FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Katia Lois Somensari Cardoso

SEGURANÇA DA INFORMAÇÃO:

Simples atitudes podem construir um ambiente mais seguro

Americana, S. P.

2014

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Katia Lois Somensari Cardoso

SEGURANÇA DA INFORMAÇÃO:

Simples atitudes podem construir um ambiente mais seguro

Trabalho monográfico, desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação da Fatec Americana, sob a orientação da Professora Mestre Maria Cristina Luz Fraga Moreira Aranha.

Área temática: Segurança da informação.

Americana, S. P.

2014

Katia Lois Somensari Cardoso RA nº 0040451111011

SEGURANÇA DA INFORMAÇÃO:

Simples atitudes podem construir um ambiente mais seguro

Trabalho de Conclusão de Curso apresentado à FATEC de Americana como parte dos requisitos para obtenção do título de Tecnólogo em Segurança da Informação.

Americana, 30 de junho de 2014.

Banca Examinadora:

Orientadora:_____
Maria Cristina Luz Fraga Moreira Aranha
Mestre, FATEC – Americana.

Professor convidado:_____
Antonio Alfredo Lacerda
Especialista, FATEC – Americana.

Professor Convidado:_____
Rogério Nunes de Freitas
Graduado, FATEC – Americana.

DEDICATÓRIA

Dedico esta monografia a Deus por estar sempre presente em minha vida.

Aos meus pais, pela compreensão, apoio e contribuição para minha formação acadêmica.

Ao meu esposo e filha, que sempre me incentivaram para realização dos meus ideais, encorajando-me a enfrentar todos os momentos difíceis da vida.

AGRADECIMENTOS

Quero agradecer, em primeiro lugar, a Deus, pela força e coragem durante esta longa caminhada.

Agradeço também a todos os professores que me acompanharam durante a graduação, em especial à Professora MSC Maria Cristina Luz Fraga Moreira Aranha, responsável pela orientação deste trabalho.

Dedico esta, bem como todas as demais conquistas, aos meus amados pais, Valdir e Aparecida, que com muito carinho e apoio, não mediram esforços para que eu chegasse até esta etapa de minha vida.

Ao meu esposo Whander, pela paciência, pelo incentivo, pela força e principalmente pelo carinho. Valeu a pena toda a distância, todas as renúncias... Valeu a pena esperar.

À minha amada filha, Beatriz, meu tesouro mais precioso, que sempre me ajudou e me apoiou em tudo.

Enfim, aos meus amigos, em especial Bruno Cesar Aparecido da Silva, Guilherme Backos e Gabriel Sanpey Mochizuki, por esses anos inesquecíveis de convivência, estudos e muitos momentos eternizados, tornando a vida acadêmica mais suave e repleta de saudades já existentes em mim.

RESUMO

Atualmente as organizações tratam diariamente com um fluxo intenso de informações. Essas informações podem estar armazenadas em diversos meios, porém a maior parte delas está em formato digital para facilitar e agilizar o acesso dos usuários às informações, tanto para o manuseio como para o armazenamento e o descarte. Contudo, essa tecnologia aumenta os riscos e as vulnerabilidades a que as organizações estão expostas, e os usuários nem sempre possuem treinamento ou conscientização adequados sobre como realizar simples procedimentos de proteção. Considerando que a integridade, a confidencialidade e a disponibilidade são os principais aspectos da segurança da informação, este trabalho apresenta um estudo sobre segurança da informação, bem como uma pesquisa para verificar se há algum tipo de falha de segurança em uma organização. Esta pesquisa utiliza a aplicação de um questionário, com perguntas fechadas, aos funcionários de um departamento da organização. Em seguida são sugeridas e utilizadas algumas práticas de treinamento e conscientização, que não envolvam recursos financeiros, para minimizar as falhas de segurança detectadas através do questionário respondido (caso ocorram). Para verificar os resultados obtidos, através das práticas exercitadas para melhoria da segurança da informação, aplica-se o mesmo questionário e comparam-se as respostas obtidas com as anteriores. Os resultados obtidos indicam quais práticas e melhorias podem ser estabelecidas como normas de segurança para aquele departamento e seus funcionários.

Palavras chave: Segurança da Informação; Importância da informação; Conscientização de usuários.

ABSTRACT

Actually, the organizations dealing with intense information flow every day. This information can be stored in various ways, but most of them are in digital format to facilitate and streamline users' access to information, both for handling, storage and disposal. However, this technology increases the risks and vulnerabilities that organizations are exposed, and users don't always have adequate training or conscience of how to do the simple procedures of protection. Considering the integrity, confidentiality and availability are the main aspects of information security, this work presents a study on information security, as well as a research to check for some failure security in an organization. The research uses a survey with closed questions to employees of a department of the organization. Then, suggesting are proposed and used on a practical training and employees awareness, which it doesn't involve financial resources, to minimize detected security failures through to the answered survey (if it occurs). To verify the results of the practice exercises to improve information security, apply the same survey and compare to the answers, previously obtained. The results indicate that practices and improvements can be established as safety standards for that department and employees.

Key words*: Information Security; Importance of information; User awareness.*

LISTA DE ILUSTRAÇÔES

LISTA DE TABELAS

LISTA DE ABREVIATURAS

CD: *Compact Disk* (Disco Compacto)

CERT.br: Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

DVD: *Digital Versatile Disk* (Disco Digital Versátil)

HD: *Hard Disck* (Disco Rígido)

IEC: *International Eletrotechnical Commission* (Comissão Eletrotécnica Internacional)

ISO: *International Organization for Standartization* (Organização internacional para padronização)

NBR: Norma Brasileira (Estabelecida pela Associação Brasileira de Normas Técnicas)

NIC: Núcleo de Informação e Coordenação do Ponto BR.

PCN: Plano de Continuidade do Negócio

RMC: Região Metropolitana de Campinas

TI: Tecnologia da Informação

SUMÁRIO

1 INTRODUÇÃO

A evolução ocorrida na área da Tecnologia da Informação (TI), desde o surgimento e o crescente uso da Internet, mostrou a necessidade do estabelecimento de boas práticas, metodologias e normas que padronizassem a questão relacionada à segurança da informação. Sabe-se que a partir do aumento de tráfego de informações na Internet, em nível global, a vulnerabilidade dessas informações também cresceu. Apesar de esforços despendidos no sentido de se implantar e usar alguma norma ou metodologia, ou até mesmo de se estabelecer boas práticas relacionadas à segurança da informação, instituições de maneira geral e, em consequência, instituições públicas de qualquer instância (municipal, estadual ou federal) têm encontrado dificuldades e resistências de seus funcionários para treiná-los e conscientizá-los desta necessidade de vital importância aos ativos da instituição (CASTRO, 2011). Considerando que a autora deste trabalho é funcionária de uma instituição pública municipal, trabalhando com documentos diversos e de importância ao município, seu interesse pelo tema justifica-se, pois a proteção dos ativos de uma instituição é cada vez mais importante para o sucesso e sobrevivência do negócio de uma organização. Falhas ou perdas de ativos causam impactos negativos às atividades e à imagem da instituição, além de poder causar prejuízo de ordem financeira (DAMIANO, 2013). Considerando estas questões, o problema proposto pela autora deste trabalho é: Como mostrar, aos funcionários que trabalham no seu departamento, a necessidade de se adotar algumas práticas relacionadas à segurança da informação, visando à proteção deste ativo?

Portanto, o objetivo geral deste trabalho é conscientizar funcionários de um departamento de instituição pública municipal a exercitar algumas práticas para melhorar o nível de segurança do principal ativo deste departamento, que é a informação armazenada em diversos meios.

Este objetivo desdobra-se nos seguintes objetivos específicos:

- realizar uma revisão bibliográfica da literatura relacionada ao problema proposto, para subsidiar seu objetivo;

- identificar o grau de conhecimento dos funcionários de seu departamento, no que diz respeito às formas de armazenamento e acesso da informação; uso e alteração

periódica de senhas; não fornecimento de informação a pessoas não autorizadas, entre outros aspectos;

- elaborar um *folder* contendo as principais orientações sobre regras básicas de segurança da informação.

Os procedimentos metodológicos adotados para este trabalho são os seguintes: análise da bibliografia existente sobre segurança da informação, relacionada, principalmente, aos recursos humanos de uma organização; obtenção de autorização do responsável do departamento onde a autora trabalha, para realizar um levantamento do conhecimento dos funcionários do departamento, referente à segurança da informação; elaboração e aplicação de uma pesquisa através de um questionário de perguntas fechadas para quantificar este conhecimento. Após a tabulação das respostas obtidas, dependendo dos resultados, realizar palestras e organizar um procedimento de conscientização dos funcionários do departamento. Este procedimento prevê o envio sistemático de *e-mails*, com mensagens curtas e objetivas, relacionadas à segurança da informação. Em paralelo, a autora criará um *folder* contendo orientações sobre adoção de medidas, relacionadas à segurança da informação (também usando os resultados obtidos na tabulação das respostas dos questionários). Após um período de tempo, o mesmo questionário será aplicado e as respostas tabuladas novamente. Os resultados das duas aplicações do questionário serão confrontados para análise dos efeitos obtidos pelas palestras, envio de *e-mails* e a distribuição do *folder*. A solução do problema proposto pode estar na organização de um programa contendo todas as atividades descritas, que seja executado sistematicamente, para a sensibilização e conscientização dos funcionários, sobre a necessidade de adoção de medidas relacionadas à segurança da informação manipulada por todos do departamento.

Este trabalho está organizado da seguinte forma: no Capítulo 2 apresenta-se o levantamento bibliográfico relacionado ao tema e ao problema proposto. No Capítulo 3 a autora desenvolve o trabalho propriamente dito. No Capítulo 4 são apresentados os resultados e as análises feitas pela autora e no Capítulo 5 apresentam-se as considerações finais e sugestões para trabalhos futuros

2 LEVANTAMENTO BIBLIOGRÁFICO

Esta seção apresenta conceitos sobre a teoria relacionada à informação, sua importância para as instituições de maneira geral e sobre a classificação que a informação recebe no que diz respeito à segurança. Em seguida é abordado o tema segurança da informação, sua importância e a necessidade de se proteger o recurso informação das ameaças que podem ser causadas pelo fator humano. Finalmente são abordados conceitos sobre conscientização de usuários em Segurança da Informação.

2.1 Conceitos de Informação

O desenvolvimento tecnológico em todas as áreas de conhecimento é parte de nossas vidas. Considerando a crescente evolução da tecnologia pode-se verificar o computador e a Internet como dois dos recursos mais significativos e de maior uso até o momento. Desde suas criações eles promoveram a mudança de paradigmas, alterando a forma como os usuários das organizações públicas e das empresas do setor privado tratam suas informações (CASTRO, 2011).

Sêmola, (2003) cita a mudança e o Crescimento da Tecnologia:

> Os computadores tomam conta dos ambientes de escritório, quebram o paradigma de acesso local à informação, e chegam a qualquer lugar do mundo através dos – cada vez mais portáteis – *notebooks* e da rede mundial de computadores: a Internet (SÊMOLA, 2003, p.3).

Essa citação aborda um dos aspectos mais importantes, na área de Segurança da Informação, pois fala sobre ”...quebram o paradigma de acesso local à informação...”. A informação é um ativo tão importante que é citada por Sêmola (2003), como sendo o “sangue” da empresa. Fontes (2006) cita, da seguinte forma, a importância da informação:

Como bem observa Fontes (2006) a informação independente de seu formato, é um ativo importante da organização. Desta forma é extremamente necessário que os ambientes e os equipamentos utilizados para processar, armazenar, e transmitir a informação sejam protegidos. Ainda segundo Fontes (2006) a organização necessita da informação para realizar o seu negócio. Portanto, é recomendável elaborar formas de proteger este ativo tão importante.

Embora grande parte das informações seja processada em ambiente computacional elas também podem existir em outros formatos, tais como: uma simples anotação em papel, folhas impressas, armazenadas em arquivos físicos, conhecimentos guardados por uma pessoa, dentre outros. O importante é que, independente do tipo de informação, ela seja protegida de forma apropriada.

Vale lembrar que a informação tem um papel muito importante tanto para a sociedade como para as organizações. Ela tem o poder de auxiliar o individuo tanto na tomada de decisão como também na resolução de problemas. Ela é considerada o ativo mais importante de uma organização (FONTES, 2006).

Sêmola (2003) define que a informação é um conjunto de dados utilizados para a transferência de uma mensagem entre indivíduos e/ou máquinas em processos comutativos (isto é, baseados em trocas de mensagens) ou transacionais (isto é, processos em que sejam realizadas operações que envolvam, por exemplo, a transferência de valores monetários).

Porém Fontes (2006) conceitua a informação como sendo muito mais que um conjunto de dados. Transformar esses dados em informação é transformar algo com pouco significado em recurso de valor para a vida pessoal ou profissional do ser humano.

Considerando os conceitos citados anteriormente por seus autores é possível notar que ambos se referem à informação de formas bem distintas. Enquanto Fontes (2006) tem uma visão mais voltada para a importância e o valor da informação, a visão de Sêmola (2003) está voltada à definição técnica sobre o conceito do que é a informação.

2.2 Classificações da Informação

Tendo em vista diferentes conceitos sobre informação, sua importância e sua segurança, houve a necessidade de se classificar a informação quanto ao seu grau de importância. Segundo a norma ISO/IEC 27002 (2005) essa classificação permite identificar qual o nível de proteção a informação requer.

A classificação da informação requer a avaliação do negócio, dos processos e atividades que são realizados pela organização. Ferreira e Araújo (2008) citam as definições que devem ser estabelecidas no início do processo, a saber:

- Classificação: Atividade que tem como objetivo atribuir o grau de sigilo necessário das informações;
- Proprietário: Profissional responsável pelo ativo da informação na organização;
- Custodiante: Profissional responsável por garantir que as informações estão de acordo com o estabelecido pelo proprietário da informação;
- Criptografia: Proteção por meio de codificação que permite proteger a informação de acessos não autorizados;
- Perfil de acesso: Define os direitos de acesso de cada informação;

Ainda conforme Ferreira e Araújo, (2006), a classificação da informação é o processo para se estabelecer o grau de importância das informações mediante seu impacto no negócio. Cada organização poderá classificar suas informações conforme seus negócios, porém os autores referenciam que muitas classificações podem confundir o proprietário da informação, sendo que apenas 3 (três) classes são necessárias para classificá-las, a saber:

- Informação pública: Essa classe de informação é de livre acesso a todos os colaboradores da empresa, pois não são confidenciais, não necessitam de investimento em recursos de proteção e se forem divulgadas fora da organização não trarão impacto nos negócios.
- Informação interna: O acesso externo a essa classe de informações deve ser evitado. Contudo se esses dados tornarem-se públicos, as consequências não serão críticas.
- Informação confidencial: Essa classe contém as informações sigilosas e que deverão ser protegidas do acesso externo; somente pessoas autorizadas deverão

acessá-las. Caso alguém não autorizado tenha acesso a elas a organização poderá ter um prejuízo financeiro. Para garantir a segurança das informações dessa classe será necessário investir em recursos de proteção.

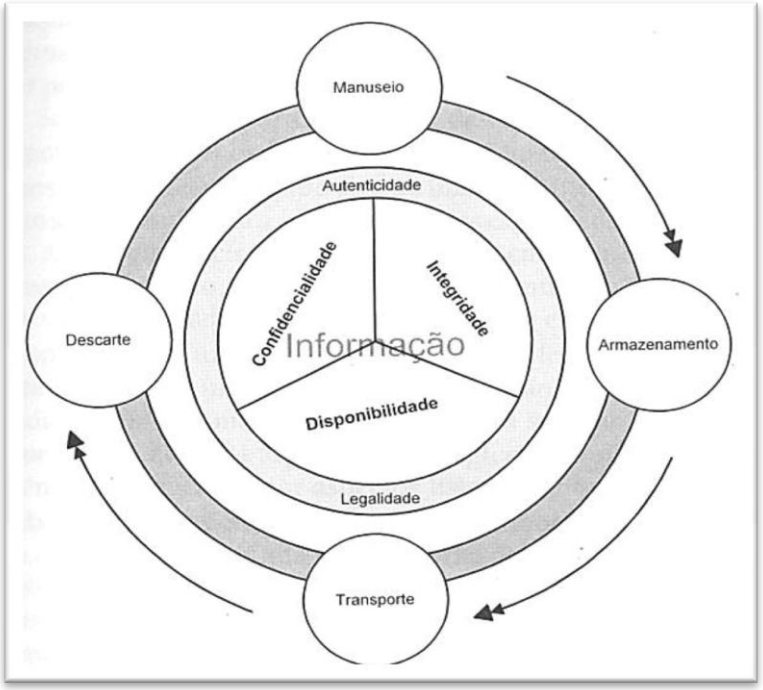
É importante ressaltar que fazer a classificação das informações é algo muito importante para uma empresa, pois minimiza os riscos de exposição indevida da informação. Contudo, ainda há organizações que não praticam tal procedimento. Quando uma empresa não classifica suas informações, considera-se que todas são confidenciais (MITNICK, 2002).

2.3 Ciclo de Vida da Informação.

Considerando o valor da informação para o negócio da empresa é importante preservar e proteger suas propriedades, para mantê-la efetivamente sob controle, durante todas as etapas do ciclo da vida da Informação. Sêmola (2003) define que o ciclo da vida da informação são os momentos vividos pela informação que podem colocá-la em situação de risco. Esses eventos acontecem quando os ativos físicos, tecnológicos e humanos utilizam a informação para manter a operação da empresa. Ainda segundo Sêmola (2003) existem 4 (quatro) momentos em que as propriedades da informações estão sujeitas às ameaças que atingem sua segurança, a saber: Manuseio, Armazenamento, Transporte e Descarte.

- Manuseio: é definido como o momento em que a informação é criada e manuseada.
- Armazenamento: é definido como o momento em que a informação é armazenada em qualquer meio de forma física ou lógica.
- Transporte: é definido como o momento em que a informação é transportada de forma física ou digital.
- Descarte: é definido como o momento em que a informação é descartada de maneira física ou lógica. A Figura 01 mostra estas classificações.

Figura 01: Ciclo da Vida da Informação.



Fonte: Sêmola (2003)

2.4 Segurança da Informação

Como citado anteriormente, considerando o valor e a importância da informação para as organizações o tema Segurança da Informação tem se tornado cada vez mais conhecido. O uso intenso da Internet, para realizar a troca de mensagens entre organizações ou pessoas, o aumento das informações digitalizadas, e o crescimento exponencial das relações entre empresas fez com que aumentasse a preocupação em relação à segurança dos dados manuseados de forma digital. Em função da quantidade de informações disponíveis e manuseadas através da Internet, houve a necessidade de se criar normas para padronizar e aperfeiçoar a gestão da informação. Uma das normas que padroniza internacionalmente a segurança da informação, ISO 27002 (2005), define este conceito como a preservação da confidencialidade, integridade e disponibilidade da informação. A autenticidade, responsabilidade, o não repúdio e confiabilidade, também são propriedades que podem estar envolvidas.

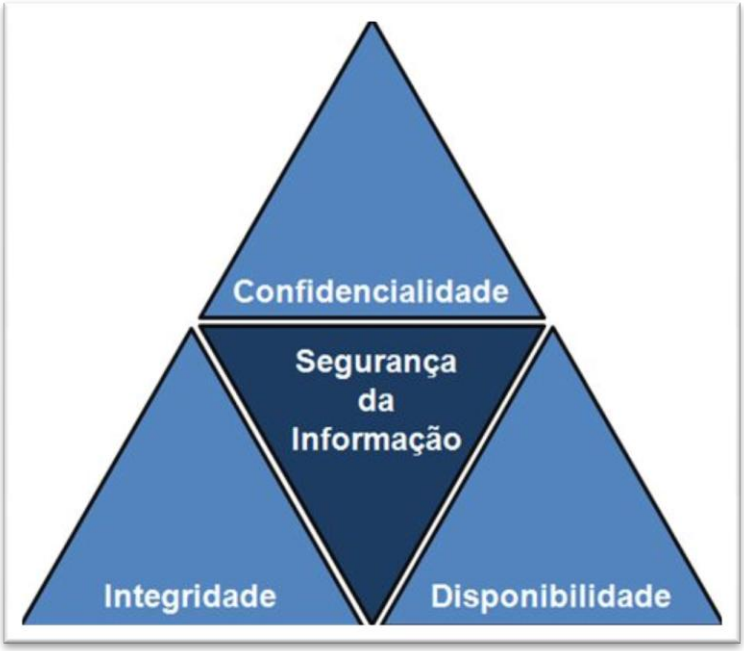
Fontes (2006) afirma que a segurança da informação pode ser definida como um conjunto de orientações, normas, procedimentos, políticas, e demais

ações que tem por objetivo proteger a informação, para garantir a disponibilidade, integridade e confidencialidade, legalidade, não repúdio de autoria.

Sêmola (2003) define a segurança da informação, como uma área de conhecimento que está voltada à proteção dos ativos de uma organização contra possíveis ameaças, tendo como principal objetivo garantir a integridade, confidencialidade e disponibilidade da informação.

Considerando os conceitos dos autores citados anteriormente nota-se que a disponibilidade, integridade e confidencialidade da informação são os atributos básicos que formam os pilares da segurança da informação, também conhecida como tríade da segurança da informação (MACEDO, 2012). A Figura 02 ilustra este conceito.

Figura 02: Pilares da Segurança da Informação.



Fonte: Macedo (2012)

2.4.1 O Conceito da Confidencialidade

O conceito da confidencialidade tem o objetivo de manter a informação em sigilo, ou seja, somente as pessoas autorizadas deverão ter acesso a ela. Sêmola (2003) cita esse conceito da seguinte forma:

> Confidencialidade – Toda informação deve ser protegida de acordo com seu grau de sigilo de seu conteúdo, visando à limitação de seu acesso e uso apenas às pessoas para quem elas são destinadas (SÊMOLA, 2003, p.45).

2.4.2 O Conceito da Disponibilidade

O conceito da disponibilidade consiste em garantir que as informações estejam sempre disponíveis aos usuários autorizados quando estes as requisitarem. Sêmola (2003) conceitua esse princípio da seguinte forma:

> Disponibilidade – Toda informação gerada ou adquirida por um indivíduo ou uma instituição deve estar disponível aos seus usuários no momento em que os mesmos delas necessitem para qualquer finalidade (SÊMOLA, 2003, p.45).

A indisponibilidade de um sistema pode causar grandes prejuízos que interferem nos negócios da empresa. Para exemplificar a situação, se uma empresa *e-commerce* fica fora do ar por alguns minutos terá um prejuízo financeiro muito grande.

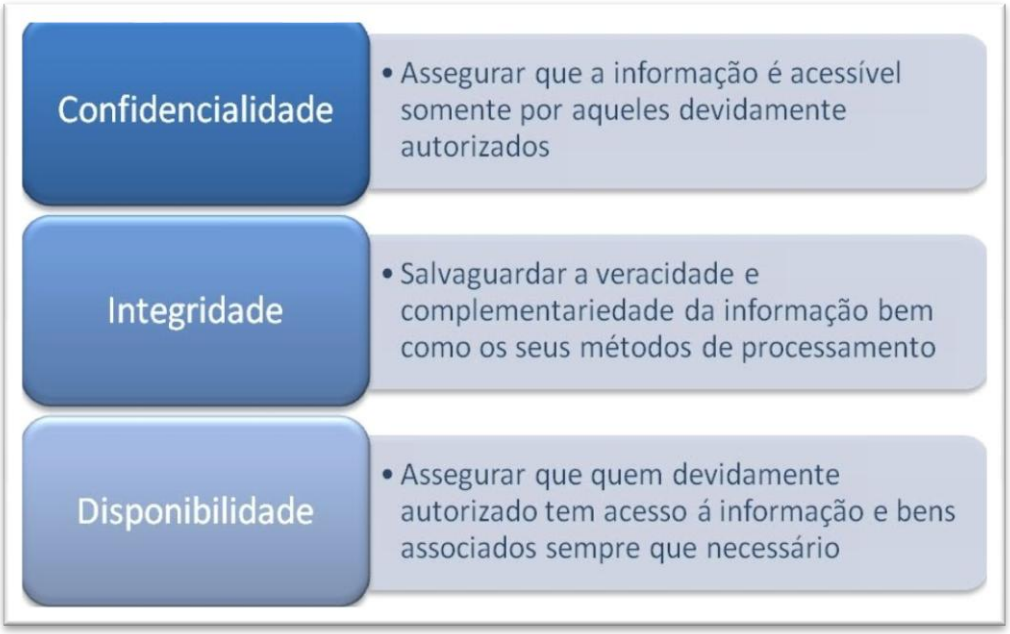
2.4.3 O Conceito da Integridade

A finalidade do conceito da integridade é garantir que os dados não sejam alterados por uma pessoa não autorizada. Caso esse princípio seja violado então o princípio confidencialidade também pode ser comprometido. Garantir a integridade da informação é garantir que os dados não sejam apagados ou alterados sem a autorização do proprietário da informação. Sêmola (2003) reforça, através de seu texto, que:

> Toda informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-las contra alterações indevidas, intencionais ou acidentais (SÊMOLA, 2003, p.45)

A Figura 03 mostra um esquema desses conceitos, normatizados pela norma de segurança ISO 27002 (2005):

Figura 03: Descrição dos aspectos da Segurança da Informação



Fonte: Norma ISO 27002 (2005**)**

2.5 Gestão da Segurança da Informação

Sêmola (2003) considera a gestão da segurança da informação organizada em três camadas, a saber: tecnológica, física e humana. A principal preocupação das organizações é com os aspectos tecnológicos (como por exemplo: computadores, redes, Internet, vírus[1], entre outros) não dando a mesma importância aos aspectos físicos e humanos, relevantes para a segurança do negócio quanto os aspectos tecnológicos.

- Camada Física: é o ambiente onde está instalado fisicamente o hardware[2], como por exemplo: computadores, servidores, *notebooks*, entre outros.
- Camada Tecnológica: é caracterizada pelo uso de software como, por exemplo: programas de computador responsáveis pela funcionalidade do hardware, realização de transação em base de dados, entre outros.

[1] **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.
[2] **Hardware:** é o conjunto de componentes eletrônicos, como por exemplo, circuitos integrados, placas etc.

- Camada Humana: é formada por todos os recursos humanos presentes na organização, principalmente os que possuem acesso direto ou não, aos recursos de TI.

O comportamento das pessoas que trabalham diretamente ou indiretamente com a área de tecnologia não é previsível. Sendo assim o fator humano torna-se o elo mais fraco da corrente, pois é sobre ele que ocorre grande parte dos vazamentos de informações (SÊMOLA, 2003). Desta forma as organizações estão cada vez mais expostas às ameaças que surgem sobre o seu principal ativo: a informação. Para minimizar o risco dessas ameaças é importante capacitar, treinar e conscientizar os principais conhecedores e manipuladores da informação sobre seus papéis, no processo de proteção das informações da organização. Para se reduzir essa exposição, as organizações devem adotar políticas de segurança da informação, normas e procedimentos que estejam sempre atualizados e difundidos a todos os seus cooperadores, através de programas e treinamentos de conscientização, como por exemplo, desconfiarem sempre que forem surpreendidos por um telefonema de alguém que não conheçam (FERREIRA E ARAÚJO, 2006).

A preservação da informação é responsabilidade de todos os colaboradores (FONTES, 2006). Porém, na maioria das vezes, esses colaboradores não estão preparados para lidar e reconhecer situações de risco. Considerando a gestão da segurança da informação é importante ressaltar que as organizações estão expostas a vários tipos de ameaças e vulnerabilidades. Para melhor entender o que representa uma ameaça e uma vulnerabilidade segue a definição de Sêmola (2003).

2.5.1 Definição de Ameaça

Segundo Sêmola (2003) uma ameaça pode ser um comportamento ou um dispositivo da informação que atinge os seus principais aspectos: confidencialidade, integridade e disponibilidade. Pode-se citar como exemplos: um concorrente, ações de *hacker*[3] ou *cracker*[4], erros humanos, insatisfação de funcionários, ferramentas de software[5], entre outros.

[3] ***Hacker:*** serve para designar um programador, com amplo conhecimento sobre sistemas, sem a intenção de causar danos.

2.5.2 Definição de Vulnerabilidade

Sêmola (2003) define vulnerabilidade como uma “evidência ou fragilidade que eleva o grau de exposição dos ativos que sustentam o negócio.” Podem-se referenciar os seguintes exemplos: falhas de infraestrutura física, falhas tecnológicas, falhas humanas, como por exemplo, ausência de conscientização provocando displicência ao criar e manter em sigilo a senha pessoal, entre outros.

2.6 Políticas de Segurança

Conforme Martins (2003), uma política de segurança da informação é um conjunto de regras e padrões sobre o que deve ser feito para assegurar que as informações de uma organização recebam proteção conveniente, de maneira a garantir a confidencialidade, integridade e disponibilidade das informações.

A política de segurança da informação é composta por normas, diretrizes e procedimentos que visam estabelecer os critérios de segurança que serão utilizados, buscando p

adronização e normalização da segurança e deverá ser divulgada a todos os que fazem uso dos ativos da informação (FERREIRA E ARAÚJO, 2006).

Sêmola (2003) cita que a política de segurança da informação, pode ser subdividida em três aspectos hierárquicos, a saber, diretrizes, normas e procedimentos, conceituados a seguir:

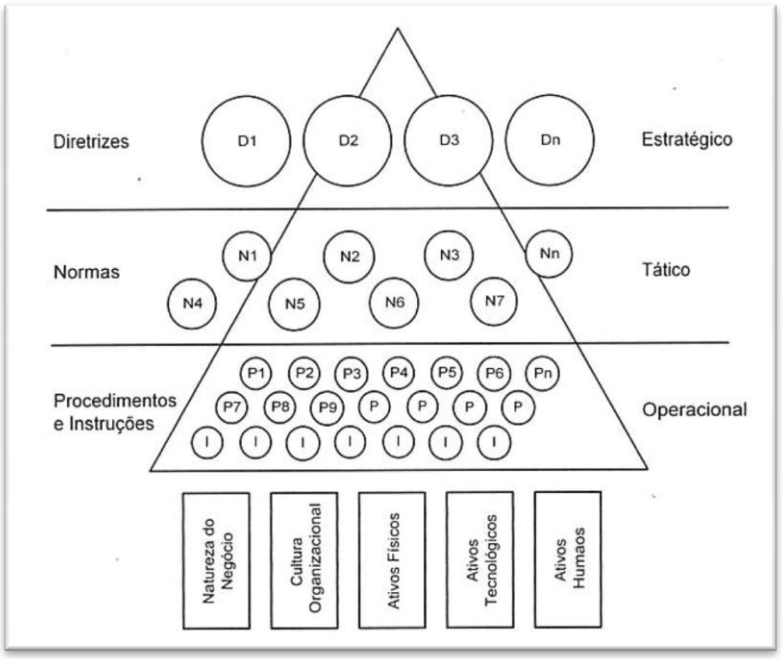
- Diretrizes de segurança da informação: São as estruturas, diretrizes e obrigações referentes à segurança da informação;
- Normas de segurança da informação: Estabelecem os métodos e obrigações definidas de acordo com as diretrizes da segurança da informação;
- Procedimentos de segurança da informação: É a concretização do disposto nas normas e na política, e permite a aplicação direta nas atividades da organização.

A Figura 04 mostra as hierarquias apresentadas anteriormente.

---

[4] ***Cracker:*** é a prática de quebra de sistemas de segurança, códigos de criptografia e senhas de acesso a redes, de forma ilegal e com a intenção de invadir e sabotar para fins criminosos.
[5] **Software:** é parte lógica do computador, como por exemplo, os programas e aplicativos.

Figura 04: Composição da Política de Segurança da Informação



Fonte: Sêmola (2003)

A política de segurança da informação deve conter metodologias regulamentadas para o ciclo da informação, manuseio, transporte, armazenamento e descarte. Entretanto, cada organização tem suas próprias prioridades, e a política de segurança da informação deve ser estruturada de acordo com a necessidade de cada uma delas, de modo personalizado (SÊMOLA, 2003).

Caruso e Steffen (1999) afirmam que não existe uma política de segurança certa ou errada, e nem já definida. A melhor política de segurança é aquela que se adequa melhor a cada organização, levando em consideração a cultura da empresa.

2.7 Por que conscientizar pessoas sobre segurança da informação?

Os problemas relacionados às falhas de segurança da informação estão presentes em todos os tipos de organização, públicas ou privadas. Mesmo considerando os investimentos em tecnologia, feitos pelas organizações, enquanto o fator humano não estiver fortalecido essa empresa estará vulnerável a inúmeros incidentes de segurança (MITNICK, 2002).

O fator humano pode ser considerado o elo mais fraco, pois não é possível prever suas ações. Outro aspecto desfavorável desse fator é o fato das pessoas serem ingênuas e curiosas. Desta forma é possível visualizar o quão vulneráveis estão às informações.

Considerando o exposto anteriormente, os principais objetivos para uma organização realizar treinamentos, campanhas e palestras sobre o tema segurança da informação é o de fortalecer o fator humano e ao mesmo tempo conscientizar os usuários do sistema de informação sobre as várias técnicas que são utilizadas para atacar a confidencialidade, integridade e disponibilidade das informações.

Fontes (2006) define que "a conscientização é mais do que um simples conhecimento". Estar conscientizado em Segurança da Informação é assimilar os conceitos de segurança e utilizá-los no dia a dia de forma habitual sem fazer disso uma tarefa pesada. Os métodos utilizados na campanha de conscientização, tais como, palestras, lembretes, panfletos, mensagens enviadas por correio eletrônico, devem ser elaborados de maneira clara e simples para que a mensagem transmitida possa ser facilmente compreendida pelo usuário. Mesmo que uma organização atenda a questão da segurança tanto dos fatores tecnológicos como dos fatores humanos, e persista em treinamentos constantes e ao mesmo tempo faça uso das melhores tecnologias atuais, essa organização estará sujeita a ameaças e vulnerabilidades. Desta maneira pode-se definir que mesmo com todos esses investimentos não se está totalmente livre de incidentes de segurança. Contudo ao minimizar essas ocorrências podem-se alcançar altos índices de segurança**.** Mitnick (2002) cita essa ocorrência: "Mesmo que uma organização invista consideravelmente em tecnologia e em treinamento dos seus colaboradores, ainda assim ela não está totalmente protegida."

Através da conscientização de pessoas é possível reduzir as vulnerabilidades a que estão expostas as informações. Fontes (2006) lista quais são os principais e mais importantes temas que devem ser trabalhados em uma campanha de conscientização, a saber: conceitos sobre informação e segurança da informação, autenticação de usuário*, logout,* cópias de segurança, continuidade do negócio, uso de antivírus, uso da Internet, uso do correio eletrônico, e engenharia social.

2.7.1 Conceitos sobre Informação e Segurança da Informação

A importância de se divulgar aos usuários do sistema os conceitos de informação e segurança da informação está ligada ao fato de que muitos deles não possuem conhecimento sobre a importância de uma informação para o processo do negócio da empresa e muito menos sabem o que é uma política de segurança da informação e o que ela visa garantir. Para que a proteção da informação seja eficaz os usuários da organização deverão compreender não somente os regulamentos e regras, mas também os conceitos de segurança (FONTES, 2006).

2.7.2 Autenticação de Usuário

Para acessar um sistema computacional, uma conta de *e-mail* ou uma área de trabalho é necessário que o usuário identifique-se. A autenticação de usuário é o reconhecimento de que o usuário é realmente quem diz ser. É uma técnica de segurança utilizada para garantir a confidencialidade e integridade das informações.

Para que o sistema faça o reconhecimento é necessário que o usuário informe seu *login* (nome de usuário) e sua senha. Porém também existem outras formas de autenticação, que são muito utilizadas como, por exemplo, a biometria[6], cartão magnético, *token*[7], entre outros.

Fontes (2006) afirma que a senha é o recurso mais utilizado pela facilidade de criação, baixo preço e alto nível de proteção. Apesar dos benefícios citados anteriormente, a utilização de senha como recurso de autenticação pode tornar-se frágil à medida que os usuários não têm o conhecimento para criar senhas fortes, e utilizam senhas que podem ser facilmente descobertas. Fontes, (2006) cita algumas regras para a composição de senhas com um alto grau de segurança, a saber:

- Nunca utilizar data de nascimento, nome de pessoas, nome de times de futebol ou ainda qualquer outra informação ligada ao usuário ou a organização.
- Não utilizar sequência obvia de caracteres.

---

[6] **Biometria**: método de identificação de pessoas a partir de suas características físicas como por exemplo: a palma da mão, impressão digital dos dedos, retina ou íris dos olhos.

[7] ***Token*****:** é um dispositivo físico de segurança semelhante a um chaveiro que auxilia o usuário quanto à segurança pessoal ao gerar uma senha temporária de proteção para as contas que ele utiliza

- A senha deverá ser composta de no mínimo 6 (seis) caracteres.
- Utilizar letras, números e caracteres especiais.
- E, o mais importante, o usuário deverá manter sigilo sobre sua senha.

É importante salientar que cada um dos recursos utilizados para o reconhecimento tem um custo para organização. Ao escolher um deles ela deverá levar em consideração o recurso que melhor atenda às necessidades de proteção (FONTES, 2006).

2.7.3 *Logoff*

Para o usuário acessar o ambiente computacional, deve se identificar. Essa autenticação normalmente é feita por meio de *login* e senha. Após a autenticação disponibiliza-se a sessão de trabalho e o usuário poderá ter acesso a suas informações (FONTES, 2006). Objetivando evitar que seus dados sejam acessados por uma pessoa que não seja o próprio usuário, ele deverá realizar o *logoff* de seu computador toda vez que se ausentar de sua estação de trabalho. O *logoff* nada mais é do que o bloqueio do computador. Através dele é possível garantir a integridade e a confidencialidade das informações. Através desse simples procedimento o usuário pode evitar que uma pessoa não autorizada e até mesmo mal intencionada apague ou altere informações importantes como se fosse o usuário.

2.7.4 Cópias de Segurança

Incidentes relacionados à segurança sempre acontecem, por essa razão é importante conscientizar os usuários do sistema computacional sobre a importância de realizar o *backup* (cópia de segurança) de suas informações importantes sempre que houver uma nova atualização. Não é possível saber quando um incidente irá acontecer, por isso deve-se estar preparado, pois se uma informação for perdida e não existir uma cópia de segurança, dificilmente ela será recuperada (FONTES, 2006).

Considerando os aspectos da importância da informação para os negócios da empresa nota-se a importância de realizar esse procedimento. As grandes organizações realizam o *backup* das informações que estão armazenadas em seus servidores automaticamente, porém existem organizações de pequeno porte que não possuem tal procedimento. Para essas empresas Fontes (2006) recomenda que o usuário faça pelo menos uma cópia de segurança das informações importantes**,** sempre que forem alteradas.

A orientação sugerida por Fontes (2006) é que essas cópias devem ser feitas em mídia externa como, por exemplo: *Pen Drive*, CD - *Compact Disk*, DVD - *Digital Versatile Disk*, HD externo – *Hard Disk*, entre outras opções. Porém independente da forma como é feita, o *backup* deve ser guardado em local diferente de onde está armazenada a informação original, objetivando a garantia de disponibilidade das informações.

2.7.5 Ações para prevenção de incidentes

Desastres podem acontecer a qualquer momento tanto com o usuário como com a organização. Para reduzir o risco de um desastre ou problema acontecer a organização poderá criar ações para prevenir, detectar ou corrigir problemas. Para o sucesso dessas ações é importante que todos os usuários estejam comprometidos. Fontes (2006) classifica essas ações da seguinte forma:

Tabela 01: Adaptação da classificação das ações em tabela.

Classificação	Objetivo	Exemplos
Ações Preventivas	O principal objetivo dessas ações é de prevenir a ocorrência de um desastre.	– Lembretes; – Instalação de software de antivírus e intrusão.
Ações Detectivas	O principal objetivo é identificar uma situação problema que acontece por não ter sido impedida pelas ações preventivas.	– Bloqueio de acesso quando ocorre mais de 5 tentativas; – Identificar uma pessoa tentando aplicar uma fraude.
Ações Corretivas	Buscam minimizar o problema existente, corrigindo a situação problema.	– Retorno das informações através da utilização das cópias de segurança; – Combate a incêndio.

Fonte: Fontes, 2006.

2.7.6 Continuidade do Negócio

As organizações, independente de seus segmentos, têm por objetivo continuar o desenvolvimento de suas atividades (ou seja, dar continuidade ao negócio). As organizações privadas desenvolvem suas ações com o objetivo de retorno financeiro. Entretanto uma organização pública também espera retribuir socialmente seus acionistas, ou seja, os cidadãos, através da prestação de serviços à população, melhoria na qualidade de vida e também através da realização de ações que fortaleçam a cidadania. “ ...Em resumo, toda organização deseja continuar “viva”, atuar no segmento escolhido, alcançar seus objetivos e cumprir sua missão.” (FONTES, 2006)

O plano de continuidade do negócio deve ser realizado para que após a ocorrência de um problema ou desastre, a organização consiga continuar existindo. Para que a empresa continue funcionando adequadamente é necessário que após uma situação de contingência os recursos humanos, tecnológicos, de conhecimento do processo, ambiente físico e de infraestrutura estejam disponíveis. Para a criação de um PCN – Plano de Continuidade do Negócio, a organização deverá avaliar quais riscos que, caso aconteçam, poderão interferir nos negócios da empresa (FERREIRA e ARAÚJO, 2006). Todos os colaboradores deverão passar por simulações de acontecimentos de desastres, para que quando ele realmente ocorrer cada um saiba qual é o seu papel. Esse plano deve constar da Política de Segurança da Informação da organização (SÊMOLA, 2003).

2.7.7 Uso de Antivírus

Os softwares antivírus servem para reduzir o risco de o computador ser infectado por algum tipo de vírus. Segundo Fontes (2006) os vírus são programas que são instalados no computador do usuário sem seu conhecimento. Após a instalação, começam a executar ações por conta própria, ou seja, sem que o usuário solicite. Considerando que nem todos os usuários possuem conhecimento sobre a forma com que esses programas mal intencionados se instalam no computador, precisam ser orientados sobre esse assunto, para que possam proteger melhor suas

informações. Fontes (2006) cita alguns cuidados que são considerados tão importante quanto o uso do antivírus, a saber:

- Sempre que receber um arquivo anexo, não execute sem antes passar o software antivírus;
- Não executar nenhum programa que receber em anexo se não estiver esperando o arquivo. Caso conheça o remetente entre em contato com ele para confirmar o envio do documento;
- Ao utilizar a Internet o usuário somente deverá realizar o *download* de qualquer arquivo ou programa se estiver navegando em *sites* seguros;
- Manter sempre atualizada a cópia de segurança para garantir sua recuperação;

Ferreira e Araújo (2006) citam que o vírus de computador é o principal problema de Segurança da Informação. Para manter um computador protegido dessa ameaça é necessário ter um software antivírus instalado na máquina e mantê-lo atualizado, ou seja, ele deve possuir uma lista de assinatura completa. Caso essa lista não esteja completa o software antivírus pode não ter efeito.

2.7.8 Uso da Internet

A Rede Mundial de Computadores, conhecida como Internet, oferece aos seus usuários um universo repleto de divertimento, além de disponibilizar uma quantidade imensa de informações. Fontes (2006) refere-se a ela como sendo uma grande biblioteca. Essa rede disponibiliza as informações solicitadas pelo usuário com rapidez diminuindo as distâncias entre pessoas e/ou organizações com apenas um *click*. Considerando todos esses atrativos oferecidos pela Internet, é importante que todos os colaboradores da organização sejam orientados sobre o correto uso dessa ferramenta. Diante do exposto, Fontes (2006) sugere algumas regras para acesso, a saber:

- O usuário somente deve acessar *sites* seguros e que estejam relacionados com suas atividades profissionais;
- O usuário deverá ser instruído a não realizar cópia alguma da Internet, que possa infringir a legislação em termos de direitos autorais.

- O ideal é que o acesso aos recursos da organização seja realizado através de identificação e autenticação. Através desse método a empresa pode saber quais recursos o usuário utiliza e também está apta a responder qualquer questionamento judicial sobre o acesso de seus colaboradores.

2.7.9 Uso do Correio Eletrônico

O correio eletrônico é uma ferramenta que facilita a comunicação fora e dentro da organização. Ela permite ao usuário receber e enviar mensagens eletrônicas ajudando assim a organização cumprir sua missão e objetivos. Contudo esse universo virtual expõe seus usuários a uma gama de ameaças eletrônicas que são difundidas através de *e-mail*. Ferreira e Araújo (2006) afirmam que apesar dessa ferramenta ser bastante eficiente na comunicação há muitas formas de fraudes que utilizam e-mail para disseminação de vírus. Em função disso, nota-se que é importante que a organização oriente seus colaboradores quanto à utilização correta e consciente dessa ferramenta. Fontes (2006) cita algumas recomendações a serem abordadas pelas organizações, como por exemplo:

- Orientar aos usuários a não utilizar seu *e-mail* profissional para enviar mensagens racistas, discriminatória, com conteúdo pornográfico, que instigue a pedofilia e o ódio e nem para realizar propagandas de produtos pessoais. Ele somente deverá ser utilizado para fins profissionais.
- Outra recomendação do autor é a de que usuários devem evitar abrir arquivos de pessoas desconhecidas. Eles somente devem executar um arquivo anexo se tiver certeza de que solicitou esse *e-mail***.**

2.7.10 Engenharia Social

Segundo a cartilha sobre segurança da informação da CERT.br[8] a engenharia social é um método de ataque no qual alguém faz uso da persuasão,

[8] **CERT.br:** Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil é mantido pelo NIC.br (Núcleo de Informação e Coordenação do Ponto BR), do Comitê Gestor da Internet no Brasil, e atende a qualquer rede brasileira conectada à Internet

muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso, não autorizado, a computadores ou informações.

Fontes (2006) designa a engenharia social como sendo um conjunto de procedimentos e ações que são utilizados para adquirir informações de uma organização ou pessoa por meio de contatos falsos sem o uso da força de arrombamento físico ou de qualquer brutalidade.

Diante do exposto anteriormente nota-se como o fator humano está mais vulnerável a estas ameaças do que se pode imaginar. É primordial para a organização que o elo mais fraco, ou seja, o fator humano, não só tenha o conhecimento do prejuízo que o vazamento de uma informação confidencial poderá causar a instituição, como também saiba se comportar em tais situações. Ferreira e Araújo (2006) listam os tipos de ataques utilizados:

- No local de trabalho: Algumas organizações deixam amostra em locais de fácil acesso as pessoas que transitam dentro da empresa informações restritas que podem ser facilmente obtidas por uma pessoa não autorizada, como por exemplo: o organograma da empresa, ou a lista de ramais entre outros.
- Por telefone: O engenheiro social poderá utilizar uma ligação telefônica para se passar por alguém que não é e persuadir o usuário a lhe dizer por exemplo sua senha, *login*, entre outros.
- No lixo: ao vasculhar o lixo o engenheiro social pode encontrar muitas informações descartadas que possuam valor e ainda podem ser utilizadas em um ataque.
- *On-line*: nesse tipo de ataque o engenheiro social utiliza o correio eletrônico para enviar mensagens publicitárias oferecendo brindes para participar de um sorteio e solicita os dados pessoais e profissionais do usuário. Com todos esses dados nas mãos fica fácil para o invasor realizar um ataque sem muito esforço.
- Inversa: Tendo em mãos a lista de ramais ou organograma da empresa o engenheiro social pode se passar por uma pessoa de autoridade da empresa e adquirir as informações desejadas.

Quando o engenheiro social realiza contato com alguém da organização, fala com propriedade sobre um determinado assunto, através da precisão das informações prestadas, ganha a confiança do colaborador da organização e até chega a prestar alguns favores para ganhar ainda mais a confiança do colaborador.

A melhor maneira de prevenir e proteger a organização contra esses ataques é realizar treinamentos e campanhas de conscientização aos colaboradores que abordem quais e como as informações devem ser protegidas de um ataque. Somente assim os colaboradores da organização estarão aptos a identificar situações de risco (FERREIRA e ARAÚJO, 2006).

Além de abordar a questão da proteção da informação, o treinamento e a campanha de conscientização devem difundir as normas procedimentos e política de Segurança da informação da organização a todos os seus colaboradores para evitar que incidentes de segurança aconteçam.

2.8 Etapas para realizar o levantamento de informações e aplicação dos métodos

O modelo Cobit (2007) cita que para conscientizar e treinar funcionários em segurança da informação são necessárias 03 (três) etapas, a saber: Identificação das Necessidades de Ensino e Treinamento, Entrega de Treinamento e Ensino e Avaliação do Treinamento Recebido.

2.8.1 Identificação das Necessidades de Ensino e Treinamento

A identificação das Necessidades de Ensino e Treinamento é a primeira etapa a ser realizada. Sua função é a de identificar quais são as necessidades de segurança no local considerando para isso o valor das informações, a cultura existente de segurança bem como a infraestrutura física e lógica, atuais e futuras da organização (COBIT, 2007).

2.8.2 Entrega de Treinamento e Ensino

A Entrega de Treinamento e Ensino é a segunda etapa a ser feita. Depois de realizar a identificação das necessidades de ensino e treinamento, é necessário

escolher o mecanismo de treinamento que será utilizado para o treinamento, quem será o instrutor desse treinamento, e quais usuários participarão dele (COBIT, 2007).

2.8.3 Avaliação do Treinamento Recebido

A Avaliação do Treinamento Recebido é a terceira e ultima etapa. Ela consiste em avaliar o conteúdo absorvido pelos usuários que participaram do treinamento, no que diz respeito à relevância, qualidade, efetividade, absorção e retenção do conhecimento (COBIT, 2007).

3-DESENVOLVIMENTO DO TRABALHO

Durante o decorrer do curso de Segurança da Informação a autora notou várias falhas de Segurança em seu local de trabalho. Isso motivou-a não só a elaborar uma pesquisa para verificar o nível de segurança do local como também a aplicar métodos de conscientização para usuários, além de propor algumas práticas para minimizar ou até mesmo solucionar pequenos problemas.

A organização participante da pesquisa é um departamento de uma instituição pública da Região Metropolitana de Campinas (RMC), que possui 20 (vinte) colaboradores e todos participaram da pesquisa. Entretanto, por essa instituição se tratar de um setor público, um dos critérios impostos pela gestão superior, para a aplicação de todas as etapas desse trabalho, foi o não envolvimento de recursos financeiros.

Anterior ao início da pesquisa foi encaminhado ao responsável pelo Departamento um documento formal para autorizar o início dos trabalhos no local. Este documento descreve todo o processo do projeto e também informa que o nome do órgão participante será mantido em sigilo (Apêndice A). Após a autorização e para conhecer quais as principais falhas de segurança dessa organização a primeira medida foi aplicar um questionário (APÊNDICE B) investigativo, de perguntas fechadas, a ser respondido por todos os funcionários do setor (vinte no total). Os resultados deste primeiro questionário permitiram materializar que o departamento em questão possuía falhas de segurança na camada física, lógica e humana e também que poderiam ferir os princípios de integridade, confidencialidade e disponibilidade da informação. (vale lembrar que os vinte funcionários do setor responderão os questionários)

Em seguida à análise dos resultados obtidos no questionário, foram sugeridas as seguintes práticas de segurança: envio de *e-mails* (APÊNDICE D) com mensagens de conscientização, apresentação de palestra pela autora (APÊNDICE C), contendo fortes sugestões de medidas de segurança que podem ser adotadas no cotidiano do departamento e elaboração e distribuição de *folder* (APÊNDICE E) para conscientizar todos os funcionários do local.

Após aplicação de todas essas etapas foi reaplicado o mesmo questionário para verificar se houve alguma mudança em relação às vulnerabilidades apresentadas. A Tabela 02 apresenta o cronograma da aplicação da pesquisa.

Tabela 02: Cronograma da aplicação da pesquisa

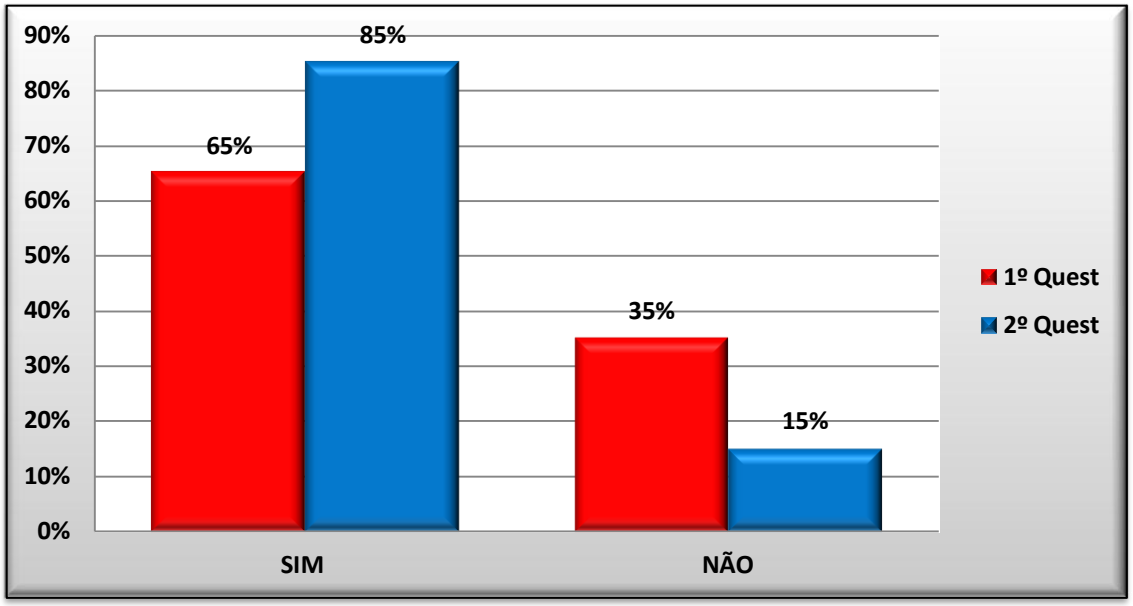
Tarefa	Data
Autorização	31 de janeiro de 2014
Aplicação do 1º questionário	De 06 a 10 de fevereiro de 2014
Apresentação da palestra	07 de março de 2014
Envio do 1º e-mail	14 de março de 2014
Envio do 2º e-mail	21 de março de 2014
Envio do 3º e-mail	28 de março de 2014
Envio do 4º e-mail	31 de março de 2014
Distribuição do folder	04 de abril de 2014
Aplicação do 2º questionário	De 10 a 14 de abril de 2014

Fonte: Autoria Própria (2014).

3.1 Apresentação dos Resultados

Retomando os aspectos sobre segurança da informação relacionados ao descuido de pessoas, falta de *backup*, a não utilização de antivírus e lembrando o interesse da autora, sobre como melhorar a segurança da informação em seu local de trabalho, e conforme descrições feitas no Capítulo 1 sobre a metodologia adotada para a solução dos problemas relacionados à segurança da informação, os resultados obtidos são apresentados a seguir, através de gráficos de barras. Os gráficos apresentam os resultados obtidos após as tabulações das respostas do primeiro questionário e após as tabulações das respostas do segundo questionário. Vale lembrar que, entre o primeiro e o segundo questionários houve a campanha de conscientização feita pela autora, envolvendo diversos recursos (como citado anteriormente).

Figura 05: Questão 1- A disponibilidade, a integridade e a confidencialidade são os principais aspectos da Segurança da Informação. Você já conhecia essa classificação?

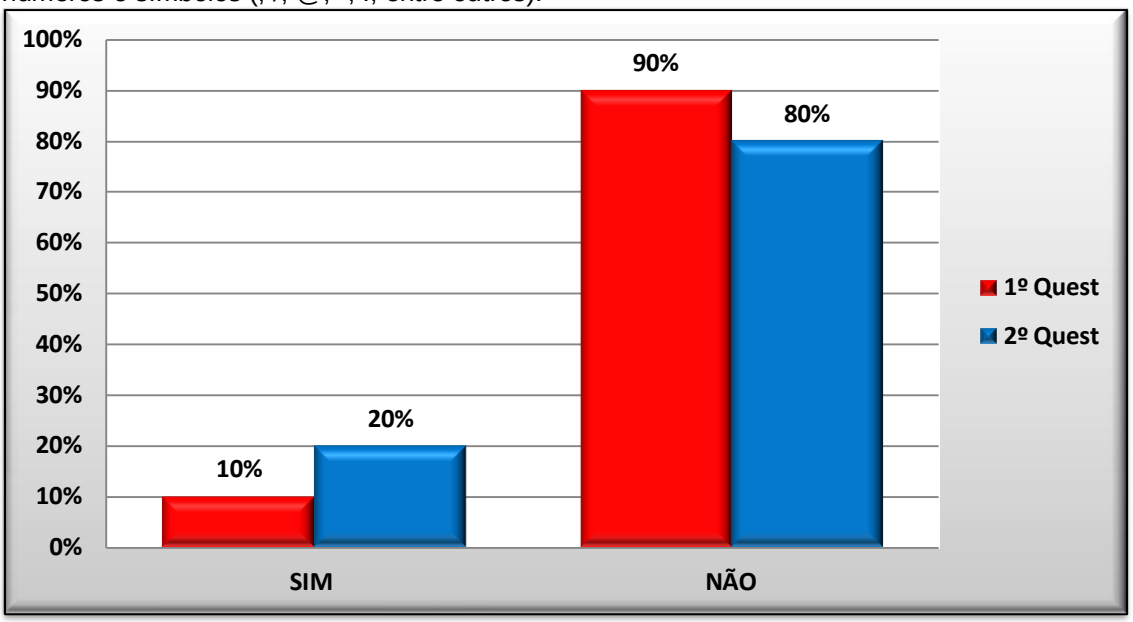


Fonte: Autoria Própria (2014).

A Figura 05 refere-se ao nível de conhecimento dos usuários sobre os princípios fundamentais da Segurança da Informação. Ao considerar que o objetivo principal dessa classificação é preservar a informação contra ameaças e vulnerabilidades que possam comprometer os negócios da empresa é possível concluir que os usuários compreendem melhor a importância da segurança da informação a partir do momento em que passam a entender esses princípios.

Para conscientizar os usuários sobre os princípios fundamentais da Segurança da Informação, foi feita uma rápida apresentação (Apêndice C), destacando os conceitos destes princípios. Foi elaborado *folder* para distribuição a todos os usuários do departamento. A partir da análise dos resultados nota-se que antes da campanha de conscientização de usuários, 65% dos entrevistados conheciam esses princípios e após a campanha, 85% dos participantes declararam que conhecem os princípios. Com isso conclui-se que os métodos utilizados contribuíram para aumentar em 20% o número de usuários em relação ao conhecimento dessa classificação.

Figura 06: Questão 2 – Em seu local de trabalho existem regras para a criação de senha? (por exemplo, a composição de uma senha segura deve conter letras maiúsculas, minúsculas, números e símbolos (, /, @, *, ., entre outros).



Fonte: Autoria Própria (2014).

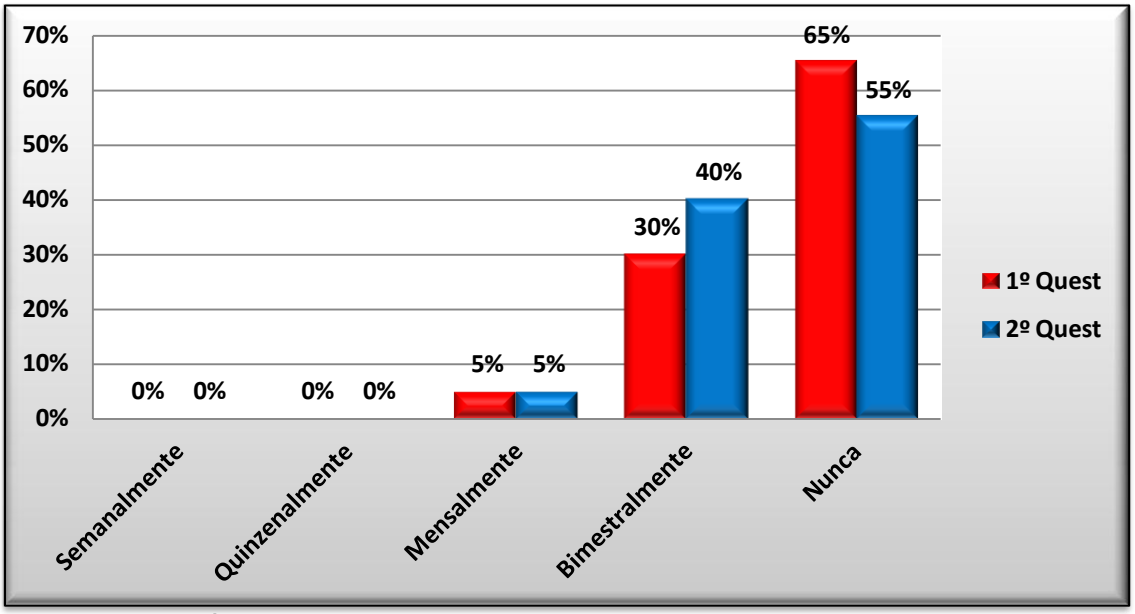
A senha é o recurso mais utilizado para se garantir um nível de segurança aceitável, pois além de seu baixo custo, ela também garante um bom nível de proteção. Porém a composição de senhas fracas pode apresentar fragilidade de segurança para a organização (FONTES, 2006). Observando a Figura 06 nota-se que antes da aplicação da campanha de conscientização 90% dos entrevistados não utilizavam uma criação de senha forte. Isto pode comprometer a segurança da informação na organização, uma vez que a senha fraca pode ser facilmente descoberta através de programas específicos, possibilitando desta forma que seu *e-mail*, sistema, ou área de trabalho possa ser acessado por alguém não autorizado.

Com o objetivo de conscientizar os usuários quanto à necessidade de compor uma senha mais segura foram encaminhados *e-mails* aos participantes da pesquisa contendo instruções para elaboração de uma senha forte. Para reforçar as orientações dadas sobre a criação e alteração de senhas, o mesmo tema foi abordado em palestra apresentada pela autora deste trabalho, e reforçado com a distribuição do *folder.*

Após a campanha pode-se verificar que 10% dos participantes da pesquisa foram conscientizados quanto á importância de se criar uma senha

forte. Contudo somente a criação de senha forte não é o bastante. Para maior segurança quanto ao código secreto de acesso é necessário modificá-lo periodicamente. A Figura 07 aponta a frequência que os entrevistados realizam a troca de suas senhas.

Figura 07: Questão 3 - Com qual frequência você realiza as trocas de suas senhas de e-mail, ou sistema:



Fonte: Autoria Própria (2014).

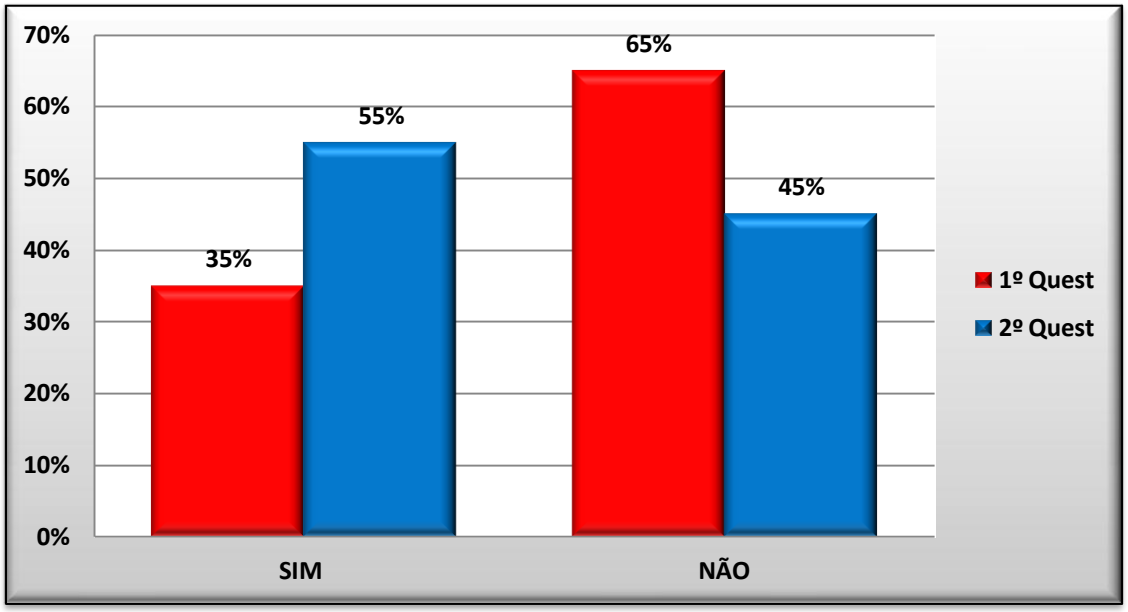
A senha, que também é conhecida como *password,* é utilizada como forma de reconhecimento. Ela autentica usuários e concede-lhes privilégios ou ainda permite o acesso a informações privilegiadas armazenadas. Por isso ela deve ser pessoal e intransferível, para manter sua conta protegida. A troca de senha deve ser efetivada periodicamente com a finalidade de evitar fraudes quanto ao roubo de identidade.

Antes da campanha, mais da metade dos entrevistados, ou seja, 65%, nunca realizaram a troca de senhas, 30% realizam a troca de suas senhas bimestralmente e 5% mensalmente. Após a campanha houve uma pequena alteração nos valores apresentados sendo que 55% dos usuários ainda não foram conscientizados da importância de se realizar a troca de senhas com frequência.

Para solucionar a questão apresentada sugere-se fortemente que a instituição adote uma política de criação de senhas. Uma das considerações a

serem feitas nesta política é a recomendação ao usuário do sistema no sentido de realizar a troca de senha periodicamente (quinzenalmente, de preferência).

Figura 08: Questão 4 - Ao ausentar-se do seu local de trabalho você realiza o *logoff* (trava) de sua área?



Fonte: Autoria Própria (2014).

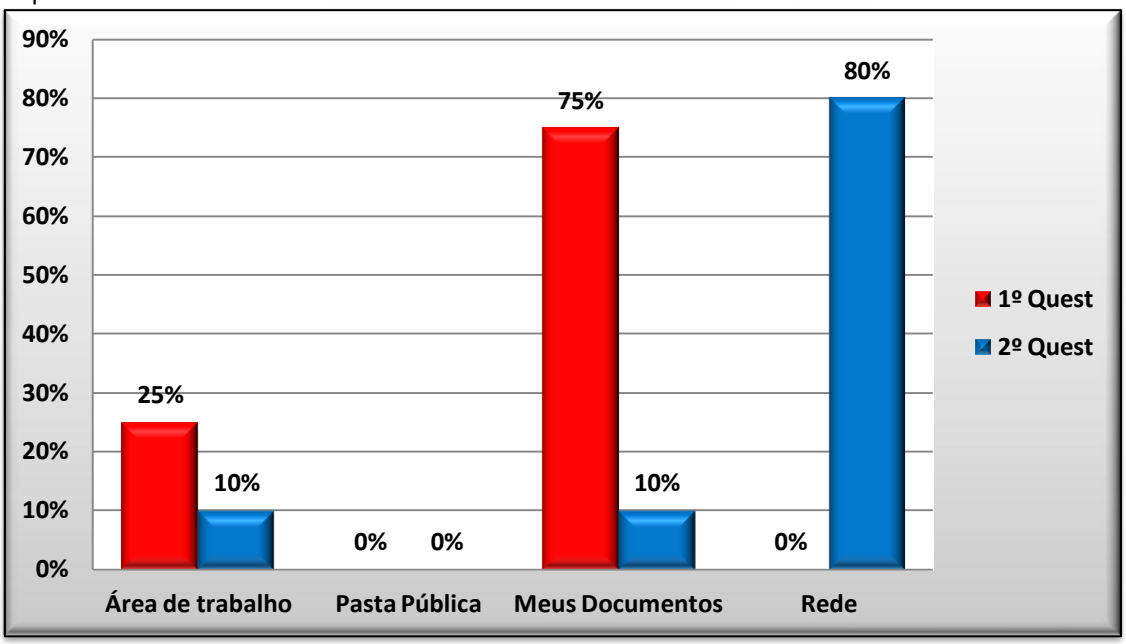
A Figura 08 ilustra o quanto as informações estão vulneráveis na ausência de seus administradores. A maior parte dos entrevistados, ou seja, 65%, não realizavam o *logoff* de sua área de trabalho, contribuindo assim para aumentar o risco de um usuário não autorizado adentrar a rede em busca de informações. Caso a informação obtenha a classificação de sigilosa, esta falha de segurança da informação pode arruinar todo trabalho da política de segurança da informação, e em consequência, pode ocorrer um incidente ou desastre, comprometendo o plano de continuidade de negócio.

A postura dos usuários é um fator essencial para que os dados da organização não sejam acessados, alterados ou até mesmo apagados por uma pessoa que não possua autorização de acesso àquelas informações. O fator humano é primordial para o sucesso da segurança de informação (FONTES, 2006).

Considerando a questão do fácil acesso à rede, outro fator a ser observado é o local onde os entrevistados armazenam suas informações. Pois com a facilidade de entrada à rede os acessos a documentos e arquivos

podem estar vulneráveis. A Figura 09 indica onde os usuários costumam armazenar suas informações

Figura 09: Questão 5 - Em seu computador de trabalho onde você costuma armazenar seus arquivos?

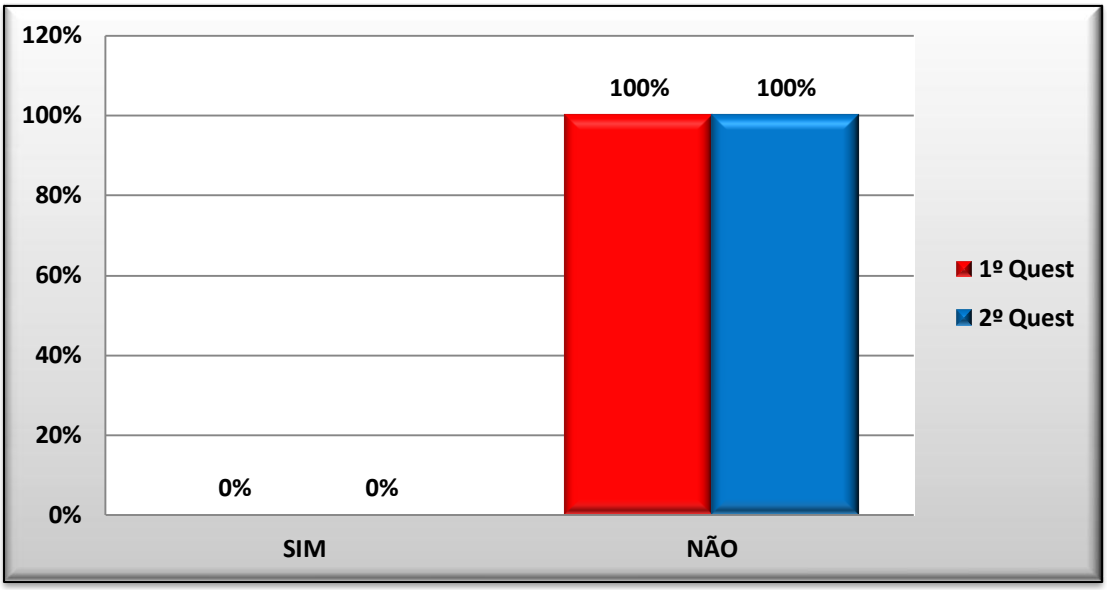


Fonte: Autoria Própria (2014).

A Figura 09 demonstra o local do computador onde os usuários estavam armazenando seus arquivos. Nota-se que 25% dos entrevistados armazenavam seus arquivos na área de trabalho, enquanto 75% dos entrevistados na pasta Meus Documentos. O local onde os usuários deixavam armazenados seus dados confidenciais pode ser facilmente explorado por uma pessoa mal intencionada e também porque estão salvos no próprio computador do usuário.

Para garantir maior segurança esses dados deveriam ser armazenados em uma pasta compartilhada na rede, para que em caso de acidentes eles possam ser facilmente recuperados. Para minimizar essa vulnerabilidade, além da campanha de conscientização, uma ação adotada foi solicitar ao Departamento de Tecnologia de Informação a criação de uma pasta compartilhada e também auxiliassem os usuários a realizar a transferência de seus arquivos para esta pasta.

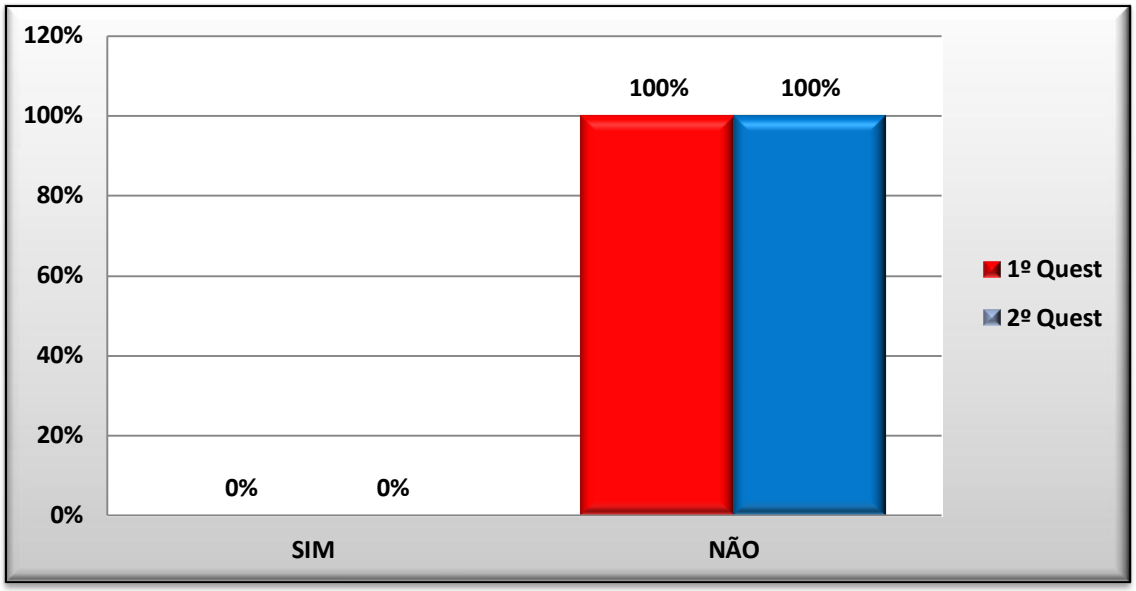
Figura 10: Questão 6 - Em seu local de trabalho existe controle interno para entrada de pessoas?



Fonte: Autoria Própria (2014).

Considerando os resultados obtidos na Figura 08, referente ao *logoff*, e também os apresentados na Figura 10, nota-se que a falta do controle de pessoas ao local, torna ainda mais vulnerável o acesso aos dados. Vale lembrar que uma das condições impostas pelo gestor do departamento considerava o não uso de recursos financeiros adicionais, o local de trabalho da autora continua sem algum tipo de controle de acesso de pessoas ao ambiente. Esta dificuldade é reforçada pelas respostas compiladas e apresentadas na próxima figura.

Figura 11: Questão 7 - Em seu local de trabalho existem câmeras de segurança?

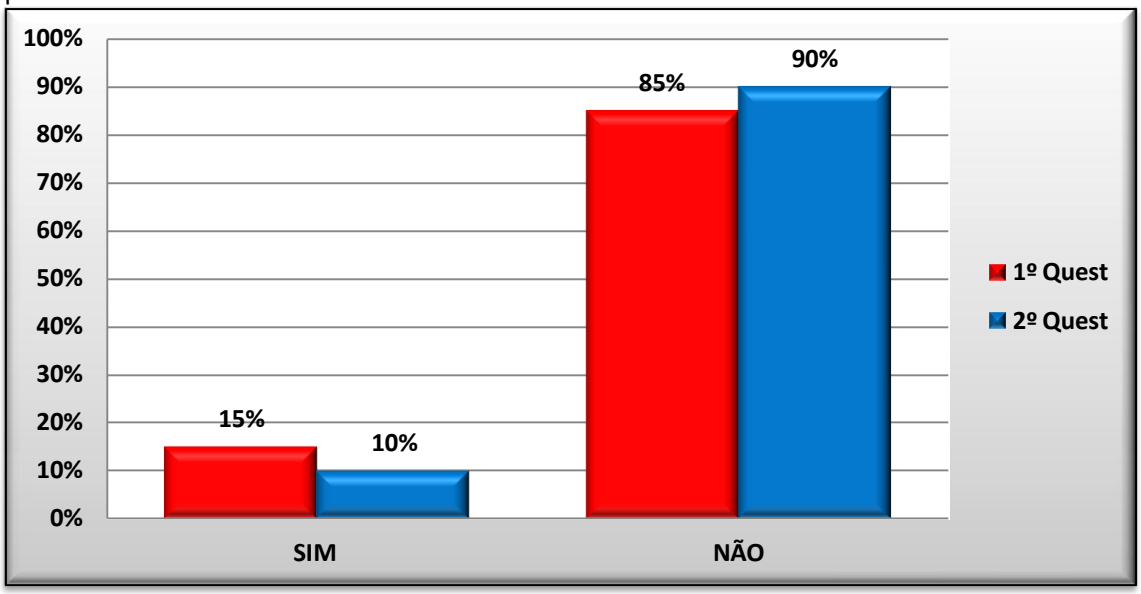


Fonte: Autoria Própria (2014).

A Figura 11 apresenta a informação sobre a falta de câmeras de segurança no local. Isso adicionado à Figura 10 deixa clara a ausência de controle de entrada de pessoas no local. Se buscarmos ainda os dados da Figura 08 sobre o *logoff*, nota-se o quão vulnerável está este departamento. Pois uma pessoa consegue adentrá-lo com facilidade, podendo encontrar os computadores desbloqueados e alterar uma informação caso queira.

Uma medida para minimizar essa vulnerabilidade seria a instalação de câmeras de segurança no local. Porém a proposta para a elaboração desta pesquisa é o de não envolver recursos financeiros. Sendo assim será encaminhado para a chefia local ao término deste projeto um relatório contendo sugestões para implementação no futuro.

Figura 12: Questão 8 - Você considera o seu local de trabalho seguro a ponto de deixar objetos pessoais e/ou de valor em sua sala?



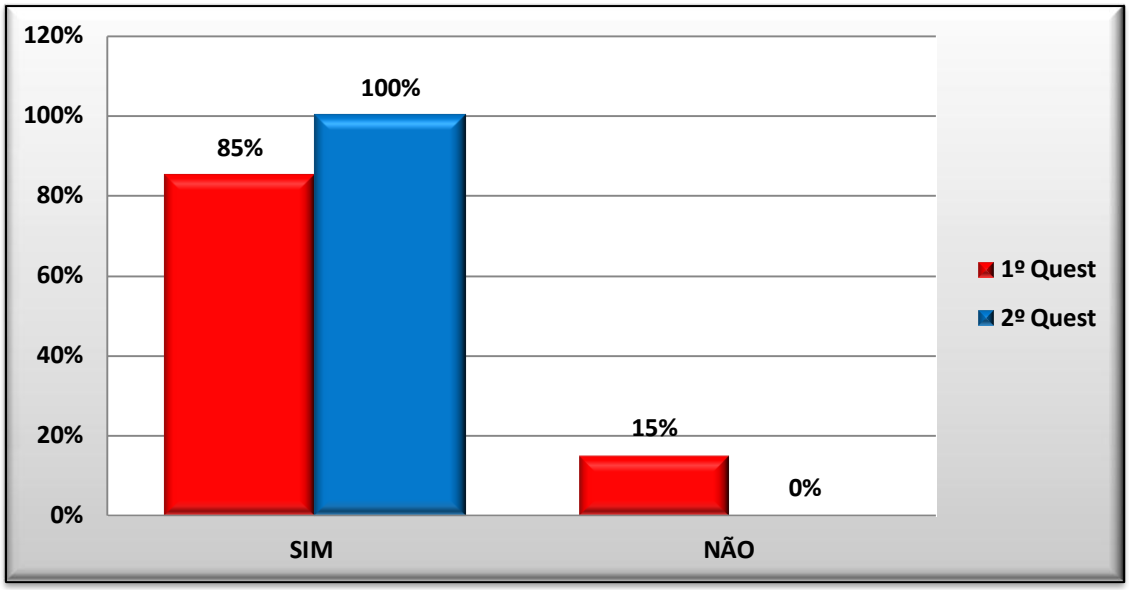
Fonte: Autoria Própria (2014).

A Figura 12 indica que após a campanha de conscientização a maior parte dos entrevistados, ou seja, 90% não consideram o seu local de trabalho seguro, e apenas 10% consideram seguro. Considerando as vulnerabilidades a que está exposto o departamento apresentadas pela pesquisa é possível notar a falta de segurança no local.

O índice de 10% que o consideram seguro pode ser justificado pelo fato de que algumas pessoas ainda não assimilaram a conscientização feita, relacionada à segurança do local inclusive. Com isso estão expostas a riscos no que diz respeito às informações e aos seus pertences pessoais.

Uma medida proposta é que o responsável pelo departamento pode optar para tornar esse local um pouco mais seguro, solicitando um investimento na aquisição de equipamentos de controle de acesso de pessoas ao local e também continuar a treinar funcionários em segurança da informação.

Figura 13: Questão 9 - Seu computador possui software antivírus?



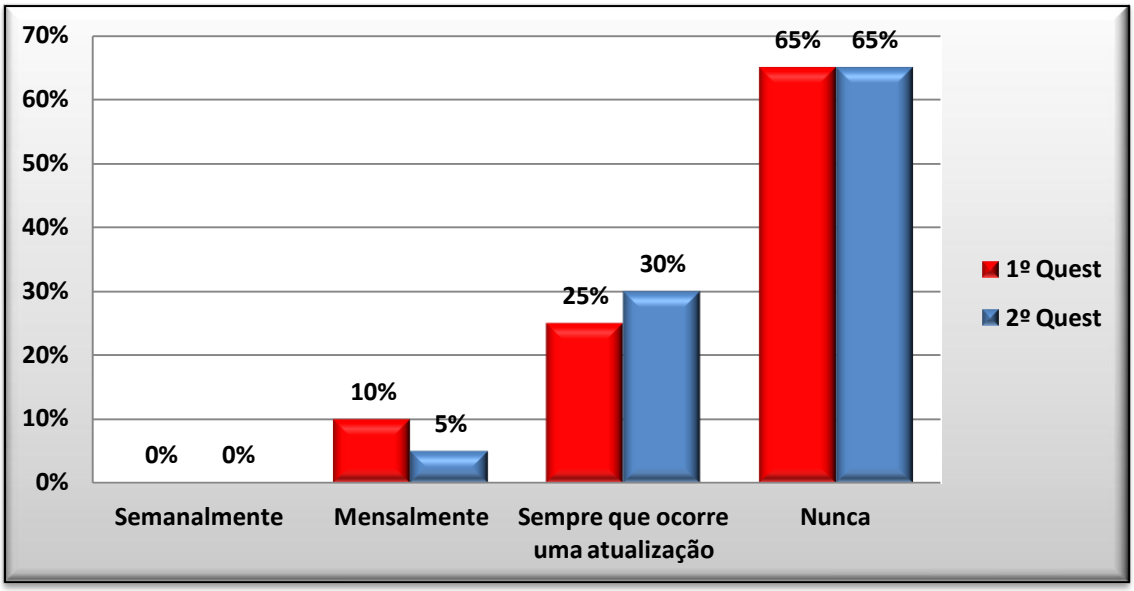
Fonte: Autoria Própria (2014).

A Figura 13 trata da questão das máquinas que possuem software antivírus instalado. Apesar de 85% dos entrevistados possuir antivírus instalado em sua estação de trabalho, nota-se que 15% dos entrevistados não possuíam esse software instalado em seus computadores. Retomando a afirmação dos autores Ferreira e Araújo (2006) de que “os vírus é o principal problema de Segurança da Informação”, percebe-se o quanto vulnerável estão os computadores que não possuem essa proteção.

Pode-se identificar que após a campanha não existia no departamento nenhum computador sem essa proteção, ou seja, 100% das máquinas. A medida utilizada para resolver essa questão foi solicitar ao Departamento de Tecnologia da Informação que identificasse quais computadores não possuíam instalado o antivírus e realizasse a instalação do software utilizado pela organização.

Contudo, para que esse computador esteja realmente protegido além da instalação é necessário mantê-lo atualizado.

Figura 14: Questão10 - Você realiza o *backup* (cópia de segurança) de suas informações?



Fonte: Autoria Própria (2014).

A Figura 14 ilustra as respostas dos usuários quanto à prática do *backup*. Ao analisar o resultado nota-se que mesmo depois das campanhas de segurança da informação aplicadas no departamento não houve nenhuma alteração na porcentagem de usuários que nunca realizam a cópia de segurança. Isto mostra o quão vulnerável estão as informações, pois em caso de perda das informações não há métodos para recuperação das mesmas.

Contudo um ponto positivo que a Figura 14 apresenta é um aumento de 5% dos usuários que passaram a realizar a cópia de segurança sempre que ocorrer uma nova atualização. Apesar dessa pequena melhora este índice ainda está longe do desejável considerando a importância das informações tratadas no local.

É essencial para garantir a disponibilidade das informações do departamento entrevistado que esse tema continue sendo abordado em outras campanhas de conscientização. Desta forma o usuário do sistema de informação se habituará a essa prática tão importante.

4 CONCLUSÃO

A solução do problema proposto pela autora, que trabalha em uma instituição pública municipal, fundamentou-se não apenas nos conhecimentos adquiridos no transcorrer de seu curso superior, no levantamento bibliográfico feito, mas principalmente, através de observações e análises feitas, após ocorrência de alguns fatos relacionados à aparente falta de cuidados com a manipulação da informação que passa ou que é determinada em seu departamento de trabalho. Vale lembrar que houve restrições orçamentárias impostas pelo responsável pelo departamento, decorrentes da legislação que rege organizações públicas de maneira geral.

Os resultados obtidos pela pesquisa realizada, apresentados na Tabela 03, mostram que, em menos de 90 (noventa) dias, período compreendido entre a solicitação da realização da pesquisa (31 de janeiro de 2014) até a aplicação, pela segunda vez, do questionário (de 10 a 14 de abril do mesmo ano), alguns aspectos relacionados à segurança da informação foram assimilados pelos funcionários. Os conceitos sobre os atributos da informação (questão 1) foi um deles. A utilização de antivírus foi assimilada por todos após o programa de conscientização (questão 9). A conscientização do uso de *logoff* da máquina de trabalho (questão 4) melhorou a postura dos funcionários, mas ainda preocupa . A utilização de uma área adequada para armazenamento de seus arquivos foi assimilada muito bem pelos funcionários (questão 5), pois antes do processo de conscientização, 0% armazenava seus arquivos na área específica para isso, na rede da organização. Após o processo o resultado subiu para 80% (foi necessária, também, a interferência da autora junto aos profissionais de TI, no sentido de deixar disponível uma área que atendesse esta finalidade). A respeito do uso de antivírus (questão 9), 100% dos funcionários usam antivírus em suas máquinas de trabalho. Pode-se afirmar que os progressos obtidos foram decorrentes dos resultados do processo de conscientização feito pela autora, a saber: palestras; envio de *e-mails;* elaboração e distribuição de *folders* com informações básicas sobre segurança da informação e cuidados básicos a serem adotados; conhecimento sobre os principais aspectos relacionados à informação (disponibilidade, confidencialidade e integridade); local de armazenamento de arquivos e uso de antivírus. Os resultados obtidos nas respostas de algumas

questões (questões 6, 7 e 8) independem do trabalho feito pela autora, pois envolvem questões financeiras. Mesmo assim, mostraram a necessidade da adoção de medidas de segurança, relacionadas ao controle de acesso físico do local, a saber: uso de câmeras de segurança no local de trabalho e controle interno para entrada de pessoas. A adoção destas medidas pode ser sugerida e reforçada pela autora deste trabalho, não só através dos resultados obtidos pela pesquisa realizada, como também através da bibliografia estudada, mas a autora não tem como garantir sua efetiva implantação, pela própria natureza de seu trabalho e do cargo que ocupa na instituição. Os resultados obtidos nas questões 2, 3, 4 e 10 mostram que o processo de conscientização surtiu algum efeito, mas na tentativa para solucionar as questões apresentadas sugere-se fortemente que a instituição adote uma política de criação de senhas e uso constante de *logoff* ao se ausentar do local de trabalho. Uma das considerações a serem feitas nesta política é a recomendação ao usuário do sistema no sentido de realizar a troca de senha periodicamente (quinzenalmente, de preferência). De qualquer forma, medidas relativamente simples, adotadas pela autora provocaram uma conscientização nos funcionários do departamento, quanto à segurança da informação, melhorando o nível de segurança das informações geradas e manipuladas pelo departamento. A manutenção periódica destas medidas certamente contribuirá, cada vez mais, para a melhoria proposta pela autora.

Uma sugestão para trabalhos futuros é a realização da análise de custo X benefício para se adotar medidas mais eficazes, relacionadas à segurança da informação, envolvendo não apenas os profissionais da área de TI da instituição, mas também outros departamentos que trabalhem direta ou indiretamente com a informação. Outra sugestão pode ser a elaboração e aprovação de boas práticas de segurança da informação a serem adotadas por todos da instituição, ou ainda, a adoção de alguma norma ou metodologia já existente na área, lembrando que treinamentos periódicos são recomendados pela bibliografia (FONTES, 2006). Mas não se deve esquecer que todas estas medidas têm forte embasamento em um plano de segurança bem elaborado, tendo um gestor responsável por sua aplicação, manutenção e melhorias (ABNT ISO/IEC 27002, 2005). Vale lembrar que a norma NBR 17799/2005 é fortemente recomendada para elaboração de planos de segurança.

Tabela 03: Classificação dos resultados obtidos após o processo de conscientização

Ruim - de 0% a < 5%	**Regular - ≥ 5% a < 15%**	**Bom - ≥15%**

Referente	**Nível**	**Resultados obtidos**
Aspectos da Segurança da Informação – S. I.	**Bom**	20% dos funcionários passaram a conhecer os princípios da S. I.
Uso de *Logoff.*	**Bom**	20% dos funcionários passaram a realizar a trava do sistema.
Local para armazenar arquivos.	**Bom**	80% dos funcionários passaram a armazenar seus arquivos na rede após a criação da pasta.
Antivírus.	**Bom**	15% das máquinas que não possuíam antivírus passaram a tê-lo. Atingindo um resultado de 100%.
Regras para criação de senhas.	**Regular**	10% dos funcionários passaram a utilizar regras para a criação de senhas.
Frequência para realizar a troca de senhas.	**Regular**	10% dos funcionários que nunca trocavam suas senhas passaram a trocar bimestralmente.
Critérios dos funcionários em relação Segurança no local de trabalho.	**Regular**	5% dos funcionários melhoraram seus critérios em relação à Segurança no local de trabalho.
Backup.	**Regular**	5% dos funcionários passaram a realizar o *backup* sempre que exista uma nova atualização.
Controle de acesso de pessoas; Câmeras de segurança.	**Ruim**	0% ainda não existe nenhum tipo de controle de acesso de pessoas e nem câmeras de segurança no local.

Fonte: Autoria Própria (2014)

A Tabela 3 apresenta uma classificação dos resultados obtidos nas tabulações dos dois questionários. Os percentuais maiores ou iguais a 15% no

segundo questionário receberam Bom. Os percentuais maiores ou iguais a 5% e menores que 15% receberam a classificação Regular. Os percentuais menores que 5% receberam a classificação Ruim. Vale lembrar que a classificação Ruim é um resultado que independe da campanha feita pela autora, pois envolve aspectos financeiros. Alguns dos resultados que receberam a classificação Regular também envolvem aspectos financeiros, como por exemplo: o *backup*. Neste caso a mídia deve ser fornecida pela instituição. Os outros resultados que receberam a classificação Regular indicam a necessidade de se continuar com a campanha de conscientização, pois somente desta forma é que será possível estabelecer a cultura entre os funcionários do departamento, relacionada à Segurança da Informação.

5 REFERÊNCIAS

ABNT NBR 10520. **Trabalhos acadêmicos -** Citações em documentos. Rio de Janeiro, 2002.

ABNT NBR 6023. **Trabalhos acadêmicos -** Referências. Rio de Janeiro, 2002.

ABNT NBR 6028. **Trabalhos acadêmicos -** Resumo. Rio de Janeiro, 2003.

ABNT ISO/IEC 27002. **Tecnologia da informação –** Técnicas de segurança – código de práticas para gestão da segurança da informação. Rio de Janeiro, 2005.

ABNT NBR 14.724. **Trabalhos acadêmicos** - Rio de Janeiro, 2011.

ABNT NBR 6024. **Trabalhos acadêmicos -** Numeração progressiva das seções de um documento. Rio de Janeiro, 2012.

ABNT NBR 6027. **Trabalhos acadêmicos** - Sumário. Rio de Janeiro, 2012.

CARUSO, C. A. A., STEFFEN F. D. **Segurança em informática e de informações**. São Paulo: SENAC.1999.

CASTRO, R.A. de A. **Segurança e garantia da informação:** um estudo de caso em organização pública. Dissertação (Mestrado em Gestão do Conhecimento e Tecnologia da Informação). Mestrado em Gestão do Conhecimento e Tecnologia da Informação. Universidade Católica de Brasília, Brasília, 2011.

COBIT 4.1. **Governança de Tecnologia da Informação**. São Paulo. 2009.

DAMIANO, A.L. **As fraudes no Internet Banking e sua evolução para o Social Banking**. Dissertação (Mestrado em Engenharia de Produção). Escola de Engenharia de São Carlos, Universidade de São Paulo, São Carlos, 2013.

FERREIRA, F; ARAUJO, M. **Política de segurança da informação**. Rio de Janeiro: Ciência Moderna, 2006.

FONTES, E. **Praticando a segurança da informação**. Rio de Janeiro: Brasport, 2008.

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

MARTINS, J.C.C. **Gestão de Projetos de Segurança da Informação**. BRASPORT Livros e Multimídia Ltda. Rio de Janeiro-RJ: 2003.

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

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

Cartilha sobre segurança da informação <http://cartilha.cert.br/glossario/#e> (acessado em 19 de maio de 2014).

MACEDO, D. **Políticas de Segurança da informação**, 2012. Disponível em <http://www.diegomacedo.com.br/politicas-de-seguranca-da-informacao/> (acessado em 18 de abril de 2014).

Por que devo atualizar o antivírus?
<http://seguranca.uol.com.br/antivirus/duvidas/por-que-devo-atualizar-o-antivirus.html#rmcl>
(acessado em 20 de maio de 2014)

VIEIRA, R **Segurança Digital:** Crakers vs Hackers**.** 2012. http://www.egov.ufsc.br/portal/conteudo/seguran%C3%A7a-digital-crackers-x-hackers (acessado em 27 de maio de 2014**).**

6. APÊNDICES

APÊNDICE A - Modelo autorização para aplicação da pesquisa

AUTORIZAÇÃO

Cidade,___de _____de 2014.

Excelentíssimo Sr. XXXXXXX XXXXXX XXXXXXX

O meu nome é Katia Lois Somensari Cardoso, sou aluna da FATEC Americana, regularmente matriculada no curso de Segurança da Informação. Pelo presente solicito autorização para aplicação de um questionário que contém perguntas relativas à condição de Segurança da Informação do departamento **XXXXXXXXXXXXXX.** Esse questionário será utilizado como estudo de caso em meu trabalho de Conclusão de Curso que tem como tema: **XXXXXXXXXXX** e é orientado pela Profª Msc Maria Cristina Luz Fraga Moreira Aranha.

Ele será aplicado em duas fases. A 1ª fase consiste em verificar as principais falhas de segurança no departamento. Após a análise dos resultados pretende-se sugerir a aplicação de algumas medidas importantes na questão de segurança de informação. A 2ª fase do questionário consiste em reaplicar o questionário, após algum tempo de exercício das medidas de segurança sugeridas, para verificar se houve alguma modificação. A participação dos funcionários é voluntária e anônima, não sendo, portanto, solicitado nome em local algum. A cidade a que pertence à organização também não será divulgada.

Diante do exposto comprometo-me a aplicar os questionários, apenas depois de autorizada e estarei à disposição para prestar os esclarecimentos necessários. Desde já agradeço e elevo votos de estima e elevada consideração.

Atenciosamente,

Katia Lois Somensari Cardoso
Aluna FATEC Americana

- -

Sim, autorizo a aplicação do questionário.

_____
Assinatura da Chefia Local

APÊNDICE B – Questionário

QUESTIONÁRIO

Data ____/____/____

1- A disponibilidade, a integridade e a confidencialidade são principais aspectos da segurança da informação. Você já conhecia essa classificação?
( )SIM ( )NÃO

2- Em seu local de trabalho existem regras para a criação de senha? (por exemplo, a composição de uma senha segura deve conter letras maiúsculas, minúsculas, números e símbolos (, /, @, *, ., entre outros).
( )SIM ( )NÃO

3- Com qual frequência você realiza as trocas de suas senhas de e-mail, ou sistema:
( ) semanalmente
( ) quinzenalmente
( ) mensalmente
( ) semestralmente
( ) nunca

4- Ao ausentar-se do seu local de trabalho você realiza o logoff (trava) de sua área?
( )SIM ( )NÃO

5- Em seu computador de trabalho onde você costuma armazenar seus arquivos?
( ) Na área de trabalho
( ) Na pasta pública
( ) Na pasta meus documentos
( ) Rede

6- Em seu local de trabalho existe controle interno para entrada de pessoas?
( )SIM ( )NÃO

7- Em seu local de trabalho existem câmeras de segurança?
( )SIM ( )NÃO

8- Você considera o seu local de trabalho seguro a ponto de deixar objetos pessoais e/ou de valor em sua sala?
( )SIM ( )NÃO

9- Seu computador possui software antivírus?
( )SIM ( )NÃO

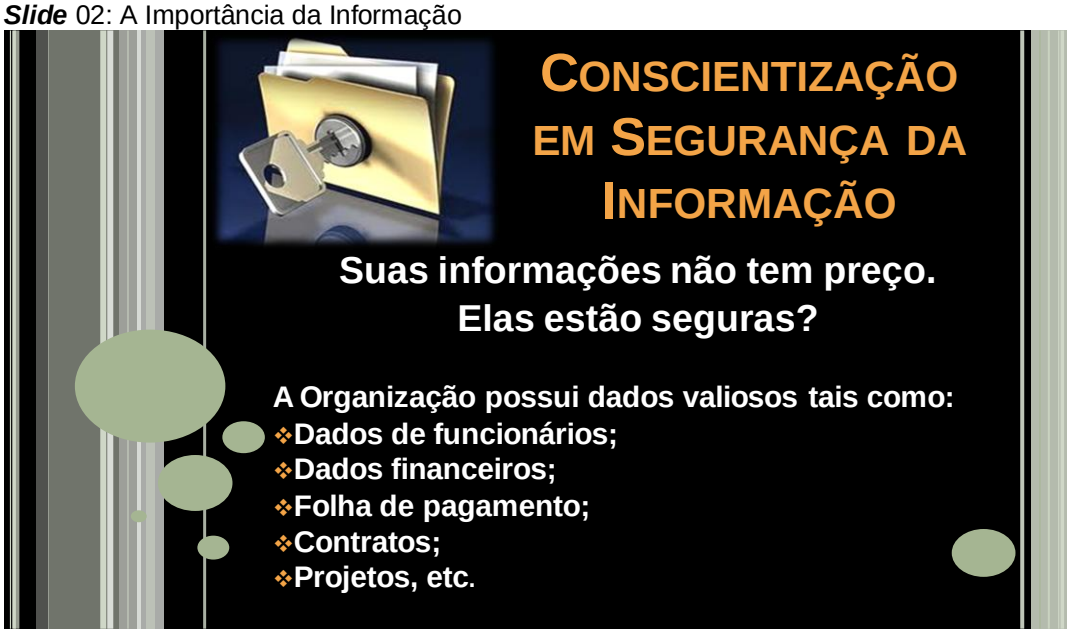
10- Você realiza o backup (cópia de segurança) de suas informações?
( ) Sim, semanalmente
( ) Sim, Mensalmente
( ) Sim, sempre que existe uma nova atualização
( ) Não, nunca

APÊNDICE C – *Slides*

Slide 01 – Introdução

Fonte: Autoria própria (2014).

Slide 02: A Importância da Informação

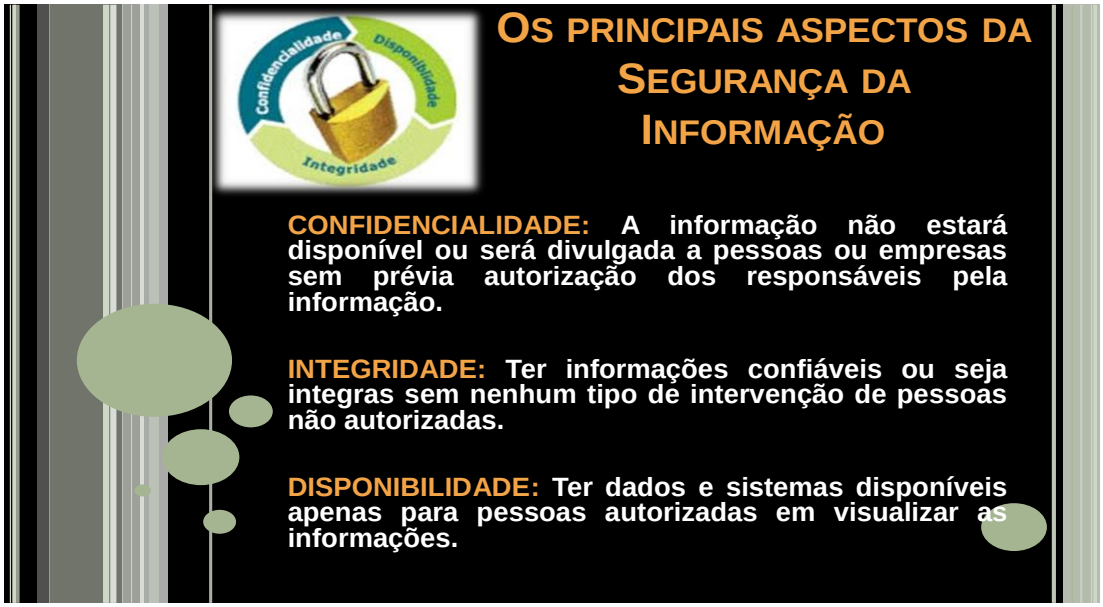


Fonte: Autoria própria (2014).

Slide 03: Segurança da Informação

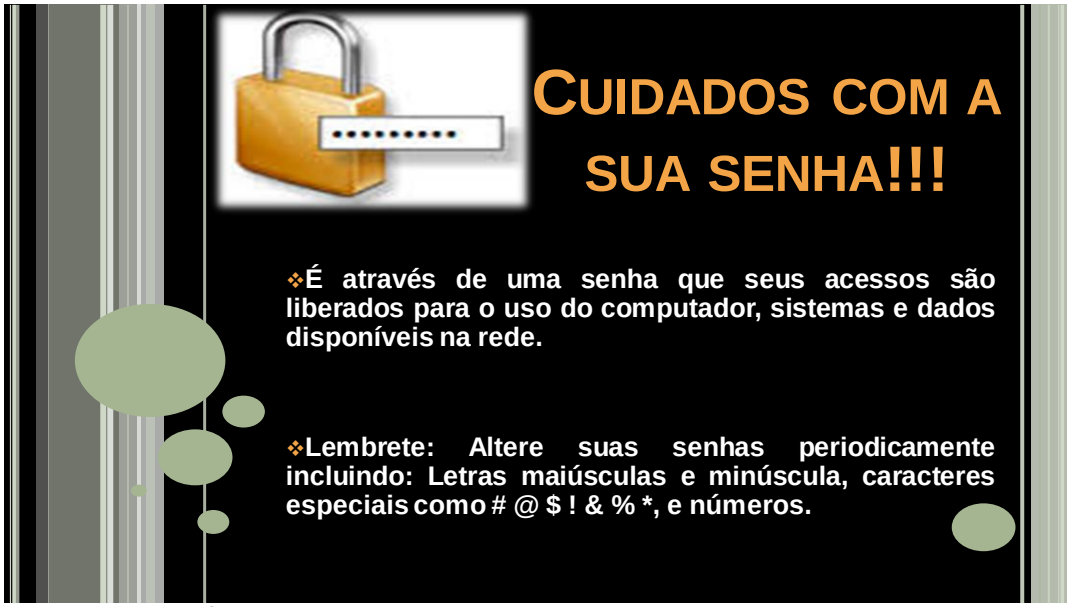
Fonte: Autoria própria (2014).

Slide 04: Principais Aspectos.



Fonte: Autoria própria (2014).

Slide 05: Senha

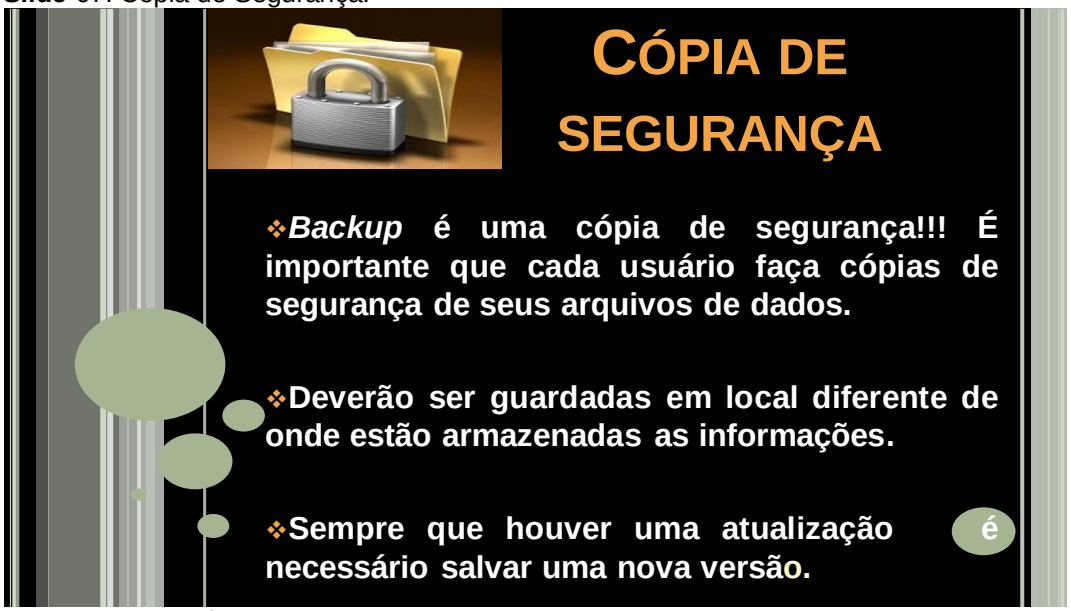


Fonte: Autoria própria (2014).

Slide 06: Senha

Fonte: Autoria própria (2014).

Slide 07: Cópia de Segurança.



Fonte: Autoria própria (2014).

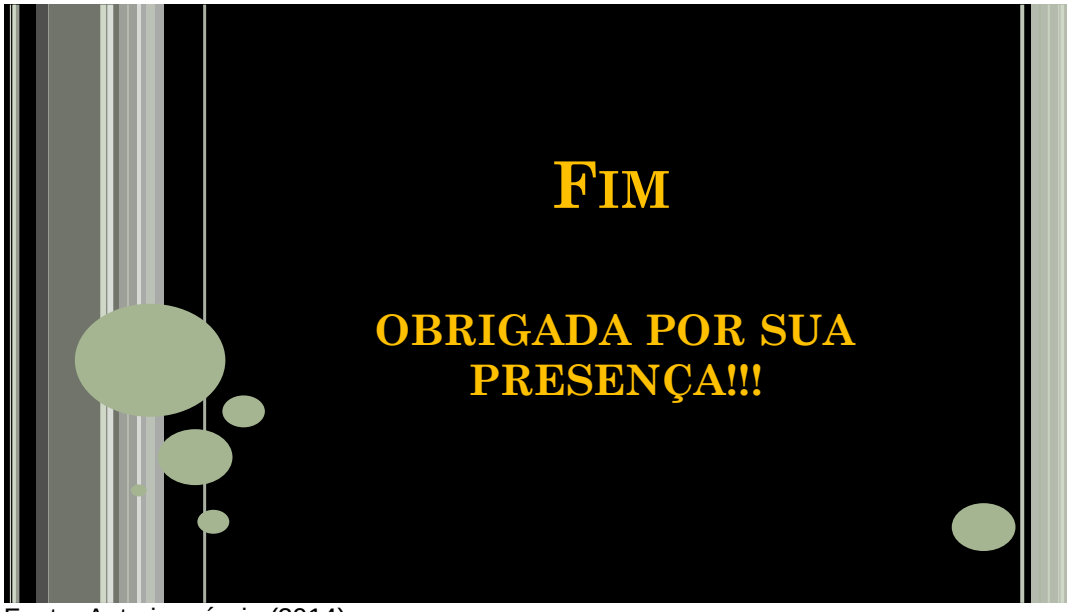
Slide 08: Antivírus.

Fonte: Autoria própria (2014).

Slide 09: Cuidados com a Área de Trabalho.

Fonte: Autoria própria (2014).

Slide 10: Final.



Fonte: Autoria própria (2014).

[9]

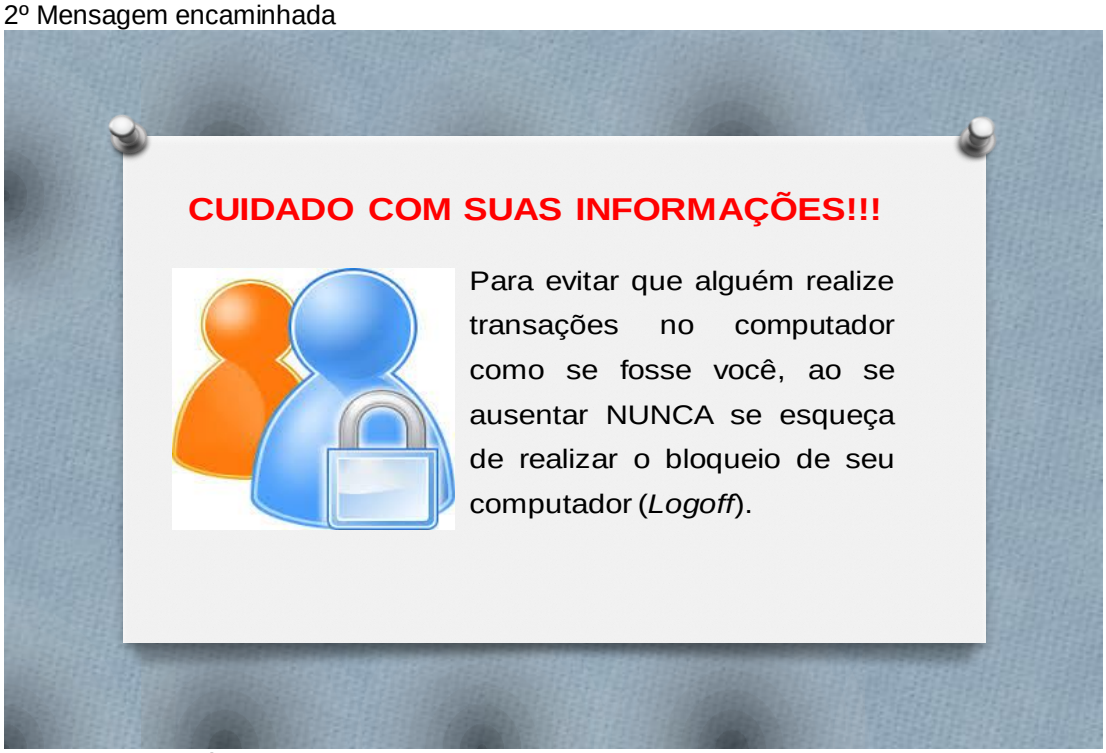
[9] Referência utilizada para elaboração dos Slides: Fontes (2006)

APÊNDICE D – Mensagens enviadas via *e-mail.*

1º Mensagem encaminhada

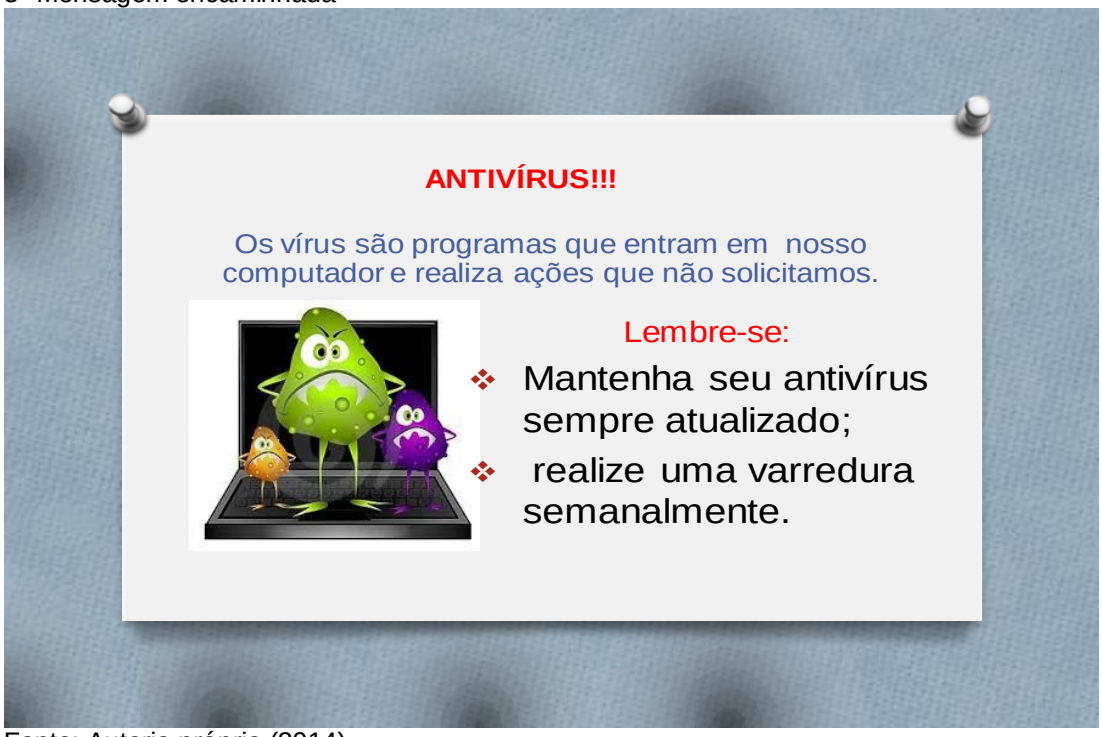
Fonte: Autoria própria (2014).

2º Mensagem encaminhada



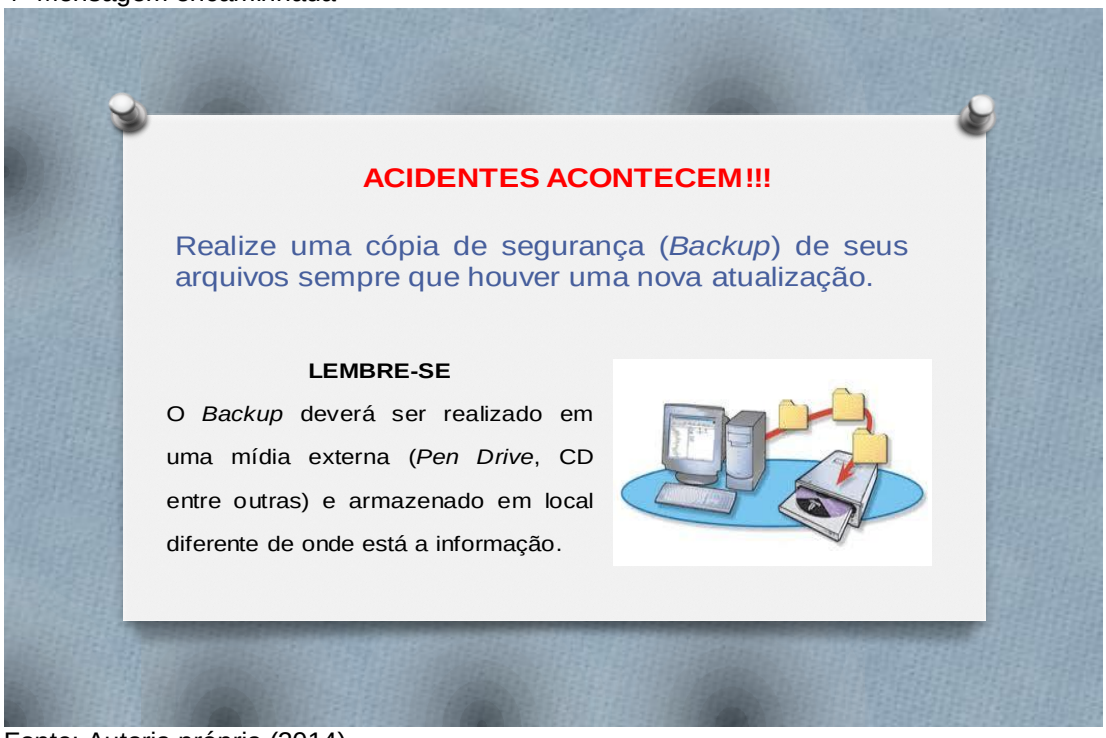
Fonte: Autoria própria (2014).

3º Mensagem encaminhada



Fonte: Autoria própria (2014).

4º Mensagem encaminhada



Fonte: Autoria própria (2014).
[10].

[10] Referência utilizada para elaboração da 1ª, 2ª, 3ª e 4ª mensagem via *e-mail*: Fontes (2006).

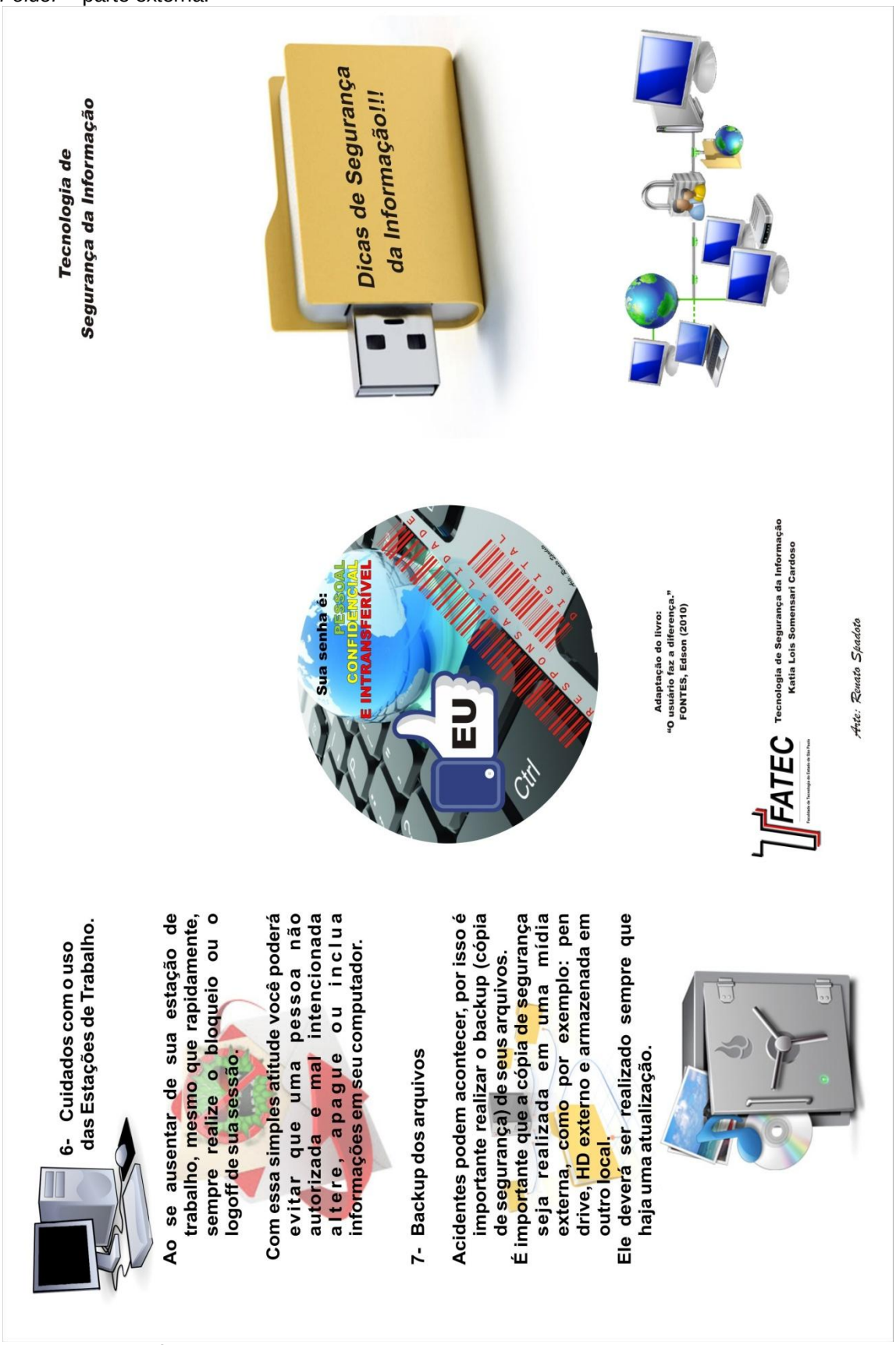
APÊNDICE E – *Folder*

Folder – parte interna

Fonte: Autoria própria (2014).

[11] Referência utilizada para elaboração do *folder*: Fontes (2006)

Folder – parte externa.



Fonte: Autoria própria (2014).