SUSTENERE Publishing Corporation

Revista Brasileira de Administração Científica
Brazilian Journal of Scientific Administration

Ago, Set, Out, Nov, Dez 2017 - v.8 - n.3

RBADM REVISTA BRASILEIRA DE ADMINISTRAÇÃO CIENTÍFICA

ISSN: **2179-684X**

This article is also available online at:
www.sustenere.co/journals

O fator humano como uma vulnerabilidade em segurança da informação

Entre as possíveis vulnerabilidades relacionadas à segurança da informação que estão presentes em um ambiente organizacional, técnicas, físicas e humanas, a literatura destaca o fator humano como o elemento mais fraco e mais importante na gestão de segurança da informação. Não é possível a criação de barreiras ou ferramentas que protejam o componente humano, da mesma forma que estas são criadas para os componentes técnicos e físicos. Este artigo tem por objetivo realizar uma análise descritiva das vulnerabilidades ocasionadas pelas ações humanas em um ambiente organizacional a partir da percepção do usuário e da equipe de suporte a TI, com o foco nas ameaças e incidentes causados pelo fator humano. Para realização do estudo, aplicou-se um questionário com dois grupos de funcionários de uma instituição de ensino federal, um grupo de funcionários foi formado por profissionais de TI e outro grupo foi formado por usuários da TI, ou seja, funcionários que não tem relação diária com a manutenção do parque de máquinas da organização. Os resultados obtidos serviram como base para proposições que demonstraram que as ações humanas, tanto de usuários não técnicos como de usuários técnicos que deveriam cuidar da segurança da informação, podem gerar sérios problemas para a segurança da informação.

Palavras-chave: Fator Humano; Informação; Vulnerabilidade; Segurança da Informação.

The human factor as a vulnerability in information security

Among the possible vulnerabilities related to information security that are present in an organizational environment, technical, physical and human vulnerabilities, literature highlights the human factor as the weakest and most important element in the information security management. It is not possible to create barriers or tools to protect the human component, just as they are created for the technical and physical components. This article aims to perform a descriptive analysis of the vulnerabilities caused by human actions in an organizational environment from the perception of the user and the IT support team, focusing on the threats and incidents caused by the human factor. To carry out the study, a questionnaire was applied with two groups of employees of a federal education institution, a group of employees was formed by IT professionals and another group was formed by IT users, that is, employees who have no relation with the maintenance of the IT park of the organization. The results obtained served as a basis for propositions that demonstrated that human actions, both by non-technical users and technical users, who should take care of information security, can generate serious problems for information security.

Keywords: Human Factor; Information; Vulnerability; Information Security.

Topic: **Sistemas e Tecnologia da Informação**

Reviewed anonymously in the process of blind peer.

Received: **20/10/2017**
Approved: **23/12/2017**

Rodolfo Francisco Paz Freire
Centro Universitário Santo Agostinho, Brasil
http://lattes.cnpq.br/1938513573530702
rodolfonarrow@gmail.com

Humberto Caetano Cardoso da Silva
Universidade Federal de Pernambuco, Brasil
http://lattes.cnpq.br/4594928852071554
http://orcid.org/0000-0001-9584-4465
humberto.ccs@gmail.com

Ricardo Gomes de Queiroz
Faculdade Santo Agostinho, Brasil
http://lattes.cnpq.br/4554869548634061
rgqueiroz@gmail.com

Amélia Acácia de Miranda Batista
Faculdade Santo Agostinho, Brasil
http://lattes.cnpq.br/4146356217218356
ameliacaciamb@gmail.com

DOI: 10.6008/SPC2179-684X.2017.003.0012

Referencing this:
FREIRE, R. F. P.; SILVA, H. C. C.; QUEIROZ, R. G.; BATISTA, A. A. M.. O fator humano como uma vulnerabilidade em segurança da informação. **Revista Brasileira de Administração Científica**, v.8, n.3, p.146-157, 2017. DOI: http://doi.org/10.6008/SPC2179-684X.2017.003.0012

INTRODUÇÃO

As transformações ocorridas na última década do século XX, que largamente impulsionaram o avanço tecnológico, tornaram a informação um importante ativo econômico. Agora a informação não é apenas um recurso, mas "O" recurso (MORESI, 2000), sendo considerada como um dos insumos mais importantes para a competição entre as empresas e utilizada principalmente como motriz de geração de conhecimento e otimização de produção.

A evolução trouxe a larga difusão dos computadores pessoais, das redes de computadores e principalmente a necessidade de compartilhamento de informação por meio da Internet. Porém, os riscos também aumentaram em grande proporção. Nesse cenário, é crucial a atuação da gestão de Segurança da Informação (SI), conceituada como uma área do conhecimento que salvaguarda os chamados ativos da informação, contra acessos indevidos, modificações não autorizadas ou até mesmo sua não disponibilidade (PEIXOTO, 2006).

Silva Netto et al. (2007) argumenta que a SI pode ser classificada em camadas ou aspectos. Essas camadas podem ser tecnológicas, físicas ou humanas (SÊMOLA, 2003) ou física, lógica e humana (ADACHI, 2004). Nas duas classificações propostas o aspecto humano se apresenta e, segundo Silva Netto et al. (2007), é o aspecto colocado em segundo plano. Para Carneiro et al. (2013) a gestão da SI deve ser tratada de forma integrada, utilizando os elementos 'pessoas', 'processos' e 'tecnologias'. É necessário que seja abandonado a dependência exclusiva de perspectivas tecnológicas e passar a utilizar uma visão mais ampla, que contempla, também, aspectos subjetivos inerentes aos seres humanos.

Para Mitnick et al. (2003), o fator humano é considerado o elemento mais importante na gestão de SI, como também o elo mais fraco da segurança. De acordo com Vidal (2006), o ponto mais vulnerável em um sistema computacional também é o componente humano. A quebra de SI, a partir das vulnerabilidades humanas, se torna cada vez mais frequente devido ao baixo custo para implementação dos ataques (MITNICK et al., 2003).

As tecnologias de proteção não têm se mostrado totalmente eficientes quando o usuário não é treinado, não tem ciência das situações de risco que poderá passar e não sabe como solucioná-las ou qual procedimento de emergência adotar. Diante do quadro abordado, este estudo tem por objetivo avaliar a vulnerabilidade aplicado ao fator humano por meio de suas ações no ambiente pesquisado. O instrumento de coleta de dados foi um questionário, destinado a funcionários, técnicos e não técnicos, de uma instituição de ensino federal.

REVISÃO TEÓRICA

Segurança da Informação e seus princípios

Com a ampla expansão do compartilhamento de informações, a SI tornou-se um ponto de extrema importância às organizações, que são alvos constantes de ameaças e vulnerabilidades internas e externas. Podemos definir a SI, de acordo com Fontes (2006) como o conjunto de orientações, normas, procedimentos, políticas e demais ações que tem por objetivo proteger o recurso informação.

A SI apresenta as seguintes propriedades principais: confidencialidade, autenticidade, integridade e disponibilidade (OLIVEIRA et al., 2011). A confidencialidade deve garantir a proteção das informações contra acessos indevidos, sejam eles internos ou externos. A autenticidade está associada a veracidade da identificação da informação. A integridade protege a informação contra modificações não autorizadas pelo proprietário. A disponibilidade consiste em evitar que a informação seja degradada ou esteja indisponível sem autorização, podendo ser acessada a qualquer instante.

Em termos de comunicação em redes de computadores, Kurose (2010) define algumas propriedades da informação como desejáveis para uma comunicação segura: confidencialidade (somente o remetente e o destinatário pretendido devem poder entender o conteúdo da mensagem transmitida); autenticidade (o remetente e o destinatário precisam confirmar a identidade da outra parte envolvida na comunicação – confirmar que a outra parte realmente é quem alega ser); integridade (mesmo que o remetente e destinatário consigam se autenticar reciprocamente, eles também querem assegurar que o conteúdo de sua comunicação não seja alterado, por acidente ou por má intenção, durante a transmissão).

Com a utilização de ferramentas cada vez mais sofisticadas, as redes de computadores e os sistemas computacionais tendem a dificultar as possibilidades de invasão e de danos as informações. Porém, o crescimento nos critérios de proteção também desencadeia o surgimento de novas ameaças. Nakamura (2007) elenca os seguintes fatores como justificativa para que a preocupação com segurança seja contínua: as novas tecnologias trazem consigo novas vulnerabilidades; necessidade de entendimento da natureza dos ataques; o aumento da conectividade resulta em novas possibilidades para invasores; a existência tanto de ataques direcionados quanto de ataques oportunistas; complexidade maior na defesa do que no ataque; e o aumento de crimes digitais.

A SI é obtida a partir da implementação de um conjunto de controles adequados incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Porém, a SI não pode se alicerçar apenas no contexto tecnológico, pois o fator humano é considerado crucial no processo de garantia de segurança. As pessoas são os elementos mais importantes na gestão de segurança, pois são elas que executam e dão suporte aos processos de uma organização (LYRA, 2008).

Ameaças e vulnerabilidades

As ameaças são fatores/ocorrências que podem violar sistemas e causar incidentes de segurança, e, dessa forma, danos ao negócio da empresa (MOREIRA, 2001). As ameaças podem ser classificadas em: Intencionais: de cunho proposital, que utilizam desde técnicas simples a ataques mais sofisticados; Acidentais: não premeditadas, que aconteceram por desconhecimento, falta de treinamento ou outros fatores; Passivas: quando ocorridas, não trouxeram prejuízos a informação; e Ativas: são alterações ou modificações da informação ou do seu estado operacional.

Gabbay (2003) cita, também, duas classificações para ameaças. As internas, causadas por funcionários, atuais ou ex-empregados, terceirizados ou prestadores de serviços, que queiram prejudicar de

alguma forma a organização. E as externas, causada por fatores que não pertencem as organizações ou que estejam provocando incidentes remotamente.

Incidentes em Segurança

Um incidente é um evento que tem grande probabilidade de impactar nos negócios e na segurança de uma organização (GUALBERTO, 2013). É a partir das fragilidades que os incidentes nascem. As vulnerabilidades são exploradas por ameaças, que por sua vez provocam incidentes. No ano de 2015, 722.205 incidentes foram reportados ao Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br, 2016), causados por *worms*, ataques DoS (*Denial of Service* – Negação de serviço) e a servidores web, invasões, *scan*, fraudes e outros. A figura 1 exibe a distribuição de cada tipo de ataque.

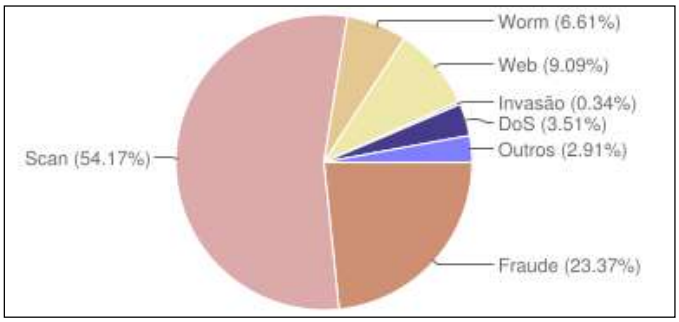

Figura 1: Percentual de incidentes reportados ao CERT.br no ano de 2015. **Fonte**: CERT.br (2016)

Quanto à origem dos incidentes, segundo a Pesquisa Global de Segurança da Informação realizada em 2014 (PwC, 2014), 37% dos incidentes eram causados por agentes internos, como funcionários, e 27% por ex-funcionários. Para os incidentes de causa externa, 32% eram causados por *Hackers*, 14% por concorrentes, 12% pelo crime organizado, e o restante por outros motivos.

Os ataques estão cada vez mais sofisticados. Engenharia social, comunicação por canais seguros, arquitetura distribuída, códigos mutáveis, entre outros fatores, são combinados para resultarem em ameaças mais invasivas e com maior rapidez de disseminação. É importantíssimo que cada organização tenha conhecimento sólido de suas estratégias, processos e estruturas afim de identificar as fragilidades e ter respostas antecipadas aos incidentes, visando reduzir os impactos prejudiciais aos negócios.

Fator humano e sua vulnerabilidade

Os incidentes quantificados na seção anterior estão em sua maioria aplicados ao meio tecnológico. Porém, não se pode esquecer dos decorrentes das fraquezas humanas. Em várias situações, quando se trata de SI, ocorre a associação da proteção com a tecnologia. Porém, mesmo em ambientes computacionais fortemente guardados, os usuários se configuram com um fator preponderante para a ocorrência de incidentes, tendo em vista que o comportamento humano é mutável de acordo com a situação em que é submetido. As situações rotineiras, por falta de conhecimento sobre como agir, ou mesmo as de risco, pelo grau de responsabilidade, tornam o fator humano e suas ações uma vulnerabilidade bastante explorada pelas ameaças de SI (CARNEIRO et al., 2013).

Na pesquisa realizada pela Modulo Technology for Risk Management em 2007, 24% das falhas em seguranças eram causadas pelos funcionários das empresas. Atitudes comuns como escrever senhas em papéis avulsos, ceder a um pedido gentil de informações sobre dados estratégicos, conceder seu *login* a um amigo de trabalho, abrir endereços virtuais a partir do e-mail corporativo, entre outras, são exemplos que parecem inofensivas mas representam falhas constantemente utilizadas por invasores. Para Silva Filho (2004), o ser humano apresenta algumas características que o torna vulnerável e suscetível a falhas como vontade de ser útil, a busca por novas amizades, a prorrogação de responsabilidades e persuasão.

As características descritas por Silva Filho (2004) são bastante utilizadas por ataques de engenharia social. A engenharia social é definida como uma ciência que estuda como o conhecimento do comportamento humano pode ser utilizado para induzir uma pessoa a determinada ação (PEIXOTO, 2006). O famoso hacker Kevin Mitnick utilizava engenharia social em mais de 80% de seus ataques (NAKARUMA, 2007). Várias técnicas podem ser utilizadas para se aplicar um ataque de engenharia social, como o ataque direto, a aquisição de confiança, o auxílio perigoso e latas de lixo (MITNICK et al., 2003).

Os alvos mais comuns para o ataque são as pessoas que desconhecem o valor da informação ou que possuem privilégios especiais e departamentos específicos, como T.I., recursos humanos, contabilidade, etc. (OLIVEIRA et al., 2011). Além da engenharia social, outros incidentes também estão relacionados ao fator humano, como espionagem, fraudes, roubos de propriedade (equipamentos ou informações), sabotagem, etc.

Silveira et al. (2017) afirma que 97% dos *malwares* lançados tem como objetivo enganar os usuários através de algum tipo de esquema. Adicionalmente, Las-Casas (2016) afirma que entre junho de 2012 e junho de 2013, 37,3 milhões de pessoas no mundo foram vítimas de ataques de *malwares* com intenção de ludibriar o usuário.

As técnicas de distribuição de *malwares* na rede são variadas, entretanto a utilização de *phishing* está entre as mais comuns. Apesar da técnica de *phishing* se utilizar de e-mails *spams* para sua disseminação, o *phishing* se diferencia do *spam* pela característica da criação de páginas ou endereços falsos, mas que tem a aparência de verídicos, visando o roubo de dados pessoais, informações bancárias ou de cartão de crédito, enquanto um e-mail spam, propriamente dito, pode ser apenas mensagens comerciais ou de conteúdo diverso que são enviadas aos usuários sem seu consentimento prévio (LAS-CASAS, 2016).

Para Las-Casas (2016), um ataque que utiliza a técnica de *phishing* se vale de artifícios como termos e tratamentos formais, menção monetária, senso de urgência, pedido de resposta, preenchimento de formulários ou indicações de procedimentos de segurança. Todos esses procedimentos são usados para dar uma sensação de veracidade àquela falsa mensagem, induzindo o usuário a abrir arquivos ou acessar sites contendo *malwares*.

METODOLOGIA

A presente pesquisa, de caráter exploratória e realizada a partir de um estudo de caso em uma instituição federal de ensino básico, técnico e superior, foi aplicada a partir da utilização de um questionário

para dois grupos de funcionários, os usuários de tecnologia e a equipe de suporte de TI. A aplicação do questionário foi realizada durante o mês de maio de 2016.

O questionário foi composto por 28 perguntas objetivas. As questões presentes no questionário foram de múltipla escolha, com única ou múltipla resposta. Ou seja, em algumas questões o respondente poderia apenas escolher uma alternativa, como no questionário para a equipe de TI 'Qual a frequência de realização do backup dos servidores?', enquanto em outras o respondente poderia escolher mais de uma alternativa, como no questionário para usuários da tecnologia, 'Quais das seguintes ameaças você tem algum conhecimento?'.

Foi preparado um questionário para a equipe de TI, e outro para os funcionários usuários que usam a tecnologia. O objetivo foi identificar se a equipe de TI tinha treinamento adequado para implementar e fazer cumprir as políticas de SI e, concomitantemente, verificar o nível de SI que os usuários da tecnologia estavam aplicando nas suas tarefas diárias.

O presente estudo teve como foco um campus de uma instituição federal de ensino, que por motivos de sigilo não terá seu nome revelado. Em relação aos usuários não ligados ao setor de T.I. (administrativos e professores), de um total de 79 pessoas, 52 respostas foram obtidas, cerca de 65.8% do contingente. Já a equipe de TI que suporta as atividades do mesmo campus, um total de 13 questionários foram respondidos. Aqui, todos os funcionários do setor de TI responderam ao questionário.

RESULTADOS E DISCUSSÃO

Análise descritiva da população

A primeira característica verificada é quanto à idade dos respondentes. Há predominação de indivíduos entre 26 e 35 anos, esta faixa representa 63,5% do total de usuários de tecnologia que responderam ao questionário. O mesmo ocorreu com funcionários da equipe de TI, onde 8 dos participantes, ou 61,5%, estavam na faixa entre 26 e 35 anos. Em relação à escolaridade dos respondentes, no grupo de funcionários, a maioria possuía pós-graduação, 44,2%, 25% possuem graduação e o restante, 30,8% até o ensino médio. Enquanto no grupo da equipe de suporte à TI, 53,8% são graduados, 7,7% tem pós-graduação e o restante, 38,5% tem até o ensino médio.

Análise das respostas da equipe de TI

Para a equipe de TI, a ameaça principal à SI é o vírus, com 46,2%, seguido pela utilização de dispositivos móveis, com 15,4%, e o restante, 38,4%, outras ameaças. Em relação à origem da ameaça, 46,2% dos respondentes informaram que a origem principal de ataques à SI é interna, 30,8% externa, e 23,1% desconhecem.

Quando perguntados qual a frequência de realização do backup dos arquivos e servidores da organização, 46,1% informaram que o backup era mensal, 38,5% afirmaram que o backup era realizado sem regularidade, 15,4% que seria semestral. Essa é uma informação importante, pois demonstra um

desalinhamento na equipe de TI. O procedimento de backup é único, então a equipe deveria ter uma ideia clara de como é a política de backup da instituição.

Quando perguntados sobre a estrutura do departamento de SI, 76,9% dos respondentes afirmaram que o departamento está mal estruturado para atender às demandas provenientes de incidentes de SI, o restante, 23,1%, disseram que o departamento de TI está estruturado para atender às demandas de incidentes de SI. Um fato que chama a atenção é que 100% dos integrantes da equipe de TI não recebeu nenhum treinamento prévio ao ser incluído na equipe. Adicionalmente, 46,2% nunca receberam treinamento algum, 38,5% receberam treinamento, mas sem nenhuma regularidade, 7,7% receberam treinamento semestral e 7,7% receberam treinamento com frequência anual.

Análise das respostas dos funcionários

Em relação ao conhecimento em Informática, os seguintes resultados foram obtidos: conhecimento intermediário (manuseio de softwares de edição, utilização de antivírus, instalação de programas, etc.) com 38,5%; conhecimento básico (navegação no Windows, editor de texto simples, acesso à Internet, etc.) com 34,6%; conhecimento avançado (programação, banco de dados, criação de sites, etc.) com 26,9%.

O estudo revelou que 77% sabem que utilizam algum sistema de informação organizacional para auxílio das atividades do trabalho, 11,5% dizem não utilizar (mesmo fazendo o uso) e 11,5% não sabem informar. Observa-se que, 23% desconhece que utiliza um sistema informativo obrigatório da instituição. Ainda, 68,5% dos funcionários não recebeu nenhuma capacitação para utilização do sistema. Com relação a frequência de atualização de conhecimento, 49% dizem não haver regularidade sobre esse procedimento e 39.2% nunca realizaram, o restante, 11,8% afirmaram ter algum tipo de atualização com frequência semestral ou anual.

Um dos pontos indicados pela literatura para o combate às ameaças provenientes de ações humanas é o treinamento (ALMEIDA et al., 2010), na pesquisa foi possível identificar que um grande percentual, 88,2%, não tem treinamento de SI com regularidade. Assim, possíveis falhas de SI podem surgir devido a fatores humanos pela simples falta de treinamento dos usuários.

Cada funcionário possuí um e-mail institucional, criado logo após sua admissão. Este e-mail é vinculado ao sistema de informação organizacional e é utilizado para comunicação interna e externa a caráter funcional. Em relação as senhas dos e-mails, 46,2% do total utilizam informações pessoais, como data de aniversário, sobrenome, nome de familiares e etc. para formá-las. A utilização conjunta de letras e números é feita pela maioria, 63,5% do total. Apenas 30,8% do total de participantes utilizam sinais na composição. Ao questionar sobre a frequência de alteração das senhas, 53,8% não alteram com regularidade e 15,4% nunca alteram, o restante, 30,8%, tem o hábito de alterar as senhas com frequências mensais ou semestrais.

A avaliação deste critério expõe uma vulnerabilidade eminente e mais grave ainda tendo em vista que 68,6% utilizam a mesma senha para *login* no sistema informativo e no e-mail. Em relação a utilização do correio eletrônico, 13,5% opinaram que abririam e-mails cujo remetente é desconhecido e 25% talvez, e apenas 61,5% não abriria mensagens de origem desconhecida. Apesar de representar a maioria, ainda é um

número baixo, visto que este tipo de ataque é largamente conhecido e tratado, não só por TI, mas também na mídia em geral. Quanto à anexos inseridos nos e-mails, 86,5% não abririam os documentos encaminhados por desconhecidos, enquanto 13,5% opinaram que 'talvez abram documentos anexados'.

Sobre a utilização dos computadores, 32,7% o divide com outras pessoas, normalmente funcionários de turnos diferentes. Ao se questionar se deixam o computador '*logado*' sem estar presente, 46,1% opinaram que raramente, 30,8% nunca, 21,2% geralmente e 1,9% frequentemente. Sobre os arquivos guardados nesses computadores, 63,4% deixam alguns arquivos importantes facilmente visíveis, 15,4% todos os arquivos e 21,2% nenhum. A maioria, composta por 80.8% dos usuários, não utiliza nenhum mecanismo de senha para proteção dos arquivos importantes. Em relação a utilização de softwares proprietários com licença falsificada, 53,8% não utiliza softwares piratas, 25% confirmaram a presença desses softwares piratas em seus computadores e 21,2% não souberam informar. Verificou-se também que 86.5% utilizam o computador de trabalho para fins pessoais (e-mails, redes sociais, etc.).

Tratando-se de antivírus, 88,5% informaram que utilizam, 7,7% não utilizam e 3,8% não souberam informar. Sobre suas atualizações, 55,8% confirmaram que o software permanece sempre atualizado, 17,3% que não permanece e 26,9% não souberam informar. Para verificações de ameaças, apenas 11,5% não sabem iniciar o processo e 1,9% não souberam informar. Caso alguma ameaça venha a ser detectada, 63.4% sabem qual ação tomar, 13,5% não sabem o que fazer e 23,1% somente em alguns casos.

Foi questionado também quanto a utilização de computadores pessoais nas atividades de trabalho. Os percentuais obtidos foram: Sempre (28,9%); Frequentemente (25%); Geralmente (9,6%); Raramente (28,8%); Nunca (7,7%). A maioria, com 73%, considera seu computador pessoal parcialmente seguro, 15,4% totalmente seguro, 11,6% inseguro/não souberam informar.

Algumas situações, cujo risco em SI é evidente, foram expostas ao longo do questionário para se avaliar a atitude dos usuários. Quando perguntado 'Um amigo de trabalho precisa fazer uma determinada ação no sistema, mas só você tem permissão para isto. Você cederia seu *login* a ele?', 13,5% informaram que sim, 53,8% que não e 32,7% ficaram indecisos.

Quando perguntado 'Você encontrou um dispositivo de mídia nas instalações de trabalho e não sabe sua procedência. Você abriria e verificaria o conteúdo dele?', 42,3% disseram que sim e 57,7% que não. Quando perguntado 'Seu chefe lhe envia um e-mail solicitando algumas informações pessoais e/ou funcionais para cadastro em uma nova plataforma. Você enviaria as informações?', 30.8% enviariam, 19.2% não e 50% de indecisos.

Em relação às ameaças percebidas pelos funcionários, foi indagado aos mesmos se conheciam as seguintes ameaças: vírus, *spam*, fraude, *phishing*, engenharia social, negação de serviço e *scan*. O resultado está exposto no figura 2. É importante salientar que é possível que um respondente possa ter sido vítima ou ter conhecimento de mais de uma ameaça. Questionados se já foram vítimas de alguma das ameaças anteriormente citada(s), 82.7% afirmaram que sim, 15.4% que não e 1.9% não souberam informar. Quanto a identificação de ataques oriundos dessas ameaças, 73.1% afirmaram que saberiam identificá-lo e 26.9% não.

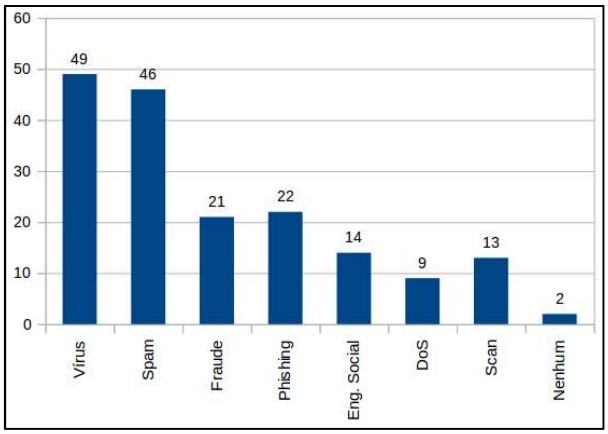

Figura 2: Quantidade de indivíduos que conhecem as ameaças

Relacionado a incidentes nos meios informacionais, foi questionado aos funcionários se eles já haviam presenciado alguma violação de segurança, como por exemplo, ataque de vírus, acesso indevido, fraude, lixo eletrônico, etc. Os percentuais apresentaram pouca diferença: 48% (sim), 38,5% (não) e 13,5% (não souberam informar). A frequência desses incidentes também foi analisada questionando se o funcionário avisa imediatamente ao setor responsável quando presencia uma violação de SI, de acordo com os respondentes: Sempre (0%); Frequentemente (9,9%); Geralmente (7,8%); Raramente (49%); Nunca (33,3%). A maioria dos funcionários, 82,3%, não reporta, ou reporta raramente, incidentes de SI à TI.

Avaliação discursiva dos resultados

A partir dos resultados obtidos por meio da quantificação das opiniões, uma série de problemas foram identificados que comprovam a vulnerabilidade nas ações dos usuários participantes do estudo. Uma das questões importantes é o pouco, ou nenhum, treinamento da equipe de TI para o enfrentamento das ameaças provenientes do aspecto humano da SI, ou de qualquer outro dos aspectos, tecnológico e físico, propostos por Silva Netto et al. (2007).

Como foi verificado, cerca de 23% desconhece o sistema de informações organizacional, de utilização obrigatória na instituição. Não existe uma cultura ou política que incluí treinamento após admissão ou mesmo que regulamente a necessidade de atualização com frequência. A maioria, 68,8%, obteve conhecimento, ou pseudotreinamento, durante o uso do sistema, índice que pode levar a erros de integridade, com a execução incorreta de atividades, confidencialidade, pois não se sabe exatamente qual o nível que um usuário precisa ter, e de disponibilidade, pois o erro do usuário poderia causar uma parada no sistema como um todo.

O e-mail, principal meio de comunicação dentro da instituição, está vulnerável por conta das senhas utilizados pelos usuários para *login*. Um grande número, 46,2% utiliza informações pessoais para compô-las. Outros fatores que aumentam os riscos e foram observados com alto percentual amostral, são: falta de regularidade de alteração das senhas (53,8%), utilização da mesma senha em outros sistemas (68,6%) e composição das senhas apenas com letras e números (63.5%). Os ataques que utilizam força bruta são os principais aproveitadores dessas vulnerabilidades em senhas.

Ter o e-mail comprometido é uma grande falha de segurança e abre portas para muitos outros incidentes. *Spam* e *phishing* são exemplos nesse meio. Dos respondentes, 88,5% possuem algum conhecimento sobre spam e apenas 42,3% em *phishing*. Mas, mesmo com índices aparentemente altos, quando tratamos de um remetente confiável, alguém de dentro da instituição, estas técnicas têm grande chance de passarem despercebidas.

Quando perguntados se enviariam informações pessoais/funcionais a pedidos de seu chefe, por e-mail, apenas 19,2% dos respondentes não enviariam. Caso um e-mail de algum chefe ou coordenador seja comprometido, existe 80,8% de chance de extração de informações de outros usuários. Há perigo não só no envio de informações como também na visualização de conteúdo dos e-mails. Cerca de 13,5% ficaram indecisos quanto a visualização de anexos encaminhados por remetentes desconhecidos. As chances seriam maiores em se tratando de um remetente confiável, encaminhando algum documento esperado pelos destinatários.

O e-mail também pode ser utilizado para coleta de informações, ponto chave para ataques de engenharia social, conhecida somente por 14 dos respondentes. De posse das informações, o engenheiro social pode manipular as vítimas, por meio da confiança e amizade adquirida, obter conteúdo sigiloso a fim de interferir em alguma decisão, roubar propriedade intelectual da instituição, ser porta de entrada para outras ameaças, entre outros danos. Um outro indício que auxilia um possível atacante de engenharia social é o fato de, em 78,9% dos computadores, documentos importantes estarem facilmente visíveis.

Uma boa parcela, 69,3% dos funcionários, deixam seu computador 'logado' sem estarem presentes. A situação pode ser utilizada por atacantes para inserção de vírus, *worms*, *spams*, *bots, botnets*, *spywares*, *backdoors*, *trojans*, *rootkits*, etc., que podem comprometer a máquina do usuário, ou mesmo a rede de toda a instituição, causando incidentes de alta gravidade em termos de SI e de operação da instituição.

CONCLUSÕES

Como pôde ser observado nesta pesquisa, as ações rotineiras, por intenção ou por falta de conhecimento, podem vir a provocar incidentes que demonstram a grande vulnerabilidade do fator humano. As organizações devem estar sempre preocupadas em propiciar um ambiente seguro não só tecnologicamente, mas também funcionalmente. Cada indivíduo deve ter conhecimento suficiente sobre SI para poder implantá-la no dia a dia.

Soluções definitivas são praticamente impossíveis. O comportamento humano é constantemente mutável e imprevisível. Porém, algumas medidas podem ser utilizadas para minimizar os incidentes e riscos, como a criação de políticas de SI com ênfase nos usuários e treinamentos no ambiente intraorganizacional, que possam refletir no ambiente doméstico, sensibilizando e conscientizando sobre o uso correto dos meios informacionais disponíveis (ALENCAR et al., 2013). É necessário que os usuários estejam sempre atentos às suas atividades diárias nas organizações, pois estas estão relacionadas as atividades de segurança. Assim, estes mesmos usuários podem tirar toda vantagem da tecnologia na realização de suas tarefas diárias sem os riscos de falhas ou perdas.

Espera-se que com a exposição das proposições levantadas no estudo, as organizações possam pensar de maneira mais abrangente sobre o impacto das ações dos colaboradores dentro das ações de segurança da instituição, indo além e colaborando com o aumento da segurança da informação até mesmo em aspectos da vida particular de cada um, pois os conceitos aprendidos em processos de treinamento de segurança da informação em ambientes organizacionais é facilmente transferível para aspectos particulares da vida do colaborador.

Um ponto fundamental é o preparo da equipe de tecnologia da informação para enfrentar os desafios da segurança, especificamente no lado humano. É comum ter maior foco em aspectos tecnológicos que em aspectos humanos (SILVA NETTO et al., 2007), deixando uma parte significativa da segurança da informação sem a devida cobertura e atenção. A equipe de tecnologia da informação é responsável pela implantação e por fazer cumprir as regras descritas em um plano de segurança da informação. Todo treinamento nos aspectos de segurança física, lógica e humana, deve ser realizado para que a equipe de TI seja uma disseminadora do conhecimento e fiscalizadora das práticas de segurança da informação.

O presente trabalho foi desenvolvido a partir de um estudo de caso em uma instituição federal de ensino, como continuidade desse trabalho recomenda-se a aplicação do questionário em outros campis, para que se tenha uma visão mais abrangente das vulnerabilidades observadas, possibilitando, também, a análise em diferentes contextos regionais.

Adicionalmente, a pesquisa pode ser realizada em empresas privadas e organizações do terceiro setor, aumentando, assim, a base de dados e possibilitando a comparação entre estes tipos de ambientes, governamental, privado e do terceiro setor. Ainda como trabalho futuro poderia ser feito um estudo de 'como' trabalhar com fatores humanos, aspectos de comunicação, satisfação, etc., para que estes fatores humanos não provoquem impactos na segurança ou que estes impactos sejam amenizados.

REFERÊNCIAS

ADACHI, T.. **Gestão de Segurança em Internet Banking**. Dissertação (Mestrado em Administração) - Fundação Getúlio Vargas, São Paulo, 2004.

ALENCAR, G. D.; LIMA, M. F.; FIRMO, A. C. A.. O efeito da conscientização de usuários no meio corporativo no combate à Engenharia Social e Phishing. In: SIMPÓSIO BRASILEIRO DE SISTEMAS DE INFORMAÇÃO, 9. **Anais**. Aracaju: UNIT, 2013.

ALMEIDA, M. B.; SOUZA, R. R.; COELHO, K. C.. Uma proposta de ontologia de domínio para segurança da informação em organizações: descrição do estágio terminológico. **Informação & Sociedade**, v.20, n.1, 2010.

CARNEIRO, L. E. S.; ALMEIDA, M. B.. Gestão da Informação e do Conhecimento no âmbito das práticas de Segurança da Informação: O fator humano nas organizações. **Bibli: Revista Eletrônica de Biblioteconomia e Ciência da Informação**, v.18, n.37, p.175-202, 2013.

CERT.br. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Estatísticas dos Incidentes Reportados ao CERT.br**. São Paulo: CERT.br, 2016.

FONTES, E.. **Segurança da Informação**: o usuário faz a diferença. São Paulo: Saraiva, 2006.

GABBAY, M. S.. **Fatores influenciadores da implementação de ações de Gestão de Segurança da Informação**: um estudo com Executivos e Gerentes de Tecnologia da Informação em empresas do Rio Grande do Norte. Dissertação (Mestrado em Engenharia de Produção) – Universidade Federal do Rio Grande do Norte, Natal, 2003.

GUALBERTO, É. S.. Proposição de uma Ontologia de Apoio à Gestão de Riscos de Segurança da Informação. **iSys – Revista de Sistemas da Informação**. Rio de Janeiro, v.6, n.1, p.30-43, 2013.

KUROSE, J. F.; ROSS, K. W.. **Redes de computadores e a Internet**: uma abordagem top-down. 5 ed. São Paulo: Addison Wesley, 2010.

LAS-CASAS, P. H. B.. Uma metodologia para identificaçao adaptativa e caracterizaçao de phishing. In: BRAZILIAN SYMPOSIUM ON COMPUTER NETWORKS AND DISTRIBUTED SYSTEMS. **Anais**. SBRC, 2016.

LYRA, M. R.. **Segurança e Auditoria em Sistemas de Informação**. Rio de Janeiro: Ciência Moderna, 2008.

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

MOREIRA, N. S.. **Segurança mínima**: uma visão corporativa da segurança de informações. Rio de Janeiro: Axcel Books do Brasil, 2001.

MORESI, E. A. D. Delineando o valor do sistema de informação de uma organização. **Ciência da Informação on Line**, Brasília, v.29, n.1, p.14-24, 2000.

NAKAMURA, E. T.; GEUS, P. L.. **Segurança de Redes em Ambientes Cooperativos**. São Paulo: Novatec, 2007.

OLIVEIRA, M. C.; VIEIRA, A. T.. **Quantificação de vulnerabilidades em segurança da informação avaliando maturidade de pessoas**. Monografia (Graduação em Tecnologia em Redes de Computadores) - Universidade Luterana do Brasil, Canoas, 2011.

PEIXOTO, M. C. P.. **Engenharia social e segurança da informação na gestão corporativa**. Rio de Janeiro: Brasport, 2006.

PwC. PricewaterhouseCoopers. **Pesquisa Global de Segurança da Informação**. Londres: PwC, P2014.

SÊMOLA, M.. **Gestão da Segurança da Informação**: uma visão executiva. Rio de Janeiro: Campus, 2003.

SILVA FILHO, A. M.. Entendendo e Evitando a Engenharia Social: Protegendo Sistemas e Informações. **Revista Espaço Acadêmico**, v.4, 2004.

SILVA NETTO, A.; SILVEIRA, M. A. P.. Gestão da segurança da informação: fatores que influenciam sua adoção em pequenas e médias empresas. **JISTEM-Journal of Information Systems and Technology Management**, v.4, n.3, p.375-397, 2007.

SILVEIRA, L. A.; REALAN, M.; AMARAL, É.. Engenharia Social: Uma análise sobre o ataque de Phishing. In: CONGRESSO SUL BRASILEIRO DE COMPUTAÇÃO, 8. **Anais**. Florianópolis: UNESC, 2017.

VIDAL, M. T. V. L.. **Segurança em redes**. Niterói: UFF, 2006.