma ameaça quando influenciados por diversos fatores, como características pessoais, estruturas

administrativas, ativos físicos e tecnológicos e normas sociais (ARANTES, 2012, p. 18). De acordo com Albrechtsen (2007, p. 2, tradução nossa), uma série de fatores psicológicos, sociais, institucionais e culturais pode influenciar na percepção de risco dos usuários da informação que ajustam seu comportamento influenciado por este contexto.

Para Frangopoulos, Eloff e Venter (2013, p. 54, tradução nossa), quando esses erros, deliberados ou não, são agravados por fatores psicossociais, pode haver consequências terríveis sobre a segurança da informação. Nesse sentido, Mitnick e Simon (2003, p. 8) orientam às pessoas a não serem otimistas e a se tornarem mais conscientes das técnicas que estão sendo usadas por aqueles que tentam atacar a confidencialidade, integridade e disponibilidade das informações. Assim, para esses autores:

> Nós nos acostumamos a aceitar a necessidade da direção segura; agora está na hora de aceitar e aprender a prática da computação defensiva. A ameaça de uma invasão que viola a nossa privacidade, a nossa mente ou os sistemas de informações da nossa empresa pode não parecer real até que aconteça. Para evitar tamanha dose de realidade, precisamos nos conscientizar, educar, vigiar e proteger os nossos ativos de informações, as nossas informações pessoais e as infra-estruturas críticas da nossa nação. (MITNICK; SIMON, 2003, p. 7).

Nesse sentido, torna-se necessário que pessoas, juntamente com suas características individuais, não sejam ignoradas pelas políticas de segurança da informação, uma vez que programar sistemas e manter as informações em segurança, torna-se um exercício muito mais complicado quando os problemas individuais comprometem o processo. No entendimento de Schneier (2004, p. 255, tradução nossa),

> A matemática é impecável, os computadores são vencíveis, as redes são péssimas e as pessoas são abismais. Aprendi muito sobre os problemas de proteção de computadores e redes, mas nenhum que realmente ajude a resolver o problema de pessoas.

Diante das palavras do autor, entende-se que os aspectos humanos se apresentam como um grande desafio à segurança da informação, de modo que precisa ser mais estudado e melhor abordado pelas normas de políticas de segurança da informação.

Não obstante, a afirmativa que pessoas são o elo mais fraco da corrente de segurança da informação representa a opinião de muitos autores[15] que abordam a temática segurança, tornando-se um estereótipo, seja por ações de desvio de conduta, seja por negligência, inocência ou descuido. Nesse sentido, Marcelo e Pereira (2005, p. 8) discorrem:

> Em qualquer instituição, por mais segura que seja, tem sempre um fator que pode desequilibrá-la: o homem. A história de que um segredo deixa de ser segredo quando alguém sabe é uma das máximas que temos dentro da segurança da informação. Os grandes engenheiros sociais sabem disto e se aproveitam das fraquezas ou gostos pessoais de seus alvos para tentar se aproximar e conseguir a informação.

Com relação a essa afirmação, para Ferreira e Araújo (2006, p. 95), "grande maioria dos incidentes tem a intervenção humana, seja de forma acidental ou não. A segurança está relacionada a pessoas e processos, antes da tecnologia". Nesse sentido, Silva (2012, p. 28) complementa sublinhando que, quando uma informação específica é manipulada, possivelmente estará em risco. Desse modo, quando as instituições, por meio dos seus gestores, permitem um acesso mais abrangente, ou seja, para um maior número de pessoas, às suas informações, os riscos de segurança aumentam de forma exponencial.

Ainda nesse contexto, Greitzer e Frincke (2010, tradução nossa) discorrem que, quando o comportamento humano se desvia do cumprimento das políticas estabelecidas, independentemente de resultar em dolo ou negligência da política de segurança organizacional, deve ser denominado como ameaça interna. Dessa forma, a ameaça interna compreende desde o funcionário que compromete a segurança da informação, por ações não intencionais, em que inadvertida ou inconscientemente dão acesso a pessoas de fora, até crimes e abusos graves, incluindo espionagem, sabotagem, terrorismo, peculato, extorsão, suborno e corrupção.

Assim, de acordo com Colwill (2010, p. 187, tradução nossa) é necessário que haja maiores investimentos das organizações no tocante aos fatores humanos, de modo que exista equilíbrio em relação aos investimentos em tecnologia,

[15] Mitnick e Simon (2003); Marcelo e Pereira (2005); Schultz (2005); Fontes (2006); Ashenden (2008); Rocha (2008); Colwill (2010); Silva (2012); e Frangopoulos, Eloff e Venter (2013).

considerando que os seres humanos irão encontrar o caminho em torno de controles mais técnicos, à medida que forem conscientizados e capacitados. O autor conclui, com base em uma pesquisa realizada pela BERR[16] em 2008 que, no Reino Unido, muitas organizações não se protegem o suficiente, bem como não asseguram proteção às informações de seus clientes. Dentre os resultados da pesquisa, destacam-se:

> [...] 52% não realizam qualquer avaliação de risco formal de segurança da informação; 67% não fazem nada para impedir que dados confidenciais saiam em *pen drives* etc.; 78% das empresas tinham computadores com discos rígidos não criptografados roubados e 84% das empresas não rastreiam e-mails enviados com dados confidenciais. (COLWILL, 2010, p.187, tradução nossa).

Dentro desse contexto, o problema de vazamento de informação nas instituições deve ser avaliado sob vários aspectos, não apenas aquele considerado de má fé, mas principalmente o decorrente de erro humano, uma vez que, sabendo-se que as pessoas manipulam informações institucionais e que o erro é inerente à natureza humana, as informações tornam-se vulneráveis. Sobre esse assunto, Fontes (2006) adverte que o vazamento de informação não ocorre somente ou exclusivamente por meio de má conduta das pessoas, mas ao contrário, 70% ou mais dos problemas ocorrem por situação de erro. Acrescenta ainda o autor que mesmo aqueles funcionários considerados confiáveis podem ter vazado informações importantes, de forma não intencional, como, por exemplo, deixar informações confidenciais em cima de mesas.

Corroborando essa ideia, Silva (2012, p. 24) mostra que não se pode deixar de enfatizar que, além do vazamento de informação realizado de forma intencional, ou seja, aquele praticado com propósito específico ou dolo, existe também o não intencional, causado muitas vezes por imperícia, negligência ou fruto de falha humana, o que ocorre com muito mais frequência. Richard Mogull, analista de segurança da informação do instituto de pesquisa Gartner[17], declara que é preciso observar e conhecer rotinas e procedimentos dentro das próprias empresas. Segundo uma pesquisa realizada pela Gartner, apenas 30% dos ataques são

---

16 *Department for Business, Enterprise and Regulatory Reform* (BERR) - Departamento do Governo do Reino Unido.

17 Empresa de consultoria que trabalha com mais de 10.000 (dez mil) empresas, incluindo executivos da área de TI, nas corporações e órgãos do governo.

provenientes de invasões externas e que cerca de 70% são oriundos de dentro das próprias instituições. Empresas investem milhões para se protegerem do ciberterrorismo e ameaças de *hackers*, mas se esquecem dos fatores humanos, referente à conscientização e capacitação de funcionários, para o caso de alguma ocorrência ou bloqueio de acesso, no tocante a retaliações, que possam prejudicar a companhia (FONTES, 2006, p.144).

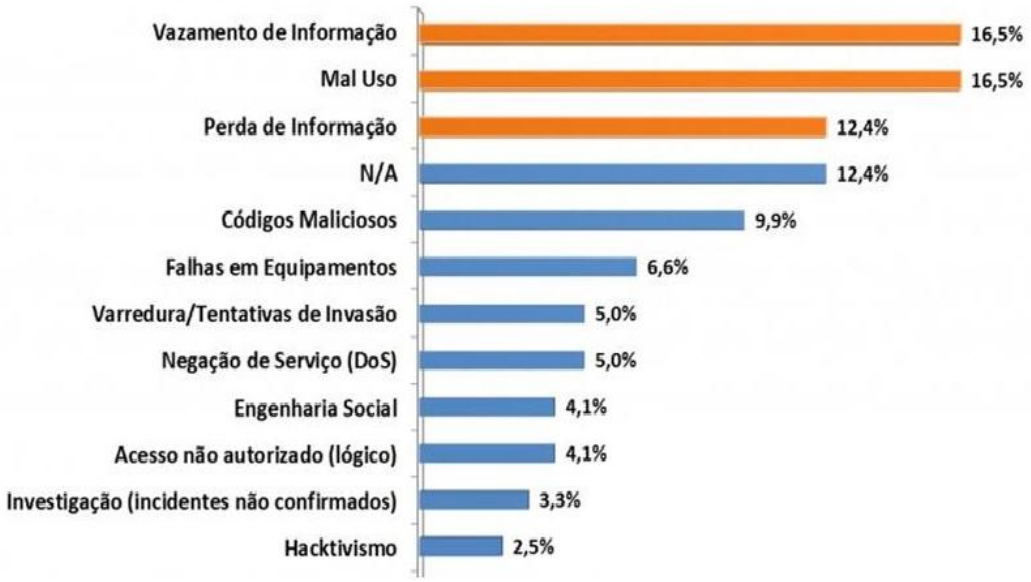
Com relação ao exposto, gerentes de redes relataram, durante a maior conferência da indústria de informática, a DefCon, realizada em Las Vegas, que "funcionários freqüentemente deixam senhas em papéis colados nas máquinas ou debaixo dos teclados e que compartilham códigos de acesso secretos com colegas." (PORTAL TERRA, 2006[18]). Com relação a esse assunto, Mitnick e Simon (2003, p. 256) enfatizam que "sob nenhuma circunstância uma senha pode ser armazenada sob o teclado ou pregada no monitor do computador."

Nesse contexto, muitos dos ataques físicos e virtuais podem ser realizados por um engenheiro social ou por um hacker, mas em sua maioria só podem ser efetivados por funcionários, tais como a divulgação não autorizada de informações sigilosas ou a sabotagem de ativos que apenas os funcionários podem acessar (COLWILL, 2010, p.187, tradução nossa).

O relatório da Pesquisa Nacional de Segurança da Informação, realizada entre maio e julho de 2014 pela DARYUS *Strategic Risk Consulting,* apresenta um panorama do modo como as instituições brasileiras abordam a segurança da informação. No entanto, esse relatório apresenta que para 65% das instituições pesquisadas, a área tecnológica é a responsável majoritária pela segurança da informação (DARYUS, 2014[17]). A Figura 7 evidencia que mais de 40% das falhas relacionadas à segurança não estão associadas às tecnologias, mas sim ao elemento humano e ao modo aos quais os dados, informações e sistemas são utilizados na instituição.

[18] Documento eletrônico não paginado.

Figura 7 - Origem provável dos incidentes



Fonte: Pesquisa Nacional de Segurança da Informação 2014 (DARYUS, 2014[19]).

Muitos são os motivos que levam instituições a se preocuparem com a dimensão humana da segurança da informação, tanto para evitar ataques de engenharia social, quanto para se precaverem contra funcionários mal intencionados, negligentes ou alheios à segurança. A adoção de práticas, procedimentos e tecnologia de segurança de informação não pode ser considerada efetiva, se não abordar os aspectos relacionados ao fator humano. Rocha (2008, p.12) observa que muitos dos incidentes de segurança que aparecem na mídia, em princípio, não teriam sido ocasionados por questões tecnológicas e nem por hackers mal-intencionados. Para ilustrar essa afirmação, destacam-se alguns exemplos transmitidos pela imprensa:

- HSBC suíço escondeu dinheiro suspeito de ditadores e celebridades - Fraudes, que somaram € 180,6 bilhões, transitaram em Genebra nas contas de 100 mil clientes e de 20 mil empresas *offshore*.

Batizada de "*SwissLeaks*", a revelação veio à tona após o ICIJ enviar para mais de 40 veículos de comunicação ao redor do mundo dados secretos levantados

[19] Documento eletrônico não paginado.

pelo técnico de informática Hervé Falciani, ex-funcionário do banco HSBC em Genebra, que estavam em posse da Justiça e órgãos fiscais de diversos países.

> Os documentos são apenas uma parte do que seria o sistema bancário suíço, duramente criticado por autoridades de todo o mundo por permitir a existência de contas secretas, uma espécie de 'buraco negro' no sistema financeiro internacional. (VEJA..., 2015[20]).

Qualquer instituição está passível à situação de vazamento da informação. Na maioria das vezes, o fato acontece com a participação de pessoas que atuam internamente na organização, ou seja, pessoas com autorização para acessar a informação. Infelizmente, algumas pessoas utilizam essa autorização para praticar delitos.

- Polícia Federal confirma vazamento do tema da redação do Enem no Piauí: PF fez perícia em celular que teria recebido tema da redação do Enem.

> O delegado regional de Combate ao Crime Organizado da Superintendência da Polícia Federal (PF) no Piauí, Alexandre Uchôa, afirmou que houve o vazamento do tema da prova de redação do Exame Nacional do Ensino Médio (Enem) de 2014. Segundo o delegado, a foto que um estudante piauiense recebeu horas antes da prova é verídica. O estudante gravou um vídeo mostrando o envelope que os candidatos recebem para guardar o celular lacrado após ter feito a prova. Ao abrir e ligar o aparelho, ele mostrou a imagem da página com o tema da redação sobre 'Publicidade infantil no Brasil'. (ARAÚJO, G., 2014[19]).

- PF vai investigar suposto vazamento de informações da operação Lava Jato

> A Polícia Federal vai realizar uma 'investigação preliminar' para apurar a origem do possível vazamento de informações da sétima fase da operação Lava Jato. A informação foi confirmada pela assessoria de imprensa do órgão nesta quarta-feira (19). A suspeita de vazamento da operação foi apontada pela PF e admitida por advogados de executivos da Engevix na última terça-feira (18). A PF informou que, se entender necessário, pode instaurar inquérito policial para apurar o caso. (PRAZERES, 2014[21]).

- Coca-Cola: condenada secretária por roubo de segredo

[20] Documento eletrônico não paginado.
[21] Documento eletrônico não paginado.

> A ex-secretária da Coca-Cola acusada de roubar segredos da gigante dos refrigerantes e tentar vendê-los à rival Pepsi por US$ 1,5 milhão foi condenada a oito anos de prisão. A sentença foi determinada nesta quarta-feira. Joya Williams, 41 anos, acusava dois cúmplices de terem roubado os documentos sem seu conhecimento. Os dois homens já foram considerados culpados no caso e aguardam sentença, podendo pegar até 10 anos de prisão. De acordo com a Bloomberg, Williams está "desapontada" com a decisão e irá entrar com recurso, segundo sua advogada de defesa, Janice Singer. O procurador Jay Pak afirmou por sua vez que o veredicto - anunciado após três dias de deliberações - foi justo. (PORTAL TERRA, 2007[20]).

Para Fontes (2006, p. 31), dependendo da importância da informação para a instituição e, evidentemente, dependendo do valor que tenha para os concorrentes ou para o mercado, a instituição precisa implementar controles sobre seu uso. Caso contrário, a informação poderá ser disponibilizada indevidamente e haverá impacto financeiro, de imagem ou operacional.

- Fabricante de semicondutores de Taiwan acusa concorrente chinesa de roubar tecnologia patenteada

> Não era incomum Y.L. Wang passar fins de semana na fábrica que ajudava a administrar para a Taiwan Semiconductor Manufatucturin Corp. (TSMC), uma das maiores fabricantes de chips do mundo. Mas nunca tinha visto seu colega C. Y. Shin na fábrica num fim de semana, até aquele sábado de setembro de 2001. Também nunca tinha visto ninguém fazer tantas fotocópias.
> Shih, gerente da divisão de transferência de tecnologia da TSMC, estava debruçado sobre a copiadora naquele final de semana, acumulando pilhas e pilhas de papel. 'Havia pilhas de arquivos cobrindo uma mesa grande', lembrou mais tarde Wang. Uma semana mais tarde, Shih abandonou a empresa para ingressar na Semiconductor Manufactoring Internacional Corp (SMIC), uma promissora empresa com sede em Xangai. Shih foi um entre os mais de 140 funcionários convencidos a sair num período de dois anos desde meados de 2001, e muitos não saíram de mãos vazias. [...] (JORNAL O ESTADO DE S. PAULO, 2005 apud FONTES, 2006, p. 29)

Fontes (2006, p. 29) assinala que, quando se pensa em vazamento de informação, normalmente se esquece que a cópia não autorizada da informação pode ocorrer pela forma mais simples que é o papel. Equivocadamente, as ações de proteção da informação mencionam apenas o envio de arquivos por correio

eletrônico, *pen drives*, gravação de CDs, acesso lógico indevido e outros meios sofisticados.

- Eli Lilly deixa vazar 600 e-mails de pacientes

> Washington – O laboratório farmacêutico Eli Lilly desculpou-se publicamente pelo vazamento do endereço de mais de 600 e-mails de pacientes com depressão, bulimia ou distúrbio compulsivo-obsessivo cadastrados no site da empresa [...]. Entidades civis americanas pedem que seja aberto inquérito para averiguar a quebra da política de privacidade assumida pela empresa. [...]
> O problema surgiu quando um funcionário da Lilly aparentemente sem treinamento enviou um e-mail rotineiro para os clientes, incluindo o endereço de todos no campo "Para:", relevando assim o endereço de cada destinatário aos demais. Para resolver o problema, a empresa concordou em fazer revisões de segurança e conformidade em seu programa de privacidade e lidar com questões envolvendo sigilo de dados com treinamento, além de outras medidas [...] (JORNAL O ESTADO DE SÃO PAULO, 2001[22]).

Infere-se que, a partir do exposto, que muitos dos processos necessários para manter as informações em segurança, em grande medida, dependem do fator humano. Intencionalmente ou por negligência, muitas vezes devido ao desconhecimento, os colaboradores são a maior ameaça à segurança da informação (NIEKERK; SOLMS 2010, p. 476, tradução nossa). Com relação à ocorrência desses erros, Fontes (2006, p. 126) destaca três ações que podem minimizá-los: conscientização dos colaboradores para o conhecimento dos riscos existentes; capacitação para ensinar a forma correta de se utilizar o recurso; e definição de processos para que os controles possam ser implementados e, com isso, aumentar a possibilidade de evitar a ocorrência do erro.

Nesse contexto, Siponen (2001, p. 25, tradução nossa) relata que sem um adequado nível de cooperação e conhecimento, muitas técnicas de segurança são susceptíveis de serem mal utilizadas ou mal interpretadas pelos colaboradores. Corroborando essa ideia, Fontes (2006) afirma que quando os colaboradores conhecem os motivos da relevância da segurança da informação, eles tendem a segui-los para efetivar a proteção das informações, tornando, desse modo, o processo de conscientização uma necessidade constante para alertar os colaboradores sobre a efetiva intenção das medidas de segurança.

[22]Documento eletrônico não paginado.

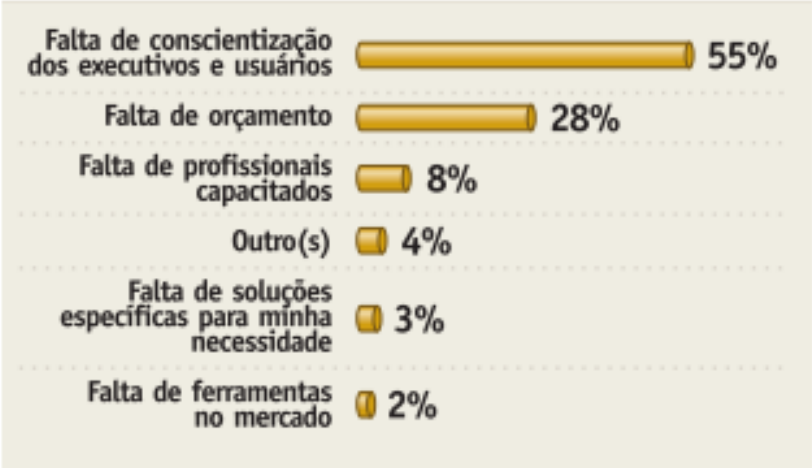
2.3.1 Programa de conscientização

Para Colwill (2010, p. 194, tradução nossa), proteger as informações institucionais é da responsabilidade de todos os colaboradores. A conscientização, formação e sensibilização são, talvez, as maiores medidas não técnicas disponíveis para aumentar a segurança da informação. Medidas e requisitos de segurança precisam ser integrados ao comportamento habitual dos funcionários, por meio de uma política clara e formação pessoal. Muitos dos problemas de ataques internos à segurança provêm da ignorância, ao invés de motivação maliciosa. No entanto, as falhas decorrentes do desconhecimento do funcionário são igualmente perigosas, uma vez que podem causar grandes impactos à instituição. Fontes (2006, p.11) define conscientização como sendo:

> [...] mais do que um simples conhecimento: estar conscientizado em proteção da informação é internalizar os conhecimentos e agir com naturalidade no cumprimento dos regulamentos. Significa que a segurança da informação deve fazer parte do dia-a-dia e não ser considerada um peso em nossas responsabilidades profissionais para com a organização.

Apenas na 10ª Pesquisa Nacional de Segurança da Informação, realizada em 2006, pelo *Módulo Technology for Risk Management*, foi abordada, pela primeira vez, a temática conscientização de funcionários. Entretanto, no resultado do relatório dessa pesquisa, a falta de conscientização dos executivos já aparecia como principal obstáculo à implementação da segurança da informação, conforme apresentado na Figura 8.

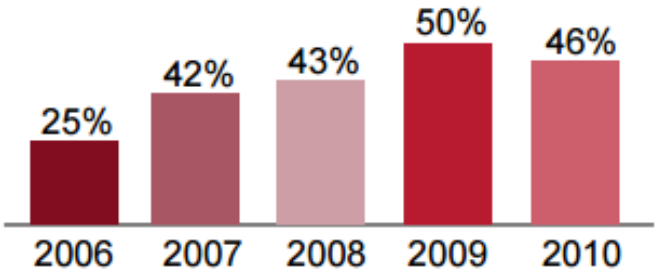
Figura 8 - Principais obstáculos para a segurança da informação



Fonte: 10ª Pesquisa Nacional de Segurança da Informação (MÓDULO TECHNOLOGY FOR RISK MANAGEMENT, 2006, p. 7).

Na Pesquisa Global de Segurança da Informação (Global Stateof Information Security Survey), desenvolvida pela PWC, em 2011, apresenta-se um cenário do comportamento das instituições com relação à conscientização dos funcionários em segurança da informação. Na Figura 9, observa-se o crescimento do número de instituições que possuem programas de conscientização em segurança da informação. Entretanto, identifica-se um decréscimo de 4% em 2010, sendo que o máximo alcançado foi de apenas 50% em 2009, evidenciando que a conscientização ainda é trabalhada de forma incipiente nas instituições.

Figura 9 - Conduz programas de conscientização em segurança da informação



Fonte: Pesquisa Global de Segurança da Informação (PWC, 2011, p. 29).

Ainda nesse sentido, de acordo com o relatório da Pesquisa Nacional de Segurança da Informação, a ação de conscientização mais utilizada por (99,99%) das instituições pesquisadas é o meio eletrônico (*e-mail*), mostrando que, apesar da conscientização ser um importante obstáculo à segurança da informação, as instituições ainda não depreendem esforços suficientes para enfrentar esse

obstáculo (DARYUS, 2014[23]). Como exemplos de ações de conscientização em SI providas por instituições brasileiras destacam-se “Dia da Segurança da Informação”, promovido pelo TCU; a Cartilha de Segurança para Internet, publicada pelo Comitê Gestor da Internet no Brasil (CGI.br); e o “Dia Internacional de Segurança em Informática (DISI)”, promovido pela Rede Nacional de Ensino e Pesquisa (RNP), entre outras iniciativas.

Ressalta-se, ainda, a necessidade de conscientização prévia sobre questões de segurança, sabendo-se que muitas instituições somente se preocupam com essa problemática após vivenciar incidentes no processo de segurança (CARNEIRO, ALMEIDA, 2013, p. 4). Entretanto, não é a forma mais eficiente de abordar a segurança, ao invés disso, as instituições devem conscientizar seus funcionários sobre a importância de manter as informações em segurança de modo a prevenir possíveis incidentes. Nesse contexto, a ABNT NBR ISO/IEC 27002 (2013, p. 15) esclarece que:

> Ao compor um programa de conscientização, é importante não focar apenas no ‘o que’ e ‘como’, mas também no ‘por que’. É importante que, os funcionários entendam os objetivos da segurança da informação e o impacto potencial, positivo e negativo do seu próprio comportamento na organização.

Com isso, os funcionários mudam o seu comportamento com o propósito de proteger as informações de forma mais concreta; isso não implica apenas em aumentar a conscientização dos funcionários, mas incluir valores culturais de segurança à instituição. Sasse *et al*. (2001, p. 129 tradução nossa) frisam que a conscientização pode preparar o ambiente, entretanto a mudança de comportamento exige mudar antigos hábitos e incluir novos por meio de capacitação dos funcionários.

Mitnick e Simon (2003, p. 203) ressaltam a importância de manter os funcionários atualizados sobre como se defender de ataques da engenharia social, por meio de um programa constante de conscientização, uma vez que, para a maioria das pessoas, o aprendizado tende a desaparecer, a menos que seja reforçado periodicamente. Uma das formas de manter a segurança como atividade latente, no cotidiano do funcionário, corresponde a sua inserção como parte

[23] Documento eletrônico não paginado.

específica da função de todas as pessoas que compõem a instituição. Isso possibilita que o funcionário reconheça o seu papel na segurança da instituição. Para os autores:

> Da mesma forma, um programa de conscientização sobre a segurança precisa convencer os empregados que, embora seja importante realizar as tarefas da função dentro do prazo, a tomada de um atalho que não atende aos procedimentos adequados de segurança pode ser prejudicial para a empresa e os colegas. (MITNICK; SIMON, 2003, p. 153).

Corroborando essa ideia, Colwill (2010, p.194-195, tradução nossa) enfatiza que existe a necessidade de conscientização sobre ameaças de segurança reais e vulnerabilidades existentes, como métodos de engenharia social, ou a utilização de fontes não confiáveis, bem como práticas de computação inseguras, de modo a se tornarem ameaças previsíveis, propensas à identificação e comunicação perante atividades maliciosas suspeitas. Assim, é imprescindível que o programa de conscientização abranja todos os funcionários, com o objetivo de assegurar que não haja alegação de desconhecimento quanto às regras de segurança.

Fontes (2006, p. 35, 2012, p. 204) recomenda que, ao contratar um novo funcionário ou prestador de serviço, a instituição deve solicitar ao contratado a assinatura do “termo de responsabilidade e confidencialidade” em que estão descritas suas principais responsabilidades com relação à informação. Além disso, a instituição deve renovar periodicamente esse termo para que haja uma maior conscientização dos funcionários. Geralmente, esse termo registra a responsabilidade do funcionário com relação a: manter o sigilo das informações da organização às quais terá acesso; seguir as normas de segurança da informação; e seguir o padrão ético da organização. Para o autor, essa formalização apresenta ao funcionário suas responsabilidades em conjunto com a instituição, além de fornecer informações referentes ao modo que a instituição deseja que a informação armazenada seja tratada e processada pelos recursos de tecnologia e no ambiente convencional. Em alguns casos, também podem ser descritas as penalidades, caso os procedimentos não sejam cumpridos.

Colwill (2010, p. 194, tradução nossa) esclarece que, para ser realmente eficaz, o processo de conscientização deve desenvolver a capacidade de identificar situações que causam riscos de segurança. Além disso, os funcionários devem estar

cientes do seu papel na proteção da informação, devendo ser capacitados não apenas para identificar riscos proeminentes, como também para possuírem comportamento proativo com relação a esses eventuais riscos. Para tanto, torna-se necessário que todos os funcionários sejam, além de conscientizados, capacitados em segurança da informação com objetivo de garantir o efetivo cumprimento da política e normas de segurança da informação da instituição.

Com relação a esse assunto, Fontes (2012, p. 172) assegura que todos os funcionários devem ser conscientizados e capacitados em segurança da informação, contribuindo como fator positivo no processo de proteção da informação.

2.3.2 Capacitação em segurança da informação

A falta de capacitação dos funcionários em relação à segurança da informação, em muito tem contribuído para os problemas de vazamentos das informações, tanto por meio de ataques de engenharia social como por vazamentos causados por desconhecimento do funcionário em relação às práticas de segurança. Capacitação para esta pesquisa deve ser entendida como “processo permanente e deliberado de aprendizagem, com o propósito de contribuir para o desenvolvimento de competências institucionais por meio do desenvolvimento de competências individuais” (BRASIL, 2006[24])

Nessa perspectiva, Mitnick e Simon (2003, p. 59-60) acrescentam que todas as pessoas são vulneráveis aos ataques da engenharia social e passíveis de falhas em relação aos procedimentos de segurança, entretanto, a única defesa efetiva de uma instituição é educar e capacitar seus funcionários, dando-lhes a prática de que precisam para mitigar possíveis problemas com a segurança.

Para os autores, os funcionários possuem regras e responsabilidades diferentes, sendo que cada cargo tem vulnerabilidades próprias. Desse modo, deve haver um nível básico de capacitação que todos da instituição possam participar e, em seguida, todos os funcionários devem ser capacitados de acordo com as suas atribuições ou o perfil do seu cargo, para seguir determinados procedimentos que minimizem as possibilidades de eventuais ataques ou falhas nos procedimentos de segurança. Por consequência, gerentes, funcionários de TI, usuários de

[24] Documento eletrônico não paginado.

computadores, equipe das áreas não técnicas, assistentes administrativos, recepcionistas, pessoal de segurança e recém admitidos (antes que tenham acesso às informações registradas tanto em suportes tecnológicos como em suporte convencional) carecerão de programas de capacitação adaptados aos requisitos específicos dos diversos grupos dentro da instituição, de modo a atender aos procedimentos de segurança da informação e a política de segurança adotada pela instituição.

Para Fontes (2006, p. 129), quando se tenta implantar um programa de capacitação em segurança da informação, a afirmação mais latente é “nós não possuímos uma cultura de segurança”. Para o autor, as instituições que não perceberem os funcionários como o último obstáculo para alcançar um nível de proteção aceitável estarão fadadas ao fracasso em seus processos de segurança.

Corroborando essa ideia, Silva (2012, p. 69) elenca algumas iniciativas necessárias para disseminar a cultura da segurança dentro das instituições, dentre elas:

- Realizar periodicamente palestras de conscientização;
- Capacitar o novo funcionário nas questões de segurança da informação;
- Enviar lembretes ou avisos importantes de segurança da informação com textos curtos por e-mail;
- Divulgar notícias publicadas na mídia sobre incidentes de segurança da informação ocorridos com outras empresas;
- Criar na *intranet* da instituição um *banner* da área de segurança da informação, no qual possam ser disponibilizadas informações da área;
- Criar os alertas de segurança da informação para os casos de e-mails indesejados e, com isso, combater o *phishingscam*, pois muitas ações de engenharia social fazem uso desses recursos;
- Incluir lembretes e mensagens nos envelopes de pagamento dos funcionários; e
- Criar um canal para críticas, sugestões e reportes para os incidentes de segurança.

Com relação ao programa de capacitação em segurança da informação, Mitnick e Simon (2003, p. 202), elucida que os aspectos do comportamento humano e da engenharia social devem ser abordados. Sublinhando-se:

- A forma como o atacante usa as habilidades da engenharia social para enganar as pessoas;
- Os métodos usados pelos engenheiros;
- Como identificar um iminente ataque da engenharia social;
- Procedimento para o tratamento de uma solicitação suspeita;
- A quem relatar as tentativas da engenharia social ou os ataques bem-sucedidos;
- Questionar todos que fazem uma solicitação suspeita, independentemente do cargo que ocupe;
- Que os funcionários não devem confiar implicitamente nas outras pessoas sem uma verificação adequada;
- A importância de verificar a identidade e a autoridade de qualquer pessoa que faça uma solicitação de informações;
- Procedimentos para proteger as informações confidenciais, entre eles a familiaridade com todo o sistema de classificação de dados;
- A localização das políticas e dos procedimentos de segurança da empresa e a sua importância para a proteção das informações e dos sistemas de informações corporativas;
- Um resumo das principais políticas de segurança e uma explicação do seu significado. Por exemplo, cada empregado deve ser instruído sobre como criar uma senha difícil de adivinhar; e
- A obrigação de cada empregado de atender às políticas e as consequências do seu não-atendimento.

Após a conscientização e capacitação, torna-se necessária a implantação de controles específicos capazes de proporcionar um ambiente de maior segurança dos ativos informacionais da instituição.

2.3.3 Controles e monitoramento

No sentido de proteger os ativos informacionais, torna-se de fundamental importância estabelecer medidas capazes de aumentar a sua segurança. Nesse sentido, deve-se identificar e selecionar os controles que podem ser utilizados para mitigar os riscos a segurança desses ativos. Para Laudon e Laudon (2004, p. 467),

> [...] os controles consistem, portanto, em todos os métodos, políticas e procedimentos organizacionais que garantem a segurança dos ativos da organização, a precisão e confiabilidade de seus registros e a adesão operacional aos padrões administrativos.

Corroborando essa definição, para a norma ISO 27000 (2013, p. 2, tradução nossa), os controles incluem qualquer processo, política, dispositivo, prática ou outras ações que minimizem o risco. Os controles devem assegurar que os riscos sejam reduzidos a um nível aceitável, considerando:

> a) requisitos e restrições da legislação e regulamentos nacionais e internacionais;
> b) os objetivos da organização;
> c) os requisitos operacionais e restrições;
> d) o custo de implantação e operação em relação aos riscos;
> e) que eles devem ser implementados para monitorar, avaliar e melhorar a eficiência e a eficácia dos controles de segurança da informação, de modo a apoiar os objetivos da organização. A seleção e implementação dos controles devem ser documentadas dentro de uma declaração de aplicabilidade para contribuir comos requisitos de conformidade.
> f) a necessidade de equilibrar o investimento na implantação e operação de controles contra a diminuição provável de resultados de incidentes de segurança da informação (ISO 27000, 2013, p. 17, tradução nossa).

Ao selecionar os controles, é necessário mensurar o impacto operacional que estes trarão à instituição. Esses impactos poderão ser manifestados de várias maneiras, como: no alto custo financeiro para implantação, na produtividade, no tempo de resposta e na aceitação dos funcionários. Além da mensuração dos

impactos, os controles precisam ser especificados, implementados, monitorados, revistos e melhorados de forma sistemática, para garantir que os objectivos específicos de segurança da informação e da instituição sejam atendidos. Entretanto, deve-se ter em mente que nenhum conjunto de controles pode alcançar a segurança da informação completa. Ações adicionais de gerenciamento devem ser implementadas para monitorar, avaliar e melhorar a eficiência e a eficácia dos controles de segurança da informação. A seleção e implementação de controles devem ser documentadas dentro de uma declaração de aplicabilidade para ajudar com os requisitos de conformidade (ISO 27000, 2013, p. 13-17, tradução nossa). A ABNT NBR ISO/IEC 27002 (2013) apresenta informações para apoiar e implementar 114 controles, distribuídos em 14 seções de controles. No quadro 9, destacam-se as seções e seus respectivos objetivos.

Quadro 9 - Seções de controles e seus respectivos objetivos

CONTROLES	OBJETIVOS
Política de segurança da informação	Prover uma orientação e apoio da direção para a segurança da informação, de acordo com os requisitos do negócio e com as leis e regulamentações relevantes. Ex.: Política específica para controle de acesso
Organização da segurança da informação	Estabelecer uma estrutura de gerenciamento, para iniciar e controlar a implementação da segurança da informação dentro da organização. Ex.: Estabelecer responsabilidades e papéis pela segurança da informação.
Segurança em recursos humanos	Assegurar que funcionários e partes externas entendam suas responsabilidades e estejam em conformidade com os papéis para os quais eles foram selecionados. Ex.: Conscientizar, educar e treinar os funcionários em segurança da informação.
Gestão de ativos	Identificar os ativos da organização e definir as responsabilidades apropriadas para a proteção dos ativos. Ex.: Classificação de ativos.
Controle de acesso	Limitar o acesso à informação e aos recursos de processamento da informação. Ex.: Procedimento seguro de entrada no sistema (*log-on*).
Criptografia	Assegurar o uso efetivo e adequado da criptografia para proteger a confidencialidade, autenticidade e/ou a integridade da informação. Ex.: Gerenciamento de chaves.
Segurança física e do ambiente	Prevenir o acesso físico não autorizado, danos e interferências com os recursos de processamento das informações e as informações da organização. Ex.: Controle de entrada física, política de mesa lima e tela limpa.

Segurança nas operações	Garantir a operação segura e correta dos recursos de processamento da informação. Ex.: Proteção contra *malware* e cópias de segurança.
Segurança nas comunicações	Garantir a proteção das informações em redes e dos recursos de processamento da informação que os apóiam. Ex.: Acordo de confidencialidade e não divulgação.
Aquisição, desenvolvimento e manutenção de sistemas	Garantir que a segurança da informação é parte integrante de todo o ciclo de vida dos sistemas de informação. Isto também inclui os requisitos para sistemas de informação que fornecem serviços sobre as redes públicas. Ex.: Procedimentos para controle de mudanças de sistemas.
Relacionamento na cadeia de suprimento	Garantir a proteção dos ativos da organização que são acessíveis pelos fornecedores. Ex.: Identificando segurança da informação nos acordos com fornecedores.
Gestão de incidentes de segurança da informação	Assegurar um enfoque consistente e efetivo para gerenciar os incidentes de segurança da informação, incluindo a comunicação sobre fragilidades e eventos de segurança da informação. Ex.: Avaliação e decisão dos eventos de segurança da informação.
Aspectos da segurança da informação na gestão da continuidade do negócio	É recomendado que a continuidade da segurança da informação seja considerada nos sistemas de gestão da continuidade do negócio da organização. Ex.: Planejando a continuidade da segurança da informação.
Conformidade	Evitar violação de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais relacionadas à segurança da informação e de quaisquer requisitos de segurança. Ex.: Identificação da legislação aplicável e de requisitos contratuais.

Fonte: Adaptado da ABNT NBR ISO/IEC 27002 (2013).

Percebe-se, assim, que à gestão da segurança da informação compete realizar atividades coordenadas e eficazes para a implementação de controles adequados à proteção dos ativos de informação, de modo a contribuir para que a instituição alcançe seus objetivos. Desse modo, identificar quais controles devem ser implementados requer um planejamento cuidadoso e atenção aos detalhes. Como exemplo, controles de acesso, que podem ser técnico (lógico), físico (gestão) ou uma combinação de ambos, fornecem um meio de garantir que o acesso aos ativos de informação seja autorizado e restrito com base nos requisitos de segurança informação (ISO 27000, 2013, p. 11-15, tradução nossa).

Posteriormente à implantação dos controles, há a necessidade de estabelecer monitoramento contínuo, por meio de várias formas, como: lembretes aos funcionários sobre o que aprenderam nos cursos de capacitação, o uso de

mensagem de destaque que aparece quando o computador é ligado, entre outras. Quanto ao monitoramento dos sistemas de informação, normalmente é feito por meio de registros de *log*[25], trilhas de auditoria ou outros mecanismos capazes de detectar invasões. De acordo com o Manual de Boas Práticas em Segurança da Informação:

> Esse monitoramento é essencial à equipe de segurança de informações, já que é praticamente impossível eliminar por completo todos os riscos de invasão por meio da identificação e autenticação de usuários. Na ocorrência de uma invasão, falha do sistema ou atividade não autorizada, é imprescindível reunir evidências suficientes para que possam ser tomadas medidas corretivas necessárias ao restabelecimento do sistema às suas condições normais, assim como medidas administrativas e/ou judiciais para investigar e punir os invasores. A forma mais simples de monitoramento é a coleta de informações, sobre determinados eventos, em arquivos históricos, mais conhecidos como *logs*. Com essas informações, a equipe de segurança é capaz de registrar eventos e detectar tentativas de acesso e atividades não autorizadas após sua ocorrência (TCU, 2012, p. 27).

O monitoramento também lida com a necessidade de avaliar a eficácia dos controles de segurança, entre eles, a aplicação das medidas disciplinares quando da violação das políticas e normas implementadas pela instituição.

2.3.4 Penalidades

Para a ABNT NBR ISO/IEC 27002 (2013, p. 13), a direção da instituição deve solicitar a todos os funcionários que pratiquem a segurança da informação. A norma orienta, também, que à direção cabe assegurar que os funcionários:

> a) estão adequadamente instruídos sobre as suas responsabilidades e papéis pela segurança da informação, antes de obter acesso às informações sensíveis ou aos sistemas de informação;
> b) recebam diretrizes que definam quais as expectativas sobre a segurança da informação de suas atividades dentro da organização;
> c) estão motivados para cumprir com as políticas de segurança da informação da organização;

[25] Registros cronológicos de atividades do sistema que possibilitam a reconstrução, revisão e análise dos ambientes e atividades relativas a uma operação, procedimento ou evento, acompanhados do início ao fim (TRIBUNAL DE CONTAS DA UNIÃO, 2012, p. 27).

> d) atinjam um nível de conscientização sobre segurança da informação que seja relevante para os seus papéis e responsabilidades dentro da organização;
> e) cumpram com os termos e condições de trabalho, que incluam a política de segurança da informação da organização e métodos apropriados de trabalho;
> f) tenham as habilidades e qualificações apropriadas e sejam treinados em bases regulares;
> g) tenham disponíveis um canal de notificação, de forma anônima, para reportar violações nas políticas e procedimentos de segurança da informação. (ABNT NBR ISO/IEC 27002, 2013, p. 13).

Diante do exposto, ressalta-se a importância da direção da instituição em apoiar as políticas de segurança e os demais procedimentos dela decorrentes, como: capacitação em SI, eventos de conscientização, implantação de controles e monitoramento. Nesse sentido, se os funcionários não forem conscientizados e capacitados sobre suas responsabilidades em SI, podem causar, por desconhecimento, uma violação na segurança. Entretanto, é necessário que seja formalizado um processo disciplinar para averiguar como a violação ocorreu e garantir aos funcionários suspeitos de cometer a violação um tratamento justo. Para a ABNT NBR ISO/IEC 27002 (2013, p. 15), o processo disciplinar deve levar em consideração fatores como:

> [...] a natureza e a gravidade da violação e o seu impacto no negócio, se este é ou não o primeiro delito, se o infrator foi ou não adequadamente treinado, as legislações relevantes, os contratos do negócio e outros fatores conforme requerido.

Assim, as políticas de segurança da informação devem contemplar "a atribuição de responsabilidades, gerais e específicas, para o gerenciamento da segurança da informação para os papéis definidos." (ABNT NBR ISO/IEC 27002, 2013, p. 2). Ainda nessa direção, o Manual de Boas Práticas em Segurança da Informação esclarece que, dentro da instituição, é de responsabilidade da "própria Política de Segurança de Informações prever os procedimentos a serem adotados para cada caso de violação, de acordo com a severidade, a amplitude e o tipo de infrator que a perpetra" (TCU 2012, p. 13). A punição pode variar desde uma simples advertência verbal ou escrita até uma ação judicial.

Em 14 de julho de 2000 foi instituída a Lei n.º 9.983, que altera o Código Penal Brasileiro. Essa lei prevê penas para os casos de violação de integridade e

quebra de sigilo de sistemas informatizados ou banco de dados da Administração Pública, conforme pode ser observado no Quadro 10:

Quadro 10 - Crimes e penalidades

ARTIGO	CRIME	PENALIDADE
Art. 313-A	Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano	Reclusão, de 2 (dois) a 12 (doze) anos, e multa.
Art. 313-B	Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente. "Parágrafo único. As penas são aumentadas de um terço até a metade se da modificação ou alteração resulta dano para a Administração Pública ou para o administrado."	Detenção, de 3 (três) meses a 2 (dois) anos, e multa.
Art. 153	"§ 1º-A. Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública:"	Detenção, de 1 (um) a 4 (quatro) anos, e multa.
Art. 325	I – permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da Administração Pública.	Reclusão, de 2 (dois) a 6 (seis) anos, e multa.
Art. 325	II – se utiliza, indevidamente, do acesso restrito	Reclusão, de 2 (dois) a 6 (seis) anos, e multa.

Fonte: Adaptado para quadro da Lei n.º 9.983 (BRASIL, 2000[26]).

Assim, entende-se a importância da conscientização dos funcionários quanto à política de segurança da informação da instituição. À medida que a PSI seja de conhecimento de todos os funcionários, não deve ser aceita a alegação de desconhecimento às regras nela estabelecidas para justificar violações. Para o Manual de Boas Práticas em Segurança da Informação (TRIBUNAL DE CONTAS DA UNIÃO, 2012, p. 14), quando for detectada uma violação, é necessária a devida averiguação, uma vez que pode ser em decorrência de um erro, de desconhecimento da PSI, de acidente, de negligência, ou de ação deliberada e

[26] Documento eletrônico não paginado.

fraudulenta. Após essa averiguação, será possível aplicar as correções necessárias, além de possibilitar que as vulnerabilidades identificadas pela equipe de segurança da informação passem a ser consideradas, podendo até incorrer nas alterações na PSI.

3 PROCEDIMENTOS METODOLÓGICOS

Esta seção descreve o percurso metodológico que foi utilizado, por esta pesquisa, para atingir aos objetivos propostos. Assim, serão apresentados: a caracterização da pesquisa, contexto da Progep, universo e amostra da pesquisa, as técnicas de coleta de dados, os procedimentos de coleta dos dados, método de análise dos dados coletados e por fim, a trajetória da pesquisa.

3.1 CARACTERIZAÇÃO DA PESQUISA

Tendo em vista que esta pesquisa objetivou **analisar a dimensão humana no processo de gestão de segurança da informação na Progep/UFPB, sob a ótica das normas do governo federal**, tornou-se necessário estabelecer uma metodologia científica na área de ciências sociais, para o embasamento desta pesquisa. Desse modo, no entendimento de Gil (2012, p. 26), a pesquisa social pode ser considerada como o "processo que, utilizando a metodologia científica, permite a obtenção de novos conhecimentos no campo da realidade social". Realidade social aqui deve ser entendida como todos os aspectos relativos ao homem em seus múltiplos relacionamentos com outros homens e com instituições sociais.

Nesse contexto, a presente pesquisa classificou-se como **pesquisa descritiva**, com **abordagem quali-quantitativa**, e quanto ao método de investigação, foi o **estudo de caso**. Assim sendo, a pesquisa descritiva se deu pela necessidade de atingir os objetivos específicos de identificar os processos informacionais prioritários na Progep/UFPB que devam ser foco de gestão de segurança da informação, e verificar como a dimensão humana é abordada nas ações de gestão de segurança da informação implementadas pela Progep/UFPB. Para Gil (2012, p. 28), a pesquisa descritiva "objetiva descrever as características de determinada população ou fenômeno ou o estabelecimento de relações entre variáveis", aplicando-se, assim, à finalidade desta pesquisa, que foi estudar as características de um grupo específico. De acordo com Triviños (1987, p. 110 -112), os estudos descritivos exigem do pesquisador uma série de informações sobre o que se deseja pesquisar, além de exigir uma precisa delimitação de técnicas, métodos e teorias que orientarão a coleta e interpretação dos dados.

A escolha pela abordagem quali-quantitativa mostrou-se necessária, visto que para analisar as informações obtidas pelos instrumentos de coleta de dados utilizados, necessitou-se da integração das duas abordagens. Nesse sentido, Richardson (2009, p. 89) esclarece que a pesquisa social deve estar orientada à melhoria das condições de vida de uma população. Para tanto, é necessário, na medida do possível, integrar métodos, abordagens e técnicas para enfrentar esse desafio (RICHARDSON, 2009, p. 89).

Quanto ao método, classificou-se como estudo de caso, uma vez que se trata de um estudo em instituição pública. Concernente a isso, Vergara (2006, p. 49) entende o estudo de caso como "um circunscrito a uma ou poucas unidades, entendidas como família, empresa, órgão público, comunidade ou país, tendo um caráter de profundidade e detalhamento". Para Yin (2001, p. 19), os estudos de casos representam uma importante estratégia quando o pesquisador coloca questões do tipo "como" e "por que", e quando o foco da pesquisa se encontra em fenômenos contemporâneos inseridos em um contexto real. Müller (2007, p. 49) considera, como uma das vantagens do estudo de caso, a possibilidade de as informações serem coletadas mediante vários instrumentos, como: observação participante, entrevistas, questionários, pesquisa documental, pesquisa etnográfica e o grupo focal, dentre as quais adotamos a observação participante, o questionário e a pesquisa documental.

3.2 CONTEXTUALIZAÇÃO DA PRÓ-REITORIA DE GESTÃO DE PESSOAS

A Universidade Federal da Paraíba (UFPB) foi criada em 1955, como Universidade da Paraíba, por meio da Lei estadual nº. 1.366, de 02.12.55. Inicialmente, seu surgimento deve-se à junção de algumas escolas superiores. Posteriormente, com a sua federalização, aprovada e promulgada pela Lei nº. 3.835 de 13 de dezembro de 1960, transformou-se em Universidade Federal da Paraíba, incorporando as estruturas universitárias das cidades de João Pessoa e Campina Grande. Em 1980, foram incorporados mais três *campi: a* Faculdade de Direito, na cidade de Sousa; Escola de Veterinária e de Engenharia Florestal, na cidade de Patos, e Faculdade de Filosofia, na cidade de Cajazeiras. Em 2002, a UFPB passou pelo desmembramento de quatro *campi*, localizados nas cidades de Campina Grande, Cajazeiras, Patos e Sousa. A Lei nº. 10.419 de 9 de abril de 2002 criou, por

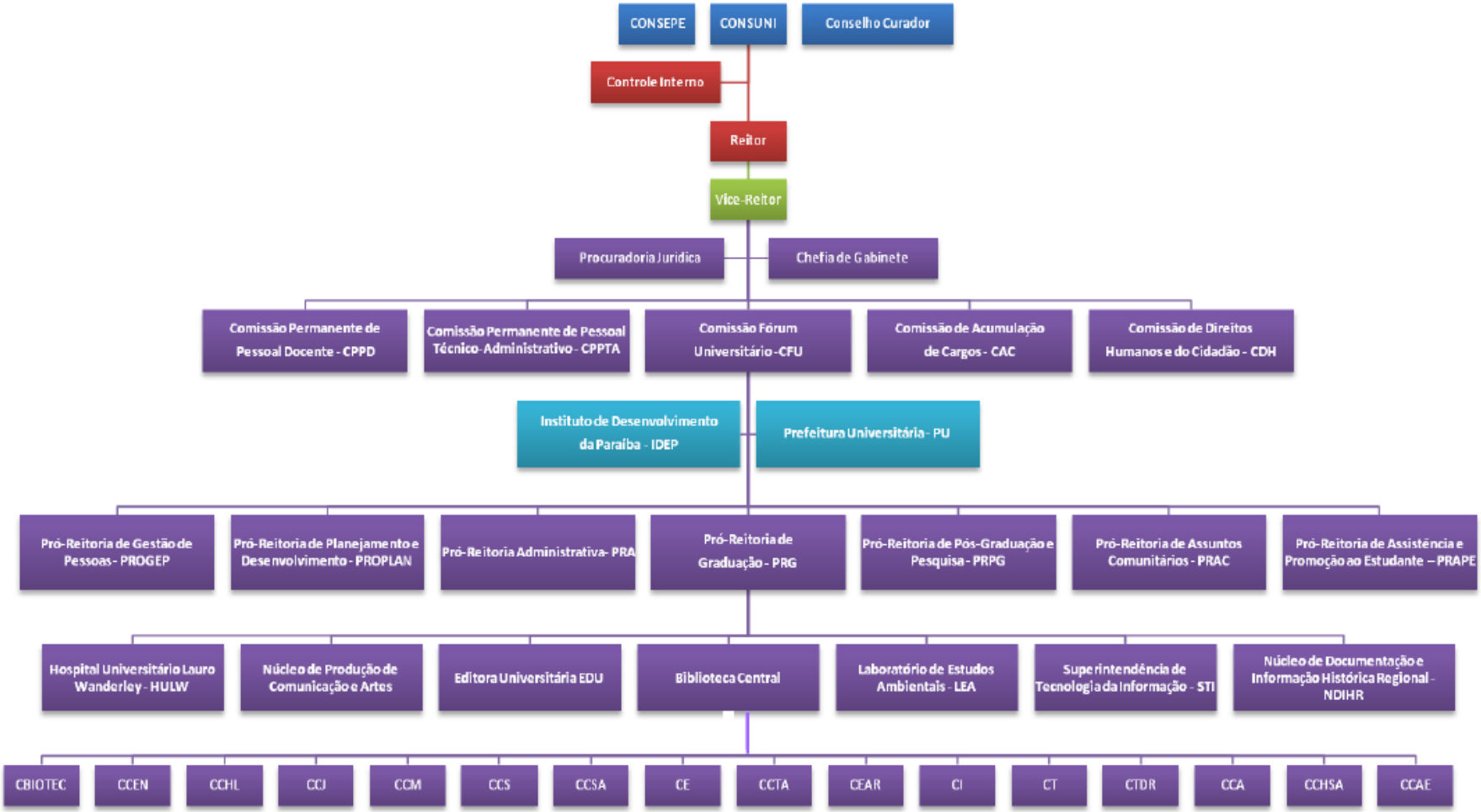
desmembramento da UFPB, a Universidade Federal de Campina Grande (UFCG), com sede e foro na cidade de Campina Grande. A UFPB ficou composta legalmente, a partir de então, pelos *campi* de João Pessoa (capital), Areia e Bananeiras. Posteriormente foi criado um *campus*, no Litoral Norte do Estado, abrangendo os municípios de Mamanguape e Rio Tinto (PDI 2014-2018, UFPB, 2015, p. 3).

Concernente aos *campi* e aos centros, a UFPB está estruturada da seguinte forma: *Campus* I, na cidade de João Pessoa, compreendendo os seguintes Centros: Centro de Ciências Exatas e da Natureza (CCEN); Centro de Ciências Humanas, Letras e Artes (CCHLA); Centro de Ciências Médicas (CCM); Centro de Ciências da Saúde (CCS); Centro de Ciências Sociais Aplicadas (CCSA); Centro de Educação (CE); Centro de Tecnologia (CT); Centro de Ciências Jurídicas (CCJ), Centro de Biotecnologia (CBIOTEC), Centro de Comunicação, Turismo e Artes (CCTA), Centro de Energias Alternativas e Renováveis (CEAR), Centro de Informática (CI) e Centro de Tecnologia e Desenvolvimento Regional (CTDR); *Campus* II*,* na cidade de Areia, compreendendo o Centro de Ciências Agrárias (CCA); o *Campus* III, na cidade de Bananeiras, abrangendo o Centro de Ciências Humanas, Sociais e Agrárias (CCHSA) e o *Campus* IV, nas cidades de Mamanguape e Rio Tinto, com o Centro de Ciências Aplicadas e Educação (CCAE).

De acordo com o Relatório de Gestão, a UFPB é composta, além dos 16 centros, por sete pró-reitorias, quatro conselhos, 45.067 alunos, 2.568 docentes, 2.739 servidores técnico-administrativos[27], 139 cursos de graduação (sendo 130 presenciais e 09 à distância), 106 cursos de pós-graduação, duas escolas de ensino médio e profissionalizante, dentre outras unidades e critérios quantificáveis (UFPB, 2013, p. 2-3). Para demonstrar a atual estrutura organizacional da instituição pesquisada, na Figura 11 observa-se o organograma funcional da UFPB.

[27] Esse número exclui os 995 servidores do Hospital Universitário Lauro Wanderley.

Figura 10 - Organograma Institucional da UFPB



Fonte: Plano de Desenvolvimento Institucional 2014-2018 (UFPB, 2015, p. 81).

Considerando a necessidade de adequar-se ao Decreto nº 3.505, de 13 de junho de 2000, que institui a política de segurança da informação nos órgãos e nas entidades da Administração Pública Federal, em 22 de outubro de 2014 a UFPB publicou sua Política da Segurança da Informação (PSI), por meio da Resolução 32/2014. A Política de Segurança da UFPB possui os seguintes objetivos:

> I. Definir o escopo da segurança da informação da UFPB;
> II. Orientar as ações de segurança com intuito de reduzir riscos e garantir a confidencialidade, integridade e disponibilidade dos ativos de TI da UFPB;
> III. Incentivar o uso de soluções integradas de segurança;
> IV. Servir de referência para auditoria, apuração e avaliação de responsabilidade. (UFPB, 2014[28]).

De acordo com o Art. 5º, a Política de Segurança da Informação da UFPB abrange os seguintes aspectos:

> I. Requisitos de segurança criptográficos [...];
> II. Requisitos de segurança no manuseio e tratamento de informação: define padrões e princípios relacionados ao manuseio de informações, o que inclui inventários, administração e propriedade sobre dados, eliminação e remoção de informação, informações disponíveis em mesas de trabalho, telas de computador, material impresso etc.
> III. Requisitos de segurança de redes e dispositivos móveis [...];
> 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, controle, responsabilidades sobre senhas, contas de usuários, uso de correio eletrônico, relato de incidentes de segurança da informação e falhas de software;
> V. Requisitos de segurança contratual e acordo de nível de serviço: define padrões e princípios relacionados à manutenção da segurança dos ativos de TI que são acessados ou fornecidos por terceiros;
> VI. Requisitos de segurança em recursos humanos: define padrões e princípios de segurança relacionados às ações realizadas por eventos ocorridos com servidores (docentes e técnico-adminstrativos), gestores, pessoal em cargos de chefia, estagiárias, tais como procedimentos a realizar quando um servidor é exonerado, quando sofre relotação, quando está em licença etc.;
> VII. Requisitos de segurança em gestão de *software* [...]
> VIII. Requisitos de segurança para aquisição de ativos de TI [...] (UFPB, 2014[26]).

[28] Documento eletrônico não paginado.

Instituída dentre as sete pró-reitorias da UFPB, a Progep foi criada pela Resolução Nº 28/2010, e encontra-se diretamente subordinada à Reitoria. De acordo com seu Regimento Interno:

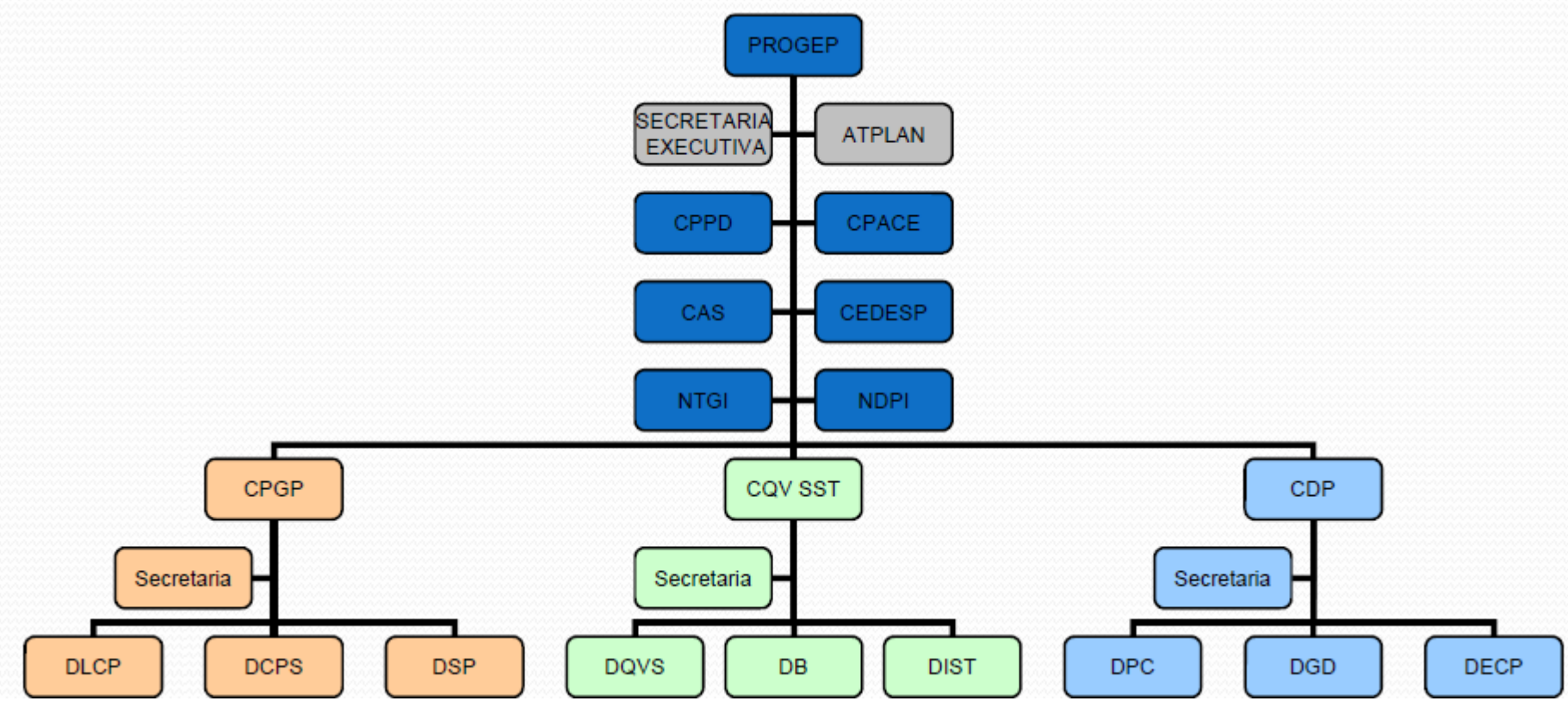
> Progep é o órgão responsável pelo planejamento e acompanhamento das estratégias e políticas de gestão de pessoas da Universidade, como também pela coordenação e acompanhamento da implantação do Plano de Desenvolvimento Institucional e das deliberações dos Conselhos Superiores da UFPB. (UFPB, 2012, p. 2).

Concernente às competências, o Regimento Interno da Progep no seu Art. 3º, apresenta:

> I - propor políticas de gestão de pessoas para os servidores da UFPB;
> II - estabelecer diretrizes estratégicas para orientar as ações das unidades administrativas inerentes à gestão de pessoas;
> III - promover ações para a melhoria da qualidade de vida, saúde e segurança no trabalho;
> IV - estabelecer diretrizes para o dimensionamento do quadro de servidores docentes e técnico-administrativos;
> V - propor programas de educação e capacitação profissional;
> VI - estabelecer um sistema de gerenciamento e controle de processos de gestão de pessoas;
> VII - consolidar o sistema de gestão do desempenho dos servidores docentes e técnico-administrativos;
> VIII - assessorar o Reitor nos assuntos de gestão de pessoas no âmbito da UFPB. (UNIVERSIDADE FEDERAL DA PARAÍBA, 2012, p. 2).

Assim, a Pró-Reitoria de Gestão de Pessoas da UFPB atualmente é composta por 138 servidores, divididos nas diversas coordenações, divisões e seções como ilustra a Figura 12.

Figura 11 - Organograma da Progep



Fonte: Relatório de 2013 da Progep[29] (UFPB, 2013).

[29] O Quadro com a definição das Siglas encontra-se no APÊNDICE A.

Nesse sentido, infere-se que estudar a dimensão humana das ações de gestão de segurança da informação poderá contribuir para Progep e para toda universidade, uma vez que servidores mais conscientes sobre o tema possibilitará estabelecer ambientes de maior segurança para as informações que estão sobre sua responsabilidade, além de multiplicar ações de gestão de segurança para as demais unidades que compõem a UFPB.

3.3 UNIVERSO E AMOSTRA DA PESQUISA

O universo da pesquisa consiste no conjunto de elementos que possuem determinadas características (RICHARDSON, 2009, p. 157; GIL, 2012, p. 89). Assim, o universo desta pesquisa foi constituído pelos **21 gestores** que compõem a Pró-Reitoria de Gestão de Pessoas da Universidade Federal da Paraíba.

Concernente à amostra, Vergara (2006, p. 50) esclarece que a "amostra é parte do universo escolhido, seguindo algum critério de representatividade". Nesse sentido, compõe como amostra desta pesquisa os diretores das divisões que integram a Progep, a saber: Divisão de Benefícios (DB), Divisão de Cadastro e Pagamento de Servidores (DCPS), Divisão de Educação e Capacitação Profissional (DECP), Divisão de Gestão de Desempenho (DGD), Divisão de Segurança do Trabalho (DIST), Divisão de Legislação e Controle de Processos (DLCP), Divisão de Planejamento e Carreira (DPC), Divisão de Qualidade de Vida (DQVD) e Divisão de Seleção e Provisão (DSP), totalizando **nove gestores da Progep.**

Com relação ao critério de escolha dos sujeitos, foi considerada a amostragem por tipicidade ou intencional, ou seja, "não probabilística e que, com base nas informações disponíveis, possa ser considerada representativa de toda população" (GIL, 2012, p. 94). A intenção de composição da amostra decorre do fato que pelos sujeitos selecionados perpassam grande parte dos processos informacionais gerados ou que transitam pela Progep. Nessa direção, segundo Fontanella, Ricas e Turato (2008, p. 20) o que há de mais significativo nas amostras intencionais não se encontra na quantidade de seus sujeitos, mas na maneira como se concebe a sua representatividade e na qualidade das informações obtidas deles.

A escolha pela Progep deu-se por ser o setor responsável pelo planejamento e acompanhamento das estratégias e políticas de gestão de pessoas; pelos programas de educação e capacitação profissional, uma vez que esta pesquisa está

fortemente ligada ao processo de conscientização e capacitação sobre segurança da informação; e pela diversidade de processos informacionais que transitam nessa Pró-Reitoria, possibilitando captar a percepção dos diretores como usuários da informação e como gestores que podem preparar o ambiente organizacional para criação de uma cultura de segurança.

3.4 TÉCNICA DE COLETA DE DADOS

Para atingir aos objetivos desta pesquisa, foi utilizada a triangulação das informações obtidas por meio do questionário, observação participante e pesquisa documental. Para Minayo, Assis e Souza (2010, p. 28) a triangulação de métodos é a visão de vários informantes e o emprego de uma variedade de instrumentos de coleta de dados que acompanha o trabalho de investigação. Nesse sentido, Azevedo *et. al* (2013, p. 4) esclarecem que a triangulação pode combinar métodos e fontes de coleta de dados qualitativos e quantitativos (entrevistas, questionários, observação e notas de campo, pesquisa documental, dentre outras). Para os autores, a triangulação enriquece a compreensão, permitindo emergir em novas ou mais profundas dimensões.

Assim, para alcançar o primeiro objetivo específico, verificar as orientações legais aplicadas à gestão de segurança da informação na Progep, foi utilizada como instrumento de coleta de dados a **pesquisa documental**. Segundo Chizzotti (1991, p. 109), documento pode ser definido como:

> [...] qualquer informação sob a forma de textos, imagens, sons, sinais etc., contida em um suporte material (papel, madeira, tecido, pedra), fixados por técnicas especiais como impressão, gravação, pintura, incrustação etc. Quaisquer informações orais (diálogo, exposições, aula, reportagens faladas) tornam-se documentos quando transcritas em suporte material.

A noção de documento corresponde a uma informação organizada sistematicamente, comunicada de diferentes maneiras (oral, escrita, visual ou gestualmente) e registrada em material durável. A pesquisa documental recorre a materiais que ainda não receberam tratamento analítico, tais como: documentos oficiais, reportagem de jornais, contratos, relatórios, entre outros (GIL, 2012, p. 51; GONÇALVES, 2001, p. 32). Nesse sentido, para atender ao objetivo específico

supracitado, foram utilizados documentos registrados de diversas formas, como: resoluções, políticas e relatórios internos à UFPB; Decretos, Instruções Normativas, Leis, Cartilhas e Normas da Administração Pública Federal; além de imagens e outros documentos que substanciaram a pesquisa no que concerne à gestão da segurança da informação.

Outro instrumento de coleta de dados utilizada foi a **observação participante.** O fato de a pesquisadora pertencer ao quadro pessoal de servidores da Progep contribuiu na escolha do referido instrumento de coleta de dados. Nesse sentido, para Minayo (2009, p. 70-71), na convivência com o grupo, o observador pode compreender aspectos que vão aflorando aos poucos, além de poder vincular os fatos às suas representações e a desvendar as contradições entre as normas e regras e as práticas vividas cotidianamente pelo grupo ou instituição observada. A autora define observação participante como:

> [...] um processo pelo qual um pesquisador se coloca como observador de uma situação social, com a finalidade de realizar uma investigação científica. O observador, no caso, fica em relação direta com seus interlocutores no espaço social da pesquisa, na medida do possível, participando da vida social deles, no seu cenário cultural, mas com finalidade de colher dados e compreender o contexto da pesquisa. Por isso, observador faz parte do contexto, pois interfere nele, assim como é modificado pessoalmente (MINAYO, 2009, p. 70).

Nesse sentido, a observação pode registrar muitos fenômenos importantes que não podem ser registrados por meio de perguntas ou em documentos quantitativos, mas podem ser observados *in loco,* na situação concreta em que os fatos acontecem como é o caso da rotina de um dia de trabalho (MINAYO, 2009, p. 71-72). Assim, a observação participante auxiliou a cumprir o objetivo específico de verificar como a dimensão humana é abordada nas ações de gestão de segurança da informação implementadas pela Progep/UFPB. Foi utilizado, também, um questionário composto de perguntas fechadas e abertas. Para Richardson (2009, p. 189) o questionário é uma série ordenada de perguntas que pode ser utilizado para obter informações acerca de grupos sociais, cumprindo pelo menos duas funções: descrever as características e medir determinadas variáveis de um grupo social.

Nesta pesquisa, o questionário com os gestores possibilitou alcançar os objetivos específicos de identificar os processos informacionais prioritários que

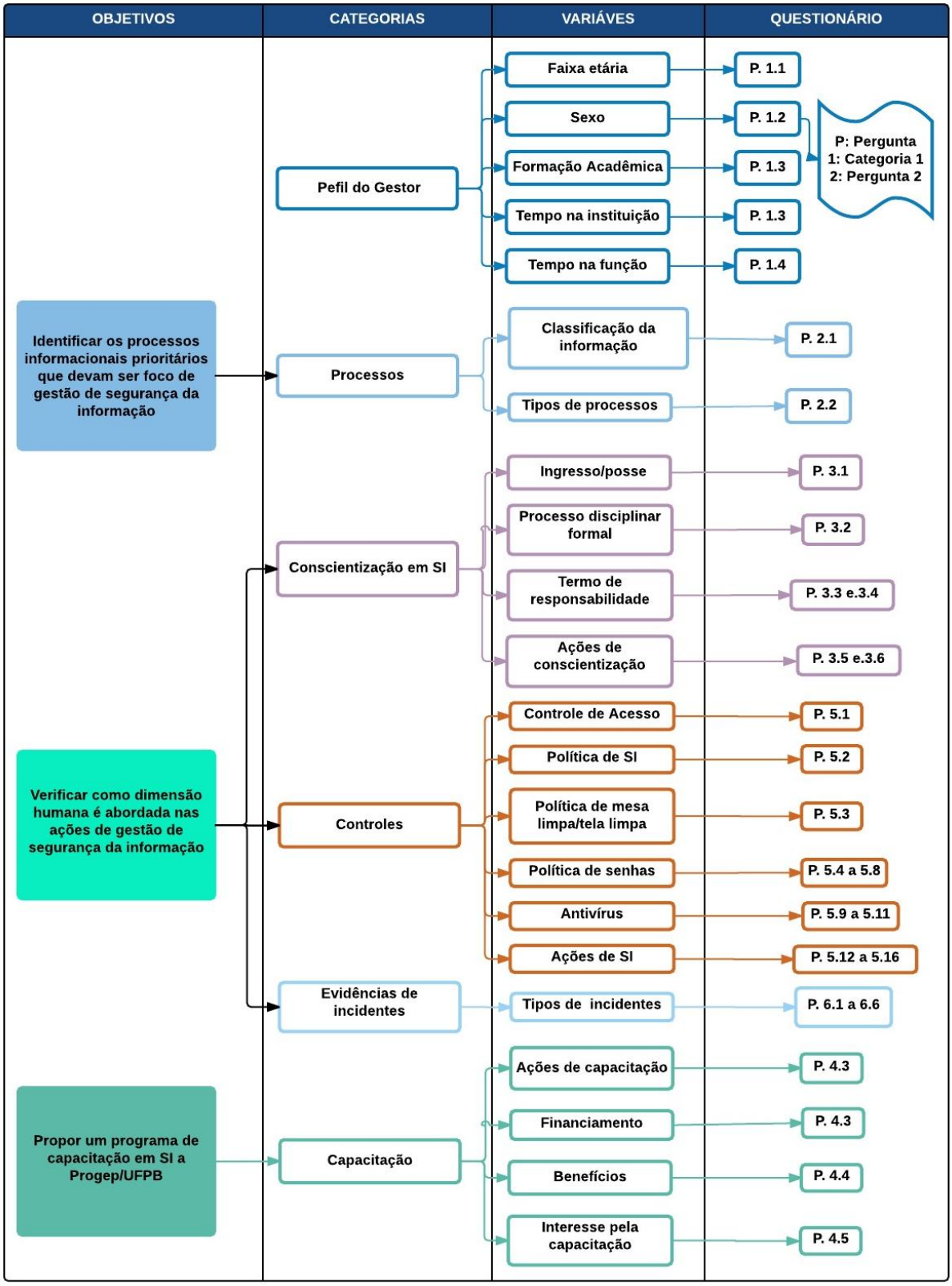
devam ser foco de gestão de segurança da informação e verificar como a dimensão humana é abordada nas ações de gestão de segurança da informação implementadas pela Progep/UFPB [30].

O questionário foi desenvolvido com base no aporte teórico que envolve a pesquisa, nos objetivos específicos, nas variáveis e nas categorias construídas. O termo variável aqui é entendido como características observáveis do fenômeno a ser estudado, existentes em todos os tipos de pesquisa. No entanto, enquanto nas pesquisas quantitativas elas são medidas, nas qualitativas elas são descritas ou explicadas. As variáveis têm características sociais, econômicas, ideológicas, demográficas, estatísticas, matemáticas, mercadológicas, entre outras. (LAKATOS; MARCONI, 2007, p. 139). Por categorias entende-se que são “as rubricas ou classes, as quais reúnem um grupo de elementos sob um título genérico, agrupamento esse efetuado em razão de características comuns destes elementos” (BARDIN, 2008, p. 145). Para definição das categorias, a pesquisa foi subsidiada pelo modelo misto de organização de categorias, que consiste na seleção de categorias ao início da pesquisa (fundamentada no referencial teórico, nos objetivos da pesquisa e na experiência da pesquisadora), entretanto, essas categorias não permanecem rígidas, podendo sofrer mudanças no decorrer da análise (LAVILLE; DIONNE, 1999, p. 222).

A Figura 12 demonstra a relação dos objetivos específicos com as categorias, variáveis e as perguntas que compõem o questionário.

[30] A aplicação apenas da observação participante não atingiria esse objetivo.

Figura 12 - Relação dos objetivos com as categorias, variáveis e o questionário



Fonte: Elaborado pela autora (2015).

O questionário (Apêndice B) foi composto de 40 questões, 12 possibilitaram aos gestores responderem de forma subjetiva, e uma das questões (P.2.1) foi direcionada a cada Divisão em particular, uma vez que se tratava dos processos específicos de cada uma delas. Em algumas questões objetivas do questionário foi utilizada a escala do tipo *Likert com cinco pontos*, onde o participante da pesquisa manifesta o seu grau de concordância desde o discordo totalmente (nível 1), até ao concordo totalmente (níveis 5) (CUNHA, 2007, p. 24).

3.5 PROCEDIMENTOS DE COLETA DE DADOS

Após a aprovação da pesquisa pelo Comitê de Ética do Centro de Ciências da Saúde (Anexo A) da UFPB, iniciou-se a realização do pré-teste com seis servidores da Progep, selecionados por serem ex-diretores ou por participarem efetivamente das decisões gerenciais, no período de 27 de outubro a 2 de novembro de 2015. Para Richardson (2009, p. 202) pré-teste é a aplicação prévia do questionário a um grupo com as mesmas características da amostra da pesquisa, permitindo corrigir possíveis falhas das questões formuladas e acrescentar novas questões ao instrumento.

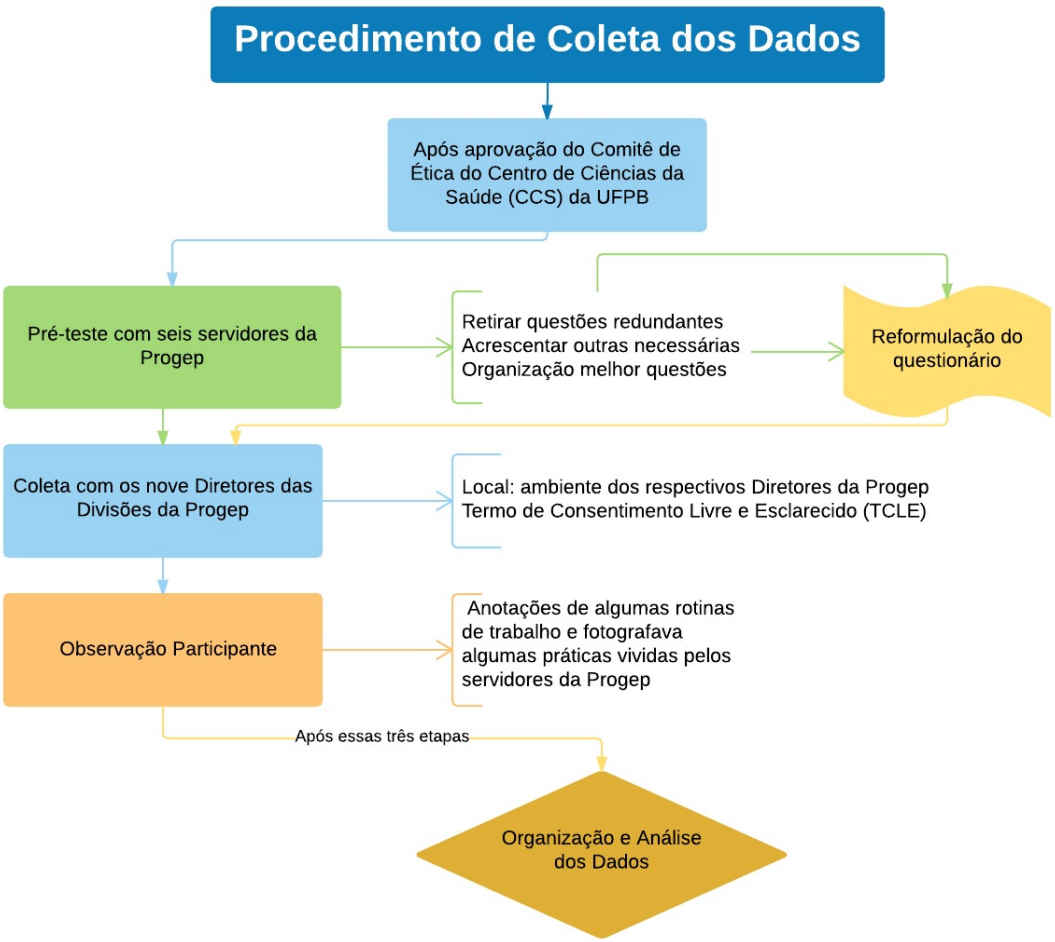
De posse das respostas, percebeu-se que o questionário necessitava passar por modificações para maior clareza, como retirar questões redundantes e acrescentar outras necessárias para atingir os objetivos da pesquisa. O pré-teste foi relevante também para a organização das questões, uma vez que a temática segurança da informação ainda é desconhecida por muitos, exigindo que as questões se apresentassem de forma mais detalhada.

Após a reformulação do questionário, iniciou-se a coleta com os nove Diretores das Divisões da Progep, no período de 4 a 15 de novembro de 2015. As respostas ao questionário aconteceram no ambiente dos respectivos Diretores da Progep com a presença da pesquisadora, momento em que foi esclarecido sobre a pesquisa e assinado o Termo de Consentimento Livre e Esclarecido (TCLE) (Apêndice C). No decorrer da coleta, os nove gestores foram atenciosos e prestativos, colaborando com a pesquisa.

Durante o período do pré-teste e da coleta dos dados, a pesquisadora realizou a observação participante, fazendo anotações das rotinas de trabalho e fotografando algumas práticas vividas pelos servidores da Progep, contribuindo para

atingir os objetivos desta pesquisa. O resumo dos procedimentos de coleta encontra-se ilustrado na Figura 13.

Figura 13 - Procedimento de coleta dos dados



Fonte: Elaborado pela autora (2015).

3.6 ANÁLISE DE CONTEÚDO

Para análise dos dados a partir da triangulação das informações obtidas por meio do questionário, observação participante e pesquisa documental, utilizou-se a Análise de Conteúdo (AC) que, para Valentim (2005, p. 124) é um dos diferentes métodos aplicados à pesquisa científica na área de Ciência da Informação. Para Bardin (2008, p. 20-21), qualquer comunicação, isto é, qualquer transporte de significação de emissor para um receptor controlado ou não, pode ser susceptível de análise do conteúdo. Nesse sentido, para análise dos dados dessa pesquisa foi utilizado o método de AC, que, segundo Bardin (2008, p.37), é entendida como:

> Um conjunto de técnicas de análise das comunicações, visando obter por procedimentos sistemáticos e objetivos de descrição do conteúdo das mensagens, indicadores (quantitativos ou não) que permitam a inferência de conhecimentos relativos às condições de produção/ recepção (variáveis inferidas) dessas mensagens. (BARDIN, 2008, p. 37).

A AC permite caminhar na descoberta do que está por trás dos conteúdos manifestos, indo além da aparência do que está sendo comunicado (MINAYO, 2009, p. 84). Em 2006, a autora já destacava que:

> Os pesquisadores que buscam a compreensão dos significados no contexto da fala, em geral, negam e criticam a análise de freqüência das falas e palavras como critérios de objetividade e cientificidade e tentam ultrapassar o alcance meramente descritivo da mensagem, para atingir, mediante inferência, uma interpretação mais profunda. (MINAYO, 2006, p. 307).

Assim, a presente pesquisa teve como aporte, para análise de seus dados, as características metodológicas da AC defendidas por Richardson (2009, p. 223-224): objetividade, sistematização e inferência. O autor refere-se à objetividade como sendo a explicitação das regras e procedimentos tomados pelo pesquisador em cada etapa do processo de AC. A objetividade implica em descrições que se baseiam em um conjunto de normas que foram seguidas para minimizar a subjetividade do pesquisador, diante de decisões que tomou durante toda a pesquisa. Já a sistematização trata da inclusão ou exclusão do conteúdo conforme regras consistentes e sistemáticas a partir da averiguação de todo o conteúdo disponível, categorizando de forma objetiva o material que foi trabalhado. E, por fim, a inferência permitiu fazer as considerações mais aprofundadas da análise do conteúdo, com base em relações com outras proposições aceitas como verdadeiras.

A escolha pela AC, como método de análise de dados, deu-se pela sua natureza científica, uma vez que compreende melhor um discurso, aprofunda-se em suas características e extraem os momentos mais importantes, além de permitir ao pesquisador abordar uma diversidade de objetos de investigação como atitudes, valores, representações, mentalidades, entre outros. Para tanto, baseou-se em teorias consistentes que serviram de explicação para as indagações do pesquisador (RICHARDSON, 2009, p. 224; LAVILLE, DIONNE, 1999, p. 214).

Laville e Dionne (1999, p. 216) não consideram a AC um método rígido no sentido de engessamento de suas etapas. Ele constitui-se como um conjunto de trilhas possíveis para revelação ou para reconstrução do sentido de um conteúdo. Nessa perspectiva, a análise dos dados da pesquisa se desenvolveu em três fases, que se organizaram cronologicamente (BARDIN, 2008, p. 121; RICHARDSON, 2009, p. 230).

1. A pré-análise;
2. A exploração do material; e
3. O tratamento dos resultados obtidos, a inferência e a interpretação.

A etapa de pré-análise foi composta por atividades não estruturadas e teve como objetivo operacionalizar e sistematizar as ideias, elaborando um esquema preciso de desenvolvimento do trabalho (RICHARDSON, 2009, p. 231). Esta fase envolveu as seguintes etapas:

a) Leitura flutuante: Consistiu em estabelecer os primeiros contatos com o material selecionado para análise no sentido em que se pudesse conhecer a estrutura da narrativa, apresentando-se como as primeiras impressões e orientações em relação às mensagens analisadas.
b) Escolha dos documentos: Etapa em que o pesquisador definiu o corpus da pesquisa, ou seja, o conjunto de documentos considerados para serem submetidos aos procedimentos analíticos e análise (BARDIN, 2008, p. 122). Para esta pesquisa, os documentos selecionados foram todos os questionários, bem como as informações obtidas na observação participante. Para tanto, seguiu-se as regras propostas por Bardin (2008, p. 122) que são: exaustividade, não deixando de fora qualquer questionário ou informações obtidas da observação participante; representatividade, a amostra foi composta por todos os diretores da Progep; homogeneidade, os questionários continham o mesmo conteúdo e foram aplicados por técnicas idênticas a sujeitos semelhantes, e; pertinência, porque os documentos, enquanto fontes de informação, coadunam com os objetivos da análise.
c) Formulação dos objetivos: Nesta etapa, trabalhou-se com os objetivos desta pesquisa, os quais nortearam as leituras e documentos a serem analisados.

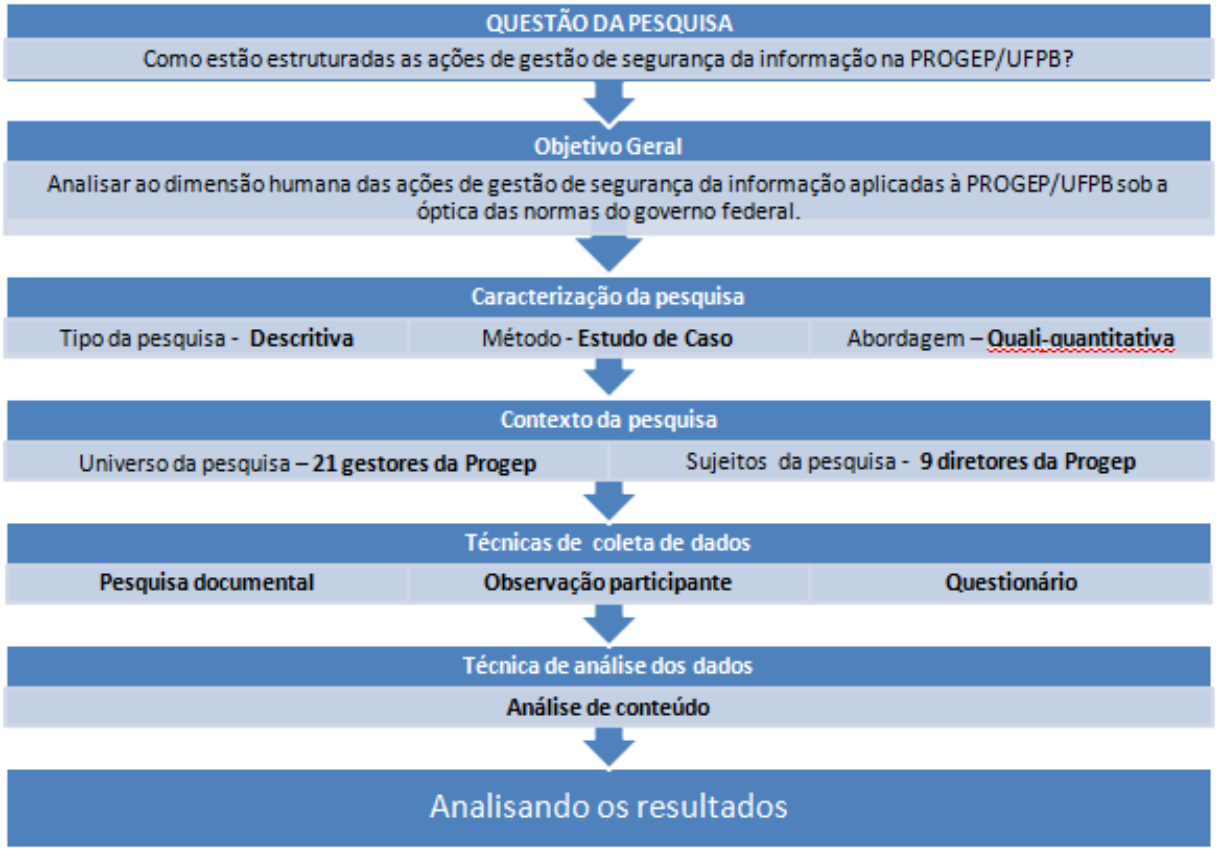
d) Referenciação dos índices: Utilizaram-se os índices para classificar algumas respostas ao questionário. Por exemplo, na categoria 3, para a resposta a questão 3.5 “quais ações de conscientização em segurança da informação que a Progep desenvolve”, a resposta “reuniões” foi classificada como um índice. A frequência deste índice é a quantidade de vezes que os sujeitos citaram o índice “reuniões” como resposta.

Preparação do material: Antes da análise propriamente dita, o material reunido foi preparado. Nesta pesquisa, as respostas objetivas do questionário foram organizadas em gráficos, utilizando o programa *GraphPad Prism* 5 (*GraphPad Software Inc*., San Diego, CA, EUA) para a elaboração dos gráficos de frequência, e as respostas subjetivas foram transcritas e organizadas em quadros, a identificação das respostas foi representada pela letra “S”, seguindo a ordem de resposta de cada pergunta do questionário, preservando a identidade do respondente. As informações e as fotografias obtidas por meio da observação participante foram organizadas de acordo com as categorias a que pertenciam.

A segunda etapa refere à exploração do material selecionado. Essa etapa consistiu essencialmente na codificação e categorização das informações. Entende-se por codificação, o processo pelo qual os dados em estado bruto são sistematicamente transformados e agrupados em unidades que permitem uma descrição exata das características relevantes do conteúdo (RICHARDSON, 2009, p. 233). Nesta pesquisa a categorização foi realizada previamente, baseada no modelo misto de organização de categorias expresso por Laville e Dionne (1999, p. 219).

A terceira etapa - consistiu no tratamento dos resultados obtidos, a inferência e a interpretação - corresponde a fazer inferências e interpretações a partir do conteúdo sistematizado pela elaboração das categorias. Nessa etapa, foram produzidos os resultados e inferências que trouxeram as respostas para o problema da pesquisa. A Figura 14 ilustra o percurso da pesquisa:

Figura 14 - Percurso da pesquisa



Fonte: Elaborado pela autora (2015).

A Figura 14 demonstra a organização estrutural desta pesquisa, descrevendo, assim, o percurso estabelecido para responder ao problema de pesquisa e atingir o objetivo proposto. Na próxima seção serão apresentados os resultados da pesquisa.

4 ANALISANDO A DIMENSÃO HUMANA DA SEGURANÇA DA INFORMAÇÃO NA PROGEP

Com base na triangulação dos dados coletados por meio da observação participante, pesquisa documental e questionários aplicados aos diretores da Progep da UFPB, esta seção apresenta a análise realizada para alcançar os objetivos propostos, bem como responder à questão que norteia esta pesquisa.

4.1 PERFIL DOS GESTORES

Para conhecer o perfil dos gestores respondentes, foram coletadas informações sobre faixa etária, gênero, formação acadêmica, tempo de instituição e tempo na função, a fim de identificar as características específicas do grupo em questão. Para uma melhor visualização das características gerais do grupo estudado, organizamos todas as informações no Quadro 11.

Quadro 11- Perfil dos gestores

FAIXA ETÁRIA	GÊNERO	FORMAÇÃO ACADÊMICA	TEMPO DE INSTITUIÇÃO	TEMPO NA FUNÇÃO
Acima de 51 anos	Feminino	Especialização	Mais de 16 anos	Mais de 10 anos
Entre 31 e 40 anos	Feminino	Mestrado	11 a 15 anos	7 a 9 anos
Entre 31 e 40 anos	Masculino	Especialização	1 a 5 anos	1 a 3 anos
Acima de 51 anos	Feminino	Especialização	6 a 10 anos	Mais de 10 anos
Entre 31 e 40 anos	Feminino	Especialização	6 a 10 anos	1 a 3 anos
Entre 20 e 30 anos	Feminino	Mestrado	1 a 5 anos	Menos de 1 ano
Acima de 51 anos	Masculino	Especialização	Mais de 16 anos	Mais de 10 anos
Acima de 51 anos	Masculino	Especialização	Mais de 16 anos	1 a 3 anos
Entre 31 e 40 anos	Masculino	Mestrado	1 a 5 anos	1 a 3 anos

Fonte: Dados da pesquisa (2015).

No que se refere à faixa etária, observa-se que três grupos obtiveram representatividade. No primeiro grupo (entre 20 e 30 anos), encontrou-se apenas um gestor, enquanto nas faixas etárias posteriores (entre 31 e 40 e acima de 51 anos), identificararam-se quatro gestores para cada grupo etário. Nesse caso, observa-se que a heterogeneidade nas faixas etárias entre os gestores pode gerar a troca de

experiências, o que possibilita o surgimento de novos comportamentos que podem contribuir na criação de um ambiente de maior segurança da informação.

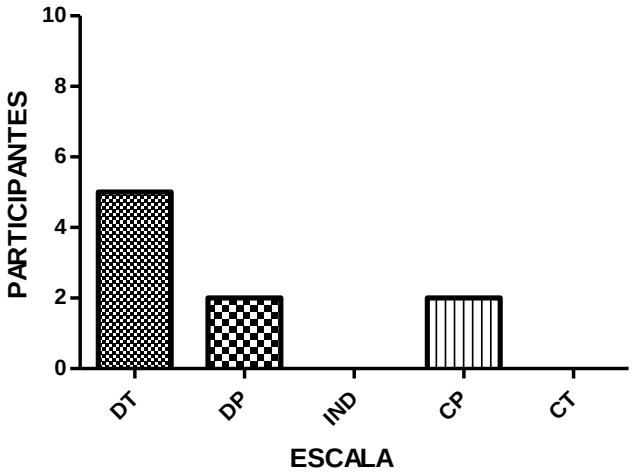
Ao avaliar a categoria gênero, percebeu-se certo equilíbrio na divisão, uma vez que cinco são do sexo feminino e quatro do sexo masculino. Quanto à formação acadêmica, três gestores são mestres e seis são especialistas, demonstrando que eles ampliaram suas formações iniciais (graduação) e buscaram maior qualificação por meio das pós-graduações (educação formal).

No que tange ao tempo de instituição e o tempo na função, observou-se que a maioria dos gestores possui mais de seis anos na instituição e apenas um gestor possui menos de um ano na função, o que demonstra experiência nas funções que ocupam.

4.2 IDENTIFICANDO OS PROCESSOS INFORMACIONAIS DA PROGEP

Para a identificação dos processos informacionais que transitam na Progep, foi criada a categoria processos, abordando dois aspectos: a existência de uma política de classificação da informação na Progep, de acordo com os requisitos legais, e a identificação da classificação dos processos pelos gestores, em relação a sua divisão. Conforme os resultados apresentados na Figura 15, foi verificada, entre os gestores, uma maior discordância quanto ao primeiro aspecto, no tocante à existência ou não de uma classificação da informação na Progep. No entanto, verificou-se que, de um pequeno número de gestores, obteve-se uma concordância parcial, inferindo-se que essa classificação não é feita de maneira formal, uma vez que não foi identificado nenhum documento que contenha os procedimentos que a defina.

Figura 15 - Classificação da informação



Fonte: Dados da pesquisa (2015).
Notas: DT- Discorda totalmente; DP- Discorda parcialmente; IND- Indiferente; CP- Concorda parcialmente; CT- Concorda totalmente.

Entretanto, nas observações foi possível identificar que havia classificação da informação, mesmo de maneira informal, devido às características específicas de algumas divisões, onde o gestor entende que determinada informação não deve ser divulgada de forma ostensiva, ou requer maior proteção. A ABNT NBR ISO/IEC 27002 (2013, p. 18-23) orienta sobre a necessidade de ser instituída uma política de classificação da informação nas instituições, uma vez que a classificação da informação assegura que esta receba um nível adequado de proteção, de acordo com a sua importância para a organização. Para a referida norma, convém que:

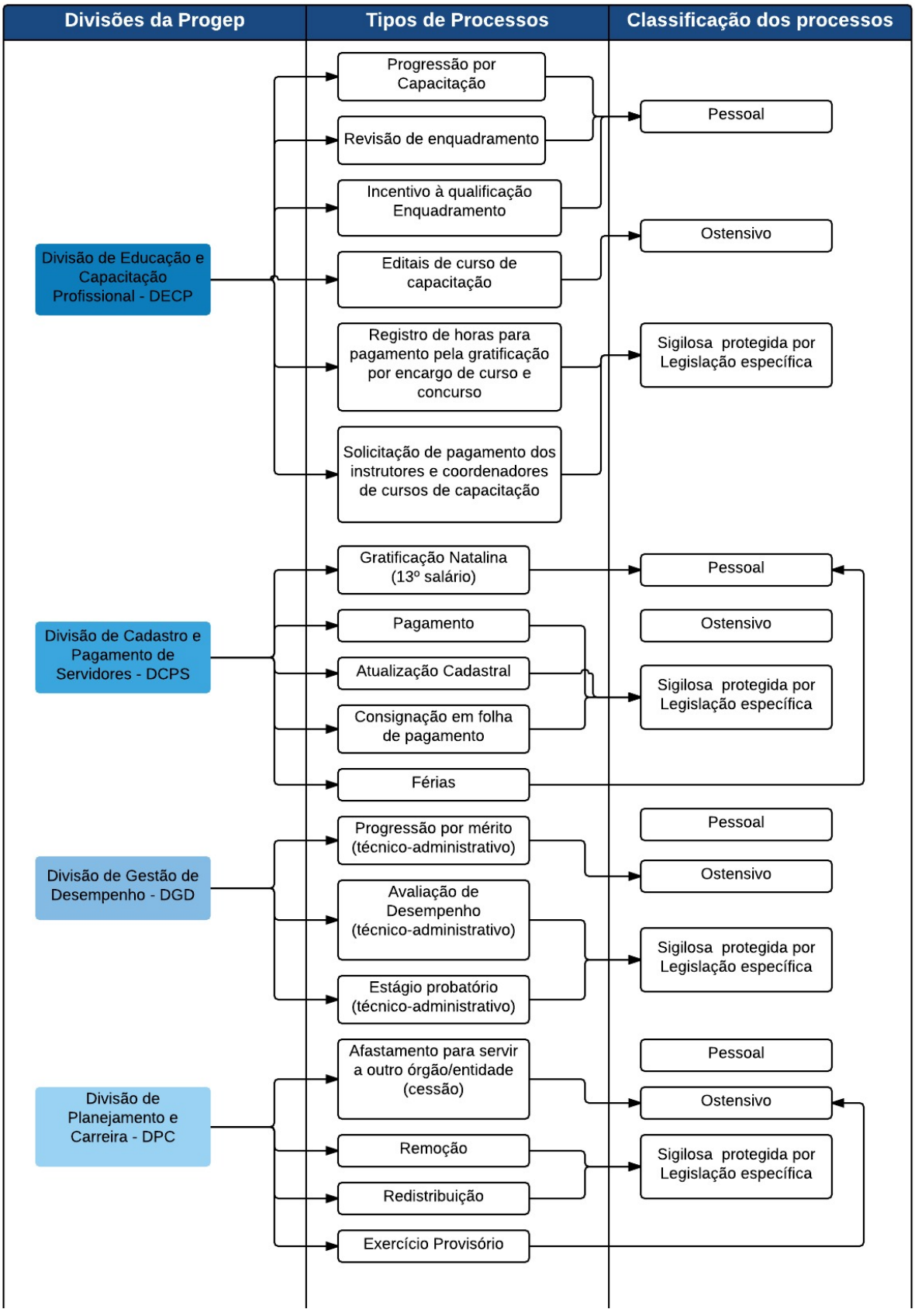
- A informação seja classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada;
- Os proprietários de ativos de informação sejam responsáveis por sua classificação;
- O esquema de classificação inclua convenções para classificação e critérios para análise crítica da classificação ao longo do tempo;
- O nível de proteção seja avaliado por meio da análise da confidencialidade, integridade e disponibilidade e quaisquer requisitos considerados para a informação;
- O esquema esteja alinhado com a política de controle de acesso;

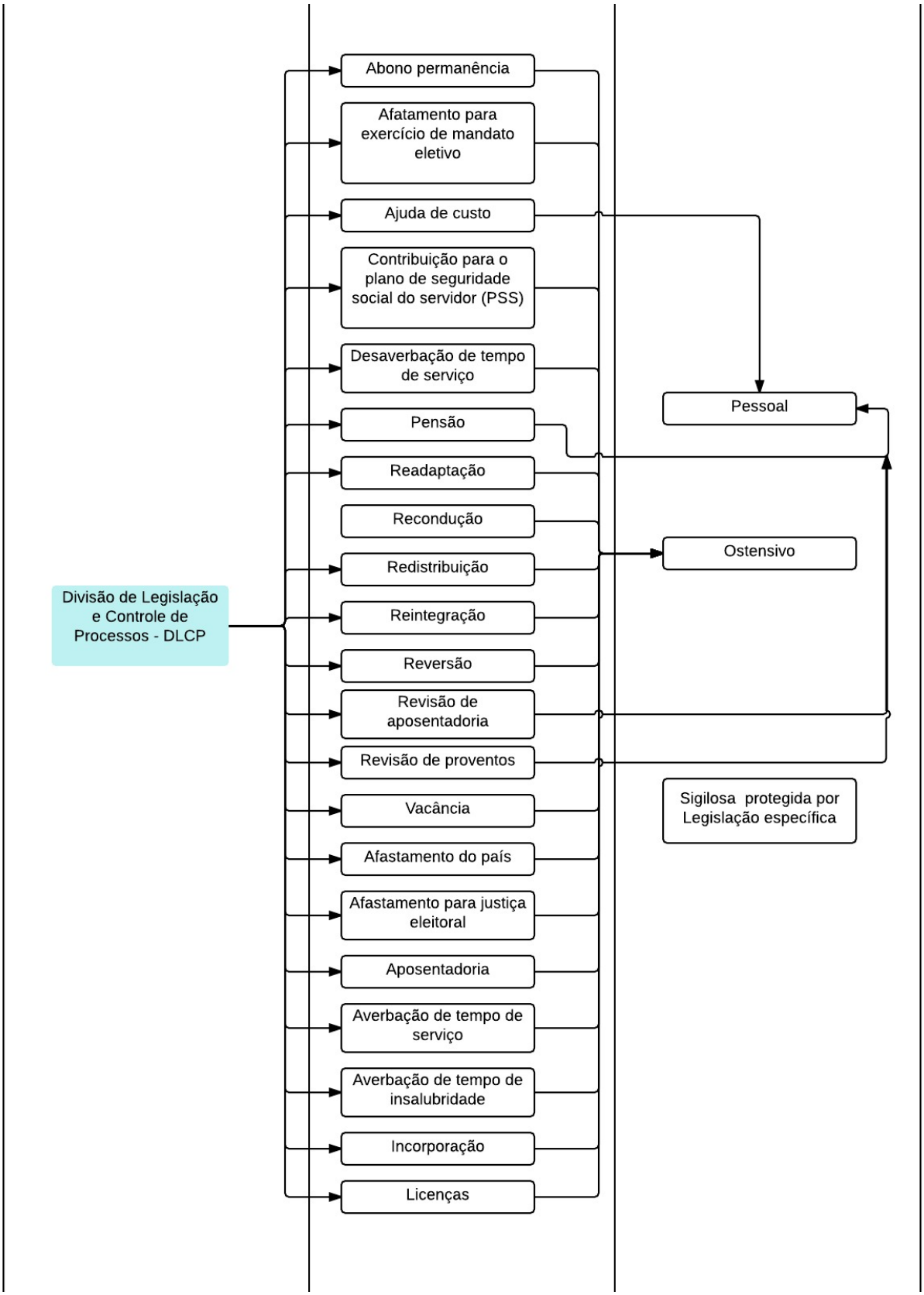
- A cada nível seja dado um nome que faça sentido no contexto do esquema de classificação;
- O esquema seja consistente em toda a organização de forma que cada pessoa possa classificar a informação e os ativos relacionados da mesma forma, e tenham um entendimento comum dos requisitos de proteção a fim de aplicar a proteção apropriada;
- A classificação seja incluída nos processos da organização de forma consistente e coerente;
- Os resultados da classificação indiquem o valor dos ativos em função da sua sensibilidade e criticidade para a organização, em termos da confidencialidade, integridade e disponibilidade;
- Os resultados da classificação sejam atualizados, de acordo com as mudanças do seu valor, sensibilidade e criticidade ao longo do seu ciclo de vida (ABNT NBR ISO/IEC 27002, 2013, p. 18-23).

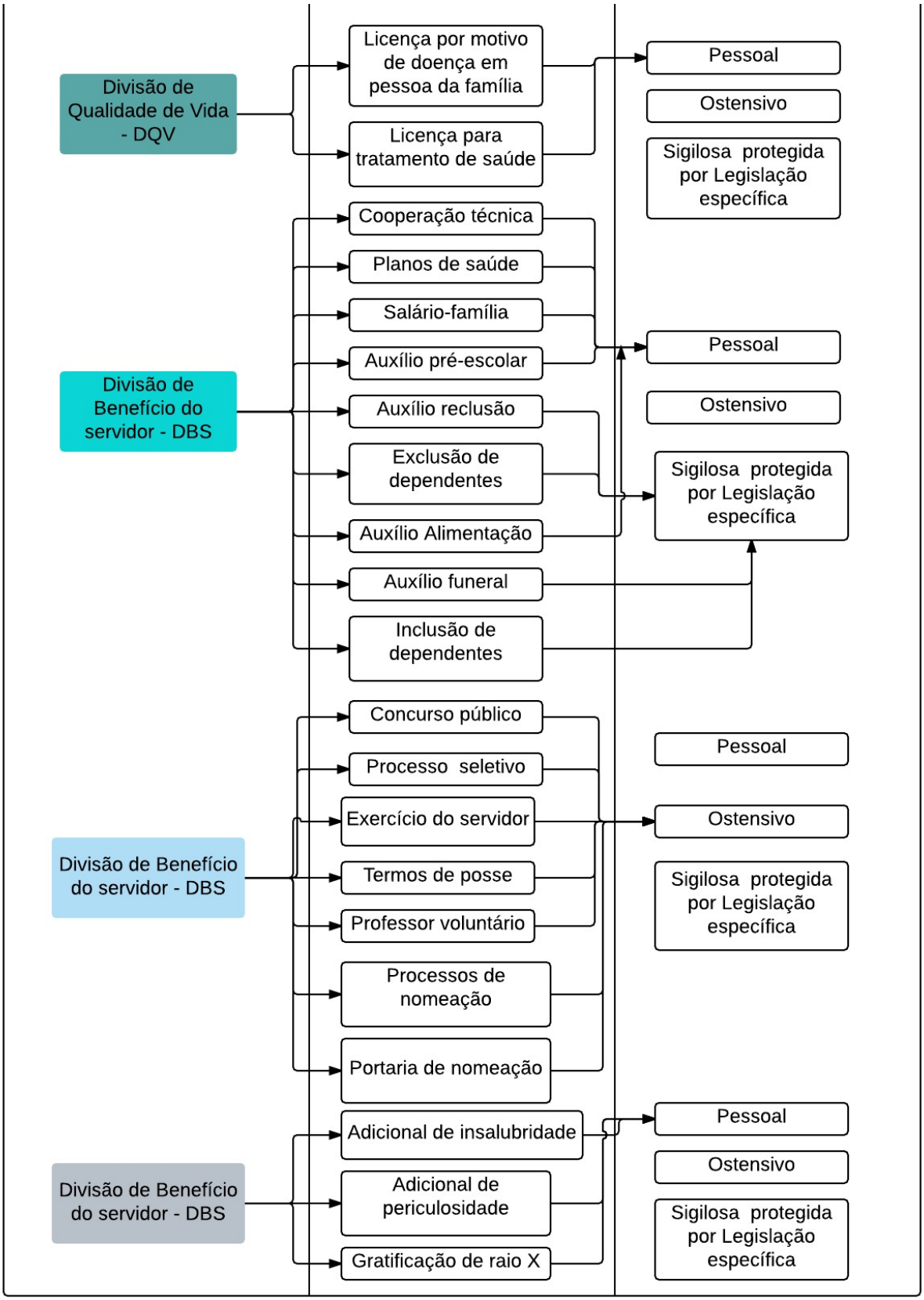
A classificação da informação possibilita, aos agentes públicos dos órgãos e entidades da Administração Pública Federal (APF), uma indicação de como tratar a informação (produção, armazenamento, disseminação, uso e destinação) de modo ético, responsável e com respeito à legislação vigente. Porém, a sua inexistência impossibilita a efetividade de uma gestão da segurança da informação. De acordo com a Norma Complementar 20/IN01/DSIC/GSIPR (BRASIL, 2014, p. 11), é de responsabilidade da alta administração do órgão ou entidade da APF aprovar as diretrizes estratégicas de segurança da informação que norteiam o tratamento da informação.

Assim, como demonstrado no Quadro 3, a Norma Complementar 20/IN01/DSIC/GSIPR (BRASIL, 2014, p.12) classifica os tipos de informação como: **ostensiva** (transparência ativa e passiva); **sigilosa – classificada quanto ao grau de sigilo** (reservada, secreta e ultrassecreta); **sigilosa – protegida por legislação específica** (decorrentes de direitos de personalidade, sigilos de processos e procedimentos, informação de natureza patrimonial) e **pessoal.** Com base nessa classificação, no segundo aspecto abordado em processos, foi solicitado que os diretores classificassem os processos de sua divisão, obtendo os seguintes resultados apresentados na Figura 16.

Figura 16 - Classificação dos processos da Progep




Abono permanência
Afatamento para exercício de mandato eletivo
Ajuda de custo
Contribuição para o plano de seguridade social do servidor (PSS)
Desaverbação de tempo de serviço
Pensão
Readaptação
Recondução
Redistribuição
Reintegração
Reversão
Revisão de aposentadoria
Revisão de proventos
Vacância
Afastamento do país
Afastamento para justiça eleitoral
Aposentadoria
Averbação de tempo de serviço
Averbação de tempo de insalubridade
Incorporação
Licenças
Divisão de Legislação e Controle de Processos - DLCP
Pessoal
Ostensivo
Sigilosa protegida por Legislação específica



Fonte: Dados da pesquisa (2015).

Percebe-se que, de acordo com Figura 16, a Progep possui três, dentre os quatro tipos de informações classificadas pela Norma Complementar 20/IN01/DSIC/GSIPR, e apenas as informações sigilosas, classificadas quanto ao grau de sigilo, não são manuseadas na Progep. De acordo com a Lei nº 12.527, (BRASIL, 2011[31]), informações sigilosas, classificadas quanto ao grau de sigilo, são aquelas "submetidas temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado".

A Figura 16 demonstra que cinco das nove divisões não possuem processos ostensivos, apenas pessoal e sigiloso, protegidos por legislação específica, ou seja, processos que necessitam de maior proteção. Nessa classificação realizada pelos gestores, alguns processos classificados como ostensivos devem ser considerados sigilosos no momento da sua elaboração, como por exemplo, os editais.

Apesar de haver muitos processos com informações pessoais e sigilosas, através da observação participante verificou-se que os processos quando tramitam pelo Sistema Integrado de Patrimônio, Administração e Contratos (SIPAC), em sua maioria, tramitam de forma ostensiva, embora, no sistema, haja também a opção de reservado e secreto. Esse comportamento pode ser decorrente da ausência de uma política de classificação da informação e da falta de conscientização do servidor em entender quais são suas responsabilidades com as informações que manuseiam. Nesse sentido, a Norma Complementar 20/IN01/DSIC/GSIPR (BRASIL, 2014, p. 4), relata a obrigação de o agente público salvaguardar a informação sigilosa e a pessoal, além de assegurar a publicidade da informação ostensiva, sob pena de ser responsabilizado de forma administrativa, civil e penalmente. Nessa perspectiva, a Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008, já declarava o dever do Estado de proteção das informações pessoais dos cidadãos (BRASIL, 2008[1]).

Diante do exposto, percebeu-se que a Progep possui muitos processos com informações sigilosas (protegida por legislação específica) e pessoais, que necessitam ser classificadas e protegidas de forma a garantir a disponibilidade, integridade, confidencialidade e autenticidade da informação distribuída e divulgada.

[31] Documento eletrônico não paginado.

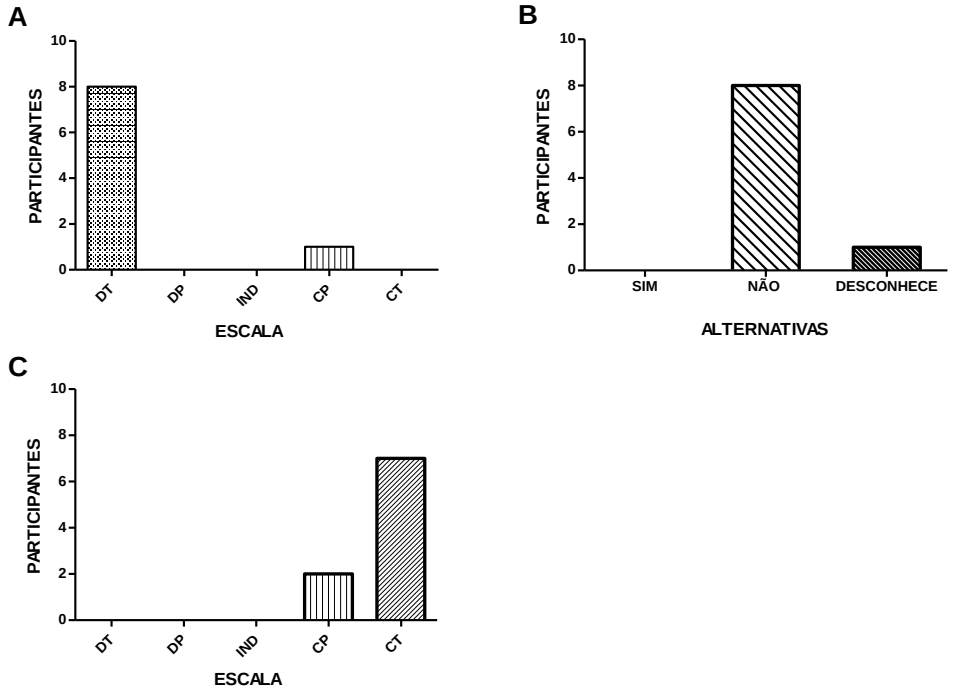
4.3 VERIFICANDO A DIMENSÃO HUMANA DAS AÇÕES DE SI NA PROGEP

Para atingir o objetivo específico de verificar como a dimensão humana é abordada nas ações de gestão de segurança da informação implementadas pela Progep, foi estabelecida as seguintes categorias: conscientização em segurança da informação, controles, e evidências de incidentes de segurança. Conforme será demonstrado, cada categoria foi organizada de modo a atender ao objetivo proposto.

4.3.1 Conscientização em segurança da informação

Nesta categoria, foi verificado inicialmente se a Progep faz menção à segurança da informação no ingresso/posse dos colaboradores, se possui um "termo de responsabilidade e confidencialidade" dando ciência do conhecimento das normas e das principais responsabilidades do servidor em relação à segurança da informação, e se considera importante a assinatura do referido termo. Conforme, ilustra Figura 17.

Figura 17- Conscientização em SI: A) Menção à segurança da informação na posse do servidor; B) Termo de responsabilidade e confidencialidade; C) Importância da assinatura do termo de responsabilidade e confidencialidade.



Fonte: Dados da pesquisa (2015).
Notas: DT- Discorda totalmente; DP- Discorda parcialmente; IND- Indiferente; CP- Concorda parcialmente; e CT- Concorda totalmente.

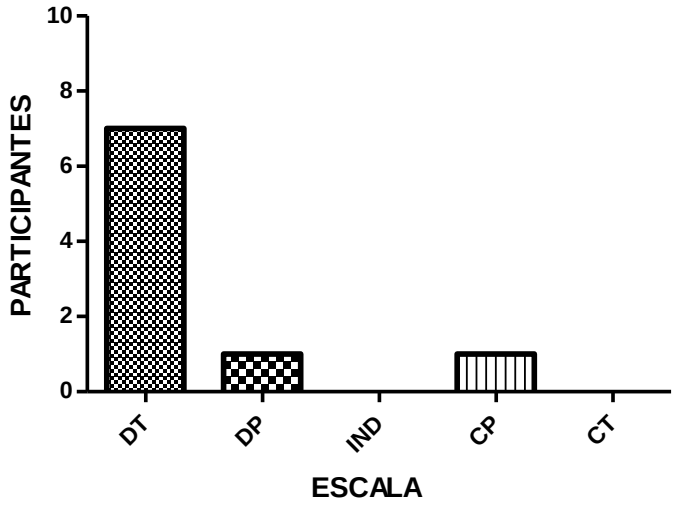
Nessa discussão, pôde-se observar que, de acordo com a Figura 17, dentre os gestores, oito relataram total discordância quanto à Progep mencionar acerca da segurança da informação no processo de ingresso/posse dos seus colaboradores; enquanto a mesma representatividade de gestores afirmou não existir um termo de "responsabilidade e confidencialidade" criado pela Progep. No entanto, verificou-se uma maior concordância quanto à importância da assinatura do referido termo.

Nesse sentido, para a ABNT NBR ISO/IEC 27002 (2013, p. 12) "convém que os papéis e responsabilidades pela segurança da informação sejam comunicados para o candidato durante o processo de pré-contratação". Além disso, todos os funcionários, fornecedores e partes externas que tenham acesso às informações institucionais devem assinar um termo de responsabilidade e confidencialidade, antes de lhes ser dado o acesso a quaisquer informações.

Fontes (2006, p. 35, 2012, p. 204) recomenda que, ao contratar um novo colaborador ou prestador de serviço, a instituição deve solicitar ao contratado a assinatura do termo de responsabilidade e confidencialidade, em que estão descritas suas principais responsabilidades referente à informação, devendo, ainda, renovar periodicamente esse termo para que haja uma maior conscientização dos funcionários. Nesse termo devem estar registradas as responsabilidades dos colaboradores quanto ao manuseio da informação, às normas de segurança da informação e o padrão ético da instituição. Para o autor, essa formalização apresenta ao funcionário suas responsabilidades em conjunto com a instituição, além de fornecer informações referentes ao modo que a instituição deseja que a informação armazenada seja tratada e processada pelos recursos de tecnologia e no ambiente convencional.

Outro aspecto abordado, no contexto da conscientização, relaciona-se com a existência de um processo disciplinar formal para ações de violações da segurança da informação. Como pode ser evidenciando na Figura 18, os resultados mostram que, do grupo de gestores, sete relataram total discordância.

Figura 18 - Processo disciplinar formal

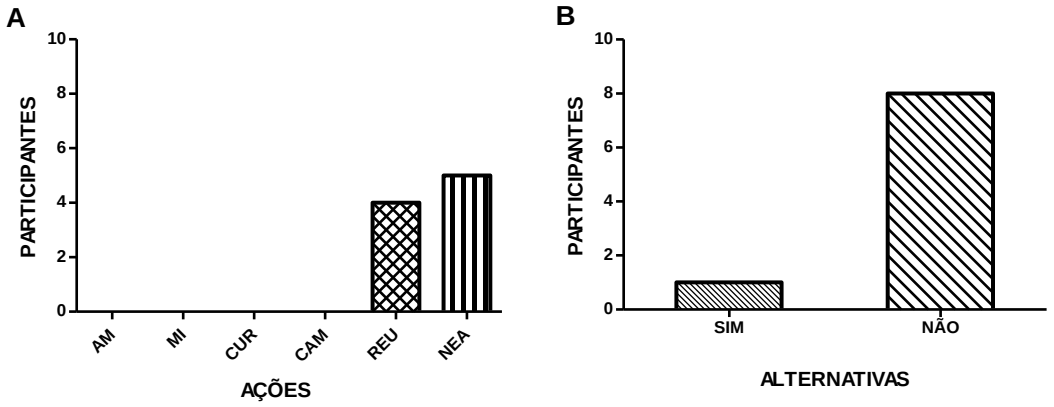


Fonte: Dados da pesquisa (2015).
Notas: DT- Discorda totalmente; DP- Discorda parcialmente; IND- Indiferente; CP- Concorda parcialmente; CT- Concorda totalmente.

No entanto, para a ABNT NBR ISO/IEC 27002 (2013, p. 15), “convém que exista um processo disciplinar formal, implantado e comunicado, para tomar ações contra funcionários que tenham cometido uma violação de segurança da informação”. Segundo a referida norma, esse processo não deve iniciar sem uma verificação prévia de que a violação da segurança da informação realmente ocorreu. O processo disciplinar formal deve assegurar: um tratamento justo e correto aos colaboradores que são suspeitos de cometer violações de segurança da informação; apresentar uma resposta de forma gradual e que leve em consideração fatores como a natureza e a gravidade da violação e o seu impacto no negócio; se este é ou não o primeiro delito; e se o infrator foi ou não adequadamente capacitado e conscientizado sobre suas responsabilidades relativas à informação. O processo disciplinar pode ser usado também como forma de dissuasão para evitar que os funcionários e as partes externas violem os procedimentos e as políticas de segurança da informação da organização, e quaisquer outras violações dessa segurança.

Referente às ações de conscientização em segurança da informação, foi analisado quais os tipos de ações desenvolvidas pela Progep. De acordo com a Figura 19, constatou-se, com os resultados, que o índice “reunião” obteve quatro frequências, enquanto o índice de “não possui ações de conscientização” obteve cinco frequências.

Figura 19 - Ações de Conscientização: A) Ações de segurança da informação; B) Notícias e relatórios de SI



Fonte: Dados da pesquisa (2015).
Notas: AM- Avisos em murais; MI- Manuais informativos; CUR- Cursos; CAM- Campanhas; REU- Reuniões; NEA- Não existem ações.

Entretanto, durante o procedimento de observação participante, foi possível perceber que as reuniões estabelecidas no setor não abordavam efetivamente a segurança da informação, apenas fazia-se menção sobre informações ou procedimentos que não deveriam ser divulgados. A inexistência de ações de conscientização em SI torna o ambiente muito fértil para a ocorrência de incidentes causados por negligência, ignorância ou erro. Para a ABNT NBR ISO/IEC 27002 (2013, p. 13), é necessário que os funcionários atinjam um nível de conscientização sobre segurança da informação que seja relevante para as suas funções na instituição.

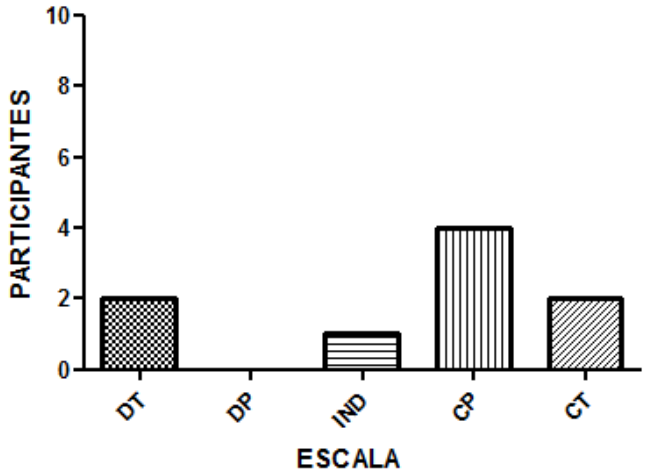
Outro aspecto abordado, conforme a Figura 19, compreende o fato de os gestores manterem-se informados sobre notícias e relatórios de segurança da informação, o que resultou em uma maior representatividade de afirmações negativas. Esse resultado implica considerar que não há ainda um despertar dos gestores para a segurança da informação.

Diante do exposto, percebe-se que a Progep ainda não depreende esforços suficientes para estar em conformidade com a norma, uma vez que a inexistência de procedimentos, como: assinatura do termo de responsabilidade e confidencialidade, processo disciplinar formal para as violações da segurança da informação e de ações de conscientização em SI, torna a Progep um ambiente vulnerável aos mais diversos tipos de ameaças.

4.3.2 Controles

Nesta categoria, foi discutida a adoção de alguns controles de segurança da informação pela Progep, em que foram analisados aspectos peculiares a controles de acesso físico, influências da política de segurança da informação, política de mesa/tela limpa, políticas de senhas, proteção contra *malware*, cópias de segurança, e comportamentos de segurança no ambiente de trabalho. Com relação à existência de controle de acesso físico no ambiente de trabalho, foram obtidos os seguintes resultados apresentados na Figura 20.

Figura 20 - Controle de acesso físico



Fonte: Dados da pesquisa (2015).
Notas: DT- Discorda totalmente; DP- Discorda parcialmente; IND- Indiferente; CP- Concorda parcialmente; CT- Concorda totalmente.

Com base na Figura 20, verifica-se a ocorrência de discordância total entre os gestores, na qual é possível inferir que essa condição foi motivada em decorrência de suas respectivas divisões não estarem inseridas nas instalações físicas da Progep, ficando localizadas em outros ambientes do prédio da Reitoria. Constatou-se também, com os resultados obtidos, concordâncias parciais e totais quanto à existência de controle de acesso físico, dos quais foi possível identificar, de forma detalhada, o seu funcionamento, como exposto no Quadro 12.

Quadro 12- Controle de acesso físico

SUJEITOS	RESPOSTAS
S1	O fluxo de pessoas é controlado para que ninguém entre sem permissão.
S2	Através de uma triagem na central de atendimento.
S3	Controle através de triagem na central de atendimento.
S4	O controle funciona fechando a porta da frente, onde os servidores da Progep só podem entrar pela porta do fundo. Discordo do nosso "controle de acesso".
S5	A Central de Atendimento ao Servidor é responsável pela triagem inicial. Caso este setor não possua as informações necessárias para sanar a demanda do servidor, o pessoal responsável pelo atendimento entrará em contato com esta divisão e solicitará o atendimento à demanda do servidor. Portanto, o acesso ao espaço físico da divisão é restrito.
S6	Há controle de acesso ao ambiente interno, mas sem identificação específica da pessoa. Há grande resistência dos usuários da UFPB em aceitar tal controle, por ser servidor como os trabalhadores da Progep.

Fonte: Dados da pesquisa (2015).

Obtendo como referência o Quadro 12 e as informações obtidas por meio da observação participante, percebeu-se que existe um controle de acesso físico que funciona a partir da interdição da entrada da Progep. Nesse caso, os servidores internos à Progep devem entrar pela porta dos fundos, sendo liberadas cópias da chave para os servidores que assim a desejarem, o que aumenta a vulnerabilidade do ambiente. Quanto aos servidores externos à Progep, estes podem ter acesso à porta da frente, caso sua demanda não seja atendida na Central de Atendimento ao Servidor (CAS), setor responsável pela triagem. Nesse caso, o servidor recebe um crachá padrão para liberação do acesso.

Com base nas falas dos sujeitos S4 e S6, pode se inferir que a forma como o controle foi implantado não está satisfazendo aos servidores, seja pela resistência dos servidores externos à Progep, seja pelo constrangimento dos servidores internos de entrarem pela porta dos fundos. A ABNT NBR ISO/IEC 27002 (2013, p. 39) orienta que o controle de acesso físico seja implantado de forma apropriada para que apenas as pessoas autorizadas tenham acesso permitido. Para esta norma, torna-se necessário que sejam levadas em consideração as seguintes diretrizes:

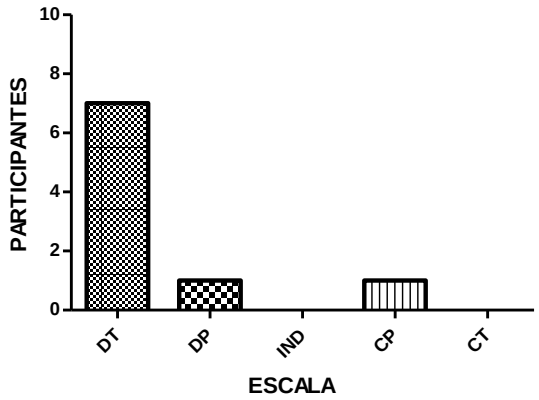
- Convém que a data e hora da entrada e saída de visitantes sejam registradas e que as permissões de acesso só sejam concedidas para finalidades específicas e autorizadas;
- Convém que o acesso às áreas em que são processadas ou armazenadas informações sensíveis seja restrito apenas ao pessoal autorizado;
- Convém que uma trilha de auditoria eletrônica ou um livro de registro físico de todos os acessos seja mantido e monitorado de forma segura;
- Convém que seja exigido que todos os funcionários, fornecedores e partes externas, e todos os visitantes, tenham alguma forma visível de identificação;
- Convém que os direitos de acesso a áreas seguras sejam revistos e atualizados em intervalos regulares, e revogados quando necessário.

Mitnick e Simon (2003, p. 229) orientam ainda que podem ser usados crachás de identificação, codificados com cores, para indicar se o portador é um funcionário, contratado, fornecedor, consultor, visitante ou estagiário. Para os autores, a cor do crachá é um modo excelente de determinar o status de uma pessoa à distância. Percebe-se que muitas são as orientações e sugestões para um controle de acesso físico eficiente.

Na Progep, apesar de existir um controle de acesso físico, ele ainda não funciona em sua plenitude, pois foi observado que muitos servidores têm dificuldades em aceitá-lo ou buscam formas de burlá-lo. Esse comportamento pode ser decorrente da maneira como o controle foi implantando e da não conscientização dos seus servidores quanto aos reais motivos de sua implantação.

Como demonstrado na Figura 21, outro aspecto abordado procurou analisar se a política de segurança da informação da UFPB influencia nas rotinas de trabalhos dos gestores participantes desta pesquisa. Foi observada uma considerável incidência de discordância total entre os gestores, o que pode ser consequência do desconhecimento da PSI da UFPB, instituída pelo Consuni, por meio da Resolução nº 32/2014, e enviada a todos os servidores técnico-administrativos e docentes pela Superintendência de Tecnologia da Informação da UFPB, por meio do Sistema Integrado de Gestão (SIG).

Figura 21 - Política de segurança da informação



Fonte: Dados da pesquisa (2015).
Notas: DT- Discorda totalmente; DP- Discorda parcialmente; IND- Indiferente; CP- Concorda parcialmente; CT- Concorda totalmente.

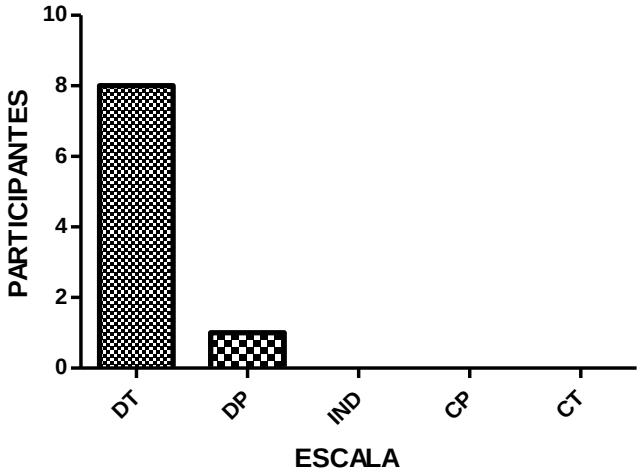
A PSI da UFPB consiste em um "quadro de referência contendo princípios que norteiam a gestão da segurança da informação e que devem ser observados por professores, alunos, servidores e demais usuários que interagirem com os ativos da UFPB." (UFPB, 2014a[9]). No Art. 4º, a PSI da UFPB apresenta seus objetivos, que consistem em:

> I – Definir o escopo da segurança da informação da UFPB;
> II – Orientar as ações de segurança com intuito de reduzir riscos e garantir a confidencialidade, integridade e disponibilidade dos ativos da UFPB;
> III - Incentivar o uso de soluções integradas de segurança;
> IV – Servir de referência para auditoria, apuração e avaliação de responsabilidade. (UFPB, 2014a[32]).

Para a ABNT NBR ISO/IEC 27002 (2013, p. 3), além da necessidade da PSI ser comunicada aos funcionários e partes externas relevantes de forma que seja entendida, acessível e relevante aos funcionários, é necessário que essa publicação seja inserida no contexto de um programa de conscientização e capacitação em segurança da informação.

[32] Documento eletrônico não paginado.

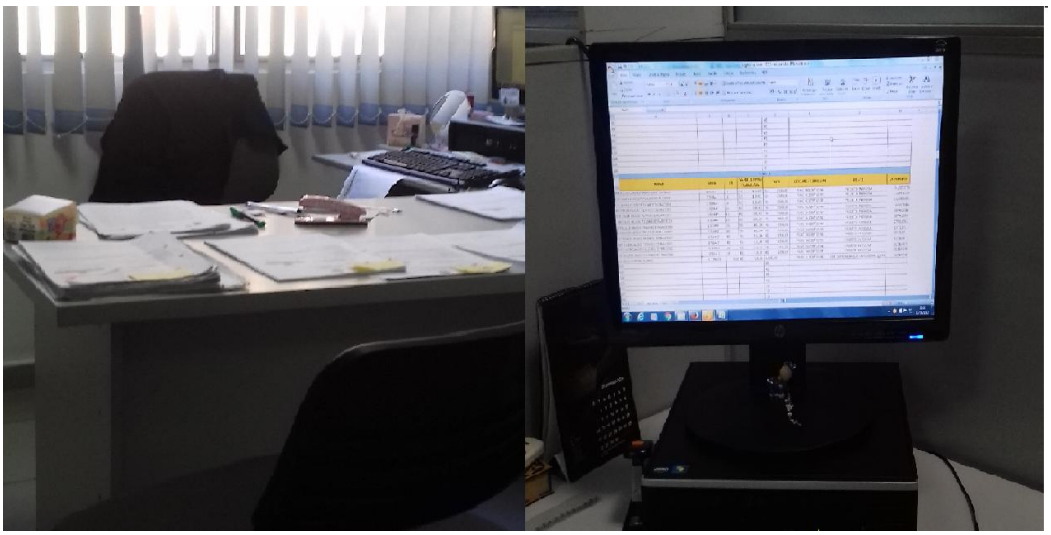
Figura 22 - Existência da política de mesa limpa/tela limpa



Notas: DT- Discorda totalmente; DP- Discorda parcialmente; IND- Indiferente; CP- Concorda parcialmente; CT- Concorda totalmente.
Fonte: Dados da pesquisa (2015).

Verificou-se também, se há uma política de mesa limpa/tela limpa para os recursos de processamento da informação, conforme ilustra a Figura 22. Os resultados mostram que a quase totalidade dos respondentes registraram discordância total da existência da referida política. Nesse seguimento, durante a fase da pesquisa documental, não foi identificada nenhuma política, norma ou procedimento que abordassem o tema, o que implicou na necessidade de se constatar os comportamentos dos servidores da Progep, referente à cultura de mesa limpa/tela limpa, como exemplificado na Figuras 23.

Figura 23 - Mesa limpa/tela limpa



Fonte: Dados da pesquisa (2015).

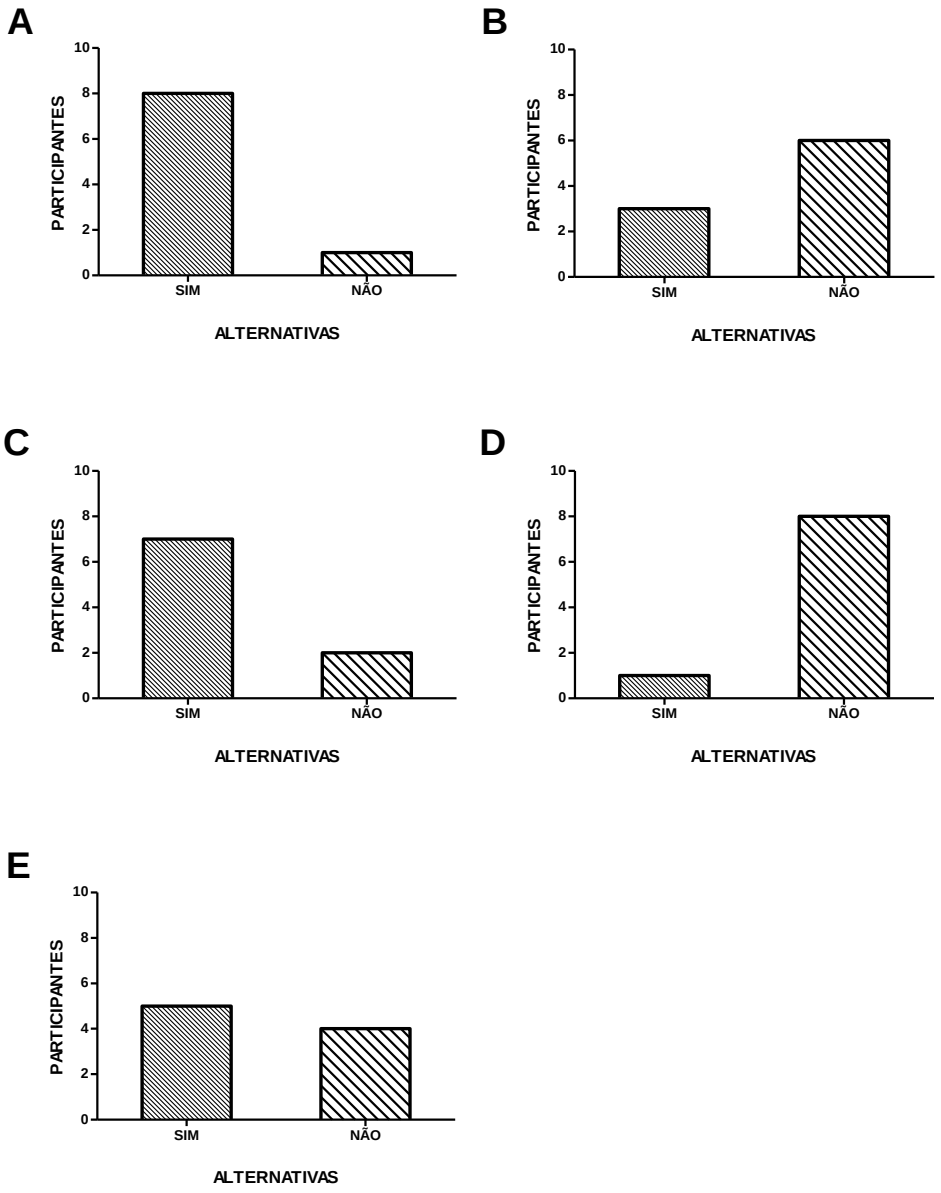
Mediante o processo de observação, percebeu-se que faz parte da rotina dos servidores deixarem documentos e processos sobre as mesas no final do expediente e telas de computadores com documentos abertos por um período prolongado de tempo durante o expediente. Para a ABNT NBR ISO/IEC 27002 (2013, p. 47), “convém que seja adotada uma política de mesa limpa de papéis e mídias de armazenamento removíveis e uma política de tela limpa para os recursos de processamento da informação”. Essa política deve levar em consideração a classificação da informação, requisitos contratuais e legais e o risco correspondente, além dos aspectos culturais da organização. Para a norma, as seguintes diretrizes devem ser cogitadas:

- Guardar em lugar seguro as informações do negócio sensíveis ou críticas, por exemplo, em papel ou em mídia de armazenamento eletrônicas;
- Manter desligados ou protegidos os computadores e terminais, por meio de mecanismos de travamento de tela e teclados controlados por senha, *token* ou mecanismo de autenticação similar quando sem monitoração e protegida por tecla de bloqueio, senhas ou outros controles, quando não usados; e
- Remover imediatamente, de impressoras, os documentos que contêm informação sensível ou classificada.

Diante do exposto, pôde-se inferir que uma política de mesa limpa/tela limpa, inserida em um programa contínuo de conscientização em segurança da informação, pode reduzir o risco de acesso não autorizado, perda e dano da informação durante e fora do horário de expediente.

Com relação às senhas de computadores, foram abordados cinco aspectos que remeteram aos procedimentos de segurança de senhas: aplicação de políticas de senhas nos sistemas utilizados, substituição periódica de senhas, uso de senhas seguras, exposição de senhas em locais de fácil acesso e compartilhamento de senhas com terceiros. Observa-se na Figura 24, os resultados obtidos.

Figura 24 – Senhas: A) Existência de política de senhas; B) Substituição de senhas; C) Senhas seguras; D) Senhas em local de fácil acesso; E) Compartilhamento de senhas



Fonte: Dados da pesquisa (2015).

Como pode ser analisado na Figura 24, referente à existência de políticas de senhas, os resultados mostraram que a quase totalidade dos gestores afirmou positivamente, condição que diferiu para o fator substituição periódica de senhas que indicou que a maioria dos gestores não possui o hábito de alterar suas senhas de acesso. Quanto ao fator para o uso de senhas seguras, verificou-se uma maior representatividade para a afirmação positiva, evidenciando que nos setores, existe uma prática de utilização de senhas com variações de caracteres, condição que foi

reforçada com a representatividade da afirmação negativa em relação ao fator exposição de senhas em locais de fácil acesso. Entretanto, em referência ao compartilhamento de senhas com terceiros, revelou-se que mais da metade dos gestores realizam o compartilhamento de suas senhas, conforme os motivos expressos no Quadro 13.

Quadro 13 - Compartilhamento de senhas

SUJEITOS	RESPOSTAS
S1	Pela demora em obter acesso para os meus colaboradores. Dificuldade de resolução de problemas técnicos.
S2	Compartilhamos as senhas de acesso às informações do setor pelo fato de facilitar o uso dos instrumentos tecnológicos pela equipe.
S3	Por necessidade do serviço. Às vezes preciso me ausentar e é necessário que outra pessoa acesse as informações.
S4	Porque confio no pessoal que trabalha comigo.
S5	Compartilho com os demais servidores do setor para ter acesso à rede da divisão.

Fonte: Dados da pesquisa (2015).

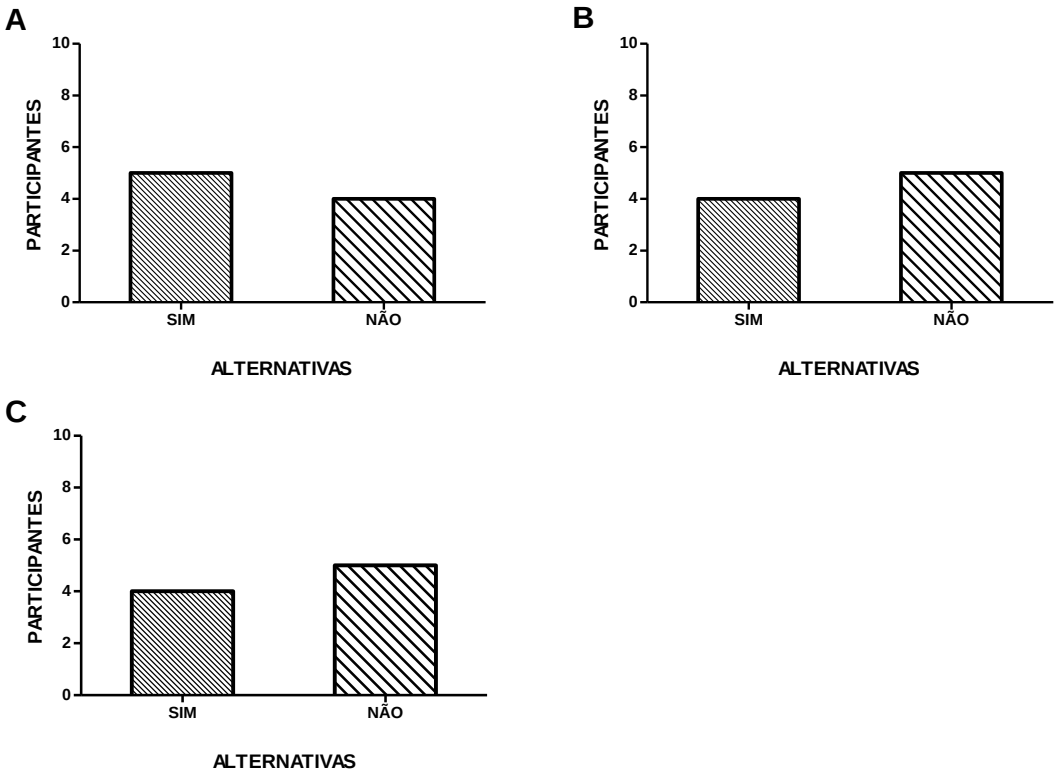
Com base no exposto, percebeu-se que existe uma preocupação dos gestores com suas senhas, todavia, verificou-se que ainda não há substituição periódica. Dentre as declarações, deve-se destacar a ideia que justifica o compartilhamento de senhas com base na confiança na equipe de trabalho (declaração do sujeito S4). Para Fontes (2006, p. 33), “de pouco adianta ter registro do arquivo de auditoria e identificações de usuários que acessaram determinada informação, se uma mesma identificação for utilizada por várias pessoas de um mesmo departamento”. Nesse seguimento, Mitnick e Simon (2003, p. 40) aconselham que nenhuma instituição permita qualquer compartilhamento de senhas, e estabeleça regras que proíbam os funcionários de compartilhar ou trocar as senhas confidenciais.

Para a ABNT/NBR ISO/IEC 27002 (2013, p. 33), convém que sistemas para gerenciamento de senhas sejam interativos e assegurem senhas de qualidade. Para tanto, faz-se necessário algumas orientações, tais como:

- Obrigar o uso individual de ID de usuário e senha para manter responsabilidades;
- Permitir que os usuários selecionem e modifiquem suas próprias senhas, incluindo um procedimento de confirmação para evitar erros;
- Obrigar a escolha de senhas de qualidade;
- Obrigar os usuários a mudarem as suas senhas temporárias no primeiro acesso ao sistema;
- Forçar as mudanças de senha a intervalos regulares, conforme necessário;
- Manter um registro das senhas anteriores utilizadas e bloquear a reutilização;
- Não mostrar as senhas na tela quando forem digitadas;
- Armazenar os arquivos de senha separadamente dos dados do sistema da aplicação; e
- Armazenar e transmitir as senhas de forma protegida.

Outro controle analisado refere-se à proteção contra *malware*, em que foi questionado acerca da utilização de um programa de antivírus indicado pela Progep. De acordo com a Figura 25, observou-se que pouco mais da metade dos gestores afirmaram positivamente acerca do uso de um programa de antivírus designado pela referida Pró-reitoria. Apurou-se que, apesar do programa em questão ser indicado pelo Núcleo de Tecnologia e Gestão da Informação (NTGI) da Progep, esse não é um antivírus corporativo. Para Ferreira (2013, p. 108), a instalação do padrão corporativo de antivírus em toda instituição é uma importante medida de controle de segurança, uma vez que se torna inexequível padronizar as medidas de segurança da informação com antivírus gratuito.

Figura 25 - Antivírus: A) Antivírus indicado pela Progep; B) Atualização de antivírus; C) Verifica a origem de arquivos anexados



Fonte: Dados da pesquisa (2015).

Referente à atualização frequente do programa de antivírus, verificou-se através dos resultados, a mesma representatividade obtida com a análise do uso do programa indicado pela Progep, porém com afirmações negativas. Deve-se considerar que o procedimento de atualização de um programa de antivírus aumenta o seu quantitativo de definições de vírus, tornando-o mais eficiente. Por esse ângulo, para Mitnick e Simon (2003, p. 83-84), cada servidor deve assumir a responsabilidade de fazer o download do conjunto mais recente de definições de vírus por conta própria. Os autores recomendam que todos configurem as opções do antivírus para que as novas definições de vírus sejam atualizadas automaticamente todos os dias. Entretanto é de responsabilidade da administração lembrar regularmente aos servidores da necessidade de manter o antivírus atualizado.

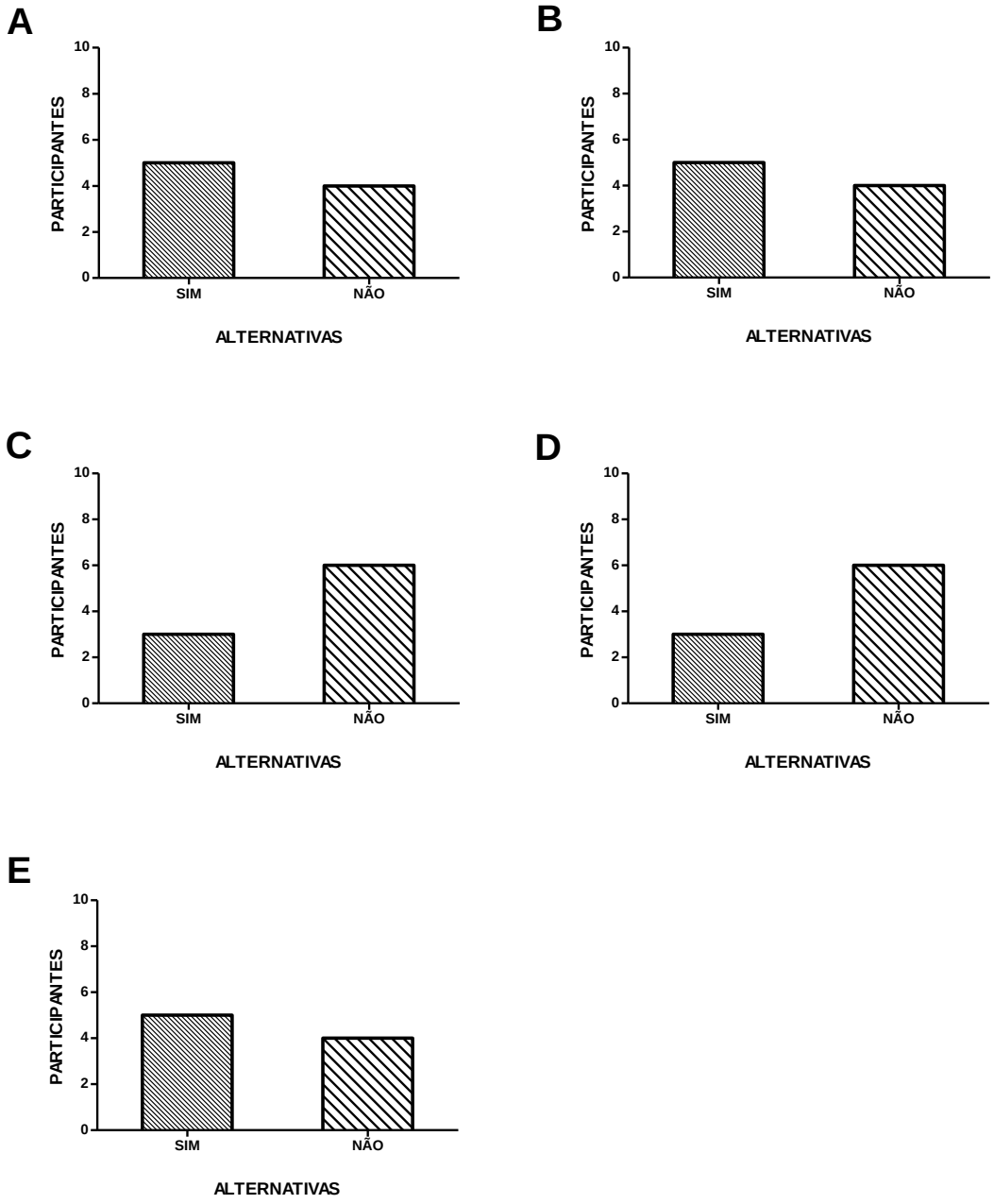
Outro aspecto discutido compreendeu a realização de varredura nos arquivos anexados no correio eletrônico, antes de sua abertura para visualização. Conforme a Figura 25, constatou-se que mais da metade dos respondentes confirmaram negativamente sobre a execução de varreduras nos arquivos inseridos em correios eletrônicos. Mitnick e Simon (2003, p. 84) esclarecem que os servidores precisam

ser sempre lembrados de várias maneiras para não abrir os anexos de correio eletrônico, a menos que tenham certeza de que a fonte é uma pessoa da instituição ou alguém de confiança.

Para a proteção contra *malware*, a ABNT/NBR ISO/IEC 27002 (2013, p. 51-52) orienta que sejam implementados controles de detecção, prevenção e recuperação, combinados com um adequado programa de conscientização da segurança da informação. A norma recomenda que alguns controles sejam considerados, como:

- Estabelecer uma política formal proibindo o uso de softwares não autorizados;
- Implementar controles para prevenir ou detectar o uso de softwares não autorizado;
- Implementar controles para prevenir ou detectar o uso de *websites* maliciosos, suspeitos ou conhecidos;
- Estabelecer uma política formal para proteção contra os riscos associados com a importação de arquivos e softwares, seja de redes externas, ou por qualquer outro meio, indicando as medidas preventivas a serem adotadas;
- Reduzir vulnerabilidades que possam ser exploradas por códigos maliciosos;
- Conduzir análises críticas regulares dos softwares e dados dos sistemas que suportam processos críticos de negócio; convém que a presença de quaisquer arquivos não aprovados ou atualização não autorizada seja formalmente investigada; e
- Instalar e atualizar regularmente softwares de detecção e remoção de códigos maliciosos para o exame de computadores e mídias magnéticas, de forma preventiva ou de forma rotineira; convém que as verificações realizadas incluam: 1) varredura, antes do uso, da existência de códigos maliciosos nos arquivos recebidos por meio de redes ou em qualquer mídia de armazenamento; 2) verificação, antes do uso, da existência de software malicioso em qualquer arquivo recebido através de correio eletrônico ou importado (*download*); e 3) verificação da existência de códigos maliciosos em páginas *web*.

Figura 26 - Ações de Segurança da Informação: A) Bloqueio de tela do computador; B) Líquidos ou alimentos próximos ao computador; C) Cópias de segurança; D) Guarda de documentos; e E) Equipamentos eletrônicos.

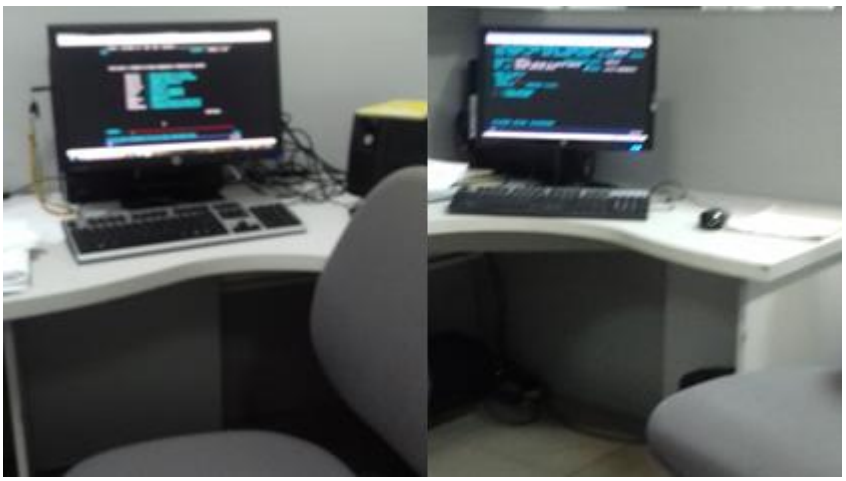


Fonte: Dados da pesquisa (2015).

Conforme a Figura 26, percebeu-se que uma representatividade de mais da metade dos participantes apontaram para a utilização de bloqueio de tela de computador, por meio de senhas, quando da necessidade de se ausentar por um período prolongado de tempo. No entanto, foi observado que rotineiramente havia

computadores com sistemas abertos na ausência do servidor, conforme apresenta a Figura 27.

Figura 27 - Sistema aberto

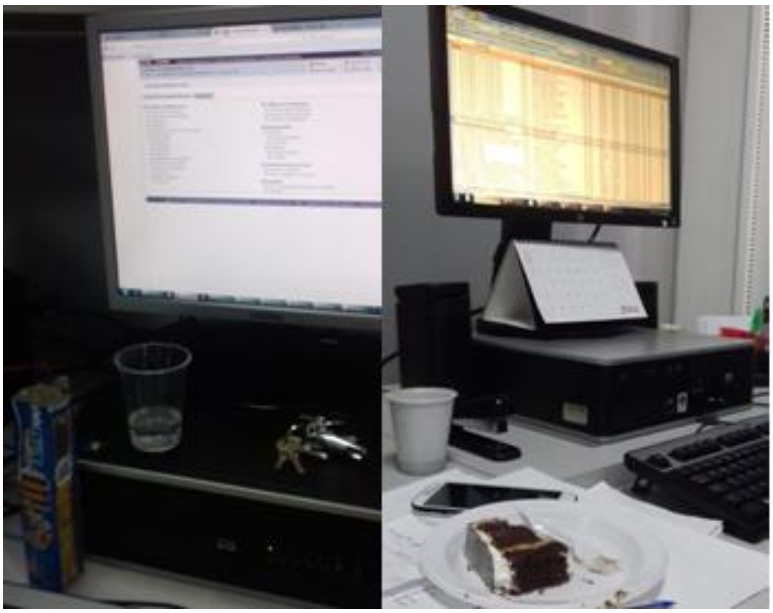


Fonte: Dados da pesquisa (2015).

Mitnick e Simon (2003, p. 249) sugerem que todos os servidores definam uma senha para a proteção de tela e um limite de inatividade não superior a dez minutos para bloquear o computador. A intenção desta política é evitar que um servidor utilize a senha de outro. A ABNT NBR ISO/IEC 27002 (2013, p. 46) estabelece que todos os equipamentos não monitorados tenham proteção adequada e que os servidores sejam informados para: a) encerrar as sessões ativas, a menos que elas possam ser protegidas por meio de um mecanismo de bloqueio, por exemplo, tela de proteção com senha; b) efetuar a desconexão de serviços de rede ou aplicações, quando não for mais necessário; c) proteger os computadores ou dispositivos móveis contra uso não autorizado através de tecla de bloqueio ou outro controle equivalente, por exemplo, senha de acesso, quando não estiver em uso.

Abordou-se também, de acordo com a Figura 26, a respeito da ingestão de líquidos ou alimentos próximos aos computadores, constatando-se uma maior representatividade para a confirmação positiva desses procedimentos rentes aos equipamentos de trabalho. Observou-se que, apesar da existência de uma copa na Progep, repetidamente os servidores fazem ingestão de alimentos próximos aos computadores, como demonstrado na Figuras 28. Entretanto, a ABNT NBR ISO/IEC 27002 (2013, p. 42) propõe que sejam estabelecidas diretrizes quanto a comer e beber nas proximidades das instalações de processamento da informação.

Figura 28 - Bebidas e alimentos próximos a computadores



Fonte: Dados da pesquisa (2015).

Retomando a Figura 26, ainda com base na análise dos resultados obtidos, averiguou-se que, quanto ao processo de cópias de segurança, mais da metade dos gestores afirmaram que não realizam procedimentos de cópias de segurança. Nesse contexto, a ABNT NBR ISO/IEC 27002 (2013, p. 52) orienta que cópias de segurança das informações, softwares e das imagens do sistema, sejam efetuadas e testadas regularmente conforme a política de geração de cópias de segurança definida. Quando da elaboração de um plano de backup, convém que alguns itens sejam considerados, como:

- Registros completos e exatos das cópias de segurança;
- A abrangência e a frequência da geração das cópias de segurança reflitam os requisitos de negócio da organização, além dos requisitos de segurança da informação envolvidos e a criticidade da informação para a continuidade da operação da organização;
- As cópias de segurança sejam armazenadas em uma localidade remota, a uma distância suficiente para escapar dos danos de um desastre ocorrido no local principal; e
- As mídias de *backup* sejam regularmente testadas para garantir que elas são confiáveis no caso do uso emergencial.

Com relação ao armazenamento de documentos impressos em armários ou gavetas protegidos com a aplicação de uma fechadura, determinou-se, a partir da Figura 26, uma maior representatividade para afirmação negativa, o que também foi constatado na observação participante, conforme exposto na Figura 29.

Figura 29 - Guarda de documentos

Fonte: Dados da pesquisa (2015).

Nesse contexto, a ABNT NBR ISO/IEC 27002 (2013, p. 47) recomenda que os processos considerados sensíveis ou críticos, por exemplo, em papel ou em mídias de armazenamento eletrônico, sejam armazenadas em lugar seguro (armário ou outras formas de mobília de segurança) quando não estiverem em uso.

Quanto aos equipamentos eletrônicos, identificou-se segundo os resultados apresentados na Figura 26, uma maior representação para a afirmação positiva em relação à exposição desses equipamentos em condições adequadas. No entanto, durante a observação participante, foram registrados incidentes relacionados com os equipamentos de ar-condicionado, dando retorno de água em computadores, e documentos armazenados em locais indevidos, como demonstra a Figura 30.

Figura 30 - Computador e documentos em locais indevidos

Fonte: Dados da pesquisa (2015).

Nesse aspecto, a ABNT NBR ISO/IEC 27002 (2013, p. 52) orienta que todas as utilidades (como suprimento de energia elétrica, telecomunicações, suprimento de água, gás, esgoto, calefação/ventilação e ar-condicionado) estejam em conformidade com as especificações do fabricante do equipamento e com os requisitos legais da localidade; e sejam inspecionadas e testadas regularmente para assegurar o seu adequado funcionamento e evitar possíveis incidentes.

4.3.3 Evidencias de incidentes

Nessa categoria, abordou-se evidências de incidentes de segurança da informação, como perda ou extravio de documentos, modificação indevida (intencional ou acidental) dos documentos, acesso desautorizado às informações, detecção de vírus pelo antivírus, e ponto de contato, conforme detalhado no Quadro 14.

Quadro 14 - Evidências de incidentes

PERDA OU EXTRAVIO DE DOCUMENTOS	
Sujeitos	**Respostas**
S1	Aconteceu algumas vezes com relatórios da divisão, provavelmente por vírus na máquina.
S2	Ocorreu com as informações referentes ao projeto de dimensionamento que estava no e-mail institucional. Considerando que a capacidade do e-mail era pequena e eu não fiz o backup. Outras informações foram perdidas por causa da desorganização no arquivamento dos documentos.

S3	Apagaram os dados do arquivo mais importante da divisão, na verdade a informação desapareceu, eram informações bem complicadas de recuperar. O arquivo não foi recuperado e até o HD da máquina foi perdido. Isso provocou muitos desconfortos e um trabalho redobrado para adquirir as informações novamente. Foi realizada uma sindicância, onde não foi apurado como aconteceu nem quem fez.
S4	Laudos desapareceram.
S5	Faltou uma melhor organização. Após uma procura detalhada, achamos o processo ou documentos. Auxiliou para melhorar a organização dos documentos.
INFORMAÇÕES MODIFICADAS INDEVIDAMENTE	
Sujeitos	**Respostas**
S1	Pasta compartilhada que foi alterada por engano.
S2	Salvando um documento em cima do outro, sem ter o backup do anterior
ACESSO DESAUTORIZADO ÀS INFORMAÇÕES	
Sujeitos	**Respostas**
S1	Foi encontrado documento da divisão na copiadora, deixado por alguém que mexeu no arquivo sem permissão. O documento era um memorando com informações necessárias para futuras comprovações.
S2	Servidor deixou o sistema com a senha aberto e outro servidor aproveitou e modificou o cadastro
DETECÇÃO DE VÍRUS PELO ANTIVÍRUS	
Sujeitos	**Respostas**
S1	Perdi diversos arquivos da divisão como relatórios, memorandos, ofícios etc.
S2	Os arquivos foram corrompidos. Arquivos de processos digitalizados.

Fonte: Dados da pesquisa (2015).

Com base no Quadro 14, percebeu-se que a maioria dos incidentes foram ocasionados, inicialmente, por falta de uso adequado dos controles, como *backup* e proteção contra *malware*. No entanto, a partir da resposta de S3, pôde-se inferir que a ausência de controles como: autenticação individual; ausência de cópias de segurança (realizadas e testadas regularmente); e de um processo disciplinar formal para a violação da segurança da informação impossibilitam a recuperação da informação excluída ou modificada indevidamente e a identificação e punição do responsável.

Para a ABNT NBR ISO/IEC 27002 (2013, p. 88), quando um incidente de segurança da informação for detectado, torna-se necessário que seja informado

imediatamente ao ponto de contato de segurança da informação, uma vez que, pode não ser óbvio se o evento resultará em um inquérito administrativo, uma ação judicial ou simplesmente registrado pelo setor de segurança. É importante destacar que existe o perigo de uma evidência necessária ser destruída, intencionalmente ou acidentalmente, antes que a gravidade do incidente seja percebida. Nesse caso, é aconselhável manter contato com autoridades competentes.

O ponto de contato sinalizado pelos respondentes para registrar incidentes de segurança da informação não foi apresentado de forma homogênea, conforme revela o Quadro 15.

Quadro 15 - Ponto de contato

SUJEITOS	RESPOSTAS
S1	NTGI ou STI
S2	Peço ajuda aos colegas capacitados, pois o setor da Progep responsável não corresponde ao pedido e nem faz atualização e limpeza das máquinas.
S3	Colega de trabalho do setor responsável.
S4	NTGI
S5	NTGI
S6	A equipe do STI, através de solicitação eletrônica.
S7	NTGI
S8	Suporte técnico da Progep.
S9	Faço os procedimentos solicitados e procuro o NTGI quando necessário

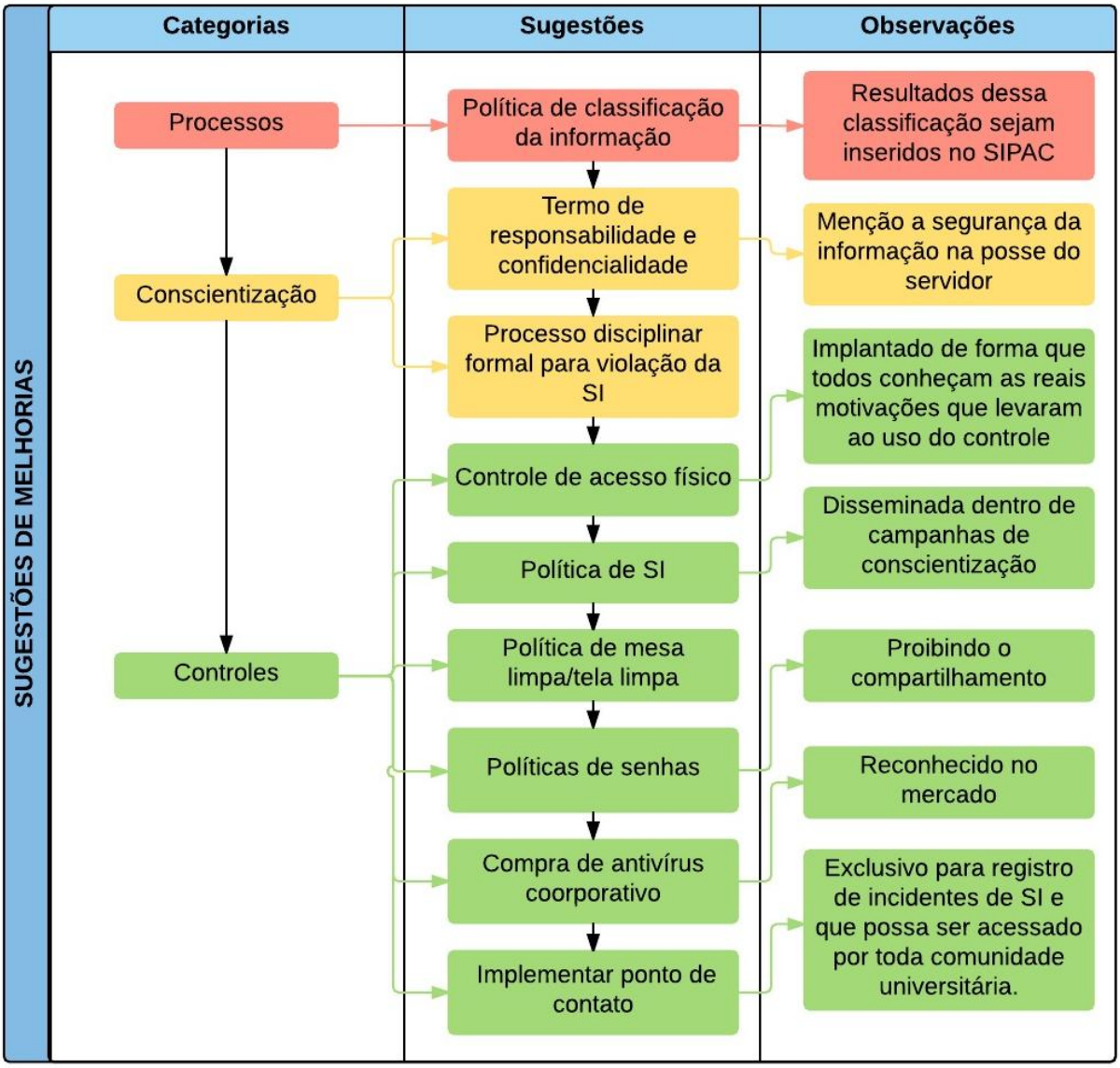
Fonte: Dados da pesquisa (2015).

Nesse contexto, um ponto de contato para notificação e detecção de incidentes deve ser implementado pela instituição para todos os funcionários e fornecedores. A UFPB possui uma central de atendimento *on-line*, localizada na página da Superintendência de Tecnologia da Informação (STI), que funciona como ponto de contato para todas as solicitações de serviços ao STI, sendo restrito aos servidores da instituição. Entretanto, a ABNT NBR ISO/IEC 27002 (2013, p. 84-85) orienta que todos os funcionários e partes externas notifiquem quaisquer fragilidades de segurança da informação, suspeita ou observada, nos sistemas ou serviços para

o ponto de contato, o mais rápido possível, de forma a prevenir incidentes de segurança da informação; e não tomar nenhuma ação isolada, porém notificar imediatamente ao ponto de contato, tomando apenas ações coordenadas. O mecanismo de notificação deve ser fácil, acessível e divulgado a todos os funcionários por meio de um programa de conscientização.

A partir das informações analisadas nas categorias processos, conscientização e controles, ilustra-se na figura 31 um resumo das sugestões apresentadas no decorrer da análise.

Figura 31 – Sugestões de melhoria



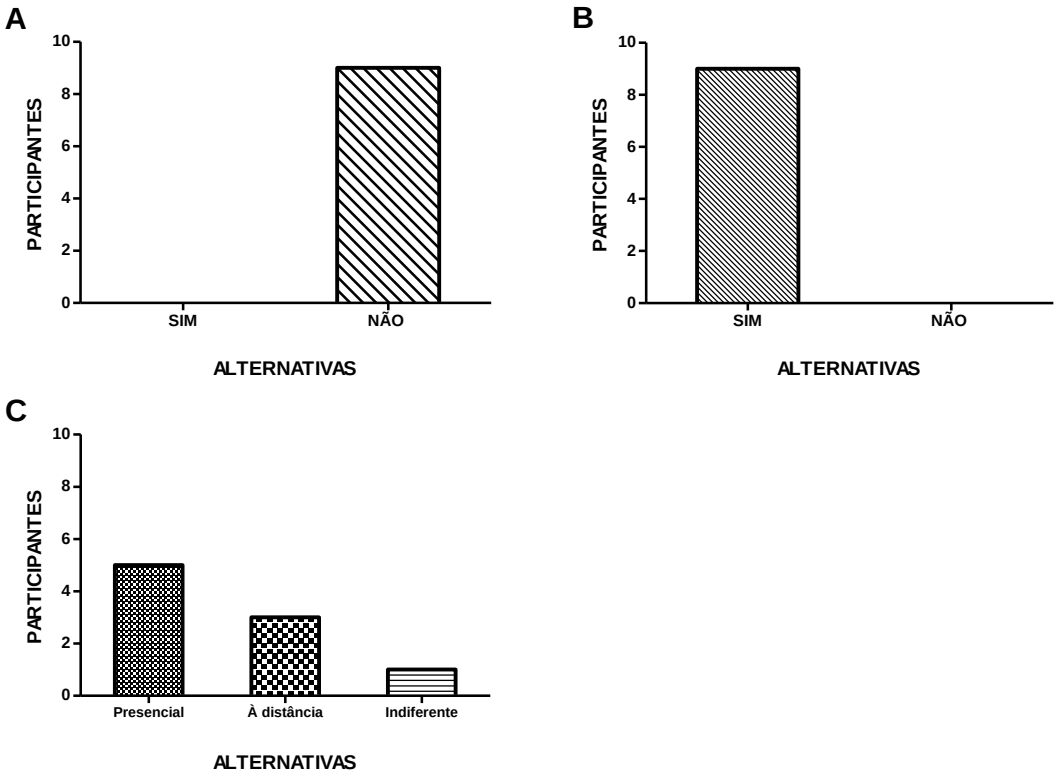
Fonte: Elaborado pela autora (2016).

4.4 PROPONDO UM PROGRAMA DE CAPACITAÇÃO EM SI PARA A UFPB

Para alcançar o objetivo específico de propor um programa de capacitação aos servidores da Progep, estabeleceu-se a categoria capacitação, que contemplou cinco aspectos. O primeiro aspecto abordou se os gestores já haviam realizado alguma capacitação em segurança da informação, cujo resultado identificou que todos os pesquisados afirmaram negativamente em relação à realização de algum tipo de capacitação nessa área. Essa condição não permitiu levantar informações para os aspectos referentes ao tipo de modalidade de curso (presencial e à distância), tipo de financiamento e os possíveis benefícios.

Com base nessas observações, foi verificada uma maior representatividade para o quinto aspecto da categoria capacitação que debateu sobre o interesse na realização de uma capacitação em segurança da informação oferecida pela Progep, bem como em qual tipo de modalidade (presencial ou à distância). Os resultados, para esse aspecto, mostraram que todos os gestores afirmaram positivamente, o que demonstrou o interesse no estabelecimento de uma capacitação em segurança da informação. A Figura 32 apresenta os resultados obtidos com a categoria capacitação.

Figura 32 - Capacitação: A) Capacitação em SI; B) Capacitação oferecida pela Progep; C) Modalidade



Fonte: Dados da pesquisa (2015).

Tendo como base a Figura 32, foi demonstrado interesse dos gestores pela referida capacitação, corroborando o que versa a orientação da ABNT NBR ISO/IEC 27002 (2013, p. 13) que ressalta: todos os funcionários da organização devem receber capacitação, educação e conscientização em segurança da informação, bem como atualizações regulares das políticas e procedimentos organizacionais relevantes para as suas funções.

Nesse sentido, Mitnick e Simon (2003, p. 228) já orientavam:

> Todas as pessoas empregadas pela empresa devem concluir um curso de treinamento em conscientização da segurança. Além disso, cada funcionário deve fazer um curso de atualização sobre conscientização de segurança em intervalos regulares, os quais não podem exceder 12 meses, conforme requisito do departamento que tem a responsabilidade do treinamento em segurança.

Para os referidos autores, um curso básico de conscientização em segurança deve ser desenvolvido de modo que todos os funcionários participem. Os novos

funcionários devem participar como parte de sua capacitação inicial. Os autores recomendam, ainda, que nenhum funcionário receba acesso a um computador, ou documento institucional, antes de ter participado de um curso básico de conscientização em segurança da informação.

Diante do exposto, para a elaboração de um programa de segurança da informação para a Progep, fez-se necessário alinhá-lo com os objetivos e as linhas de desenvolvimento/diretrizes do Plano de Capacitação e Qualificação da UFPB, exercícios 2014-2015, publicado por meio da Resolução n. 27 de 2014, além de criar o objetivo e os resultados esperados com a implantação do programa. Nesse contexto, o referido programa foi inserido dentro da linha de desenvolvimento "gestão estratégica da informação", que tem por objetivo capacitar o servidor para o uso das novas tecnologias da informação e da gestão da informação, de modo a contribuir de forma eficaz para que as metas da instituição sejam atingidas (UFPB, 2014b, p. 22).

Quanto ao programa de capacitação em segurança da informação, esse terá por objetivo conscientizar os servidores de suas responsabilidades com a segurança da informação e desenvolver competências capazes de usar os controles e os meios pelos quais essas responsabilidades sejam realizadas. O programa será composto por dois eventos de capacitação. De acordo com o Decreto 5.707 de 2006, evento de capacitação pode ser entendido como "cursos presenciais e à distância, intercâmbios, seminários e congressos, que contribuam para o desenvolvimento do servidor e que atendam aos interesses da administração pública federal direta, autárquica e fundacional." (BRASIL, 2006[33]).

Os dois eventos de capacitação, propostos para o programa de segurança da informação, são classificados como cursos, sendo um na modalidade presencial, outro à distância. Seus conteúdos programáticos têm como referência as orientações da ABNT NBR ISO/IEC 27002 (2013, p. 21). O projeto completo dos eventos encontra-se no (Apêndice E), e a estrutura geral é a seguinte:

- Curso de conscientização em SI,
    - Modalidade presencial,
    - Carga horária – 20h

[33] Documento eletrônico não paginado.

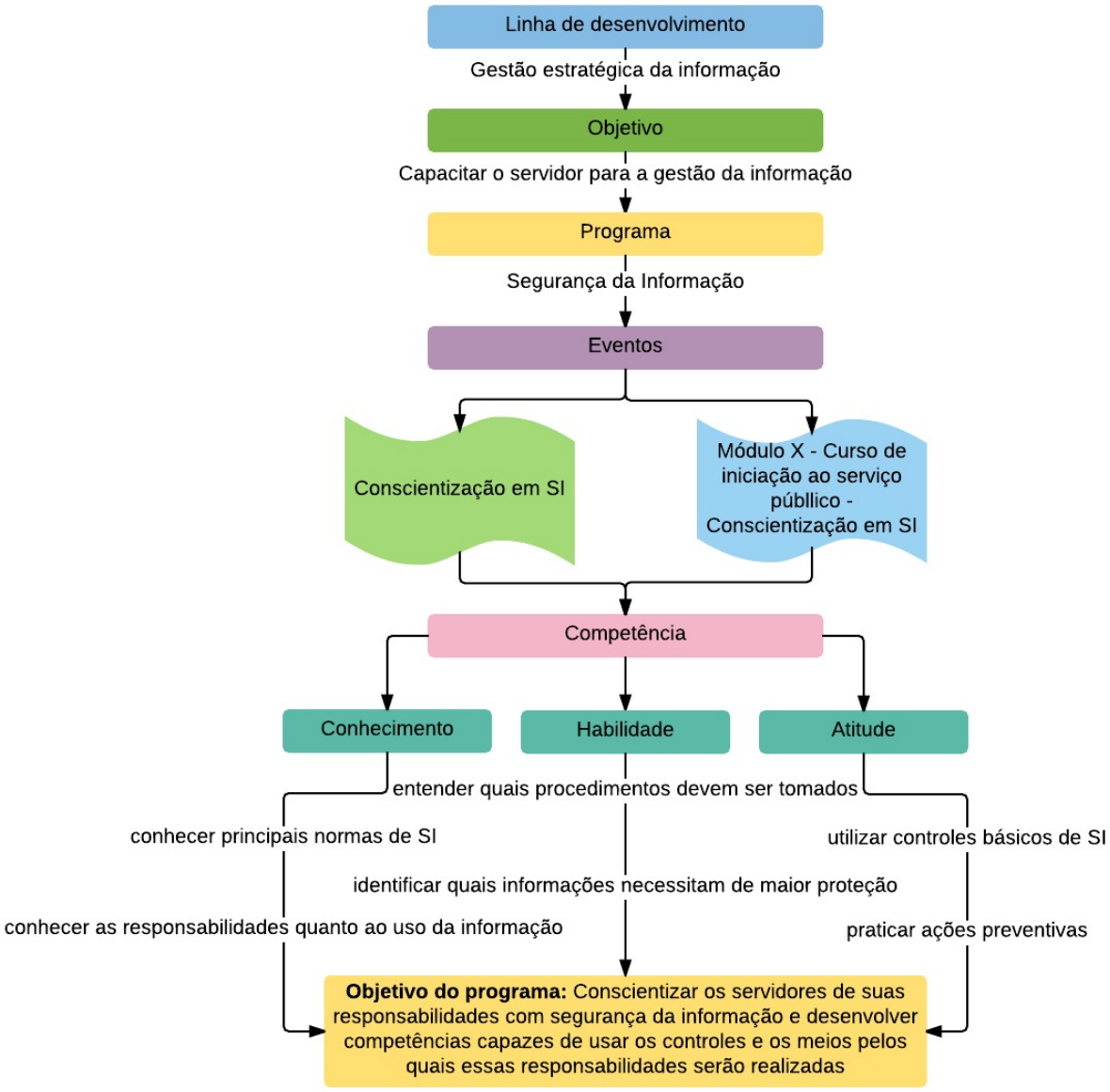
- Público alvo – todos os servidores docentes e técnico-administrativos das classes A, B,C,D e E da UFPB.
- Conteúdo Programático – conceitos e princípios básicos de segurança da informação; principais normas (a necessidade de estar em conformidade com as obrigações e regras de segurança da informação, conforme definido nas políticas, normas, decretos e leis); noções de classificação da informação, responsabilidade pessoal por seus próprios atos; procedimentos básicos de segurança da informação (tais como, notificação de incidente de segurança da informação); controles básicos (tais como segurança da senha, controles contra códigos maliciosos e política de mesa limpa e tela limpa); e pontos de contato.

- Módulo X do Curso de iniciação ao serviço público - Conscientização em SI,
  - Modalidade à distância
  - Carga horária – 20h
  - Público alvo – servidores docentes e técnico-administrativos em estágio probatório ou que foram redistribuídos nos últimos três anos.
  - Conteúdo programático - conceitos e princípios básicos de segurança da informação; principais normas (a necessidade de estar em conformidade com as obrigações e regras de segurança da informação, conforme definido nas políticas, normas, decretos e leis); noções de classificação da informação, responsabilidade pessoal por seus próprios atos; procedimentos básicos de segurança da informação (tais como, notificação de incidente de segurança da informação); controles básicos (tais como segurança da senha, controles contra códigos maliciosos e política de mesa limpa e tela limpa); e pontos de contato.

A inserção do módulo de conscientização em segurança da informação, no curso de iniciação ao serviço público, proporcionará aos novos servidores: conhecer a política da UFPB e as principais normas de SI; iniciar suas atribuições entendendo quais os procedimentos que devem ser tomados diante de determinada informação;

e esclarecer sobre suas responsabilidades e possíveis penalidades diante do manuseio indevido da informação. Essas informações sendo fornecidas no início do exercício profissional possibilitam ao novo servidor desenvolver as competências individuais necessárias ao desempenho de suas funções, visando melhor atender aos interesses da instituição, além de evitar possíveis sanções em virtude da falta de conhecimento necessário às práticas previstas nas normas e políticas de segurança da informação. A Figura 33 ilustra a proposta de inserção do programa de SI no Plano de Capacitação e Qualificação da UFPB, exercícios 2016-2017.

Figura 33 - Proposta de inserção do programa segurança da informação



Fonte: Elaborado pela autora (2015).

5 CONSIDERAÇÕES FINAIS

Para compreensão de como a segurança da informação vem sendo trabalhada nas universidades públicas e, consequentemente, como os controles sugeridos pelas normas são considerados por essas instituições, esta pesquisa se propôs a analisar a dimensão humana do processo de gestão de segurança da informação da Progep da UFPB. Essa temática ainda é pouco explorada no Brasil, e, mais raramente, em instituições públicas federais, apesar de as estatísticas do Centro de Tratamento de Incidentes de Segurança de Rede de Computadores da Administração Pública Federal - CTIR Gov evidenciarem que o Brasil, em 2015, ocupou o segundo lugar entre os países com o maior número de notificação de incidentes. Salienta-se que, além das pesquisas se mostrarem incipientes, em sua maioria, restringem-se à parte tecnológica, em detrimento dos processos e da dimensão humana.

O desenvolvimento de uma pesquisa sobre a dimensão humana no campo da segurança da informação permitiu perceber que altos investimentos em tecnologias sem a capacitação e conscientização das pessoas que, em algum momento, irão manuseá-las, contribui efetivamente para a incidência do erro humano e, consequentemente, para um ambiente bastante vulnerável a diversos tipos de ameaças. Para tanto, foi importante compreender como funciona o processo de gestão da segurança da informação e como as pessoas são inseridas nesse processo.

Com relação aos aspectos metodológicos, a utilização da triangulação dos dados obtidos, a partir dos instrumentos de coleta utilizados (observação participante, pesquisa documental e questionários), permitiu cruzar as informações de modo a refutar ou ratificar as respostas dos questionários. A amostra composta por todos os diretores nos possibilitou uma visão holística de como a Progep percebe a segurança da informação.

Os resultados possibilitaram, inicialmente, identificar a necessidade da UFPB em elaborar uma política de classificação da informação, uma vez que sua inexistência impossibilita a gestão da SI. Verificou-se, ainda, a conveniência de que os resultados dessa classificação precisam ser inseridos no SIPAC, de forma que sejam discriminados os tipos de processos, permitindo que a tramitação ocorra obedecendo à classificação do processo (sigiloso, pessoal ou ostensivo).

Quanto à conscientização em segurança da informação, observou-se a inexistência de ações que poderiam contribuir no processo de conscientização dos servidores, como: menção à segurança da informação no momento de ingresso/posse de colaboradores e servidores, o que evidenciaria a preocupação da instituição com a SI; elaboração do termo de responsabilidade e confidencialidade, dando ciência ao servidor sobre as suas responsabilidades e as penalidades decorrentes do uso indevido da informação; processo disciplinar formal para a violação da segurança da informação, o que pode desestimular servidores e colaboradores a praticar qualquer tipo de violação à segurança das informações; e ações como manuais informativos, campanhas, palestras e reuniões que também podem colaborar com a formação de uma cultura de segurança na instituição.

Na utilização dos controles de SI, observaram-se iniciativas de implantação de determinado controle, porém, os procedimentos acabaram sendo realizados de forma equivocada, sem a observância das orientações normativas. Como foi constatado, a execução de um controle de acesso físico, implementado com intuito de interditar o acesso da frente da Progep, resultou na disponibilização de cópias da chave do acesso dos fundos aos servidores da Progep, acentuando, assim, a vulnerabilidade de seu ambiente físico. De outro modo, para evitar esse tipo de sistema de segurança, poderia ser aplicado os procedimentos de registro de entrada e saída de pessoas, bem como a utilização de crachás com código de barras que diferenciem estagiários, terceirizados e servidores externos e internos à Progep.

Outro importante aspecto observado pela pesquisa refere-se à publicação da política de segurança da informação da UFPB, ocorrida apenas em 24 de outubro de 2014, por meio da Resolução CONSUNI 32/2014. Verificou-se que sua elaboração se estabeleceu apenas 14 anos após o Decreto Nº 3.505/2000, que institui a política de segurança da informação nos órgãos e entidades da Administração Pública Federal, demonstrando que a instituição percorreu considerável período de tempo sem se ater ao compromisso de desenvolver ações, projetos, programa, normas e procedimentos que procurassem conscientizar a comunidade universitária da importância da segurança da informação, conforme orienta as normas do governo federal.

Foi possível constatar, após a publicação da Resolução 32/2014, que apesar de ter sido divulgada aos servidores docentes e técnico-administrativos pelo SIG, essa política ainda não se tornou conhecida por todos, como evidenciado nesta

pesquisa. Essa forma de divulgação não é suficiente à implementação de políticas de segurança, uma vez que é necessário que haja um programa de conscientização em segurança da informação em que a disseminação dessa política seja acompanhada por outras ações e normas que coadunam para uma mudança de comportamento.

Dentre as políticas analisadas, precisa ser considerada a de mesa limpa/tela limpa como controle necessário para mitigar o acesso não autorizado e a perda ou dano à informação, visto que essa política pode contribuir para a conscientização dos servidores, de modo a deixar mais latente a necessidade de maior cuidado com as informações que estão sendo manuseadas. Outra política que precisa ser implementada e formalizada pela UFPB, bem como inserida em um programa de conscientização, refere-se à política de senhas. Observou-se que, apesar de utilizarem senhas seguras, as mesmas são compartilhadas com os servidores da mesma divisão, criando, com isso, uma falsa sensação de segurança. Nesse sentido, é importante destacar a necessidade de compra de antivírus corporativo já consolidado no mercado, padronizando o referido controle, de modo a torná-lo mais eficaz.

Durante a pesquisa, observou-se também a necessidade de um ponto de contato exclusivo para registro de incidentes de segurança da informação, que seja extensivo a alunos, fornecedores e colaboradores.

Diante do exposto, evidenciou-se que a gestão da segurança da informação ainda não é trabalhada de forma contundente nas instituições públicas federais, demonstrando serem ainda insuficientes as ações de segurança da informação, de modo que possam contribuir com os objetivos da instituição. Referente às contribuições desta pesquisa para a UFPB, a Progep, por meio de sua Coordenação de Desenvolvimento de Pessoas e da Divisão de Educação e Capacitação Profissional, inseriu o curso de Conscientização em Segurança da Informação no instrumento que compõe as demandas de capacitação dos docentes e servidores técnico-administrativos. Essas demandas já haviam sido identificadas pela Progep durante o Levantamento de Necessidade de Capacitação (LNC) para 2016-2017. Na LNC, os gestores da UFPB ratificaram a necessidade do referido curso. Desse modo, conforme proposta apresentada nesta pesquisa foi inserido o Programa Segurança da Informação no Plano de Capacitação e Qualificação dos Servidores da UFPB – Exercício 2016-2017, bem como os cursos de Conscientização em

Segurança da Informação, conforme projeto apresentado no Apêndice E. As primeiras turmas do curso de conscientização estão previstas para iniciarem ainda neste semestre.

Nesta pesquisa, apresentou-se como principal limitador, a greve dos servidores das universidades públicas federais no ano de 2015 e que se prolongou por quase cinco meses, o que inviabilizou a aplicação da primeira opção de método de coleta que seria o grupo focal, o que poderia ter proporcionado a esta pesquisa uma discussão enriquecedora sobre como a SI está sendo abordada pela Progep.

Com base no exposto, os resultados desta pesquisa podem auxiliar a minimizar a incidência de ameaças à segurança da informação na Progep, bem como contribuir com a criação de uma cultura de segurança na UFPB.

Esta pesquisa não encerra esta discussão. Essa é uma temática que necessita de uma maior compreensão de modo a gerar considerações consistentes a esse assunto tão presente e significativo. Para futuras pesquisas, pode-se considerar: acompanhar os servidores que realizaram a capacitação em conscientização da segurança da informação de modo a avaliar se houve ou não uma mudança de comportamento, e se essa mudança está contribuindo para criação de uma cultura de segurança da informação nos setores onde estes servidores estão inseridos; a elaboração de um modelo de classificação para Instituições de Ensino Superior que pudesse ser utilizado pelas universidades e institutos federais; e pesquisar sobre a mudança ou não no comportamento dos servidores após a implantação de políticas de segurança da informação nas instituições federais.

REFERÊNCIAS

ALBRECHTSEN, E. A qualitative study of users' view on information security. **Computers & Security**, v. 26, n. 4, p. 276-289, 2007. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0167404806002033>. Acesso em: 20 fev. 2015

ARANTES, T. F. **Práticas organizacionais de estímulo à segurança da informação e percepção de mudança organizacional**: influência nas atitudes e comportamentos de segurança. 2012. 108 f. Dissertação (Mestrado em Psicologia Social do Trabalho e das Organizações) – Universidade de Brasília, Brasília, 2012. Disponível em: <http://repositorio.unb.br/bitstream/10482/10573/1/2012_TalitaFreireArantes.pdf>. Acesso em: 02 fev. 2015.

ARAÚJO, C. A. A. de. Fundamentos da CI: correntes teóricas e o conceito de informação. **Perspectivas em Gestão & Conhecimento**, João Pessoa, v. 4, n.1, p.57-79, jan./jun. 2014.

ARAÚJO, W. J.; AMARAL, S. A. A segurança do conhecimento nas práticas da gestão da segurança da informação e da gestão do conhecimento. In: ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO. 11., Rio de Janeiro, 2010. **Anais**... Rio de Janeiro: UFSCar, 2014.

ARAÚJO, W. J. **Segurança do conhecimento nas práticas da gestão de segurança da informação e da gestão do conhecimento**. 2009. 280 f. Tese (Doutorado em Ciência da Informação) – Universidade de Brasília, Brasília, 2009.

ARAÚJO, G. **Polícia federal confirma vazamento do tema da redação no Enem do Piauí**. PORTAL G1, 2014. Disponível em:<http://g1.globo.com/pi/piaui/noticia/2014/12/policia-federal-confirma-vazamento-do-tema-da-redacao-do-enem-no-piaui.html>. Acesso em: 20 mar. 2015.

ARAÚJO, S. G. L. A.; BATISTA, R. R.; ARAÚJO, W. J. Aspectos humanos da segurança da informação. In: ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO. Enancib.16, 2015,João Pessoa,. **Anais**... João Pessoa: UFPB, 2015.

ASHENDEN, D. Information security management: a human challenge? **Information Security Technical Report**, v. 1, p. 95-201, 2008. Disponível em: <http://www.sciencedirect.com/science/article/pii/S1363412708000484>. Acesso em: 02 fev. 2015.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001**: tecnologia da informação: técnicas de segurança: sistemas de gestão da segurança da informação: requisitos. Rio de Janeiro, 2013.

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

_____. **Catálogo**: segurança, qualidade, padrão e confiança. 2014. Disponível em: <https://www.abntcatalogo.com.br/normagrid.aspx>. Acesso em: 16 abr. 2015.

ASSOCIAÇÃO NACIONAL DE PESQUISA E PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO. **ENANCIB**: encontro nacional de pesquisa em ciência da informação. [20--]. Disponível em: <http://enancib.ibict.br/index.php/enancib/index>. Acesso em: 23 abr. 2015.

ÁVILA, R. O; SILVA, R. P. Brasil informacional: a segurança cibernética como desafio à segurança nacional. In: ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO, 12., 2011, Brasília. **Anais**... Brasília: UNB, 2011.

AZEVEDO, C.E.F; OLIVEIRA, L.G.L; GONZALEZ, R. K; ABDALLA, M. M. A. **A Estratégia de Triangulação**: objetivos, possibilidades, limitações e proximidades com o pragmatismo.In: IV Encontro de Ensino e Pesquisa em Administração e Contabilidade. Brasília 2013. Disponível em: <http://www.anpad.org.br/diversos/trabalhos/EnEPQ/enepq_2013/2013_EnEPQ5.pdf >. Acesso em: 5 maio 2015.

BARDIN, L. **Análise de conteúdo**. Tradução de Luís Antero Reto e Augusto Pinheiro. Lisboa: Edição 70, 2008.

BARMAN, S. **Writing information security polices**. Indianapolis: New Riders, 2002.

BEAL, A. **Gestão estratégica da informação**: como transformar a informação e a tecnologia da informação em fatores de crescimento de alto desempenho nas organizações. São Paulo: Atlas, 2011.

_____. **A segurança da informação**: princípios e melhores práticas para a proteção dos ativos de informação. São Paulo: Atlas, 2008.

BORKO, Harold. Information science: what is it?. **American documentation**, v. 19, n. 1, p. 3-5, 1968.

BRASIL. Decreto nº 3.505, de 13 de junho de 2000. Institui a política de segurança da informação nos órgãos e entidades da administração pública federal e dá outras providências. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 14 jun. 2000. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/D3505.htm>. Acesso em: 25 jul. 2014.

_____. Presidência da República. Gabinete de Segurança Institucional. **Estratégia de segurança da informação e comunicações e de segurança cibernética da administração pública federal 2015-2018**: versão 1.0. Brasília: Presidência da República, 2015. Disponível em: <http://dsic.planalto.gov.br/documentos/publicacoes/4_Estrategia_de_SIC.pdf>. Acesso em: 25 maio 2015.

_____. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública

Federal. **Estatísticas de Incidentes de Rede na APF**: Ano 2015. Brasília: Presidência da República, 2016. Disponível em: < http://www.ctir.gov.br/arquivos/estatisticas/2015/Estatisticas_CTIR_Gov_Ano_2015.pdf>. Acesso em: 02 mar 2016.

_____. Presidência da República. Gabinete de Segurança Institucional. **Instrução Normativa 20/IN01/DSIC/GSIPR**. Diretrizes de segurança da informação e comunicações para instituição do processo de tratamento da informação nos órgãos e entidades da Administração Pública Federal. DF, 15 jul. 2014. Disponível em: <http://dsic.planalto.gov.br/documentos/nc_20_TRATAMENTO_DA_INFORMACA.pdf>. Acesso em: 22 abr. 2015.

_____. Presidência da República. Gabinete de Segurança Institucional. **Instrução Normativa GSIPR n. 1**, de 13 de junho de 2008. Disciplina a gestão da segurança da informação e comunicações na administração pública federal, direta e indireta e dá outras providências. DF, 13 jun. 2008. Disponível em: <http://dsic.planalto.gov.br/legislacaodsic/23-dsic/legislacao/52-instrucoes-normativas>. Acesso em: 22 abr. 2015.

_____. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. **Normas Complementares à IN Nº 01 GSI/PR/2008**. Segurança da Informação e Comunicações. 2015. Disponível em: <http://dsic.planalto.gov.br/legislacaodsic/23-dsic/legislacao/53-normas-complementares>. Acesso em: 01 abr. 2015.

_____. Presidência da República. Casa Civil. **Decreto-Lei n. 5.707**, de 23 de fevereiro de 2006. Institui a Política e as Diretrizes para o Desenvolvimento de Pessoal da administração pública federal direta, autárquica e fundacional, e regulamenta dispositivos da Lei 8.112, de 11 de dezembro de 1990. Diário Oficial da União, Brasília, ano CXLIIII, n. 40, seção 1, p. 3-4. Disponível em: <http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=24/02/2006&jornal=1&pagina=1&totalArquivos=240>. Acesso em jan 2015. 2006 a.

_____. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Lei nº 9.983, de 14 de julho de 2000**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal e dá outras providências. 2000. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L9983.htm>. Acesso em: 01 abr. 2015.

CAPURRO, R.; HJØRLAND, B. O conceito de informação. **Perspectivas em Ciências da Informação**, Belo Horizonte, v. 12, n. 1, p. 148-07, jan./abr. 2007**.** Disponível em: <http://portaldeperiodicos.eci.ufmg.br/index.php/pci/article/view/54>. Acesso em: 12 jul. 2014.

CARNEIRO, L. E. S; ALMEIDA, M. B. Segurança da informação: uma investigação na perspectiva do usuário de sistemas de informação corporativos em uma organização de saúde. In: CONFERÊNCIA IBERO AMERICANA DE COMPUTAÇÃO APLICADA, 2013, Porto Alegre. **Anais eletrônicos**... Porto Alegre, 2013. Disponível em: <http://mba.eci.ufmg.br/downloads/IADIS%20Conference%20Seg%20Inform%20camera%20ready%20web.pdf>. Acesso em: 11 mar. 2015.

CHIZZOTTI, A. **Pesquisa em ciências humanas e sociais**. São Paulo: Cortez, 1991.

COLWILL, C. Human factors in information security: the insider threat - Who can you trust these days?.**Information Security Technical Report**, v. 14, p. 186-196, nov. 2009. Disponível em: <http://www.sciencedirect.com/science/article/pii/S1363412710000051>. Acesso em: 02 fev. 2015.

CUNHA, L. M. A. **Modelos Rasch e escalas de Likert e Thurstone na medição de atitudes**. 2007. 78 f. Dissertação (Mestrado em Probabilidades e Estatística) – Faculdade de Ciências, Universidade de Lisboa, Lisboa, 2007

DARYUS. **Pesquisa Nacional de Segurança da Informação**. Daryus *Strategic Risk Consulting*, 2014, Disponível em: <http://datasus.saude.gov.br/images/Pesquisa_Nacional_de_Seguran%C3%A7a_da_Informa%C3%A7%C3%A3o_2014_-_DARYUS.pdf >. Acesso em: 20 mar. 2015.

DENZIN, N. K. **The research act**. 3. ed. Englewood Cliffs, NJ: Prentice Hall, 1989.

FERREIRA, F. N. F; ARAÚJO, M. T. **Política de segurança da informação**. Rio de Janeiro: Ciência Moderna, 2008.

FERREIRA, J. O.; ARAÚJO, W. J. Análise de risco no sistema de concessão de diárias e passagens (SCDP): estudo de caso sob a ótica da segurança da informação no departamento contábil da UFPB. In: ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO, 14., 2013, Florianópolis. **Anais**... Florianópolis: UFSC, 2013.

FERREIRA, J. O. Análise sob a ótica da segurança em sistemas de informação: estudo de caso aplicado ao Sistema de Concessão de Diárias e Passagens (SCDP) no Departamento Contábil da UFPB / Ferreira. Dissertação de Mestrado em Ciência da Informação – João Pessoa, 2013.

FERNANDES, J. H. C. Segurança da informação: nova disciplina na ciência da informação? In: ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO, 11., 2010, Rio de Janeiro. **Anais**... Rio de Janeiro: IBICT, 2010.

FONTES, E. L. G. **Políticas e normas para a segurança da informação**: como desenvolver, implementar e manter regulamentos para a proteção da informação nas organizações. Rio de Janeiro: Brasport, 2012.

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

FONTANELLA, B. J. B.; RICAS, J.; TURATO, E. R. Amostragem por saturação em pesquisas qualitativas em saúde: contribuições teóricas. **Cad saúde pública**, v. 24, n. 1, p. 17-27, 2008.

FRANGOPOULOS, E. D.; ELOFF, M. M.; VENTER, L. M. Psychosocial risks: can their effects on the security of information systems really be ignored? **Information Management & Computer Security**, v. 21, n. 1, p. 53-65, 2013. Disponível em: <http://www.emeraldinsight.com/doi/full/10.1108/09685221311314428>. Acesso em: 10 fev. 2015.

GIL, A. C. **Métodos e técnicas de pesquisa social**. 6 ed. São Paulo: Atlas, 2012.

GONÇALVES, E. P. **Conversas sobre iniciação à pesquisa científica**. Alínea, 2001.

GREITZER, F.L; FRINCKE, D. A. Combining traditional cyber security audit data with psychosocial data: towards predictive modeling for Insider threat mitigation. **InsiderThreats in Cyber Security**, v. 49, p. 85-113, 2010.

INFORMATION SYSTEMS AUDITAND CONTROL ASSOCIATION. **COBIT 5 for Information Security**. Rolling Meadows, IL: ISACA, 2012. Disponível em: <https://www.isaca.org/COBIT/Documents/COBIT-5-for-Information-Security-Introduction.pdf>. Acesso em: 13 abr. 2015.

INTERNATIONAL ORGANIZATION FOR STANDARTIZATION (ISACA). **ISO/IEC 27000**: information technology: security techniques: information security management systems: overview and vocabulary. 2014. Disponível em: <http://k504.org/attachments/article/819/ISO_27000_2014.pdf>. Acesso em: 22 abr. 2015

ISONI, M. M.; VIDOTTI, S. A. B. G. Percepções de segurança e ameaças em ambientes de tecnologias da informação. In: ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO, 8., 2007, Salvador. **Anais**... Salvador: UFBA, 2007.

JORNAL O ESTADO DE SÃO PAULO. **Eli Lilly deixa vazar 600 e-mail de pacientes**. 2001, Disponível em: <http://internacional.estadao.com.br/noticias/geral,eli-lilly-deixa-vazar-600-e-mails-de-pacientes,20010705p25471>. Acesso em: 20 mar. 2015.

LAKATOS, E. M; MARCONI, M. A. **Fundamentos da metodologia cientifica**. 6. ed. São Paulo: Atlas, 2007.

LAUDON, K. C.; LAUDON, J. P. **Sistemas de informação gerenciais: administrando a empresa digital**. São Paulo: Prentice Hall, 2004.

LAVILLE, C; DIONNE, J. **A construção do saber**: manual de metodologia da pesquisa em ciências humanas. Tradução de Heloisa Monteiro e Francisco Settineri. Porto Alegre: Artmed; Belo Horizonte: Editora UFMG, 1999.

MARCELO, A; PEREIRA, M. **A arte de hackear pessoas**. Rio de Janeiro: Brasport, 2005.

MARCIANO, J. L. P.; MARQUES, M. L. O enfoque social da segurança da informação. **Ci. Inf.**, Brasília, v. 35, n. 3, p. 89-98, set./dez. 2006.

MARCIANO, J. L. P. **Segurança da informação**: uma abordagem social. 2006. 212 f. Tese (Doutorado em Ciência da Informação) – Universidade de Brasília, Brasília, 2006.

MINAYO, M. C. S. (Org). **Pesquisa social**: teoria, método e criatividade. 28. ed. Petrópolis: Vozes, 2009.

MINAYO, M. C. S.; ASSIS, S. G.; SOUZA, E. R. (Org.). Avaliação por triangulação de métodos: Abordagem de Programas Sociais. Rio de Janeiro: Fiocruz, 2010.

MITNICK, K. D.; SIMON, W. L. A. **A arte de enganar**: ataque de hackers - controlando o fator humano na segurança da informação. São Paulo: Pearson Education do Brasil, 2003.

MÓDULO TECHNOLOGY FOR RISK MANAGEMENT. **10ª Pesquisa Nacional de Segurança da Informação**. Módulo Technology For Risk Management, 2006. Disponível em: <https://www.modulo.com.br/media/10a_pesquisa_nacional.pdf.>Acesso em: 23 de mar. de 2015.

MÜLLER, S. P. M. **Métodos para pesquisa em CI**. Brasília: Thesaurus, 2007.

NIEKERK, V. J. F; SOLMS, V. R. Information security culture: a management perspective. **Computers & Security**, v. 20, p. 476-486, 2010. Disponível em: <http://www.sciencedirect.com/science/article/pii/S1071581907000560>. Acesso em: 06 mar. 2015.

PORTAL TERRA. **Coca-cola**: condenada secretária por roubo de segredo. 2007, Disponível em: <http://veja.abril.com.br/noticia/economia/hsbc-suico-escondeu-dinheiro-suspeito-de-ditadores-e-celebridades/>. Acesso em: 20 de mar. 2015.

PRAZERES, L. **PF vai investigar suposto vazamento de informações da operação Lava Jato**. PORTAL UOL, 2014. Disponível em: <http://noticias.uol.com.br/politica/ultimas-noticias/2014/11/19/pf-vai-investigar-suposto-vazamento-de-informacoes-da-operacao-lava-jato.htm>Acesso em: 20 de mar. 2015.

PWS. **Pesquisa global de segurança da informação**. PWS, 2014. Disponível em: <https://www.pwc.com.br/pt_BR/br/publicacoes/servicos/assets/consultoria-negocios/pesq-seg-info-2014.pdf>. Acesso em: 04 maio 2015.

PWS. **Pesquisa global de segurança da informação**. PWS, 2011. Disponível em: <://www.pwc.com.br/pt/estudos-pesquisas/pesquisa-global-seguranca-informacao.jhtml > Acesso em: 04 maio 2015.

RICHARDSON, R. J. **Pesquisa social**: métodos e técnicas. 3 ed. São Paulo: Atlas, 2009.

ROCHA, P. C. C. **Segurança da informação**: uma questão não apenas tecnológica. 2008. 61 f. Trabalho de Conclusão de Curso (Especialização) – Departamento de Ciência da Computação, Universidade de Brasília, Brasília, 2008.

SASSE, M. A.; BROSTOFF, S.; WEIRICH, D. Transforming the 'weakest link': a human/computer interaction approach to usable and effective security. **BT Technology Journal**, v. 19, n. 3, p. 122–131, July 2001. <http://hornbeam.cs.ucl.ac.uk/hcs/publications/Sasse%2BBrostoff%2BWeirich_A%20human-computer%20interaction%20approach%20to%20usable%20and%20effective%20security_BTTJ2001.pdf >. Acesso em: 11 mar. 2015

SCHNEIER, B. **Secrets and lies**: digital security in a networked world. New York: Wiley, 2004.

SCHULTZ, E. The human factor in security.**Computers & Security**, v. 24, p. 425-426, 2005. Disponível em: <http://www.sciencedirect.com/science/article/pii/S1071581907000560>. Acesso em: 10 fev. 2015.

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

SARACEVIC, T. Ciência da informação: origem, evolução e relações. **Perspectiva em Ciência da Informação**, Belo Horizonte, v. 1, n. 1, 1996.

SILVA, A. E. N. **Segurança da informação**: vazamento de Informações: as informações estão realmente seguras em sua empresa? Rio de Janeiro: Ciência Moderna Ltda, 2012.

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

SILVA, N. B. X.; ARAÚJO, W. J. AZEVEDO, P. M. Análise de informações pessoais na web: métrica para identificar o grau de exposição da informação. In: ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO, 14., 2013, Florianópolis. **Anais**... Florianópolis: UFSC, 2013.

SILVA, S. L; ARAUJO, W. J. Modelo para o descarte seguro da informação em suporte digital. In: ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO, 15. Belo Horizonte. 2014, **Anais**... Belo Horizonte: ECI, UFMG, 2014. p. 3572-3579.

SIPONEN, M. T. Five dimension sofinformation security awareness. **Computers and Society**, v. 31, n. 2, p. 24-49, jun. 2001. Disponível em: <http://dl.acm.org/citation.cfm?id=503348>. Acesso em: 06 fev. 2015.

SYSADMIN, AUDIT, NETWORKING AND SECURITY. **Interested in learning more about security?**. SANS Institute, 2007. Disponível em :

<http://www.sans.org/reading-room/whitepapers/policyissues/information-security-policy-development-guide-large-small-companies-1331>. Acesso em: 22 abr.2015.

_____. **Clean Desk Policy**. SANS Institute, jun. 2014. Disponível em: <http://www.sans.org/security-resources/policies/general/pdf/clean-desk-policy>. Acesso em: 14 abr. de 2015.

TRIBUNAL DE CONTAS DA UNIAO (TCU). **Boas práticas em segurança da informação**. 3. ed. Brasília, 2007.

_____. **Relatório de levantamento**. Avaliação da governança de tecnologia da informação na Administração Pública Federal. 2014. Disponível em: <http://www.tcu.gov.br/Consultas/Juris/Docs/judoc/Acord/20141114/AC_3117_45_14_P.doc>. Acesso em: 15 jan. 2015.

_____. **Relatório de levantamento**. Avaliação da governança de tecnologia da informação na Administração Pública Federal. 2012. Disponível em: http://portal2.tcu.gov.br/portal/page/portal/TCU/comunidades/tecnologia_informacao/pesquisas_governanca/D500BE942EEF7793E040010A89001367>. Acesso em: 01 abr. 2015.

TRIVIÑOS, A. N. S. **Introdução à pesquisa em ciências sociais**: a pesquisa qualitativa em educação. São Paulo: Atlas, 1987.

UNIVERSIDADE FEDERAL DA PARAÍBA (UFPB). **Resolução 32/2014**. Política de Segurança da Informação. UFPB. 2014a. Disponível em: <http://www.ufpb.br/cgti/?q=node/47>. Acesso em: 01 Abr. 2015.

_____. Conselho Universitário. **Resolução n. 27 de 2014**. UFPB. 2014b. Autoriza a implementação do Plano de Capacitação e Qualificação, para os exercícios de 2014-2015, desta Universidade. Disponível em: < http://www.ufpb.br/sods/consuni/resolu/2014/Runi27_2014.pdf>. Acesso em 30 de mar. 2015.

_____. **Plano de Desenvolvimento Institucional 2014-2018**. UFPB. 2015. Disponível em: <http://www.ufpb.br/sites/default/files/pdfs/PDI%20UFPB%202014-2018_Final3%20-27.05.pdf>. Acesso em: 07 jun. 2015.

_____. **Relatório de Gestão**. 2013. Disponível em: <http://www.ufpb.br/sites/default/files/pdfs/Relatorio-de-Gestao-2013-UFPB.pdf>. Acesso em: 07 maio. 2015.

_____. **Regimento Interno da Pró-Reitoria de Gestão de Pessoas PROGEP.** 2012. Disponível em: <http://www.progep.ufpb.br/?q=regimento>. Acesso em: 07 maio 2015.

VALENTIM, M. L. P.(Org.). **Métodos qualitativos de pesquisa em Ciência da Informação**. São Paulo: Polis, 2005.

VEJA.COM. **HSBC suíço escondeu dinheiro suspeito de ditadores**. 2015. Disponível em: <http://veja.abril.com.br/noticia/economia/hsbc-suico-escondeu-dinheiro-suspeito-de-ditadores-e-celebridades/>. Acesso em: 20 de mar. 2015.

VERGARA, S. C. **Projetos e relatórios de pesquisa em administração**. 7. ed. São Paulo: Atlas, 2006.

VIANNA, E. W. **Análise do comportamento informacional na gestão da segurança cibernética da Administração Pública Federal**. 2015. 131 f. Dissertação (Mestrado em Ciência da Informação) – Universidade de Brasília, Brasília, 2015.

YIN, R. K. **Estudo de caso**: planejamento e métodos. 2. ed. Porto Alegre: Bookman, 2001.

APÊNDICE A - SIGLAS DOS SETORES DA PROGEP

SETORES	DEFINIÇÃO
PROGEP	Pró-Reitoria e Gestão de Pessoas
ATPLAN	Assessoria Técnica e de Planejamento
CAS	Central de Atendimento ao Servidor
CDP	Coord. de Desenvolvimento de Pessoas
CEDESP	Centro de Desenvolvimento do Servidor Público
CPACE	Comissão Permanente de Acumulação de Cargos e Empregos
CPGP	Coord. de Proc. de Gestão de Pessoas
CPPD	Comissão Permanente de Pessoal Docente
CQVSST	Coord. Qualidade de Vida, Saúde e Segurança no Trabalho
DB	Divisão de Benefícios
DCPS	Divisão de Cadastro e Pagamento de Servidores
DECP	Divisão de Educação e Capacitação Profissional
DGP	Divisão de Gestão de Desempenho
DIST	Divisão de Segurança do Trabalho
DLCP	Divisão de Legislação e Controle de Processos
DPC	Divisão de Planejamento e Carreira
DQVB	Divisão de Qualidade de Vida
DSP	Divisão de Seleção e Provisão

Fonte: Dados da pesquisa (2015).

APÊNDICE B – QUESTIONÁRIO

UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO

QUESTIONÁRIO - Divisão de Educação e Capacitação Profissional (DECP)

As informações resultantes deste questionário serviram como subsídio para a pesquisa intitulada: A DIMENSÃO HUMANA NO PROCESSO DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO: um estudo aplicado à Pró-Reitoria de Gestão de Pessoas da Universidade Federal da Paraíba, da Mestranda Sueny Gomes Léda Araújo. As informações serão utilizadas estritamente para fins acadêmicos, podendo os resultados ser publicados em eventos ou periódicos científicos, sempre sem fins lucrativos e resguardando a identidade dos respondentes.
Agradecemos sua contribuição!

1 Perfil do Gestor

1.1 Faixa etária:
( ) Entre 20 e 30 anos
( ) Entre 31 a 40 anos
( ) Entre 41 a 50 anos
( ) Acima de 51 anos

1.2 Sexo: ( ) Masculino ( ) Feminino

1.3 Formação Acadêmica:
( ) Ensino Médio
( ) Graduação
( ) Especialização
( ) Mestrado
( ) Doutorado

1.4 Tempo de instituição:
( ) Menos de 1 ano
( ) 1 a 5 anos
( ) 6 a 10 anos
( ) 11 a 15 anos
( ) Mais de 16 anos

1.5 Tempo na função:
( ) Menos de 1 ano
( ) 1 a 3 anos
( ) 4 a 6 anos
( ) 7 a 9 anos
( ) Mais de 10 anos

2 Processos

2.1 Existe classificação da informação quanto aos requisitos legais (sigilosa, pessoal e ostensiva) na Progep.

Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
01	02	03	04	05

2.2 Classifique os processos da sua divisão quanto aos requisitos legais, colocando:

S - Sigiloso protegido por legislação específica (informações bancária, fiscal e contábil**; p**rocesso administrativo disciplinar em curso; acesso a documento preparatório, inquérito policial etc.);

P - Pessoal (informação relacionada à pessoa natural identificada ou identificável, relativa à intimidade, vida privada, honra e imagem); e

O - Ostensivo (pode ser mostrado, sem restrição).

( ) Progressão por Capacitação (Técnico-administrativo)

( ) Revisão de Enquadramento (Técnico-administrativo)

( ) Incentivo à Qualificação (Técnico-administrativo)

( ) Editais de Curso de Capacitação para Servidores

( ) Registro de Horas de Pagamento pela Gratificação por Encargo de Curso e Concurso

( ) Solicitação de pagamento dos instrutores e coordenadores dos cursos de capacitação

3 Conscientização em segurança da informação

3.1 Existe menção a segurança da informação no momento de ingresso/posse dos colaboradores.

Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
01	02	03	04	05

3.2 A Progep possui processo disciplinar formal para as violações da segurança da informação.

Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
01	02	03	04	05

3.3 A Progep possui um “termo de responsabilidade e confidencialidade” dando ciência do conhecimento das normas e suas principais responsabilidades em relação à segurança da informação? ( ) Sim ( ) Não

3.4 Considera importante a assinatura do termo de responsabilidade e confidencialidade.

Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
01	02	03	04	05

3.5 Mantém-se informado sobre as notícias e relatórios de Segurança da Informação?

( ) Sim ( ) Não

3.6 Quais ações de conscientização em segurança da informação a Progep desenvolve?

( ) Avisos em murais

( ) Manuais informativos

( ) Campanhas. Quais

( ) Reuniões

( ) Não possui ações

( ) Outros. Quais?

4 Capacitação

4.1 Você já realizou alguma capacitação em Segurança da Informação? ( ) Sim ( ) Não

Se sim, o que levou você a realizar esse curso?

4.2 Em que modalidade o curso se apresentou? ( ) Presencial ( ) À distância

4.3 Foi financiado pela Progep? ( ) Sim ( ) Não

4.4 Quais benefícios o curso trouxe para o seu ambiente de trabalho?

4.5 Você gostaria de fazer um curso em Segurança da Informação oferecido pela Progep?

( ) Sim ( ) Não

Se sim, em que modalidade? ( ) Presencial ( ) À distância ( )Indiferente

5 Controles

5.1 Existe controle de acesso físico no seu ambiente de trabalho.

Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
01	02	03	04	05

Se concorda, como funciona?

5.2 A Política de Segurança da Informação da UFPB influencia nas suas rotinas de trabalho.

Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
01	02	03	04	05

Se concorda, de que forma?

5.3 Há política de mesa limpa/tela limpa para os recursos de processamento da informação.

Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
01	02	03	04	05

5.4 Os sistemas que você utiliza possuem política de senhas? ( ) Sim ( ) Não

5.5 Substitui suas senhas periodicamente? ( ) Sim ( ) Não

5.6 Utiliza senhas seguras (com variação de caracteres)? ( ) Sim ( ) Não

5.7 Deixa sua senha em locais de fácil acesso? ( ) Sim ( ) Não

5.8 Compartilha senhas com terceiros? ( ) Sim ( ) Não

Se sim, por quê?

5.9 O programa de antivírus que você utiliza foi indicado pela Progep? ( ) Sim ( ) Não

5.10 Atualiza o antivírus de seu computador com frequência? ( ) Sim ( ) Não

5.11 Verifica a origem de arquivos anexados em e-mail e passa antivírus antes de abri-los?

( ) Sim ( ) Não

5.12 Bloqueia a tela do computador por meio de senha antes de se ausentar por período prolongado?
( ) Sim ( ) Não

5.13 Ingere líquidos ou alimentos próximo a computadores? ( ) Sim ( ) Não

5.14 Sua divisão realiza cópias de segurança das informações? ( ) Sim ( ) Não

5.15 Os documentos impressos são guardados em armários ou gavetas com chaves?

( ) Sim ( ) Não

5.16 Os equipamentos eletrônicos estão expostos a condições adequadas? ( ) Sim ( ) Não

6 Evidencias de incidentes de segurança

6.1 Nos últimos 5 anos você sofreu com a perda ou extravio de algum documento em sua estação de trabalho ou no sistema? ( ) Sim ( ) Não

Se sim. Como isso ocorreu e com que tipo de informação?

6.2 Você tem conhecimento de informações que foram modificadas de forma acidental ou intencional na sua estação de trabalho nos últimos 5 anos? ( ) Sim ( ) Não

Se sim. Como isso ocorreu?

6.3 A informação está sempre disponível para o desenvolvimento de suas atividades profissionais.

Discordo totalmente	Discordo parcialmente	Indiferente	Concordo parcialmente	Concordo totalmente
01	02	03	04	05

6.4 Já tomou conhecimento de algum evento de acesso desautorizado às informações ou sistema de informação em sua unidade de trabalho? ( ) Sim ( ) Não

Se sim, como aconteceu?

6.5 O antivírus de seu computador de trabalho já detectou algum vírus? ( ) Sim ( ) Não

Você foi prejudicado? ( ) Sim ( ) Não

Se sim, o que aconteceu?

6.6 Se o antivírus encontrar alguma ameaça no seu computador, a quem você se reporta?

APÊNDICE C - TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO

UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
DEPARTAMENTO DE CIÊNCIA DA INFORMAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO

Esclarecimentos,

Este é um convite para você participar da pesquisa "A DIMENSÃO HUMANA NO PROCESSO DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO: um estudo aplicado à Pró-Reitoria de Gestão de Pessoas da Universidade Federal da Paraíba", desenvolvida pelos pesquisadores Sueny Gomes Léda Araújo, aluna do curso de mestrado do Programa de Pós-Graduação em Ciência da Informação da Universidade Federal da Paraíba, sob orientação do Prof. Dr. Wagner Junqueira de Araújo.

A pesquisa pretende compreender como a dimensão humana é considerada no processo de gestão da segurança da informação na Pró-Reitoria de Gestão de Pessoas (Progep) da Universidade Federal da Paraíba (UFPB) de modo a atender as normas do governo federal. Desse modo, o motivo que nos leva a fazer esta pesquisa é analisar a dimensão humana no processo de gestão de segurança da informação na Progep da UFPB, sob a ótica das normas do governo federal.

Caso decida participar, você deverá responder um questionário semi-estruturado, contendo 43 questões que objetivam identificar quais ações de segurança da informação, baseadas na dimensão humana, são implementas pela Progep. Esclarecemos que durante aplicação do questionário não haverá a necessidade de gravação de voz e/ou imagem.

Durante o preenchimento dos questionários, a previsão de riscos é mínima, ou seja, o risco que você corre é de um possível constrangimento em responder as perguntas. Desse modo, como forma de prevenção quanto a isso, você poderá ler antecipadamente as perguntas, estando livre para tirar suas dúvidas. Lembramos, ainda, que caso seja necessário, o pesquisador poderá auxiliá-lo no preenchimento do questionário. Você tem a opção de responder ao questionário na presença de algum colega de trabalho, familiar ou sozinho, caso se sinta mais à vontade.

Os benefícios que você irá obter com esta pesquisa serão os de conscientização sobre a importância da dimensão humana da Segurança da Informação e o conhecimento das ações e das necessidades de uma gestão da segurança da informação na Progep da UFPB.

Você tem o direito de se recusar a participar ou retirar seu consentimento, em qualquer fase da pesquisa, sem nenhum prejuízo para você.

Os dados que você nos fornecerá serão confidenciados e serão divulgados apenas em congressos ou publicações científicas, não havendo divulgação de nenhum dado que possa lhe identificar.

Esses dados serão guardados pelos pesquisadores responsáveis pela pesquisa em local seguro e por um período de 05 (cinco) anos.

Se você tiver algum gasto pela sua participação na pesquisa, ele será assumido pelos pesquisadores e reembolsado.

Este documento foi impresso em duas vias. Uma ficará com você e a outra com os pesquisadores: Sueny Gomes Léda Araújo e seu orientador Prof. Dr. Wagner Junqueira de Araújo.

Consentimento Livre e Esclarecido

Após ter sido esclarecido (a) sobre os objetivos, importância e o modo como os dados serão coletados pela pesquisa, além de conhecer os riscos, desconfortos e benefícios que ela trará para mim e ter ficado ciente de todos os meus direitos, concordo em participar da pesquisa “A DIMENSÃO HUMANA NO PROCESSO DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO: um estudo aplicado à Pró-Reitoria de Gestão de Pessoas da Universidade Federal da Paraíba” e autorizo a divulgação das informações por mim fornecidas em congressos e/ou publicações científicas desde que nenhum dado possa me identificar.

João Pessoa, _____ de _____ de 20____.

_____

Assinatura do participante da pesquisa

_____

Assinatura da testemunha

Contato com o Pesquisador Responsável:

Caso necessite de maiores informações sobre o presente estudo, favor entrar em contato com **Sueny Gomes Léda Araújo** pelo número _____ ou pelo e-mail: _____, e com o **Prof. Dr. Wagner Junqueira de Araújo** pelo telefone _____ ou pelo e-mail: _____.ou

Comitê de Ética em Pesquisa do Centro de Ciências da Saúde da Universidade Federal da Paraíba

Campus I - Cidade Universitária - 1º Andar - CEP 58051-900 - João Pessoa/PB

(83) 3216-7791 - e-mail: eticaccsufpb@hotmail.com

Atenciosamente,

_____

Assinatura do Pesquisador Responsável

APÊNDICE D – AUTORIZAÇÃO DA PROGEP

Universidade Federal da Paraíba
Centro de Ciências Sociais Aplicadas
Departamento de Ciência da Informação
Programa de Pós-Graduação em Ciência da Informação

João Pessoa, 02 de outubro de 2015.

Ao **Ilmo. Sr. Francisco Ramalho de Albuquerque**
Pró-Reitor da Pró-Reitoria de Gestão de Pessoas - Progep

SOLICITAÇÃO DE AUTORIZAÇÃO PARA REALIZAÇÃO DE PESQUISA ACADÊMICO-CIENTÍFICA

Solicitamos autorização para a realização de atividades de pesquisa acadêmico-científica nesta Pró-Reitoria. A pesquisa será realizada em nível de mestrado, no Programa de Pós-Graduação em Ciência da Informação da Universidade Federal da Paraíba, cujo tema é denominado: "A DIMENSÃO HUMANA NO PROCESSO DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO: um estudo aplicado à Pró-Reitoria de Gestão de Pessoas da Universidade Federal da Paraíba", desenvolvida pela aluna Sueny Gomes Léda Araújo, sob a orientação do Prof. Dr. Wagner Junqueira de Araújo.

A referida pesquisa tem por objetivo analisar a dimensão humana no processo de gestão da segurança da informação na Progep da UFPB, sob a ótica das normas do governo federal.

A mestranda e seu orientador estão a sua disposição para quaisquer esclarecimentos que considere necessário, em qualquer etapa do processo de pesquisa.

Atenciosamente,

Sueny Gomes Léda Araújo
Mestranda
suenyleda@gmail.com

Prof. Dr. Wagner Junqueira de Araújo
Orientador
wagnerjunqueira.araujo@gmail.com

De acordo,

Francisco Ramalho de Albuquerque
Pró-Reitor da Progep

APÊNDICE E – PROJETO DO CURSO DE CONSCIENTIZAÇÃO EM SI

UNIVERSIDADE FEDERAL DA PARAÍBA
PRÓ-REITORIA DE GESTÃO DE PESSOAS – PROGEP
COORDENAÇÃO DE DESENVOLVIMENTO DE PESSOAS – CDP
DIVISÃO DE EDUCAÇÃO E CAPACITAÇÃO PROFISSIONAL – DECP

PROPOSTA DE EVENTO DE CAPACITAÇÃO – CURSO DE CONSCIENTIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO

JOÃO PESSOA

2016

I – IDENTIFICAÇÃO DO PROJETO

1.1 TÍTULO DO EVENTO**:** Conscientização em segurança da informação

1.2 NATUREZA DO PROJETO: Curso

1.3 MODALIDADE: Presencial/Distância

1.4 AMBIENTE ORGANIZACIONAL: Todos

1.5 NÚMERO DE EVENTOS: 02 Turmas 30 participantes cada (presencial) 02 Turmas 60 participantes cada (à distância)

1.6 NÚMERO TOTAL DE VAGAS/PARTICIPANTES: 180 participantes

1.7 CARGA HORÁRIA POR TURMA/EVENTO: 20h/aula

1.8 CRONOGRAMA PREVISTO PARA PRIMEIRA TURMA:

Inscrição:
Realização:
Horário:
Turno:
Local – CEDESP

1.9 COORDENAÇÃO DO PROJETO:

1.9. 1 – Coordenador do Projeto:

Nome: XXXXXXXXXXX
Lotação: DECP/PROGEP
Telefone: XXXXXXXXX
E-mail: XXXXXXXXX

1.9.2 – Coordenador do Evento:

Nome: XXXXXXXX
Lotação: XXXXXXX
Telefone: XXXXXXX
E-mail: XXXXXXXXX

II – ORGANIZAÇÃO ACADÊMICA

2.1 OBJETIVOS DO PROJETO

- Conscientizar os servidores de suas responsabilidades com segurança da informação e desenvolver competências capazes de usar os controles e os meios pelos quais essas responsabilidades serão realizadas.

2.2 PERFIL DA COMPETENCIA

- Depreender suas responsabilidades com as informações que manuseiam, utilizando de forma eficiente os controles pelos quais essas responsabilidades serão realizadas.

2.3 CONTEÚDO PROGRAMÁTICO

- Conceitos e princípios básicos de segurança da informação;
- Principais normas (a necessidade de estar em conformidade com as obrigações e regras de segurança da informação, conforme definido nas políticas, normas, decretos e leis);
- Noções de classificação da informação;
- Responsabilidade pessoal por seus próprios atos;
- Procedimentos básicos de segurança da informação (tais como, notificação de incidente de segurança da informação);
- Controles básicos (tais como, segurança da senha, controles contra códigos maliciosos e política de mesa limpa e tela limpa); e
- Pontos de contato.

Ao final do MÓDULO o servidor será capaz de demonstrar as seguintes competências:

- Conhecer as principais normas de segurança da informação;
- Entender quais procedimentos deve ser tomado diante de determinada informação;
- Conhecer suas responsabilidades e as penalidades decorrentes do manuseio da informação;
- Identifica quais informações necessitam de maior proteção;
- Utilizar controles básicos de segurança da informação; e
- Praticar ações preventivas.

2.4 Metodologia

Aulas expositivas dialogadas, debates, estudos de caso, dinâmicas de grupo, exibição de vídeos, relato de experiências e trabalho em equipe.

O módulo que compõe o curso de Iniciação ao Serviço Público será oferecido por meio do Ambientes Virtuais de Aprendizagens – AVAS.

2.5 Avaliação do Projeto

Será considerado aprovado aquele que obtiver nota igual ou superior a 7,0 nas avaliações realizadas durante o processo de aprendizagem, além da frequência mínima obrigatória de 75% no curso.

Para o módulo do curso de Iniciação ao Serviço Público será aprovado aquele que realizar no ambiente virtual de aprendizagem (*on line*), no mínimo 75% das atividades, obtendo nota igual ou superior a 7,0

2.6 Certificação

Ao final do curso deverá ser emitido um certificado de participação, através da Pró-Reitoria de Gestão de Pessoas – PROGEP, validado pela Divisão de Educação e Capacitação Profissional – DECP, conforme Programa de Capacitação dos Servidores devidamente instruído pela Política Nacional de Desenvolvimento de Pessoal (Art. 5º do decreto 5.707/2006).

A emissão do certificado depende do preenchimento do Formulário de Avaliação do Curso. Com o certificado o servidor técnico fica apto a solicitar sua progressão por capacitação junto a Divisão de Educação e Capacitação Profissional – DECP.

ANEXO A – AUTORIZAÇÃO DO COMITÊ DE ÉTICA

UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIÊNCIAS DA SAÚDE
COMITÊ DE ÉTICA EM PESQUISA

C E R T I D Ã O

Certifico que o Comitê de Ética em Pesquisa do Centro de Ciências da Saúde da Universidade Federal da Paraíba – CEP/CCS aprovou por unanimidade na 9ª Reunião realizada no dia 22/10/2015, o Projeto de pesquisa intitulado: **"A DIMENSÃO HUMANA NO PROCESSO DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO: UM ESTUDO APLICADO ÀPRÓ-REITORIA DE GESTÃO DE PESSOAS DA UNIVERSIDADE FEDERAL DA PARAÍBA"**, da pesquisadora Sueny Gomes Leda Araújo. Prot. nº 0556/15. CAAE: 50089915.8.0000.5188.

Outrossim, informo que a autorização para posterior publicação fica condicionada à apresentação do resumo do estudo proposto à apreciação do Comitê.

Andrea M. C. Lima
Andrea Márcia da C. Lima
Mat. SIAPE 1117510
Secretária do CEP-CCS-UFPB