XVII Encontro Nacional de Pesquisa em Ciência da Informação **(XVII ENANCIB)**

GT 4 – Gestão da Informação e do Conhecimento nas Organizações

ANALISE DA DIMENSÃO HUMANA NO PROCESSO DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

ANALYSIS OF HUMAN DIMENSION IN THE PROCESS OF INFORMATION SECURITY MANAGEMENT

Sueny Gomes Léda Araújo[1] e, Wagner Junqueira de Araújo[2].

Modalidade da apresentação: Comunicação Oral

Resumo: A informação apresenta-se como um importante ativo para as instituições, necessitando ser gerenciada e protegida de forma adequada contra destruição indevida, indisponibilidade temporária, adulteração ou divulgação não autorizada. Diante desse contexto, buscou-se com esta pesquisa abordar sobre a gestão da segurança da informação concentrando-se na dimensão humana, dada à relevância do tema na Administração Pública Federal. Para isso, respondeu-se 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, foi necessário atingir o objetivo de analisar a dimensão humana no processo de gestão de segurança da informação na Progep/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. Desse modo, foi utilizada a pesquisa documental, observação participante e entrevista, como instrumentos de coleta de dados. 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: elaboração do termo de responsabilidade e confidencialidade, e processo disciplinar formal para a violação da segurança da informação. 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 permitiu propor medidas que podem 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: Gestão da Informação. ABNT NBR ISO/IEC 27002:2013. Gestão da Segurança da Informação.

---

[1] Mestre em Ciência da Informação pelo Programa de Pós-graduação em Ciência da Informação da Universidade Federal da Paraíba-UFPB (2016).

[2] Doutor em Ciência da Informação Pela Universidade de Brasília (2009); Mestre em Ciência da Informação - UNB (2001). Professor do Programa de Pós Graduação em Gestão em-Organizações Aprendentes -MPGOA. Professor Adjunto IV - Departamento de Ciência da Informação da Universidade Federal da Paraíba - UFPB.

Abstract: *The information is presented as an important asset for institutions and needs to be protected adequately against undue destruction, temporary unavailability, unauthorized tampering or disclosure. In this context, we sought with this research approach on information security focusing on the human dimension, given the relevance of the subject in the Federal Public Administration. For this, was answered the following question: how the human dimension is considered in the management process information security in the Dean of Personnel Management (Progep) of the Federal University of Paraíba (UFPB) in the way to meet the standards of the federal government?. Therefore, it was necessary to achieve the objective of analyzing the human dimension in the information security management process in Progep/UFPB from the perspective of the rules of the federal government. This research is characterized as descriptive research with qualitative and quantitative approach and the method of investigation is case study. Thus, were used the documentary research, participant observation and interview as data collection instruments. The results allowed identifying the need of UFPB to elaborate an information classification policy, since its absence prevents the management of information security. As for information security awareness, was observed the absence of actions that could contribute to the awareness process to public server, such as: preparation of term of responsibility and confidentiality and formal disciplinary proceedings for breach of information security. 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 with the regulatory guidelines. Based on the above, the results of this research allowed us to propose measures that can minimize the impact of threats to information security in Progep / UFPB and contribute to the creation of a safety culture in federal institutions.*

Keywords: *Information Management. ABNT NBR ISO/IEC 27002:2013. Information Security Management.*

1 INTRODUÇÃO

Os ativos informacionais correspondem a elementos que assegurem os processos de negócio de uma determinada instituição, desse modo, requer um gerenciamento preciso que possa coordenar toda a complexidade que gira em torno do ciclo de vida das informações. Como importante constituinte da expansão organizacional, a gestão dos ativos informacionais precisa considerar, como um dos procedimentos essenciais, sua segurança. No campo da gestão 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.

Os estudos sobre segurança da informação implementados na Ciência da Informação no Brasil, estão em parte, relacionados aos processos informacionais ou aos sistemas de informação. Os resultados apresentados nesta comunicação são resultados de uma pesquisa

que observou a relação dos indivíduos de uma determinada área da organização junto aos processos informacionais que eles manipulam, com foco na segurança da informação.

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, o governo federal publicou 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).

Nesse, 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).

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

2 DIMENSÃO HUMANA DA SEGURANÇA DA INFORMAÇÃO

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 contexto, com a vasta tecnologia existente voltada para proteção da informação, seria 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, não se pode presumir que produtos tecnológicos de segurança, funcionando de forma isolada, possam garantir uma segurança efetiva. Acreditar nisso pode levar a falsa ideia de segurança, ou seja, 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.

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, 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, o que evidencia a necessidade de um processo de conscientização constante para alertar os colaboradores sobre a efetiva intenção das medidas de segurança.

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".

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.

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. 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. De acordo com a norma ISO 27000 (2013, p. 2, tradução nossa), os controles incluem qualquer processo, política, dispositivo, prática ou outras ações que minimizem o risco.

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 alcance seus objetivos.

3 METODOLOGIA E DESENVOLVIMENTO

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. 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.

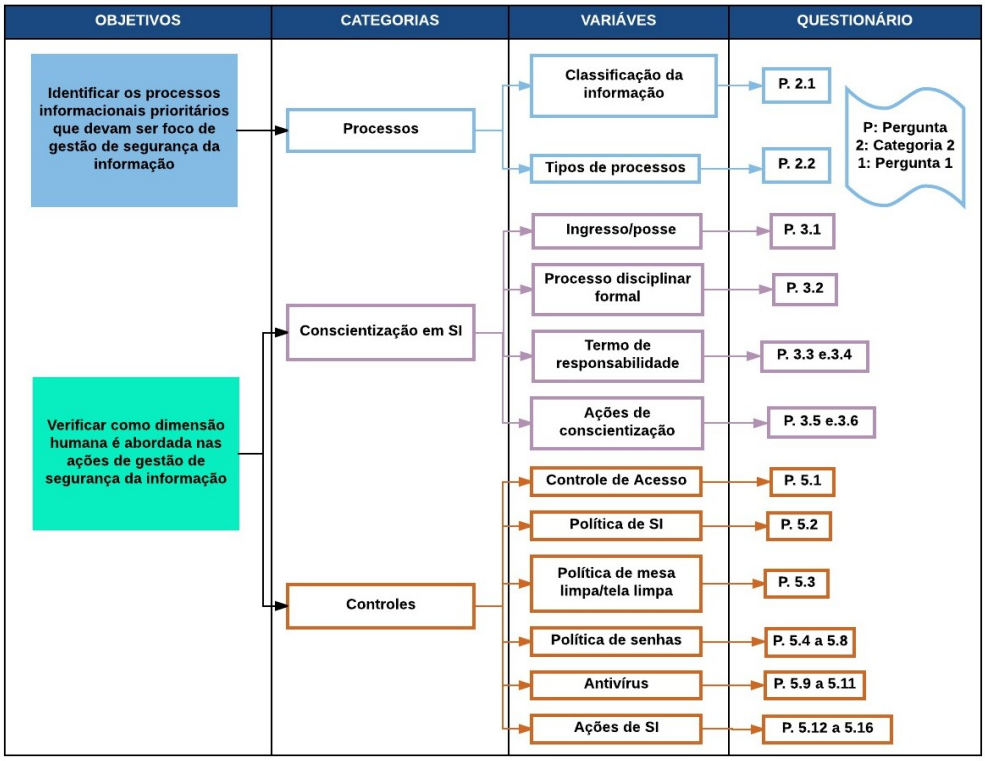
O universo desta pesquisa foi constituído pelos 21 gestores da Progep/UFPB. Quanto a amostra foi composta pelos nove diretores que compõe a Progep. Com relação ao critério de escolha da amostra, foi considerada a amostragem por tipicidade ou intencional, ou seja, "não probabilística e que, com base nas 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.

Assim, para verificar as orientações legais aplicadas à gestão de segurança da informação na Progep, foi utilizada como instrumento de coleta de dados a pesquisa documental, utilizando 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 que auxiliou a 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. Em algumas questões objetivas foi utilizada a escala do tipo *Likert.* O questionário com os gestores possibilitou 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.

O questionário foi desenvolvido com base no aporte teórico que envolve a pesquisa, nos objetivos específicos, nas variáveis e nas categorias construídas. A Figura 1 demonstra algumas das relações dos objetivos específicos com as categorias, variáveis e as perguntas que compõem o questionário.

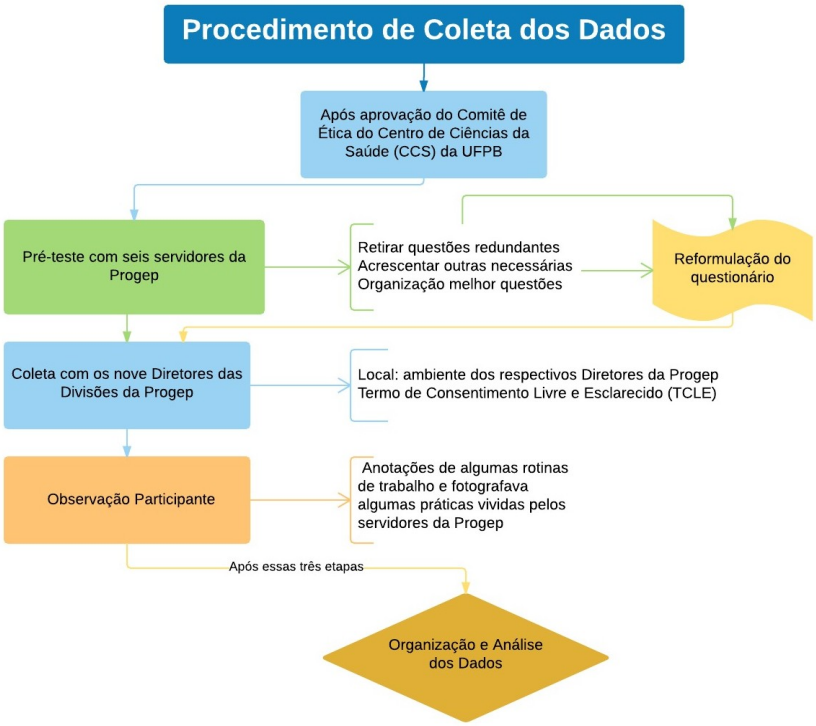
Figura 1 - Relação dos objetivos com as categorias, variáveis e o questionário.



Fonte: Elaborado pelos autores (2015).

A coleta de dados foi realizada no período de 27 de outubro a 15 de novembro de 2015. O resumo dos procedimentos de coleta encontra-se ilustrado na Figura 2.

Figura 2 - Procedimento de coleta dos dados



Fonte: Elaborado pelos autores (2015).

Para análise dos dados, utilizou-se a Análise de Conteúdo que segundo Bardin (2008, p. 20-21), pode ser utilizada para qualquer comunicação, isto é, qualquer transporte de significação de emissor para um receptor controlado ou não.

4 RESULTADOS: APRESENTAÇÃO E DISCURSÃO

Esta seção apresenta a análise realizada para alcançar os objetivos propostos, bem como responder à questão que norteia esta pesquisa. 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 classificação dos processos pelos gestores, em relação a sua divisão. Conforme os resultados identificados, sete gestores apresentaram discordância total quanto a existência de classificação da informação na Progep, dois gestores apontaram 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.

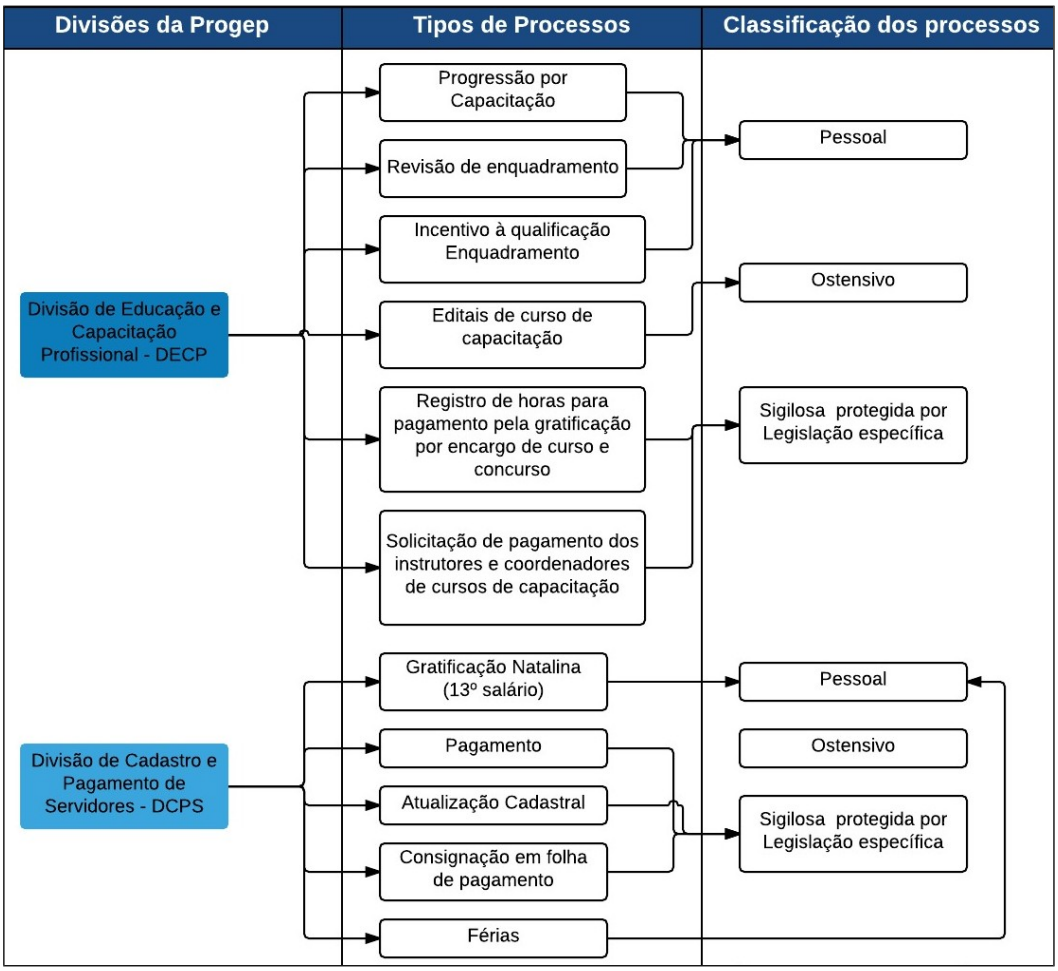
Entretanto, nas observações foi possível identificar que havia classificação da informação, mesmo de maneira informal, devido às características específicas de algumas divisões, onde o gestor entende que determinada informação não deve ser divulgada de forma ostensiva, ou requer maior proteção. A ABNT 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.

A classificação da informação possibilita, aos agentes públicos dos órgãos e entidades da Administração Pública Federal, 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 Administração Pública aprovar as diretrizes estratégicas de segurança da informação que norteiam o tratamento da informação.

Nesse sentido, 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, a Figura 3 apresenta alguns desses resultados.

Figura 3- Classificação dos processos da Progep



Fonte: Dados da pesquisa (2015).

Percebe-se que, de acordo com Figura 3, 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), 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".

O resultado da pesquisa identificou 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).

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.

Na categoria, conscientização em segurança da informação, 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 à assinatura do referido termo.

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

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.

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. Nesse sentido, os resultados mostram que, do grupo de gestores, sete relataram a inexistência desse tipo de processo. 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".

Na categoria controles 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, seis gestores afirmaram a existência do referido controle. Entretanto seu funcionamento ocorre de forma inadequada, conforme relata um dos gestores ao afirmar que: "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".

Com base nessa fala, 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. 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.

Outro aspecto abordado procurou analisar se a Política de Segurança da Informação (PSI) da UFPB influencia nas rotinas de trabalhos dos gestores participantes desta pesquisa. Nesse sentido, sete gestores apontaram discordância total, o que pode ser consequência do desconhecimento da PSI da UFPB, instituída por meio da Resolução nº 32/2014, e enviada a todos os servidores técnico-administrativos e docentes pela Superintendência de Tecnologia da Informação (STI) da UFPB, por meio do Sistema Integrado de Gestão (SIG).

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: definir o escopo da segurança da informação da UFPB; orientar as ações de segurança com intuito de reduzir riscos e garantir a confidencialidade, integridade e disponibilidade dos ativos da

UFPB; incentivar o uso de soluções integradas de segurança; servir de referência para auditoria, apuração e avaliação de responsabilidade (UFPB, 2014).

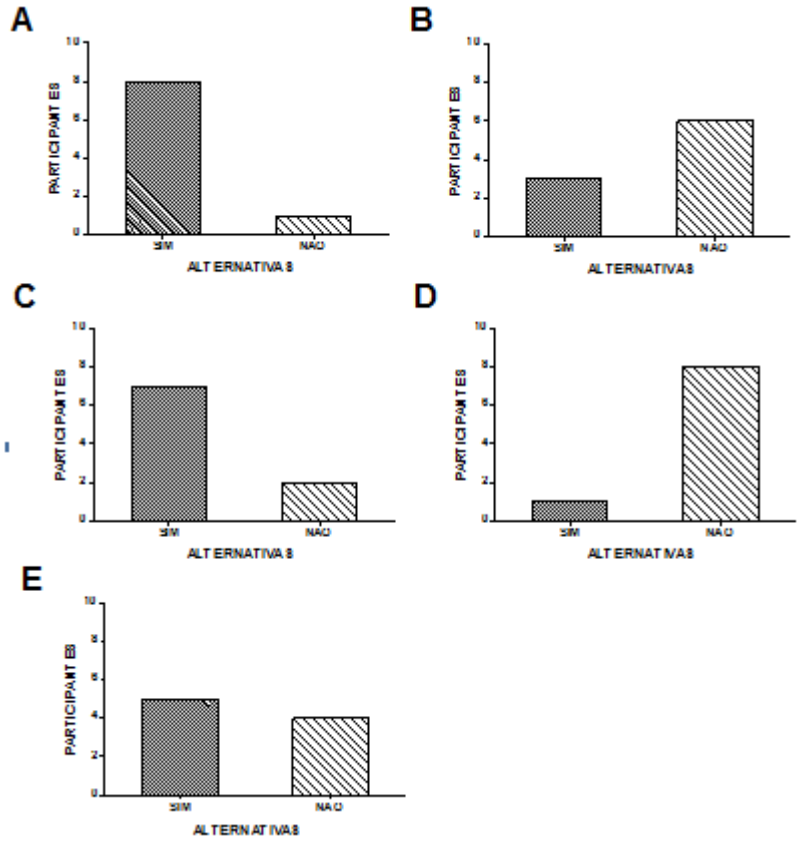
Para a ABNT NBR ISO/IEC 27002 (2013, p. 3), além da necessidade de a PSI ser comunicada aos funcionários e partes externas relevantes de forma que seja entendida, acessível e relevante aos funcionários, é necessário que essa publicação seja inserida no contexto de um programa de conscientização e capacitação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

Verificou-se também, se há uma política de mesa limpa/tela limpa para os recursos de processamento da informação. Os resultados mostram que oito gestores registraram discordância total da existência da referida política. 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.

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 4, os resultados obtidos.

Figura 4 – 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



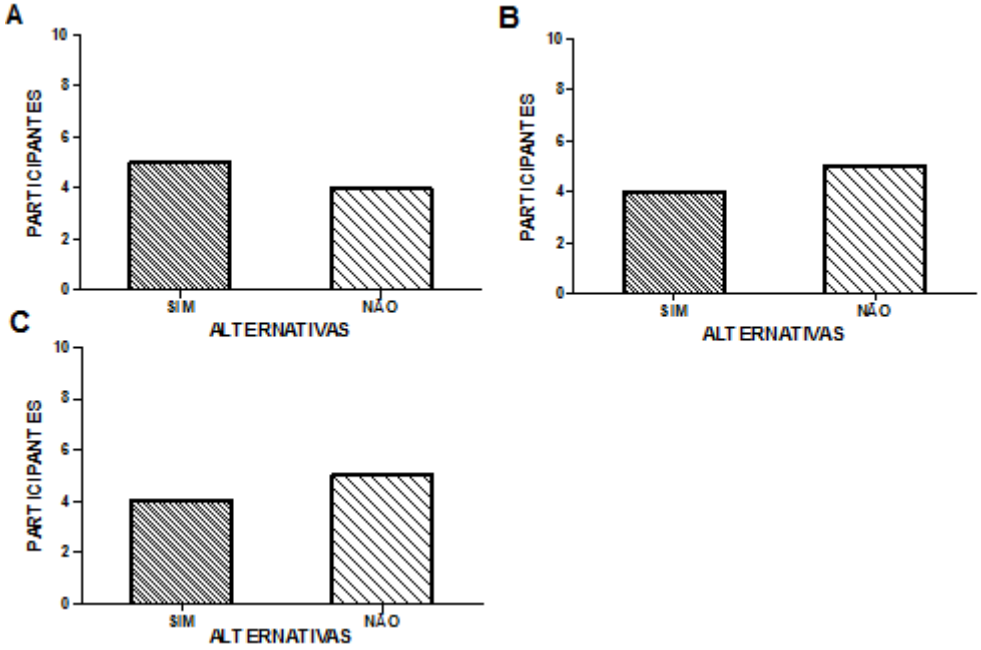
Fonte: Dados da pesquisa (2015).

Conforme observado na Figura 4, 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 seis 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. Dentre os motivos que levam ao compartilhamento de senhas destaca-se a resposta de um dos gestores: "porque confio no pessoal que trabalha comigo". Para Fontes (2006, p. 33), de pouco adianta ter registro do arquivo de auditoria e senhas de usuários que acessaram determinada informação, se uma mesma senha for utilizada por várias pessoas de um mesmo departamento.

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 5, observou-se que pouco mais da metade dos gestores afirmaram positivamente acerca

do uso de um programa de antivírus designado pela referida Pró-reitoria. Perece-se que, apesar do programa em questão ser indicado pelo Núcleo de Tecnologia e Gestão da Informação 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 51 - Antivírus: A) Antivírus indicado pela Progep; B) Atualização de antivírus; C) Verifica a origem de arquivos anexados.



Fonte: Dados da pesquisa (2015).

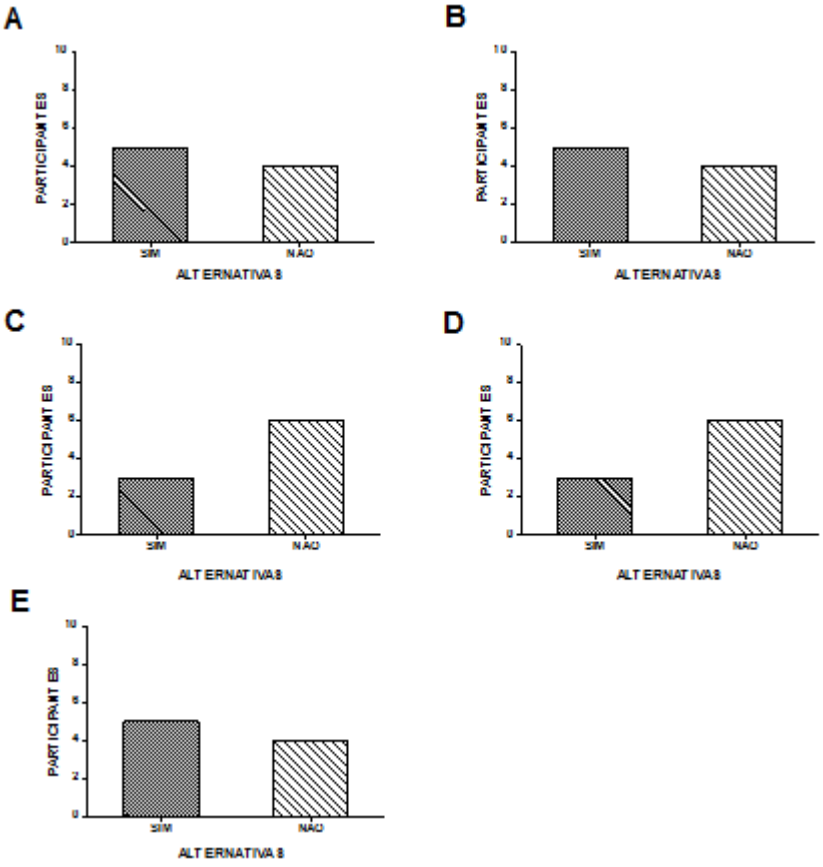
Referente à atualização frequente do programa de antivírus, verificou-se que a maioria dos gestores apresentou afirmações negativas. Deve-se considerar que o procedimento de atualização de um programa de antivírus aumenta o seu quantitativo de definições de vírus, tornando-o mais eficiente. Por esse 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.

Outro aspecto discutido compreendeu a realização de varredura nos arquivos anexados no correio eletrônico, antes de sua abertura para visualização. Conforme a Figura 5, 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.

Algumas ações de segurança da informação foram abordadas, como bloqueio da tela do computador, ingestão de líquidos ou alimentos próximos a computadores, cópias de segurança, guarda de documentos e instalação de equipamentos eletrônicos. Nesse contexto, conforme Figura 6, 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.

Figura 6 - 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).

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 6, 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. 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.

Retomando a Figura 6, 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 esse procedimento. Nesse contexto, a ABNT NBR ISO/IEC 27002 (2013, p. 52) orienta que cópias de segurança das informações sejam efetuadas e testadas regularmente conforme política definida. Quando da elaboração de um plano de cópias de segurança, 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, identificou-se, a partir da Figura 6, uma maior representatividade para afirmação negativa. 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 ainda na Figura 6, 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. 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.

Outra questão abordada foi a quem eles se reportam quando acontece um incidente de segurança da informação, ou seja, qual o "ponto de contato". Nesse sentido, os gestores não apresentaram uniformidade em suas respostas. 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.

5 CONSIDERAÇÕES FINAIS

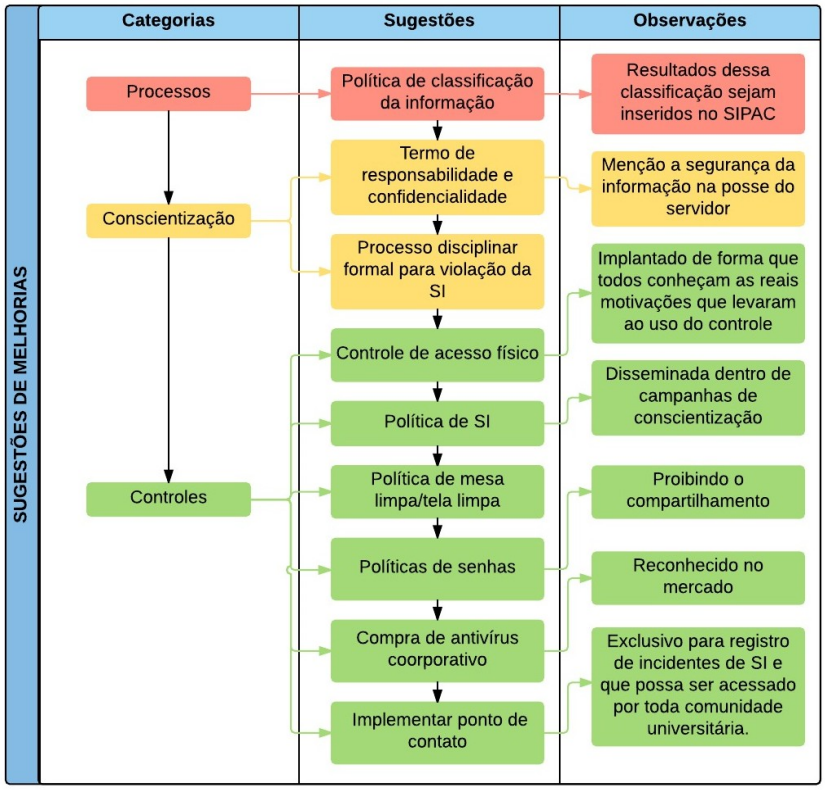
A gestão da segurança da informação, deve ser considerada como uma parte relevante dos processos de gestão da informação, contudo ainda é uma temática pouco explorada no campo da Ciência da Informação no Brasil, e, mais raramente, em Instituições Públicas Federais, apesar de as estatísticas do Centro de Tratamento de Incidentes de Segurança de Rede de Computadores da Administração Pública Federal - CTIR Gov evidenciarem que o Brasil em 2015 ficou em segundo lugar 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 deixam uma ampla oportunidade para o erro humano e 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.

A partir das informações analisadas nas categorias processos, conscientização e controles, ilustra-se na Figura 7 um resumo das sugestões apresentadas no decorrer da análise.

Figura 72 – Sugestões de melhoria



Fonte: Elaborado pela autora (2016).

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. Verificando-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.

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 Plano de

Capacitação e Qualificação dos Servidores da UFPB – Exercício 2016-2017, bem como elaborou o Termo de Responsabilidade e Confidencialidade para os novos servidores.

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, pelo contrário, essa é uma temática que precisa de 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 da informação 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.

REFERENCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002**: tecnologia da informação: técnicas de segurança: código de prática para a gestão da segurança da informação. Rio de Janeiro, 2013.

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

BRASIL. Presidência da República. Gabinete de Segurança Institucional. **Estratégia de segurança da informação e comunicações e de segurança cibernética da administração pública federal 2015-2018**: versão 1.0. 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. **Lei Federal n. 12.527**, de 8 de novembro de 2011. Regula o acesso à informação previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei n º 11.111, de 5 de maio de 2005.

_____. 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. 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.

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.

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.

FONTES. **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

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

INTERNATIONAL ORGANIZATION FOR STANDARTIZATION. **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

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.

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.

TRIBUNAL DE CONTAS DA UNIÃO (TCU). **Relatório de levantamento**. Avaliação da governança de tecnologia da informação na Administração Pública Federal. 2014.

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.