DOI: 10.5433/1981-8920.2018v23n2p596

ESTUDO DOS ASPECTOS HUMANOS DA SEGURANÇA DA INFORMAÇÃO APLICADO NA PRÓ-REITORIA DE GESTÃO DE PESSOAS DA UNIVERSIDADE FEDERAL DA PARAÍBA - UFPB

TÍTULO STUDY OF HUMAN ASPECTS OF INFORMATION SECURITY APPLIED AT THE DEAN'S OFFICE OF PEOPLE MANAGEMENT OF THE FEDERAL UNIVERSITY OF PARAÍBA - UFPB

Wagner Junqueira de Araújo[a]
Sueny Gomes Leda Araújo[b]
Rafaela Romaniuc Batista[c]

RESUMO
Introdução: O universo de atividades que permeia a tecnologia da informação está sujeito a várias formas de ameaças que comprometem seriamente sua segurança. A própria tecnologia é responsável por fornecer parte da solução para esses problemas. Porém, parte das vulnerabilidades e ameaças a que os sistemas de informação estão expostos podem ser atribuídas às deficiências nos procedimentos organizacionais e ao comportamento humano. Nesse contexto, torna-se salutar estudar, sob a ótica da Ciência da Informação, uma das variáveis subjetivas do processo de segurança da informação, que está relacionada às pessoas. Para tanto, este trabalho apresenta um relato de experiência sobre o comportamento dos servidores da Pró-Reitoria de Gestão de Pessoas – Progep da Universidade Federal da Paraíba – UFPB com relação à segurança da informação. **Objetivo:** Identificar quais as ações de segurança da informação, relacionadas aos aspectos humanos, são utilizadas pela Pró-Reitoria de Gestão de Pessoas – Progep da Universidade Federal da Paraíba – UFPB. **Metodologia:** Essa pesquisa caracterizou-se como sendo de cunho descritivo, com abordagem quanti-qualitativa. Para coleta de dados foi aplicado um questionário *on-line* enviado por e-mail aos servidores da Progep, durante o período compreendido entre os dias 11 e 25 de julho de 2014. **Resultados:** Foi verificado que 93% dos respondentes não possuíam conhecimentos sobre segurança da informação, 50% raramente trocam suas senhas. Contudo, destaca-se que 60% se recusaram a passar o antivírus em suas estações de trabalho. **Conclusões:** Foi identificada a inexistência

[a] Doutor em Ciência da Informação pela Universidade de Brasília (UnB). Professor do Departamento de Ciência da Informação da Universidade Federal da Paraíba (UFPB). E-mail: wagnerjunqueira.araujo@gmail.com
[b] Doutoranda em Ciência da Informação da Universidade Federal da Paraíba (UFPB). E-mail: suenyleda@gmail.com
[c] Doutoranda em Ciência da Informação Universidade Federal da Paraíba (UFPB). E-mail: rafaela.romaniuc@gmail.com

de procedimentos para sensibilizar os servidores da importância de manter as informações organizacionais em segurança, bem como a falta de uma política de segurança que oriente como se comportar diante de eventuais ameaças.

Descritores: Gestão da segurança da informação. Política de segurança da informação. Aspectos humanos da segurança da informação. Gestão de pessoas.

1 INTRODUÇÃO

A atual sociedade é caracterizada pela explosão informacional em decorrência da disseminação e do uso das tecnologias de informação e comunicação (TICs). Nesse sentido,

> [...] embora o conhecimento e a sua comunicação sejam fenômenos básicos de toda sociedade humana, é o surgimento da tecnologia da informação e seus impactos globais que caracterizam nossa sociedade como uma sociedade da informação (CAPURRO; HJORLAND, 2007, p. 149).

Contudo, este universo de conteúdos digitais 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 parte das vulnerabilidades pode ser atribuída aos processos de gestão organizacional e ao comportamento humano. Segundo Mitnick e Simon (2003, p. 3), "[...] é natural querer se sentir seguro e isso leva muitas pessoas a buscarem uma falsa ideia de segurança". Em relação às instituições públicas federais, a prática voltada à preservação da segurança da informação é orientada por normas, leis e decretos que abrangem os recursos computacionais, de infraestrutura, além dos recursos humanos. Para tanto, este trabalho apresenta um relato de experiência sobre o comportamento dos servidores da Pró-Reitoria de Gestão de Pessoas (Progep) da Universidade Federal da Paraíba – UFPB com relação à segurança da informação.

Diante desse panorama e da relevância dos aspectos humanos no contexto da segurança da informação, esta pesquisa teve como objetivo identificar quais ações de segurança da informação relacionadas aos aspectos

humanos são utilizadas pela Progep/UFPB. Desse modo, caracteriza-se como relato de experiência, em que as primeiras reflexões para o seu desenvolvimento surgiram em decorrência da pesquisa realizada no Japão em 2010 e publicada no artigo *Human aspects of information security: An empirical study of intentional versus actual behavior* (KOMATSU; TAKAGI; TAKEMURA, 2013).

Esse estudo se justifica pela necessidade de ampliar as pesquisas e discussões sobre o tema gestão segurança da informação no âmbito da Ciência da Informação. Corroborando essa ideia, Araújo (2009) expõe que o tema segurança da informação ainda é pouco explorado como objeto de pesquisa da Ciência da Informação, ainda que no mundo conectado em rede as informações necessitem de processos e controles de segurança para garantir e preservar suas informações de uma série de novas ameaças. Desse modo, torna-se relevante a compreensão de como uma unidade organizacional dedicada a tratar com pessoas, como a Progep/UFPB, está fazendo uso de suas políticas de segurança da informação.

2 CIÊNCIA DA INFORMAÇÃO E A SEGURANÇA DA INFORMAÇÃO

A Ciência da Informação – CI 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 realiza uma síntese das três definições de CI, 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 (BORKO, 1968, p. 3, tradução nossa).

Freire e Silva alertam para a necessidade de uma área que trate 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 (FREIRE; SILVA, 2012, p. 3).

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 gestão da informação podem emergir, incluindo os relacionados à gestão da segurança da informação que, nos últimos anos, 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.

A Internet, como fator fundamental nesse mundo digital globalizado, contribui para o crescimento contínuo de transações eletrônicas que incluem correspondências particulares, operações comerciais, bancárias, entre outras (FERREIRA, 2013). Contudo, traz para a gestão da informação novos problemas de segurança, a ponto de se tornar uma preocupação inclusive das entidades governamentais. Para o Governo Federal Brasileiro, a segurança da informação é definida como:

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

Quantos aos objetivos da segurança da informação, a ABNT NBR ISO/IEC 27001 aborda que a segurança da informação visa garantir três aspectos básicos que são classificados em:

> Confidencialidade – propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados;
> Integridade – propriedade de salvaguarda da exatidão e completeza de ativos;
> Disponibilidade – propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada. (ABNT NBR ISO/IEC 27001, 2013, p. 2).

Complementando, Sêmola define a segurança da informação como "[...] uma área do conhecimento dedicada à proteção de ativos da informação contra acesso não autorizado, alterações indevidas ou sua indisponibilidade" (SÊMOLA, 2014, p. 43).

São três os pilares que sustentam os procedimentos de gestão de segurança da informação: Tecnologia, Processo e Pessoas. Mitnick e Simon (2003) alertam que muitas organizações desenvolvem soluções de segurança da informação que diminuem os riscos relacionados ao uso dos computadores, no entanto, deixam de fora a vulnerabilidade mais significativa, que segundo os autores, é o fator humano.

3 ASPECTOS HUMANOS NA SEGURANÇA DA INFORMAÇÃO

Diferentes tipos de vulnerabilidades relacionadas com os sistemas de informação, sejam estes computacionais ou não, podem ser atribuídas ao seu elemento humano, ou seja, aos usuários. Quando esses usuários se tornam alvo, o comprometimento da segurança torna-se iminente, independentemente de medidas técnicas que reforçam a segurança da informação, bem como a segurança física (FRANGOPOULOS; ELOFF; VENTER, 2013, tradução nossa).

Percebe-se que existe um viés que favorece as soluções tecnológicas quando trata do tema. Apesar de a tecnologia fornecer diferentes meios para

incrementar o nível de segurança da informação, há a necessidade de mudar esse viés de modo a incluir a variável subjetiva, fator humano.

Corroborando essa ideia, Colwill (2010, p. 195, tradução nossa) esclarece que a "[...] tecnologia pode fornecer um meio para controlar o acesso à informação e ajudar no monitoramento e detecção de atividade maliciosa, mas é o ambiente de trabalho e os fatores humanos que irão fornecer as bases reais para o sucesso."

Mitnick e Simon (2003) citam o exemplo dos aeroportos para evidenciar a importância do fator humano na segurança. Os autores relatam que, embora a segurança nos aeroportos seja incontestável, muitas vezes somos surpreendidos por notícias de passageiros que passaram com armas pelos detectores de metais. No entanto, na maioria das vezes, não são as máquinas que falham, mas as pessoas que as operam.

É importante ressaltar que, além de violações causadas por ataques, também não se deve ignorar aqueles incidentes de segurança interna que são causados deliberadamente ou acidentalmente pelo usuário, seja por negligência, erro ou descuido, comprometendo, assim, a segurança da informação. Isso acontece porque os usuários de sistemas de informação são seres humanos com habilidades individuais e deficiências que não podem ser categorizadas e tratadas de forma generalizada pelas políticas de segurança de informação. Quando esses erros, deliberados ou não, são agravados por fatores psicossociais, pode haver consequências terríveis (FRANGOPOULOS; ELOFF; VENTER, 2013, tradução nossa).

Nesse sentido, segundo Mitnick e Simon (2003) devemos nos tornar mais conscientes das técnicas que estão sendo utilizadas por aqueles que tentam atacar a confidencialidade, integridade e disponibilidade das informações. Esses autores enfatizam ainda que:

> 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. E devemos implementar essas precauções hoje mesmo (MITNICK; SIMON, 2003, p. 7).

Nesse sentido, torna-se necessário que pessoas e as 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) *apud* Frangopoulos, Eloff e Venter (2013, p. 4),

> [...] 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, os aspectos humanos se apresentam como um grande desafio para a gestão da segurança da informação, de modo que precisa ser mais estudado e melhor abordado pelas normas de políticas de segurança da informação.

3.1 O que as normas dispõem sobre aspectos humanos na segurança da informação?

Normas são documentos orientadores que trazem regras que norteiam a gestão da segurança da informação nas instituições. Não se pretende, nesse estudo, realizar um levantamento detalhado dessas, mas destacar trechos que abordam os aspectos humanos.

O 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 define, no seu Art. 3º, quais são os objetivos da Política da Informação: "[...] III - promover a capacitação de recursos humanos para o desenvolvimento de competência científico-tecnológica em segurança da

informação [...]". No Art. 4º, para os fins desse decreto, cabe à Secretaria-Executiva do Conselho de Defesa Nacional adotar as seguintes diretrizes:

> I - elaborar e implementar programas destinados à conscientização e à capacitação dos recursos humanos que serão utilizados na consecução dos objetivos de que trata o artigo anterior, visando garantir a adequada articulação entre os órgãos e as entidades da Administração Pública Federal;
> II - estabelecer programas destinados à formação e ao aprimoramento dos recursos humanos, com vistas à definição e à implementação de mecanismos capazes de fixar e fortalecer as equipes de pesquisa e desenvolvimento, especializadas em todos os campos da segurança da informação (BRASIL, 2000).

A Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008, que disciplina a gestão de segurança da informação e comunicações na administração pública federal, direta e indireta, indica que:

> Art. 3º Ao Gabinete de Segurança Institucional da Presidência da República - GSI, por intermédio do Departamento de Segurança da Informação e Comunicações - DSIC, compete:
> IV - elaborar e implementar programas destinados à conscientização e à capacitação dos recursos humanos em segurança da informação e comunicações (Instrução Normativa GSI/PR nº 1, 2008).

A ABNT NBR ISO/IEC 27005, de 2008, que trata da gestão de riscos de segurança da informação, prescreve que devemos identificar as ameaças. Afirma que "as ameaças têm o potencial de comprometer os ativos (tais como informações, processos e sistemas)" e, ainda, o Anexo C dessa norma ressalta que deve ser dada atenção especial ao fator humano como um tipo de ameaça. Nessa norma, ao abordar as ameaças que tem como origem os seres humanos, englobam-se desde terroristas, hackers, espiões industriais, até o pessoal interno. A norma descreve que "o pessoal interno pode constituir uma ameaça por várias motivações: curiosidade, ego, obtenção de informações úteis para serviços de inteligência, ganho monetário, vingança, erros e omissões não intencionais" (ABNT NBR ISO/IEC 27005, 2008).

A ABNT NBR ISO/IEC 27001, de 2013, especifica os requisitos para estabelecer, manter e melhorar continuamente um sistema de gestão da

segurança da informação dentro do contexto da organização (ABNT NBR ISO/IEC 27001, 2013, p. 2). Quanto aos aspectos humanos, esses são abordados no tópico:

> 7.2 – Competência, que a organização deve: a) determinar a competência necessária das pessoas que realizam trabalho sob o seu controle e que afeta o desempenho da segurança da informação; b) assegurar que essas pessoas são competentes com base na educação, treinamento ou experiência apropriados. (ABNT NBR ISO/IEC 27001, 2013, p. 9).

O tema também é abordado no Anexo A, o qual referencia o controle e objetos de controle, nos seguintes pontos:

> A.7 Segurança em recursos humanos
> A.7.1 Antes da contratação
> Objetivo: Assegurar que funcionários e partes externas entendem as suas responsabilidades e estão em conformidade com os papéis para os quais eles foram selecionados.
> A.7.1.1 Seleção
> Controle: Verificações do histórico devem ser realizadas para todos os candidatos a emprego, de acordo com a ética, regulamentações e leis relevantes, e devem ser proporcionais aos requisitos do negócio, aos riscos percebidos e à classificação das informações a serem acessadas.
> A.7.2 Durante a contratação
> Objetivo: Assegurar que os funcionários e partes externas estão conscientes e cumprem suas responsabilidades pela segurança da informação.
> A.7.2.1 Responsabilidades da direção
> Controle: A direção deve requerer aos funcionários e partes externas que pratiquem a segurança da informação de acordo com o estabelecido nas políticas e procedimentos da organização.
> A.7.2.2 Conscientização, educação e treinamento em segurança da informação
> Controle: Todos os funcionários da organização e, onde pertinente, partes externas devem receber treinamento, educação e conscientização apropriados, e as atualizações regulares das políticas e procedimentos organizacionais relevantes para suas funções. (ABNT NBR ISO/IEC 27001, 2013, p. 15 e 16).

Diante do exposto, pode-se inferir que o elemento humano deve fazer parte das políticas de segurança da informação, apesar de muitas das políticas

de segurança da informação serem exclusivas nesse aspecto. Para Mitnick e Simon (2003, p. 200), as

> [...] instituições precisam desenvolver programas de treinamento adaptados a grupos distintos, como: os gerentes, o pessoal de TI, os usuários de computadores, o pessoal das áreas não técnicas, os assistentes administrativos, pessoal da recepção e segurança.

A preocupação dos autores deve ser foco de discussões em diferentes áreas, sendo salutar a inserção do profissional da informação nestas discussões, pois esse pode trabalhar com uma visão geral do fluxo informacional de uma organização podendo colaborar com a elaboração e implantação das políticas para gestão da segurança da informação.

4 POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

Uma política de segurança da informação deve ser elaborada por um grupo multidisciplinar que integre diversos aspectos e necessidades. É fundamental que se defina um processo de criação, manutenção e divulgação da política, que envolva a alta direção e inicie os trabalhos com a elaboração das diretrizes e normas. A maturidade da segurança de uma instituição está ligada diretamente à compreensão de sua política de segurança e à disseminação dessa cultura por seus ativos humanos (SÊMOLA, 2014).

Mitnick e Simon (2003) definem as políticas de segurança como um conjunto de instruções objetivas e claras, que fornecem as diretrizes para o comportamento dos empregados com relação à guarda das informações, e são um fator crucial na elaboração de controles efetivos para contra-atacar as possíveis ameaças à segurança. Essas políticas estão entre as mais significativas no que diz respeito a evitar e detectar os ataques da engenharia social.

O Tribunal de Contas da União define política de segurança da informação como sendo:

> [...] um conjunto de princípios que norteiam a gestão de segurança de informações e que deve ser observado pelo corpo técnico e gerencial e pelos usuários internos e externos. As diretrizes estabelecidas nesta política determinam as linhas mestras que devem ser seguidas pela organização para que sejam assegurados seus recursos computacionais e suas informações (TCU, 2007, p. 26).

Para Mitnick e Simon (2003), os controles efetivos de segurança são concretizados pela capacitação dos empregados, bem como por políticas e procedimentos bem documentados. Um exemplo citado pelos autores são as políticas sobre a abertura dos anexos de correio eletrônico, os quais podem instalar vírus, permitindo uma invasão, método que é muito usado pelos invasores.

A questão sobre os vírus de computadores foi utilizada nesta pesquisa para identificar as implicações relacionadas aos usuários da PROGEP, pois são os elementos mais básicos para a implementação de uma política de segurança. A Política de Segurança da Informação (PSI) foi instaurada na UFPB, por meio da resolução nº 32/2014. “Esta resolução estabelece o cuidado necessário que todo servidor, professor e aluno da instituição deve ter ao fazer uso dos recursos de tecnologia da informação (TI), especialmente ao acessar a rede UFPB e seus recursos”.

O vírus de computador é um tipo de *software* amplamente conhecido e disseminado. De acordo com a cartilha do CERT:

> Vírus é um programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos. Para que possa se tornar ativo e dar continuidade ao processo de infecção, o vírus depende da execução do programa ou arquivo hospedeiro, ou seja, para que o seu computador seja infectado é preciso que um programa já infectado seja executado (CERT, 2012, p. 24).

Para Morimoto (2010, p. 389), vírus pode ser entendido como um programa que

> [...] espalha através de arquivos infectados, páginas que exploram vulnerabilidades no navegador, e-mails, e assim por diante, geralmente utilizando alguma técnica de engenharia social que leve o usuário a clicar em um link ou executar um arquivo.

Nesse contexto, dentro das instruções da política de segurança da informação, deve-se incluir a instalação de um software antiviral em toda instituição. O uso desse software ajuda a detectar e remover códigos maliciosos, se fazendo necessário que esteja instalado e frequentemente atualizado. Apesar de existir uma variedade desses softwares gratuitos, acredita-se que os que geram custos às instituições sejam mais confiáveis devido às atualizações serem mais constantes. Além de mais eficientes, os softwares pagos contribuem positivamente com as políticas de segurança das instituições (FERREIRA, 2013).

No desenvolvimento desta pesquisa, foi analisado, dentre outros pontos, o nível de conhecimento das políticas de segurança da informação da instituição; a intenção; ou uso, de softwares antivírus pelos servidores da PROGEP.

5 PROCEDIMENTOS METODOLÓGICOS

Quanto à sua tipologia, podemos considerar a pesquisa como estudo de caso. Segundo YIN (2005, p. 32), o estudo de caso é caracterizado pela "[...] análise de um fenômeno contemporâneo relacionado à segurança da informação em uma organização real, objetivando encontrar respostas para um problema existente".

Em relação a sua natureza, caracteriza-se como pesquisa descritiva, uma vez que "objetiva descrever as características de determinada população ou fenômeno ou o estabelecimento de relações entre variáveis. Envolve o uso de técnicas padronizadas de coleta de dados: questionário e observação sistemática" (GIL, 1991, p. 45).

Para a coleta de dados, foi utilizado um questionário de perguntas fechadas que, “geralmente, cumpre pelo menos duas funções: descrever as características e medir determinadas variáveis de um grupo social. As perguntas ou afirmações desse questionário apresentam categorias ou alternativas de respostas fixas e preestabelecidas” (RICHARDSON, 1995, p. 142).

O questionário foi criado como formulário *on-line* usando o *Google Docs* e enviado por e-mail a todos os coordenadores e diretores da Progep, no período de 11 a 25 de julho de 2014. O e-mail continha um texto de esclarecimento e informações sobre a pesquisa, juntamente com dois *links:* um do questionário e outro do antivírus *BitdefenderQuickScan* sugerido para analisar o computador antes de iniciar o questionário. O texto continha, ainda, uma solicitação para que os coordenadores reenviassem o e-mail para sua equipe, uma vez que não se possuía o e-mail de todos os servidores na secretaria da Progep.

Quanto à sua estrutura, o questionário foi composto por quatorze questões e dividido em três tópicos: dados pessoais, contendo duas perguntas que serviram para identificar os servidores quanto à idade e ao tempo de serviço; no segundo tópico, abordou-se a parte institucional, com quatro questões sobre a política de segurança da informação na Progep/UFPB; o último tópico, denominado segurança da informação, continha cinco perguntas sobre ações de segurança da informação e uso de senhas e três referente à utilização/não utilização do programa de antivírus sugerido. Essa metodologia replica a utilizada no trabalho implementado por Komatsu, Takagi, e Takemura (2013).

O universo foi composto pelos cento e quarenta e oito servidores da Progep/UFPB. O estudo teve uma amostragem não probabilística, por conveniência e acessibilidade, “[...] comumente aplicada em estudos exploratórios, onde não é requerido um elevado nível de precisão” (GIL, 1999, p. 101). A amostra foi composta por 46 servidores, representando 31% do universo da pesquisa, um número significativo, considerando o fato de que o

instrumento foi enviado por e-mail. Esse indicador ainda foi influenciado pelo mês em que a pesquisa foi realizada, em julho, período em que muitos servidores se encontravam de férias. Diferente do observado na pesquisa realizada por Ayako Komatsu, Daisuke Takagi e Toshihiko Takemura, que obteve 2.254 respondentes em apenas um dia em que a pesquisa se manteve disponível na internet.

6 ANÁLISE DOS DADOS

As questões iniciais do formulário contribuíram para identificar o perfil dos servidores da PROGEP, quanto à idade e tempo de serviço. Constatamos que 19 servidores, dos 46 que responderam ao questionário, possuem entre 30 e 39 anos e 17 possuem mais de 10 anos de serviço na UFPB.

Quando questionados sobre a política de segurança da informação, 98% responderam que não conheciam e, que caso exista, não é disseminada. É necessário esclarecer que, durante a fase de coleta de dados, a UFPB não havia publicado sua própria política de segurança da informação. Entretanto, as questões tinham como referência as normas do governo federal. A publicação da PSI da UFPB só veio ocorrer três meses depois, em outubro de 2014.

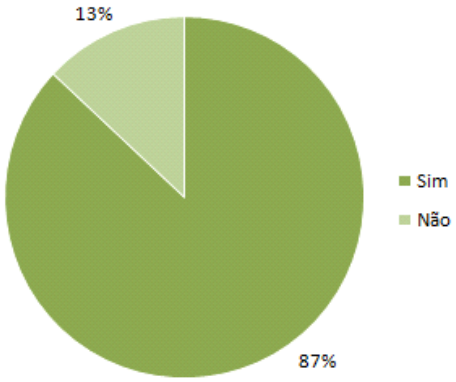
Quanto à capacitação em segurança da informação, 93% dos servidores responderam que não possuíam capacitação nessa área. De acordo com Mitnick e Simon (2003, p. 200), o programa de treinamento e conscientização sobre segurança “deve ser desenvolvido de modo que todos os empregados tenham de participar. Os novos empregados devem participar dele como parte de seu treinamento inicial”. Os autores recomendam que nenhum empregado tenha acesso a um computador antes de ter participado de uma sessão básica de conscientização sobre a segurança.

No entanto, quando perguntado se a UFPB oferece antivírus corporativo, 98% responderam que não, como referenciado anteriormente por Ferreira (2013), a instalação do padrão corporativo de software antiviral 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 software antiviral gratuito.

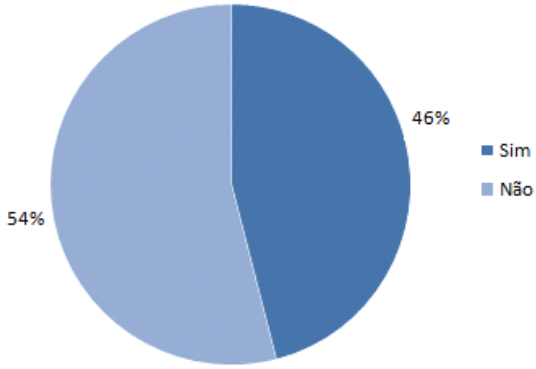
O último tópico abordou o comportamento do servidor quanto à segurança da informação. Assim, identificamos que 87% possuíam antivírus no computador de trabalho, Gráfico 1. No entanto, apenas 46% realizavam atualizações, como mostra o gráfico 2. Referente à infecção por vírus, 76% responderam que foram vítimas dessa infecção e 98% conheciam alguém que tenha sofrido ataque por vírus.

Gráfico 1 - Possui antivírus



Fonte: Dados da pesquisa (2014).

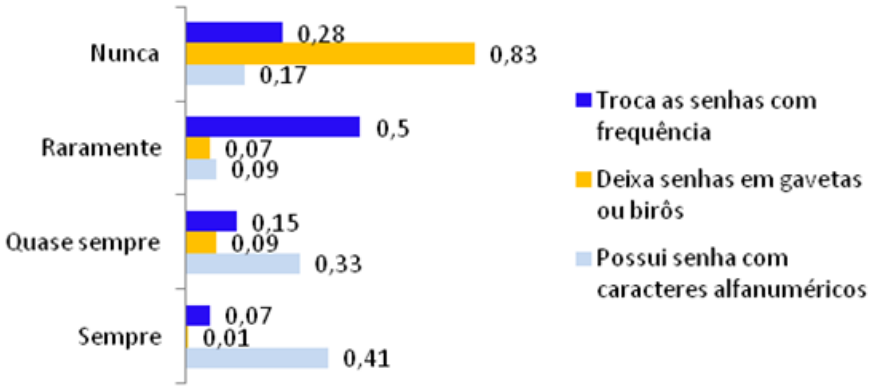
Gráfico 2 - Realiza Atualização



Fonte: Dados da pesquisa (2014).

Sobre o comportamento do servidor quanto ao uso de senhas, identificou-se que 50% raramente as trocam; e 83% indicaram que nunca deixam senhas em gavetas ou birôs. Nesse contexto, Mitnick e Simon (2003) afirmam que os servidores não devem jamais anotar suas senhas e deixá-la próximo ao computador. Anotar as senhas só é recomendado quando o servidor possui várias contas em diferentes sistemas de computadores. Nesse sentido, todas as senhas escritas devem estar seguras em um local longe do computador. Em nenhuma circunstância uma senha pode ser armazenada próximo ao teclado ou pregada no monitor do computador. Quanto às senhas alfanuméricas, elas são sempre utilizadas por 41% dos respondentes, como ilustra o Gráfico 3.

Gráfico 3 – Uso de senhas



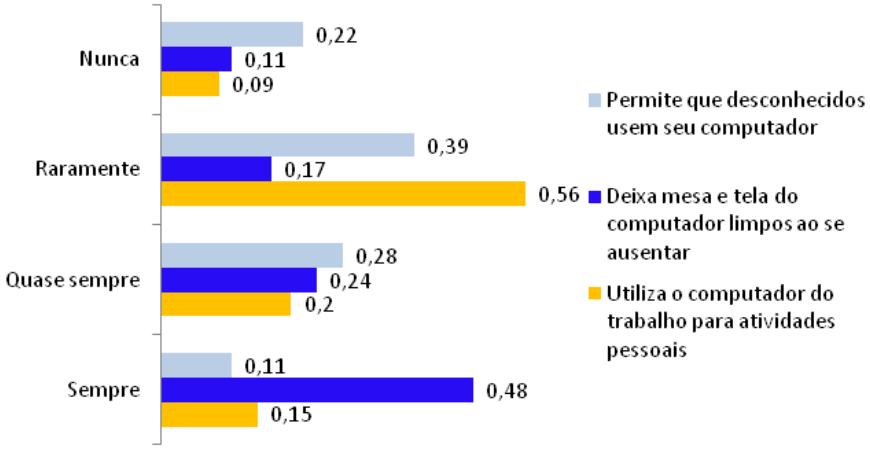
Fonte: Dados da pesquisa (2014).

Concernente ao uso de computadores, como mostra o gráfico 4, 39% dos servidores raramente permitem que desconhecidos usem seu computador de trabalho. Corroborando essa ideia, os autores Mitnick e Simon (2003, p.249) alertam que

> [...] todos os empregados são responsáveis por definir uma senha de proteção de tela e um *timeout* de inatividade com tempo não superior a dez minutos. A intenção desta política é evitar que uma pessoa não autorizada use o computador de outra pessoa.

Além disso, essa política evita que os sistemas de computadores da empresa sejam facilmente acessados por estranhos que tenham tido acesso ao prédio da Reitoria. Na Progep, 48% dos respondentes sempre deixam a tela do computador e o birô limpos ao se ausentarem do ambiente de trabalho e 56% raramente utilizam o computador do trabalho para atividades pessoais, conforme é ilustrado no Gráfico 4.

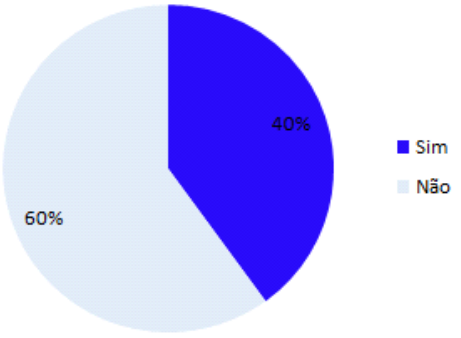
Gráfico 4 – Compartilhamento de computadores



Fonte: Dados da pesquisa (2014).

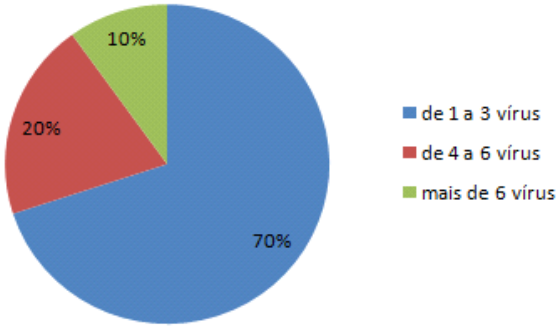
Quanto ao uso do antivírus indicado, 60% dos respondentes não o utilizaram, o que foi o oposto obtido na pesquisa de referência em que, segundo Komatsu, Takagi e Takemura (2013, p. 5, tradução nossa) "[...] torna-se necessário investigar o comportamento coletivo, a fim de persuadir as pessoas a adotarem comportamentos para lidar com as medidas de segurança de informações". Os autores obtiveram um número muito maior de pessoas que usaram o antivírus, e fizeram o alerta para verificar o comportamento da minoria.

Gráfico 5 – Uso do antivírus



Fonte: Dados da pesquisa (2014).

Gráfico 6 - Quantidade de vírus identificados



Fonte: Dados da pesquisa (2014).

Dentre os 40% dos respondentes que utilizaram o antivírus sugerido, 28% identificaram vírus em suas estações de trabalho. Desse percentual, 70% apontaram a existência de 1 a 3 vírus, como mostra o gráfico 6. Diante dessa realidade, torna-se evidente a necessidade de implementação de medidas de segurança na Propep que venham a minimizar os riscos de ameaças, seja pelos vírus identificados ou pela postura dos usuários.

6 CONSIDERAÇÕES FINAIS

Os aspectos humanos relacionados à segurança da informação em instituições públicas ainda é um tema pouco explorado no Brasil. Embora existam trabalhos nesse contexto, a maioria se restringe à segurança relacionada à tecnologia. No entanto, trata-se de uma temática que precisa de maior compreensão de modo a gerar considerações consistentes a esse assunto tão presente e significativo. Os resultados destes trabalhos podem auxiliar a minimizar a incidência das inúmeras ameaças à segurança da informação, bem como criar uma cultura organizacional de segurança.

Apesar de o Decreto nº 3.505/2000 instituir a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal e deste ser um tema recorrente na mídia de maneira geral, a Universidade Federal da Paraíba publicou sua política de segurança da informação apenas em 24 de outubro de 2014, por meio da Resolução CONSUNI 32/2014. (UNIVERSIDADE..., 2014).

É possível inferir que o comportamento dos servidores da Progep, no tocante à segurança da informação, quando da aplicação desta pesquisa, estava diretamente relacionado à inexistência de procedimentos para sensibilizar os servidores da importância de manter as informações em segurança, bem como de procedimentos padronizados do comportamento humano diante de eventuais ameaças. A partir do relato de experiência dos servidores, percebe-se a necessidade de programas de conscientização,

capacitação dos servidores, termo de responsabilidade e uma política de segurança sólida composta por instruções e objetivos claros.

Esta pesquisa não encerra essa discussão, pelo contrário, demonstra a necessidade de sua ampliação, pois os ambientes organizacionais estão em constante alteração. Serão necessários outros estudos que abordem a segurança da informação, no contexto da UFPB, por exemplo, para compreendermos a relevância da implantação de uma política de segurança da informação neste tipo de organização, se a implantação desta gerou uma mudança no comportamento do público estudado, bem como para identificar eventuais lacunas na política estabelecida.

REFERÊNCIAS

ARAÚJO, W. J. de. **A 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.

ABNT. NBR ISO/IEC 27001:2013: **Tecnologia da Informação - Técnicas de segurança - Sistemas de gestão da segurança da informação - Requisitos**. Rio de Janeiro, Associação Brasileira de Normas Técnicas, 2013.

ABNT. NBR ISO/IEC 27005:2008: **Tecnologia da Informação - Técnicas de segurança – Gestão de riscos de segurança da informação**. Rio de Janeiro, Associação Brasileira de Normas Técnicas, 2008.

ABNT. NBR ISO/IEC 27002:2007: **Tecnologia da Informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação**. Rio de Janeiro, Associação Brasileira de Normas Técnicas, 2007.

BORKO, H. Information science: what is it? **American Documentation**, v. 19, n. 1, p. 3-5, jan. 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 de jul. de 2014.

CAPURRO, R.; HJÖRLAND, B. O conceito de informação. **Perspectivas em Ciência da Informação**, v. 12, n. 1, p. 148-207, 2007. Disponível em: <http://portaldeperiodicos.eci.ufmg.br/index.php/pci/article/view/54>. Acesso em: 12 jul. 2014.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL (CERT). **Cartilha de Segurança para Internet**. 2012. Disponível em: <http://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 12 jul. 2014.

COLWILL, C. **Human factors in information security: The insider threat &Who can you trust these days?** Disponível em: <http://csb.uncw.edu/people/cummingsj/classes/MIS534/Articles/Ch11InternalThreatsUsers.pdf>. Acesso em: 12 jul. 2014.

FEDERAL, Governo. **Instrução Normativa GSI/PR Nº 1**. Brasília, DF: Diário Oficial da União, 2008.

FERREIRA, J. de O. **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. 123 f. Dissertação (Mestrado em Ciência da Informação) – Universidade Federal da Paraíba, João Pessoa, 2013.

FRANGOPOULOS, E. D.; ELOFF, M. M.; VENTER, L. M. **Information Management & Computer Security**, v. 21, n. 1, 2013. Disponível em: <www.emeraldinsight.com/0968-5227.htm>. Acesso em: 26 jul. 2014.

GIL, A. C. **Como elaborar projetos de pesquisa**. 3. ed. São Paulo: Atlas, 1991.

GIL, A. C. **Métodos e técnicas de pesquisa social.** 5.ed. São Paulo: Atlas, 1999.

KOMATSU, A; TAKAGI, D.; TAKEMURA, T. Human aspects of information security: An empirical study of intentional versus actual behavior. **Information Management & Computer Security**, v. 21, n. 1, 2013.

MITNICK, K. D.; SIMON, W. L. **Mitnick:** A arte de enganar**.** São Paulo: Pearson Makron Books, 2003.

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

POLIZELLI, D. L.; OZAKI, A. M. (Org.) **Sociedade da informação:** os desafios da era da colaboração e da gestão do conhecimento. São Paulo: Saraiva, 2008

RICHARDSON, R. J. **Pesquisa Social:** métodos e técnicas. São Paulo: Atlas, 1995.

SÊMOLA, M. **Gestão da Segurança da Informação:** uma visão executiva. Rio de Janeiro: Campus, 2014.

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

TAYLOR, R.S. Professional aspects of information science and technology. In: CUADRA, C. A. **Annual Review of Information Science and Technology**. New York: John Wiley, v. 1, 1966, p. 15-40.

TRIBUNAL DE CONTAS DA UNIÃO (TCU). **Boas práticas em segurança da informação.** 2. ed. Brasília, 2007.

UNIVERSIDADE FEDERAL DA PARAÍBA**. Resolução CONSUNI 32 de 22 de outubro de 2014**. Institui a política de segurança da informação da UFPB, normaliza procedimentos com esta finalidade e dá outras providências. João Pessoa, 2014.

YIN, R.K. **Estudo de caso:** planejamento e métodos. 3. ed. Porto Alegre: Bookman, 2005.

STUDY OF HUMAN ASPECTS OF INFORMATION SECURITY APPLIED AT THE DEAN'S OFFICE OF PEOPLE MANAGEMENT OF THE FEDERAL UNIVERSITY OF PARAÍBA-UFPB

ABSTRACT

Introduction: The universe of activities that permeate information technology is subject to various forms of threats that seriously compromise its security. The

technology itself is responsible for providing part of the solution to these problems. However, some of the vulnerabilities and threats to which information systems are exposed can be attributed to deficiencies in organizational procedures and human behavior. In this context, it is positive to study, from the Information Science viewpoint, one subjective variables of the information security process, which is related to people. For this, this paper presents an experience report about the behavior of the public servants of the Dean's Office of People Management - Progep of the Federal University of Paraíba - UFPB related to information security. **Objective:** Identify which information security actions, related to human aspects, are used by the Dean's Office of People Management - Progep of the Federal University of Paraíba - UFPB. **Methodology:** This research was characterized as descriptive, with quantitative-qualitative approach. For data collection, an online questionnaire was sent by e-mail to Progep's Public Servants, during the period from July 11 to 25, 2014. **Results:** It was found that 93% of respondents had no knowledge of information security, 50% rarely exchange their passwords. But the most alarming was that 60% refused to pass the virus scan on their workstations. **Conclusions:** Was identified by the research that there are no procedures to raise awareness among public servants about the importance of keeping safety the organizational information as well as the lack of a security policy that guides how to behave in the face of any threats.

Descriptors: Information security management. Information security policy. Human aspects of information security. People management.

ESTUDIO DE LOS ASPECTOS HUMANOS DE LA SEGURIDAD DE LA INFORMACIÓN APLICADO EN EL DECANO DE GESTIÓN DE PERSONAS DE LA UNIVERSIDAD FEDERAL DE PARAÍBA-UFPB

RESUMEN

Introducción: El universo de actividades que permea la tecnología de la información está sujeto a varias formas de amenazas que comprometen seriamente su seguridad. La propia tecnología es responsable de proporcionar parte de la solución a estos problemas. Sin embargo, parte de las vulnerabilidades y amenazas a las que se exponen los sistemas de información se pueden atribuir a las deficiencias en los procedimientos organizativos y el comportamiento humano. En este contexto, se vuelve saludable estudiar, bajo la óptica de la Ciencia de la Información, una de las variables subjetivas del proceso de seguridad de la información, que está relacionada a las personas. Por lo tanto, este trabajo presenta un relato de experiencia sobre el comportamiento de los servidores del decano de Gestión de Personas - Progep la Universidad Federal de Paraíba - UFPB con respecto a la seguridad de la información. **Objetivo:** Identificar qué acciones de seguridad de la información, relacionadas con los aspectos humanos, son utilizadas por el Decano de Gestión de Personas - Progep de la Universidad Federal de Paraíba - UFPB. **Metodología:** Esta investigación se caracterizó como de carácter descriptivo, con abordaje cuantitativo y cualitativo. Para la recolección de datos se utilizó un cuestionario en línea enviado por correo electrónico a los servidores del Progep durante el período de 11 a 25 julio, 2014.

Resultados: Se verificó que el 93% de los encuestados no tenía conocimiento de seguridad de la información, el 50% rara vez cambian sus contraseñas. Pero lo más alarmante es que el 60% se negó a escanear sus estaciones de trabajo con antivirus. **Conclusiones:** Se identificó la inexistencia de procedimientos para sensibilizar a los servidores de la importancia de mantener la información organizacional en seguridad, así como la falta de una política de seguridad que oriente como comportarse ante posibles amenazas.

Descriptores: Gestión de seguridad de la información. La política de seguridad de la información. Aspectos humanos de seguridad de la información. Gestión de personas.

Recebido: 10.03. 2017
Aceito: 27.02.2018