Segurança da Informação: como garantir a integridade, a confidencialidade e a disponibilidade das informações em uma organização educacional privada de Teresina

Edenilza Pereira dos Santos[1]
Eulene Cruz Moura[2]
Jandira de Morais Silva[3]

REUMO: O objetivo desta pesquisa é verificar o conhecimento dos colaboradores quanto à segurança da informação no ambiente corporativo da Faculdade Santo Agostinho. O referencial teórico da pesquisa está balizado nos seguintes autores: James O'brien; Kenneth C Laudon e Luciano Alves Santos. Trata-se de uma pesquisa qualitativa, cujos resultados apontam para a necessidade dos colaboradores priorizarem a segurança dos dados, uma vez que esta preocupação deve ser de todos os funcionários e não apenas do setor que gerencia o sistema; outro ponto importante é a falta de conhecimento da importância das informações o que é vital para a empresa, a fim de evitar invasões aos sistemas de informação da instituição e que isso facilita o acesso de pessoas não autorizadas a informações que deveriam circular apenas entre os detentores das senhas daquele sistema.

PALAVRAS-CHAVE: Conhecimento. Segurança.

[1] Graduada em Administração com Habilitação em Negócios pela FSA, especializanda em Gestão Financeira e SIG pela Faculdade Santo Agostinho.
[2] Graduada em Administração com Habilitação em Negócios pela FSA, especializanda em Gestão Financeira e SIG pela Faculdade Santo Agostinho.
[3] Graduada em Administração com Habilitação em Negócios pela FSA, especializanda em Gestão Financeira e SIG pela Faculdade Santo Agostinho.

Information security: how to ensure the integrity, confidentiality and availability of information in a private educational organization of Teresina

ABSTRACT: The goal of this research is to verify the knowledge of staff on the safety of the information in the corporate environment measureswhere Saint Augustine. The frame is tagged the' oretical ontents in the following authors: James O'Brien; Kenneth C Laudon and Luciano Alves dos Santos. It is a qualitative research results indicate that the data security priorizarem, since this concern must be for all employees and industry not only manages the system; another important point is the lack of knowledge of the importance of the information which is vital for the company, in order to avoid intrusions to the institution's information systems and that this makes unauthorized access to information that should move only between holders of passwords that system.

Keywords: knowledge. Security.

INTRODUÇÃO

A informação de uma empresa é seu principal patrimônio. Convencidos desta realidade, buscou-se desenvolver uma pesquisa, cujo principal objetivo seria investigar o grau de conhecimento dos colaboradores da Faculdade Santo

Agostinho quanto a segurança da informação e os riscos de ataques de engenharia social no seu ambiente corporativo, avaliando a confidencialidade, integridade e disponibilidade da informação que cada um detém e como ela é tratada por cada indivíduo. A segurança da informação depende da atitude de quem lida com ela. Portanto, se a empresa deseja manter o sigilo do seu negócio é necessário cercar-se de colaboradores comprometidos em manter a segurança dessas informações. A atitude de cada usuário é essencial para não comprometer o coletivo e essa atitude garante ou não a confidencialidade, a integridade e a disponibilidade destas informações.

A informação desempenha um papel estratégico dentro das organizações, tornando-se uma necessidade crescente e indispensável para qualquer setor da atividade humana. Justamente por isso, surge a preocupação em garantir a sua segurança e protegê-la de acessos indevidos. Sendo assim, seja qual for a forma em que a informação é apresentada (impressa, escrita ou falada) faz-se necessário que ela seja sempre protegida adequadamente.

Independente do meio que a informação circula, ela sempre é destinada a pessoas, que a priori podem e devem acessá-las. É exatamente este o alvo da engenharia social.

Usuários que tenham o devido cuidado com a informação tornarão sua empresa mais segura e menos vulnerável. Colaboradores atentos e bem informados jamais permitirão que pessoas não autorizadas consigam acesso a informações importantes, evitando assim lesar a instituição ou as pessoas.

Portanto, os usuários de sistemas precisam saber o que é a informação para sua empresa, qual a sua importância e porque a segurança dessa informação é fundamental para a continuidade do negócio.

A escolha da Faculdade Santo Agostinho como ambiente para o desenvolvimento desta pesquisa se deu a partir da observação pela maneira como seus colaboradores lidam com a tecnologia da informação disponível nos vários sistemas da instituição.

A partir desta observação, chegou-se a uma pergunta: como uma organização educacional privada pode garantir a integridade, a confiabilidade e a disponibilidade das informações que armazena em seus vários sistemas?

Pensando nisso, este estudo buscou verificar o grau de conhecimento dos colaboradores quanto à segurança da informação no ambiente corporativo da Faculdade Santo Agostinho com o objetivo de investigar os pontos vulneráveis e buscar alternativas para dificultar o acesso indevido a essas informações que

são de fundamental importância para a vida da instituição.

Os estudos apontaram que muitos colaboradores não têm muita preocupação com a segurança da informação por não conhecerem os riscos nesta área. Outros até se preocupam em guardar bem suas senhas, mas não pensam duas vezes antes de abrir um email suspeito, por exemplo. Diante disso, propôs-se uma campanha de conscientização que alcançasse a todos aqueles que lidam com a informação, no sentido de mostrar que existem formas simples, capazes de evitar invasões a informações importantes ou mesmo causar danos aos sistemas.

REFERENCIAL TEÓRICO

Cada vez mais as organizações, seus sistemas de informação e redes de computadores são colocados à prova por diversos tipos de ameaças, incluindo vazamento de informações, fraudes, roubos e invasões (físicas e lógicas). Problemas causados por vírus e hackers são freqüentes e proliferam a cada dia.

A Política de Segurança da Informação serve como base ao estabelecimento de normas e procedimentos que garantem a segurança da informação, bem como determina as responsabilidades relativas à segurança dentro da empresa.

> A Informação é um ativo que, como qualquer outro ativo importante para os negócios ter um valor para uma organização e consequentemente, precisa ser protegidas adequadamente. A segurança de informações protege as informações contra uma ampla gama de ameaças, para assegurar a continuidade dos negócios, minimizar prejuízos e maximizar o retorno de investimentos e oportunidades comerciais. (NBR ISSO/IEC 17799:2001, p. 2).

Para atender as principais necessidades da empresa, uma Política de Segurança da Informação deve ser clara e concisa, de fácil compreensão, coerente com as ações da empresa, amplamente divulgada e revisada periodicamente.

A Política de Segurança da Informação visa preservar a confidencialidade, a integridade e a disponibilidade das informações. Deve descrever a conduta adequada para o seu manuseio, controle, proteção e descarte.

Na sociedade da informação, ao mesmo tempo em que as informações são

consideradas o principal patrimônio de uma organização, estão também sob constante risco, como nunca estiveram antes. Com isso, a segurança da informação torna-se um ponto crucial para a sobrevivência das instituições. Sendo assim, faz-se necessário a implantação de um Programa de Segurança bem estruturado capaz de reduzir as vulnerabilidades dos sistemas de informação e fazer evoluir as suas capacidades de inspeção, detecção, reação e reflexo.

Engenharia Social

São práticas utilizadas para obter acesso a informações importantes ou sigilosas em organizações ou sistemas por meio da enganação ou exploração da confiança das pessoas. Para isso, o golpista pode se passar por outra pessoa, assumir outra personalidade, fingir que é um profissional de determinada área, acessar os sistemas de uma organizações sem o uso da força bruta e assim explorar suas falhas de segurança. As pessoas quando não tem o conhecimento necessário, podem ser facilmente manipuladas e de forma "inocente", abrir caminho para acessos indevidos.

Os fatores humanos sempre ficam em segundo plano quando existe tecnologia de ponta para garantir a segurança. Porém, deixar as pessoas desinformadas sobre as questões de segurança pode expor a empresa a riscos desnecessários, uma vez que os invasores usam de habilidade para enganar os usuários, alinhada a inclinação natural das pessoas de confiar umas nas outras e de querer ajudar, para persuadi-las a abrir-lhes a porta de entrada, quebrando a segurança da informação através da exploração de falhas ou do próprio nome e senha do usuário.

Por sermos humanos, seres imperfeitos, modificamos nosso comportamento natural em situações de risco, fazendo com que, inconscientemente, tomemos decisões baseados em confiança, permitindo assim que o engenheiro social possa explorar de maneira eficaz nossas falhas e burlar a segurança da informação.

Chama-se de engenharia social a habilidade de enganar um ou mais usuários para quebrar a segurança da informação, que pode ser caracterizada pela preservação de três fatores:

- **Confidencialidade:** garantia de que a informação só será acessada por usuários autorizados;
- **Integridade:** exatidão, completeza da informação e dos métodos

de processamento;

- **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Engenharia social compreende a inaptidão dos indivíduos manterem-se atualizados com diversas questões pertinentes à tecnologia da informação, além de não estarem conscientes do valor da informação que eles possuem e, portanto, não terem preocupação em proteger essa informação conscientemente. É importante salientar que a engenharia social é aplicada em diversos setores da segurança da informação independente de sistemas computacionais, software e ou plataforma utilizada. O elemento mais vulnerável de qualquer sistema de segurança da informação é o ser humano, o qual possui traços comportamentais e psicológicos que o tornam suscetível a ataques de engenharia social. Dentre essas características, pode-se destacar:

- **Vaidade pessoal e/ou profissional:** O ser humano costuma ser mais receptivo a avaliação positiva e favorável aos seus objetivos, aceitando basicamente argumentos favoráveis a sua avaliação pessoal ou profissional ligada diretamente ao benefício próprio ou coletivo de forma demonstrativa.
- **Autoconfiança:** O ser humano busca transmitir, em diálogos individuais ou coletivos, o ato de fazer algo bem, coletivamente ou individualmente, buscando transmitir segurança, conhecimento, saber e eficiência, buscando criar uma estrutura base para o início de uma comunicação ou ação favorável a uma organização ou individuo.
- **Formação profissional:** O ser humano busca valorizar sua formação e suas habilidades adquiridas nesta faculdade, buscando o controle em uma comunicação, execução ou apresentação seja ela profissional ou pessoal buscando o reconhecimento pessoal inconscientemente em primeiro plano.
- **Vontade de ser útil :** O ser humano, comumente, procura agir com cortesia, bem como ajudar outros quando necessário.
- **Busca por novas amizades :** O ser humano costuma se agradar e sentir-se bem quando elogiado, ficando mais vulnerável e aberto a dar informações.

- **Propagação de responsabilidade :** Trata-se da situação na qual o ser humano considera que ele não é o único responsável por um conjunto de atividades.
- **Persuasão :** Compreende quase uma arte a capacidade de persuadir pessoas, com o objetivo de obter respostas específicas. Isto é possível porque as pessoas possuem características comportamentais que as tornam vulneráveis à manipulação.

De acordo com Luciano Santos (2004):

> A engenharia social não é exclusivamente utilizada em informática, a engenharia social é uma ferramenta que explora as falhas humanas em organizações físicas e jurídicas, onde operadores de sistemas de segurança da informação possuem poder de decisão parcial ou total, seja ele físico ou virtual. Porém devemos considerar que as informações pessoais, não documentadas, conhecimentos, saber, não são informações físicas ou virtuais, elas fazem parte de um sistema em que possuem características comportamentais e psicológicas na qual a engenharia social passa a ser auxiliada por outras técnicas como: leitura fria, linguagem corporal, leitura quente, termos usados no auxílio da engenharia social para obter informações que não são físicas ou virtuais mas sim comportamentais e psicológicas.

Na visão do autor, as invasões aos sistemas das empresas tornam-se possíveis pela presença de "má fé" aliada a "boa fé". De um lado, há alguém completamente disposto a oferecer ajuda, do outro, alguém que usa essa disposição para abrir uma oportunidade de obter de forma ilícita informações sigilosas.

METODOLOGIA

3.1 Tipo de estudo

A idéia central da pesquisa que foi realizada consiste em investigar como o ambiente estudado trata suas informações e qual o nível de confidencialidade, integridade e disponibilidade, características essenciais, para garantir a

segurança das organizações. Para o estudo da pesquisa, utilizaremos abordagem qualitativa. De acordo com Oliveira (2007, p. 37) "[...] uma pesquisa qualitativa é um processo de reflexão e análise da realidade através da utilização de métodos e técnicas para compreensão detalhada do objeto de estudo dentro de um contexto histórico ou estruturado." A pesquisa terá caráter exploratório, pois:

> Estas pesquisas têm como objetivo proporcionar maior familiaridade com o problema, com vistas a torná-lo mais explícito ou constituir hipóteses. Pode-se dizer que estas pesquisas têm como objetivo principal o aprimoramento de idéias ou a descoberta de intuições. (GIL, 2002, p. 41)

A pesquisa desenvolvida é bibliográfica e de campo. A pesquisa bibliográfica é desenvolvida com base em material já elaborado, podendo ser constituída principalmente de livros e artigos científicos, mas também em outras fontes.

Foram utilizados métodos quantitativos e qualitativos através de uma metodologia interativa, que consiste numa interação entre pesquisadores e membros a serem pesquisados.

Para coleta de dados, utilizamos a técnica de observação, aplicação de questionários, entrevistas, pesquisa na internet e em livros.

O universo pesquisado foi a Faculdade Santo Agostinho, com amostra de 70% dos colaboradores de todos os setores que utilizam computadores como instrumento de trabalho e entrevista com a liderança do setor de Centro de Processamento de Dados – CPD.

3.2 Local e período da pesquisa

A pesquisa foi realizada nos meses de outubro e novembro de 2009 na sede da Faculdade Santo Agostinho, localizada na v. Valter Alencar nº 665 bairro São Pedro, nesta cidade.

3.3 Sujeitos da pesquisa

A população do estudo foi constituída pelos colaboradores da Instituição nos níveis operacional e gerencial. Levamos em consideração que as informações relevantes da empresa trafegam e foram tratadas nos dois níveis.

3.4 Técnicas utilizadas na pesquisa

A pesquisa foi realizada através de observação de campo para melhor coleta de dados e de entrevistas semi-estruturadas, apoiada em roteiro com perguntas capazes de direcionar o entrevistado e conduzi-lo ao objetivo. A abordagem junto aos colaboradores foi realizada com agendamento prévio de datas e horário, observando a disponibilidade de cada um sem interferir na suas atividades e no desempenho de suas funções.

3.5 Análise dos dados

Os dados obtidos na observação e nas entrevistas foram catalogados e analisados de acordo com a técnica de análise (tabulação).

3.6 Aspectos éticos da pesquisa

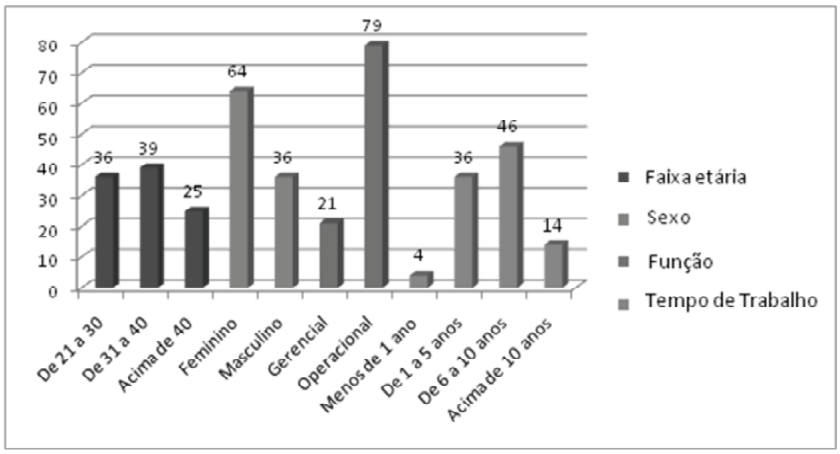
A presente pesquisa tem a intenção de colaborar para a melhoria da segurança das informações e não trará riscos ou prejuízos aos colaboradores ou a instituição, pois buscou atender a todos os princípios éticos inerentes ao processo de pesquisa com seres humanos. Aos sujeitos, será garantido o anonimato.

ANÁLISE DOS DADOS

Esta pesquisa teve como objetivo verificar o conhecimento dos colaboradores quanto à segurança da informação no ambiente corporativo da Faculdade Santo Agostinho. Para coletarmos esses dados, foram aplicados questionários para 35 colaboradores contendo 25 questões. Sintetizamos os dados coletados em quatro gráficos de colunas: o primeiro refere-se aos funcionários destacando faixa etária, sexo, função e tempo de serviço. O segundo gráfico trata das senhas dando ênfase: Mais alguém utiliza sua senha; Utiliza senha de outro funcionário; Anota senha em algum local; Alguém utiliza sua senha para trabalho rápido; Ao sair efetua log off; Seu setor tem informações confidenciais; Quais informações tem acesso. No terceiro gráfico enfatizamos a Engenharia Social do qual trata sobre: já ouviu falar em Engenharia Social; recebeu instruções de Engenharia Social; Necessita informar-se sobre Segurança da Informação; Seus conhecimentos são suficientes para defender-se das armadilhas da internet; A empresa lhe da

garantias para trabalhar sem se preocupar com a Segurança da Informação; Como procede ao receber e-mails de desconhecidos. O quarto gráfico retrata sobre os funcionários do CPD, enfocando: Se os equipamentos de informática estão protegidos; Utilizam criptografia; Existe antivírus coorporativo; Existe utilização de senhas fortes; As senhas de acesso expiram automaticamente; É permitida a utilização de senhas compartilhadas. Cada título do gráfico representa uma categoria analisada, senão vejamos.

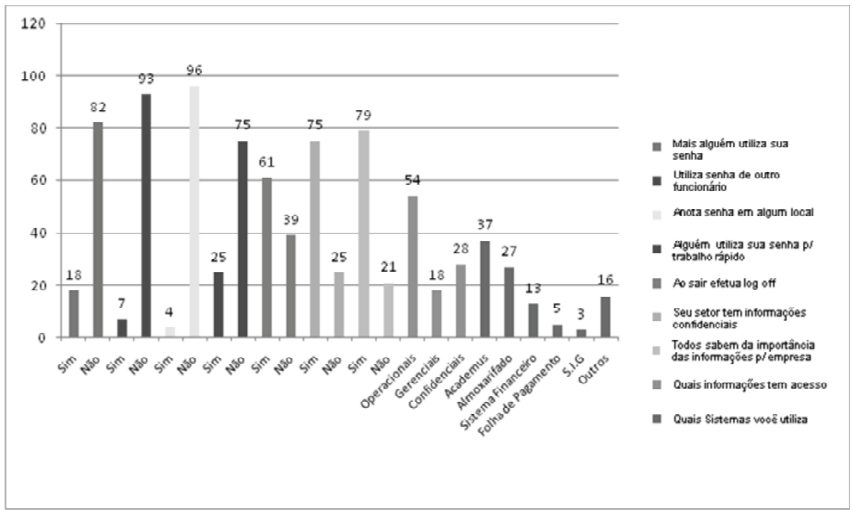
FUNCIONÁRIO
Gráfico 1:



Fonte: Faculdade Santo Agostinho

Conforme o gráfico 1: Faixa etária - 39% dos respondentes têm acima de 40 anos de idade, 36% têm entre 31 e 40 anos e 25% são da faixa etária entre 21 e 30 anos de idade. Sexo 64% dos respondentes são do sexo feminino e 36% são do sexo masculino. Função 79% dos respondentes desenvolvem função operacional e 21% desenvolvem suas funções na área gerencial. 46% dos respondentes trabalham na empresa a mais de 6 anos, 36% entre 1 e 5 anos, 14% trabalham na empresa a mais de 10 anos e 4% trabalham na empresa a menos de 1 ano.

SENHAS
Gráfico 2:



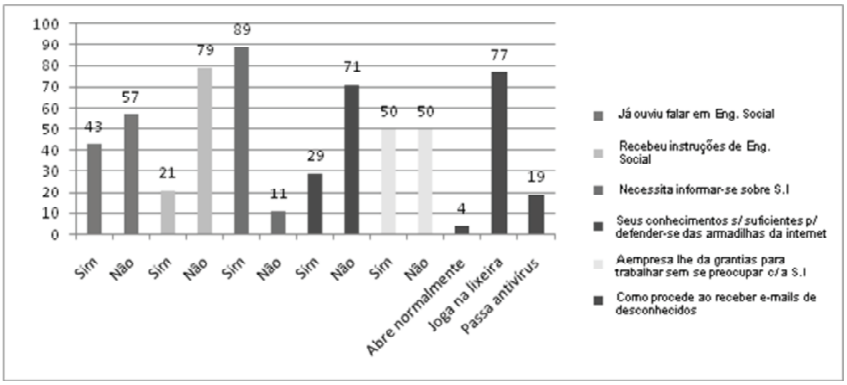
Fonte: Faculdade Santo Agostinho

De acordo com gráfico 2 que trata das senhas eis as questões feitas aos entrevistados: Alguém além de você sabe a sua senha utilizada para acessar informações da empresa? 82% dos respondentes não dividem sua senha de acesso aos sistemas da empresa e 18% admitem dividir suas senhas com colegas de departamento. Você utiliza a senha de algum outro funcionário para acesso à informação da empresa? 93% dos respondentes admitem usar senhas dos colegas para acessar os sistemas da empresa e 7% não dividem suas senhas de acesso com colegas de departamento; Você anota as suas senhas em algum local próximo ao computador, na agenda, ou local similar? 96% dos respondentes anotam suas senhas em locais de fácil acesso e apenas 4% tomam o cuidado de não deixar anotadas suas senhas; Você anota as suas senhas em algum local próximo ao computador, na agenda, ou local similar? 75% dos respondentes permitem que outras pessoas trabalhem usando sua senha de acesso aos sistemas e 25% não permitem que suas senhas sejam utilizadas por colegas. Você deixa outras pessoas utilizarem sua senha para algum trabalho rápido? 75% dos respondentes permitem que outras pessoas trabalhem usando sua senha de acesso aos sistemas e 25% não permitem que suas senhas sejam utilizadas por

colegas. Ao sair você costuma deixar seu computador bloqueado? 61% dos respondentes deixam seus computadores desbloqueados permitindo assim que outros acessem as informações contidas e 39% tomam o cuidado de bloquear seus computadores. O seu setor possui informações consideradas confidenciais? 75% dos respondentes possuem informações sigilosas da empresa e apenas 25% não possuem informações sigilosas em seus computadores. Na sua opinião, todos os funcionários do seu setor sabem a importância da informação para a empresa? 79% dos respondentes conhecem a importância da informação para a empresa e 21% não sabem a importância não possuem informações sigilosas em seus computadores. Quais os tipos de informações que você tem acesso? 54% dos respondentes têm acesso a informações apenas operacionais, 28% a informações gerenciais e 18% a informações confidenciais. Dos sistemas abaixo, quais você utiliza? 36% dos respondentes utilizam o sistema academus, 27% utilizam o sistema almoxarifado, 13% utilizam o sistema financeiro e contábil, 3% utilizam o sistema folha de pagamento e 16% utilizam outros sistemas da empresa.

ENGENHARIA SOCIAL

Gráfico 3:



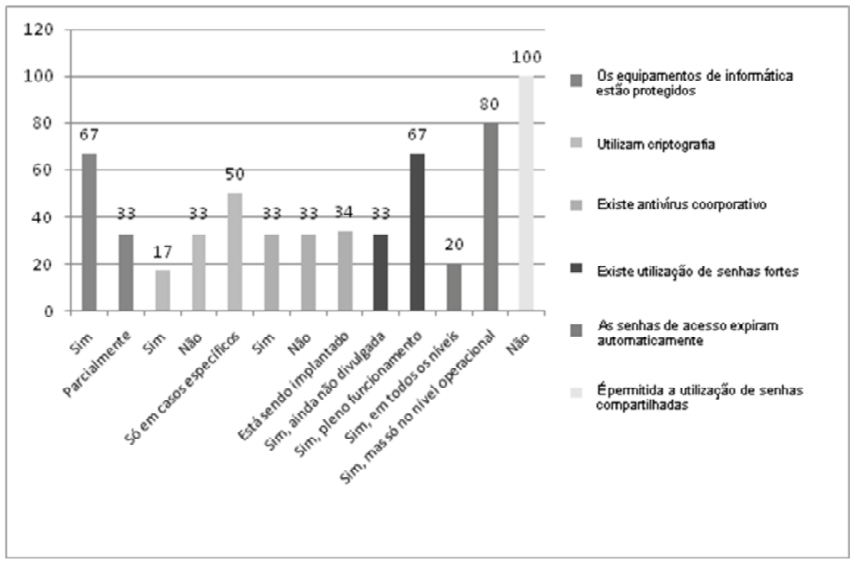
Fonte: Faculdade Santo Agostinho

Conforme gráfico 3 que diz respeito a Engenharia Social surgiram os questionamentos: Você já ouviu falar em Engenharia social? 57% dos respondentes já ouviram falar em engenharia social e 43% nunca ouviram falar em engenharia social. Já recebeu instruções de como se defender de Engenharia Social? 79% dos respondentes não saberiam como se defender da engenharia

social e 21% conhecem diferentes forma de se defender de engenharia social. Você sente necessidade de receber informações a respeito de segurança da informação? 89% dos respondentes sentem necessidade de receber informações sobre a segurança da informação e 11% não sentem necessidade de receber essas informações. Você acha que seus conhecimentos são suficientes para se defender das armadilhas existentes na internet? 71% dos respondentes não acham suficientes seus conhecimento sobre segurança e 29% acham que os conhecimentos que possuem são suficientes para defender as informações contra as armadilhas da internet. A empresa oferece garantias para que você trabalhe sem ter que se preocupar com a segurança das informações? 50% dos respondentes entendem que a empresa oferece as garantias necessárias para que possa trabalhar sem ter que se preocupa com a seguranças das informações e 50% acham que não oferece. Como você procede quando recebe um e-mail de desconhecidos e/ou com anexos? 77% dos respondentes afirmam que não abrem email de desconhecidos, 19% utilizam o antivírus antes de abrir emails e 4% abrem sem se preocupar com a segurança.

FUNCIONÁRIOS DO CPD

Gráfico 4:



Fonte: Faculdade Santo Agostinho

Conforme gráfico 4 no qual entrevistamos os funcionários do CPD, investigamos: Os principais equipamentos de informática (Switches, Servidores, Roteadores, ...) estão realmente protegidos de acesso não autorizado? 77% dos respondentes afirmaram que os equipamentos utilizados pela rede estão realmente protegidos invasão, 19% acham que esta proteção é só parcial e 4% acreditam que o equipamento não está protegido contra invasões. Utilizam criptografia na comunicação que envolva informação da empresa? 50% dos respondentes utilizam a criptografia somente em situações que exijam esse comportamento, 33% afirmaram que não utilizam a criptografia e 17% sempre utilizam a criptografia como ferramenta para proteger as informações confidenciais da empresa. Existe antivírus coorporativo com atualização automática das estações? 33% dos respondentes afirmaram que estão em pleno funcionamento, 33% afirmaram que não e 34% responderam que está sendo implantado. Existe uma política para utilização de senhas fortes? 67% dos respondentes afirmaram que sim e está em pleno funcionamento, 33% responderam que sim, mas ainda não foi divulgada. As senhas de acesso a rede expiram automaticamente em um determinado período de tempo? 80% dos respondentes afirmaram que sim, mas somente em nível operacional e 20% responderam que sim em todos os níveis. É permitida a utilização de senhas compartilhadas um senha única para usuários de um setor por exemplo? 100% dos respondentes afirmaram que não.

CONSIDERAÇÕES FINAIS

Durante a pesquisa, foi possível observar que o grau de conhecimento dos colaboradores da Faculdade Santo Agostinho em relação a proteção das informações contidas nos sistemas da Instituição é baixo e que pouco se sabe sobre as formas existentes de proteção.

Diante desta realidade, concluiu-se que para proteger a informação, é necessário aumentar o conhecimento sobre segurança da informação e sua importância para a empresa. A proposta para diminuir ou mesmo eliminar o perigo de evasão de informações sigilosas dos sistemas da Faculdade Santo Agostinho deve começar pela capacitação profissional e a disseminação de conhecimentos específicos voltados para a área de Tecnologia da Informação.

Para tanto, propõe-se treinamentos com profissionais qualificados na área da segurança da informação, acompanhados de palestras capazes de despertar

e conscientizar os usuários dos sistemas de que assumir uma postura responsável diante das informações por eles tratadas diariamente é a única forma de mantê-las em sigilo e resguardar os sistemas de invasores.

Para finalizar, Consideramos que as informações obtidas durante a pesquisa foram relevantes e contribuíram com a melhoria, o crescimento e o desenvolvimento organizacional e certamente a partir das informações adquiridas com o trabalho, providencias estão sendo tomadas na tentativa de bloquear qualquer tipo de invasão aos sistemas da instituição.

REFERENCIAS

GIL, Antônio Carlos. **Como elaborar projeto de pesquisa**. 4. Ed. São Paulo; Atlas, 2002.

OLIVEIRA, Maria Marly de. **Como fazer pesquisa qualitativa**. Petrópolis, Rio de Janeiro; Vozes, 2007.

CERVO, Amado Luiz. **Metodologia Científica**. 5. ed. São Paulo: Prentice Hall, 2002.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT. L. **Norma ISSO/ IEC 17799**: Código de prática para a segurança da informação nas empresas**.** Curitiba, 2003.

O'BRIEN, James A. **Sistemas de Informação**: E as Decisões Gerenciais na era da Internet. 2. Ed. São Paulo: Saraiva, 2004.

LAUDON, Kenneth C. **Sistemas de Informações Gerenciais**. 7. ed. São Paulo: Pearson Prentice Hall, 2007.

SANTOS, Luciano Alves Lunguinho. **Engenharia social**: segurança da informação. Disponível em: http://www.diagorasalencar.com/apostilas/ engenharia_social_e_seguranca.pdf>.

Acesso em 05 de abril de 2009.

FÁVERO, Alberto Evandro. **Política de segurança da informação**. Rio de

Janeiro: Ed. Ciência Moderna Ltda, 2006.

SILVA, Pedro Tavares. **Segurança dos sistemas de informação**: gestão estratégica da segurança empresarial. Lisboa, Portugal: Ed. Centro Atlântico Ltda, 2003.

Tribunal de Contas da União. **Boas práticas em segurança da informação**. 3 ed. Brasília : TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2008.