UNIVERSIDADE FEDERAL DO PARÁ

CAMPUS UNIVERSITÁRIO DE CASTANHAL

FACULDADE DE COMPUTAÇÃO

CURSO DE BACHARELADO EM SISTEMAS DE INFORMAÇÃO

MACARTHENY CARVALHO DE OLIVEIRA

FATORES HUMANOS – UMA PROPOSTA PARA IMPLEMENTAÇÃO DE PLANO DE CONSCIENTIZAÇÃO COM FOCO NAS VULNERABILIDADES HUMANAS DENTRO DE UMA EMPRESA

CASTANHAL-PA

2018

MACARTHENY CARVALHO DE OLIVEIRA

FATORES HUMANOS – UMA PROPOSTA PARA IMPLEMENTAÇÃO DE PLANO DE CONSCIENTIZAÇÃO COM FOCO NAS VULNERABILIDADES HUMANAS DENTRO DE UMA EMPRESA

Trabalho de Conclusão de Curso apresentado como exigência para obtenção do grau de Bacharel em Sistemas de Informação, pela Universidade Federal do Pará – UFPA.

Orientadora: Profª. Drª. Yomara Pires.

Coorientador: Profº. Me. Daniel da Silva Souza

Castanhal-PA

2018

MACARTHENY CARVALHO DE OLIVEIRA

FATORES HUMANOS – UMA PROPOSTA PARA IMPLEMENTAÇÃO DE PLANO DE CONSCIENTIZAÇÃO COM FOCO NAS VULNERABILIDADES HUMANAS DENTRO DE UMA EMPRESA

Trabalho de Conclusão de Curso apresentado como exigência para obtenção do grau de Bacharel em Sistemas de Informação, pela Universidade Federal do Pará – UFPA.

Banca Examinadora

Profª. Drª. Yomara Pires – ORIENTADORA

Faculdade de Computação (FACOMP) – UFPA – Castanhal

Prof. Me. Daniel da Silva Souza – COORIENTADOR

Prof. Me. Igor Ruiz Gomes

Faculdade de Computação (FACOMP) – UFPA – Castanhal

Profº. Drº. Tássio Costa de Carvalho

Faculdade de Computação (FACOMP) – UFPA – Castanhal

Castanhal, 13 de Julho de 2018

DEDICATÓRIA

Dedico este trabalho à memória de meu avô Adelício e à memória de minha amiga Cleide

AGRADECIMENTOS

Primeiramente, agradeço minha mãe, Rosa, que sempre me apoiou na minha caminhada acadêmica e tornou esse momento possível pelo seus esforços.

À minha esposa, Caroline, pelo companheirismo há tantos anos! Conhecimento compartilhado e pela filha linda que temos.

Gostaria de agradecer a Universidade Federal do Pará e aos meus mestres por todo conhecimento adquirido ao longo dos anos, principalmente aos orientadores Professora Drª. Yomara Pires e ao Professor Me. Daniel da Silva Souza.

RESUMO

Na era dos avanços tecnológicos, torna-se cada vez maior o número de crimes cibernéticos. As técnicas utilizadas por cibercriminosos são vastamente diversificadas, o que torna o combate a esses ataques uma tarefa árdua e contínua. As organizações, que são alvos recorrentes desses ataques, investem em tecnologias sofisticadas, entretanto acabam ignorando ou dando pouca importância aos fatores humanos, reforçando o fato de este ser o elo mais fraco da segurança. Neste contexto, esta monografia busca alertar sobre os riscos relacionados as vulnerabilidades humanas e destacar a engenharia social como uma das principais técnicas utilizadas para explorar estas vulnerabilidades e que, por ser uma prática que nem sempre faz uso de tecnologias para subtrair os ativos de seus donos ou responsáveis, acaba sendo subestimada. Desta forma, após realizados levantamentos e estudos voltados à segurança da informação, com base nas recomendações das ISO 27001 e 27002, foram desenvolvidos questionários sobre políticas de segurança da informação e aplicados à um grupo de funcionários de uma indústria do estado do Pará que, por motivos de segurança e privacidade, será chamada neste trabalho pelo nome fictício de Ômega S.A. Com a análise dos dados obtidos nesta atividade, foi possível ressaltar as vulnerabilidades humanas dentro da empresa e, assim, elaborar e propor a implementação de um plano de conscientização de segurança da informação para esta indústria.

Palavras-chave: Engenharia Social. ISO 27001. ISO 27002. Política de segurança da informação. Vulnerabilidades Humanas.

ABSTRACT

In the era of technological advances, becomes even greater the number of cyber crimes. The techniques used by cybercriminals are vastly diversified, what turns the combat to this attacks an arduous and continuous task. The organizations, that are recurring targets of this attacks, invest in sophisticated technologies, however, ended up ignoring or giving little importance to human factors, reinforcing the fact that these are the weakest link of the security. In this context, this monograph tries to alert about the risks related to human vulnerabilities and emphasize the social engineering as one of the main techniques used to explore these vulnerabilities, for being a practice that not always uses the technology to subtract assets from its owners and managers, end up being underestimated. Thus, after carried out a survey of studies about information security, based on the recommendations of ISO 27001 and 27002, were developed questionnaires about information security and applied to a group of employees of an industry from the Pará State that, for security and privacy reasons, will be called on this work by the fictitious name Ômega S.A. With the analyse of the data obtained in this activity, was possible to emphasize the human vulnerabilities into the company, and so, to elaborate and propose the implementation of an awareness plan of information security to this industry.

Keywords: Social Engineering. ISO 27001. ISO 27002. Information Security Politics. Human Vulnerabilities.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS

BS – *British Standard*

ISO – *International Standardization Organization*

PDCA – *Plan-Do-Check-Act*

IEC – *International Electrotechnical Commission*

ABNT – Associação Brasileira de Normas Técnicas

NBR – Norma Brasileira

T.I. – Tecnologia da Informação

DoS – *Denial Of Service*

DDoS – *Distributed Denial Of Service*

PSI – Políticas de Segurança da Informação

SGSI – Sistema de gestão da segurança da informação

SUMÁRIO

1. INTRODUÇÃO

Com a demanda de crescimento do setor industrial, é compreensível que este setor seja cada vez mais adepto às novas tecnologias da informação para auxiliar nas tarefas realizadas e, assim, otimizá-las. Ter acesso a várias informações em um dispositivo móvel, por exemplo, ao invés de buscar tais informações em arquivos físicos. Ter o controle e saber como administrar todas as informações relacionadas ao seus produtos desde o início do processo de produção até o produto final chegar ao cliente é de grande valia e a tecnologia da informação vem para adicionar no sentido de como estas informações serão mantidas, analisadas e eventualmente descartadas quando não forem mais úteis.

Pode-se afirmar que não é mais tão necessário ter espaços enormes para armazenamento de pastas com documentos de informações sobre clientes, especificações de produtos, rendimento mensal, relatórios de produção, folha de pagamentos dos funcionários, dentre diversas outras informações de grande importância. Todas estas informações podem ser armazenadas em *Hard Disk* (HD), *in cloud*, em servidores locais e tantas outras formas, reduzindo tempo e custos com manutenção de grandes espaços físicos para armazenar informações.

A tecnologia da informação, ou apenas T.I., possibilitou a redução do tempo para obter conjuntos de dados, maximizou a disponibilidade destes, proporcionou redução de gastos para tratar tais informações, dentre outros vários benefícios. Agilidade, praticidade, comodidade, economia são algumas das características que podemos atribuir ao uso da internet, intranet, data bases, enfim, uma infinidade de aplicações que a T.I. pode ter.

Desde que a T.I. surgiu vem alavancando o crescimento das empresas levando em consideração que é possível desenvolver análises sobre a produção mais rapidamente, apresentar demonstrativos mais precisos para investidores, atender de forma mais ágil os clientes, seja por meio de *e-mails* ou aplicativos de mensagens, como por exemplo apresentando conjuntos de informações solicitadas para um fechamento de um negócio.

Com isto, vê-se que as facilidades oferecidas pelo uso da tecnologia podem ser diversas, contudo, esta infinidade de material em forma digital está sujeito a uma enorme gama de ameaças físicas e/ou virtuais, que podem comprometer seriamente a integridade, disponibilidade e confiabilidade dos dados contidos nesse material

digital, sendo assim, para que esses dados tenham seus valores preservados faz-se necessário a conscientização de todos que são responsáveis por tais informações.

Sendo cientes da importância dos investimentos na segurança da informação, as empresas brasileiras atualmente seguem aumentando os investimentos em segurança da informação ano após ano, de acordo com um artigo publicado no O Globo (2015) o crescimento nos investimentos em segurança da informação crescem de 30 a 40% anualmente no Brasil, porém mesmo aumentando os investimentos ainda é muito difícil acompanhar a velocidade com que os criminosos aperfeiçoam seus golpes por meios virtuais ou físicos para ter acesso a esses dados.

O Brasil é um dos países mais afetados por crimes virtuais e grande parte do sucesso destes crimes é, de certo modo, facilitado por falhas no fator humano, que continua sendo o elo mais fraco de todo o mecanismo de segurança, devido a ideia inicial de que as maiores ameaças são voltadas ao *software* e não ao *peopleware*.

O foco principal deste trabalho é o fator humano que, por vezes, é tratado como um mero coadjuvante nas políticas de segurança da informação de diversas empresas e isto acaba tornando-se um grande erro de acordo com MITNICK (2003).

> "[...] Todos que acham que os produtos de segurança sozinhos oferecem a verdadeira segurança estão fadados a sofrer da ilusão da segurança, Esse é o caso de viver em um mundo de fantasia: mais cedo ou mais tarde eles serão vítimas de um incidente de segurança."

> "A medida que os especialistas contribuem para o desenvolvimento contínuo de melhores tecnologias de segurança, tornando ainda mais difícil a exploração de vulnerabilidades técnicas, os atacantes se voltarão cada vez mais para a exploração do elemento humano. Quebrar a "firewall humana" quase sempre é fácil, não exige nenhum investimento além do custo de uma ligação telefônica e envolve um risco mínimo."

Utilizar a engenharia social é mais comum do que pode-se imaginar e ao decorrer desta monografia, será detalhado mais sobre as formas de como é possível explorar de modo simples o fator humano e como essa prática deve ser combatida.

Desta forma, a presente pesquisa foca em apresentar a importância que deve ser dada ao fator humano nas políticas de segurança da informação em uma indústria em específico e, por motivos de confidencialidade, adotaremos o nome fictício de "Ômega S.A.", que será apresentada na seção 3.

Esta grande importância que o fator humano deve ter, é embasada em um levantamento bibliográfico que engloba a ISO/IEC 27001, ISO/IEC 27002, livros, monografias e artigos que tratam do assunto, dentre outras fontes.

1.1. Problemática

Há hoje uma tendência crescente das empresas brasileiras em investir em segurança da informação, contudo, é recorrente o fato de que acabam dando pouca ou nenhuma importância ao fator humano e a Ômega S.A não é exceção entre as demais empresas.

Analisando a situação atual da Ômega S.A. podemos concluir que a mesma possui inúmeros problemas relacionados à segurança da informação, desde câmeras de monitoramento inoperantes até ausência de *backups* de documentos importantes, e não consegue aplicar uma solução para tais problemas de forma eficiente, sendo boa parte destes problemas são relacionados a ausência de políticas de segurança da informação.

Na seção 3, serão detalhados todos estes problemas, a forma como os colaboradores e a gerência lidam com a segurança da informação, como esses problemas interferem no trabalho dos colaboradores da Ômega S.A. e se os colaboradores tem noção do valor das informações que tem acesso.

1.2. Objetivos Gerais

Esta monografia tem por finalidade propor um plano de conscientização para a Ômega S.A., sua gerência e colaboradores, alertando sobre a importância do fator humano na segurança da informação e como ele pode fragilizar qualquer política de segurança da informação, caso não haja os cuidados corretos com esses fatores humanos. É papel deste trabalho também apresentar sugestões sobre políticas de segurança para a Ômega S.A.

1.3. Objetivos Específicos

(a) Realizar levantamento da situação atual da indústria em relação ao fator humano e a segurança da informação;

(b) Analisar o comportamento dos colaboradores de todos os setores da indústria para melhor compreensão de como eles tratam a segurança da informação na situação atual da empresa;

(c) Elaboração do plano de conscientização de segurança da informação com foco no fator humano.

1.4. Organização da Monografia

Esta monografia está dividida em 5 seções, apresentadas com suas descrições a seguir:

A Seção 2 apresenta Fundamentação teórica, apresenta a conceituação teoria dos pontos importantes para o desenvolvimento desta monografia sob a perspectiva de vários autores, apresenta também as normas ISO, 27001 e 27002 que são de fundamental importância para a segurança da informação;

A Seção 3 apresenta o Estudo da metodologia aplicada, nesta seção são apresentadas as características da metodologia aplicada para coleta de dados necessárias para desenvolver a proposta dessa mamografia. Nessa seção também é apresentado a empresa que objeto desse estudo;

A Seção 4 apresenta os Resultados desse estudo que foram obtidos a partir de dados coletados de entrevistas em forma de questionários aplicados a um grupo de colaboradores da Ômega S.A. e a proposta de plano de conscientização para reduzir os riscos que os ativos da empresa são expostos;

Seção 5 apresenta a Conclusão deste trabalho explanando o que foi obtido ao termino da pesquisa.

2. FUNDAMENTAÇÃO TEÓRICA

Essa seção apresenta a fundamentação teórica coletada a partir de levantamento bibliográfico que foi utilizado como base para desenvolver este trabalho.

2.1. Informação

Informação é conceituada por WURMAN (1995, p. 43) como:

> "Informação deve ser aquilo que leva à compreensão [...] O que constitui informação para uma pessoa pode não passar de dados para outra. Se não faz sentido para você a denominação de informação não se aplica"

Segundo o Dicionário Aurélio de Português Online, informação pode ser definida como ato ou efeito de informar. Já para Dicio, Dicionário Online de Português, uma definição na informática que a informação possui é: reunião dos dados que, colocados num computador, são processados, dando resultados para um determinado projeto.

Sobre a informação a ISO/IEC 27002 afirma que o valor da informação vai além das palavras escritas, números e imagens. Conhecimento, conceitos, ideias e marcas são exemplos de formas intangíveis da informação. Em um mundo interconectado, a informação e os processos relacionados, sistemas, redes e pessoas envolvidas nas suas operações, são informações que, como outros ativos importantes, têm valor para o negócio da organização e, consequentemente, requerem proteção contra vários riscos.

A informação apresenta-se de diversas formas: e-mails, falada em conversas, manuscrita, fotografias, gráficos, números, vídeos, áudios dentre outras, e devem ser classificadas de acordo com sua importância. Assim, temos as informações públicas, internas, confidenciais e secretas. Wadlow (2000) expõe a necessidade desta classificação da informação em níveis de prioridade para cada empresa. Veja a seguir as definições para cada classificação:

- Informações públicas – Informações que podem ser expostas ao público sem consequências danosas. Manter sua integridade não é de fundamental importância;
- Informações internas – Informações que não devem ser acessadas com frequência, contudo caso aconteça o acesso não autorizado isto não causará a inoperância da empresa. Sua integridade é importante, mas não é vital;

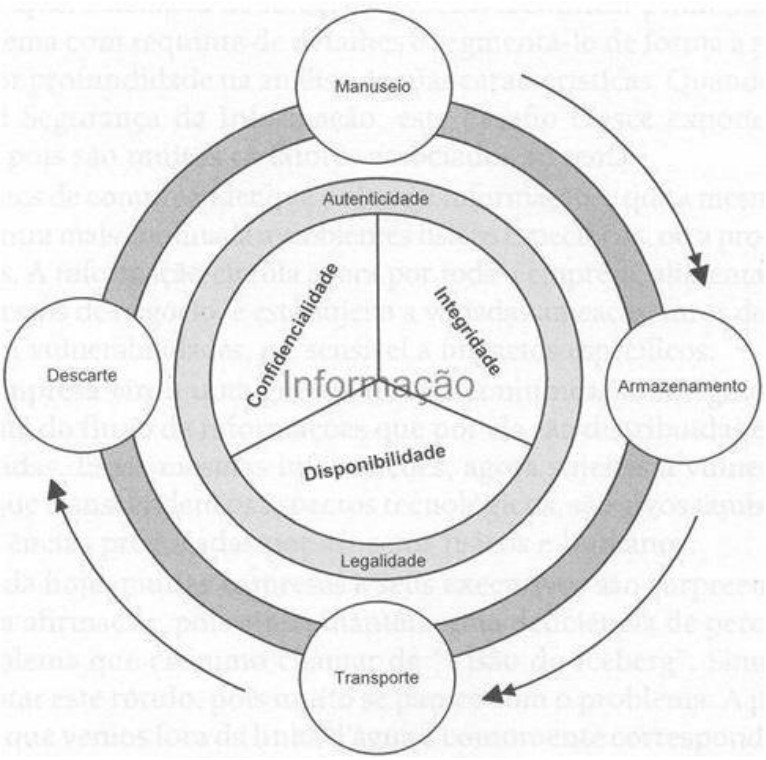
- Informações confidenciais – Informações que devem ser limitadas a empresa. Sua perda pode causar grandes problemas para a operação da organização, prejuízos financeiros, falta de credibilidade com clientes e grandes vantagens aos concorrentes;
- Informações secretas – Informações de fundamental importância para a empresa, deve ser limitada a um grupo extremamente pequeno de pessoas dentro da empresa. A violação destas informações pode gerar a inoperância da empresa e prejuízos inestimáveis.

Uma outra característica da informação é o seu ciclo de vida, a ISO 27002 considera que:

> "A informação tem um ciclo de vida natural, desde a sua criação e origem, armazenagem, processamento, uso e transmissão, até a sua eventual destruição ou obsolescência. O valor e os riscos aos ativos podem variar durante o tempo de vida da informação (por exemplo, revelação não autorizada ou roubo de balanços financeiros de uma companhia, é muito menos importante depois que elas são formalmente publicadas), porém a segurança da informação permanece importante em algumas etapas de todos os estágios.".

Para SÊMOLA (2003), o ciclo de vida da informação passa por apenas quatro etapas, representadas pela Figura 1:

Figura 1. Ciclo de Vida Informação



Fonte: SÊMOLA, 2003. Gestão da Segurança da Informação: uma visão executiva, 11.São Paulo: Campus.

- Manuseio – O instante em que uma informação qualquer é gerada e manipulada, podemos exemplificar isto como o momento em que após reunir alguns dados em uma planilha, são gerados gráficos que expressam os custos de produção de um determinado produto;
- Armazenamento – O instante em que informação é armazenada, independe da forma como ela é armazenada, por exemplo de forma escrita em um papel, em um banco de dados local, em mídias removíveis como *pendrives*, *Hard Disc* e etc.;
- Transporte – Instante que a informação é transportada, por exemplo, por mensagens de texto por *softwares* de mensagens instantâneas, por e-mails, por ligações via voz, vídeo conferencia e etc.
- Descarte – Instante em que a informação é eliminada, excluindo arquivos dos bancos de dados, do computador de mesa, picando arquivos impressos e etc.
- As informações necessitam de cuidados sem que nenhuma destas etapas do seu ciclo de vida sejam negligenciada pela segurança da informação.

2.2. Segurança da Informação

Existem inúmeras definições para segurança de informação, porém todas elas convergem para o mesmo sentido que consiste na proteção de conjuntos de dados pessoais ou empresariais, de acessos, modificações ou cópias sem autorização prévia. Para que assim seja assegurado o valor das informações.

De acordo com a ISO 27002 a segurança da informação é definida como:

> "Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio"

A segurança da informação se dá da seguinte forma:

> "A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados monitorados, analisados criticamente e melhorados, onde necessário, para garantir os objetivos do negócio e de segurança da organização sejam atendidos. Convém que isto seja feito em conjunto com outros processos de gestão do negócio.".

A segurança da informação tem grande relevância na criação de novas oportunidades de negócios, pois é ela que proporciona os princípios básicos para que as informações se mantenham confiáveis, disponíveis e íntegras. Sobre esses três princípios da segurança da informação:

- Confidencialidade – É o princípio da segurança da informação que assegura que a informação só será acessada por pessoas com prévia autorização, é importante salientar que o aspecto mais importante deste princípio é o de garantir a identificação de quem acessa tais informações.
- Disponibilidade – É o princípio da segurança da informação que assegura que as informações estejam disponíveis sempre que sua utilização seja necessária. Em uma indústria todos os processos são interligados, são dependentes um do outro, podemos exemplificar isto com uma liberação de uma carga que necessita de determinados documentos que devem acompanhar a carga e para que esses documentos sejam gerados as informações devem estar disponíveis no sistema da empresa, porém estas informações estão unicamente armazenados no sistema da empresa e esse sistema está passando por instabilidades e tais informações estão indisponíveis, isto pode gerar prejuízos a longo prazo, por conta da indisponibilidade de informações.
- Integridade – É o princípio da segurança da informação que assegura que as informações não sejam alteradas indevidamente, enquanto são armazenadas

ou transferidas entre um emissor e um receptor. Uma informação sem integridade pode comprometer toda uma cadeia produtiva, gerar custos extras e retrabalho, assegurar que a informação tenha integridade é fundamental.

2.2.1 Políticas de Segurança da Informação

De posse do conhecimento dos conceitos da segurança da informações, seguiremos para as políticas de segurança da informação, também referida como PSI. Afinal, o que são estas políticas de segurança da informação e qual seu objetivo? A PSI é um documento que contém um conjunto de orientações claras sobre as diretrizes a serem seguidas dentro de uma corporação por todos seus colaboradores com a finalidade de proteger os ativos, esse documento deve ser exposto a todos os colaboradores, deixando explicitada sua importância, sendo imprescindível para o bom funcionamento dos processos da corporação. Deve ser frisado que a direção deve apoiar sua implantação, pois sem tal apoio a PSI não apresenta os resultados que deveria.

A PSI deve estabelecer padrões para a utilização aceitável dos ativos da empresa, visando sempre a segurança dos mesmos, de acordo com CAMPOS (2007) “Atualmente, a PSI é adotada em grande parte das organizações em todo o mundo, inclusive no Brasil. Mesmo aquelas empresas que ainda não tem uma política efetiva, reconhecem a necessidade de elaborar e implementar uma” deixando clara a importância que a PSI tem dentro de uma organização.

As diretrizes da PSI devem ser baseadas nas recomendações propostas na norma ABNT NBR ISO 27002. Devem estar inclusos na PSI a forma como as informações devem ser utilizadas, manipuladas e descartadas após a perda de sua relevância, seguindo, é claro, a particularidade de cada corporação em relação a classificação de valores das informações e seu ciclo de vida. Para que a PSI seja implantada com sucesso, devem ser estabelecidos responsáveis por sua elaboração, divulgação interna e também para partes externas relevantes, monitoramento de seu funcionamento e revisão quando necessário for.

De acordo com a classificação das informações devem ser definidos níveis de acesso, onde são determinados quais informações estarão disponíveis para cada colaborador, de que forma estas informações serão acessadas e quando elas serão acessadas. Desta forma é bem mais simples identificar os responsáveis por quaisquer que sejam os danos causados a estas informações e então aplicar de

punições cabíveis, desde de que tais punições sejam previamente instituídas na PSI e com termos de sigilo e responsabilidade assinados pelos colaboradores.

Concluindo esse apanhado sobre a PSI, há a necessidade de estabelecer um tempo padrão para solucionar determinados incidentes para que haja um padrão de qualidade mínimo a ser atendido.

2.2.2 Ativos

De acordo com SOUSA (2013), ativos, de forma bem simples, são todas as coisas que tenham valor para a organização. Deste modo, ele classifica estes ativos da seguinte maneira:

a) Ativos de informação: Base de dados e arquivos, contratos e acordos, documentação de sistema, informações sobre pesquisa, manuais de usuário, material de treinamento, procedimentos de suporte ou operação, planos de continuidade do negócio, procedimentos de recuperação, trilhas de auditoria e informações armazenadas;

b) Ativos de software: Aplicativos, sistemas, ferramentas de desenvolvimento e utilitários;

c) Ativos físicos: Equipamentos computacionais, equipamentos de comunicação, mídias removíveis e outros equipamentos;

d) Serviços: Serviços de computação e comunicações, utilidades gerais, como aquecimento, iluminação, eletricidade e refrigeração;

e) Pessoas e suas qualificações, habilidades e experiências;

f) Intangíveis, tais como a reputação e a imagem da organização.

Devemos partir do pressuposto que todos os ativos tem determinada importância para os processos de uma corporação, pois por mais abundantes e baratos que possam parecer alguns destes ativos, estes devem ser mantidos em segurança. Vale salientar que alguns ativos merecem um nível de segurança maior de acordo com a classificação destes, a partir de um inventário de ativos, longe dos riscos que os cercam e que podem ocasionar falhas nos processos. Tais riscos podem ser classificados em três categorias: ameaças, vulnerabilidades e incidentes.

2.2.3 Ameaças

Para DIAS (2000), ameaça pode ser definida como “evento ou atitude indesejável (roubo, incêndio, vírus, etc.) que potencialmente remove, desabilita, danifica ou destrói um recurso”.

SÊMOLA (2003) afirma que as ameaças podem ser classificadas em grupos de acordo com sua intencionalidade:

- Naturais – São ameaças causadas por fenômenos naturais, tais como enchentes, terremotos, incêndios naturais, tempestade, etc.;
- Involuntárias – São ameaças causas pelo desconhecimento, também são causadas por acidentes, erros, falta de energia elétrica e etc.;
- Voluntárias – São ameaças propositais causadas por humanos como *crackers*, invasores, espiões, incendiários e etc.

Com o advento da *internet* as ameaças se tornaram mais recorrentes devido ao anonimato que esse ambiente proporciona. Teoricamente, um usuário da rede mundial de computadores pode se passar por qualquer pessoa desde que tenha aparato suficiente para tal tarefa e, neste ponto, o fator humano é bastante explorado pelos engenheiros sociais. Devido a esse problema é que em muitos casos é necessário a adoção de mecanismos como certificado eletrônico. A este respeito temos a figura 2 que ilustra esta situação a seguir:

Figura 2. Desindividualização na web

"On the Internet, nobody knows you're a dog."

Fonte: Web[1]

Para CAMPOS (2007) a ameaça é definida da seguinte forma:

> "A ameaça é um agente externo ao ativo de informação, que se aproveitando de suas vulnerabilidades poderá quebrar a confidencialidade,

[1] http://www.pensierocritico.eu/files/steiner.bmp

> integridade ou disponibilidade da informação suportada ou utilizada por esse ativo”

A partir desta definição podemos apresentar algumas das ameaças que são utilizadas para explorar o fator humano no contexto empresarial que em diversas situações acaba sendo uma das principais vulnerabilidades da segurança da informação. Vejamos a seguir algumas das ameaças:

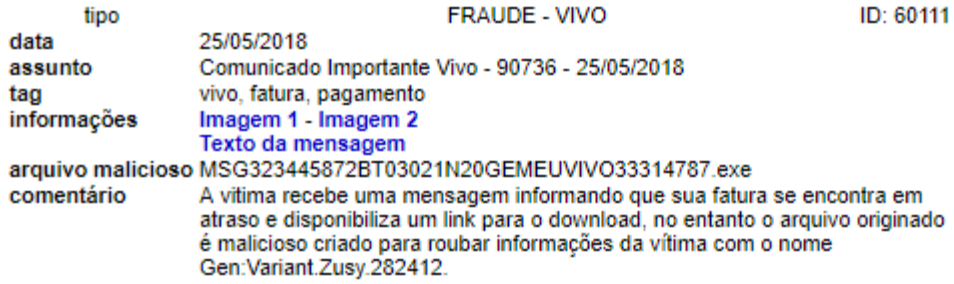
- Cavalos de Tróia – Os *Trojans* ou cavalos de Tróia que são encontrados com mais frequência são *Backdoors* e *Keyloggers*, respectivamente abrem portas para futuras invasões e roubam senhas. *Trojans* tem como características não possuírem capacidade de se multiplicar e exercem sua função anexados a arquivos como músicas, jogos e etc., no momento em que o programa ou arquivo que o *Trojan* está anexado, o mesmo é executado também. De acordo com ASSUNÇÃO (2002):

  > “Possui muitas características similares aos vírus, tais como: perde da arquivos, falhas na memória, erros em periféricos, etc. A grande diferença é que o trojan pode ser considerado um vírus inteligente, pois é controlado à distância pela pessoa que o instalou.”

- Spam – *Spam* de acordo com a central de proteção e segurança da *Microsoft* define-se como: qualquer tipo de comunicação online não desejada. É possível receber *spam* via *e-mail*, que é o mais comum, SMS, mensagens instantâneas e em redes sociais, como o *Facebook*. Há muitos relatos de *spam* via *WhatsApp* e *Telegram*. Os *spams* enchem as caixas de mensagens com promoções e anúncios, mas não apenas isto, alguns deles são parte de golpes para roubar informações como senhas de contas bancárias, outros apresentam boletos falsos para a vítima pagar sob falsas ameaças de ter seu nome colocado no SPC e/ou SERASA, dentre outros tipos de fraude.

Em seu site, a Rede Nacional de Ensino e Pesquisa (RNP) disponibiliza um catálogo atualizado de fraudes que vem armazenando informações destas fraudes desde o ano de 2008, que em sua maioria são *spams* disseminados via *e-mail,* vejamos um exemplo nas Figuras a seguir:

Figura 3. Fraude Vivo



tipo	FRAUDE - VIVO	ID: 60111
data	25/05/2018	
assunto	Comunicado Importante Vivo - 90736 - 25/05/2018	
tag	vivo, fatura, pagamento	
informações	Imagem 1 - Imagem 2 Texto da mensagem	
arquivo malicioso	MSG323445872BT03021N20GEMEUVIVO33314787.exe	
comentário	A vitima recebe uma mensagem informando que sua fatura se encontra em atraso e disponibiliza um link para o download, no entanto o arquivo originado é malicioso criado para roubar informações da vítima com o nome Gen:Variant.Zusy.282412.	

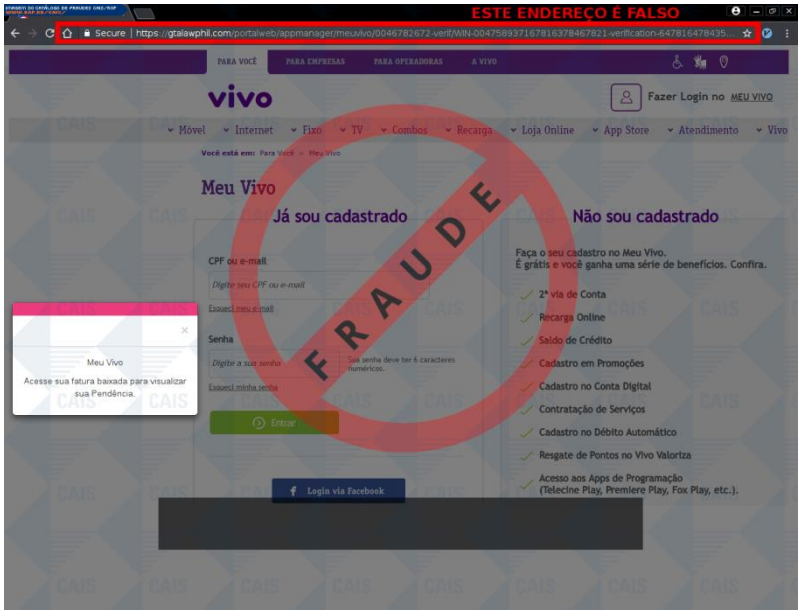
Fonte: Catálogo de fraudes RNP[2]

[2] https://www.rnp.br/servicos/seguranca/catalogo-fraudes

Figura 4. Fraude Vivo 2

Fonte: Catálogo de fraudes RNP[3]

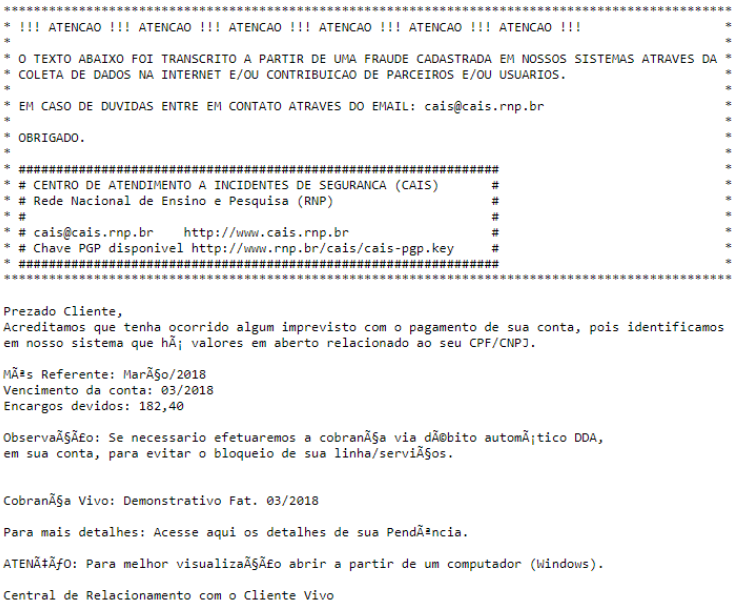
Figura 5. Fraude Vivo 3



Fonte: Catálogo de fraudes RNP[4]

[3] https://www.rnp.br/servicos/seguranca/catalogo-fraudes
[4] https://www.rnp.br/servicos/seguranca/catalogo-fraudes

Figura 6. Fraude Vivo Texto



```
*****************************************************************************************
* !!! ATENCAO !!! ATENCAO !!! ATENCAO !!! ATENCAO !!! ATENCAO !!! ATENCAO !!!           *
*                                                                                       *
* O TEXTO ABAIXO FOI TRANSCRITO A PARTIR DE UMA FRAUDE CADASTRADA EM NOSSOS SISTEMAS ATRAVES DA *
* COLETA DE DADOS NA INTERNET E/OU CONTRIBUICAO DE PARCEIROS E/OU USUARIOS.             *
*                                                                                       *
* EM CASO DE DUVIDAS ENTRE EM CONTATO ATRAVES DO EMAIL: cais@cais.rnp.br                *
*                                                                                       *
* OBRIGADO.                                                                             *
*                                                                                       *
* ############################################################                          *
* # CENTRO DE ATENDIMENTO A INCIDENTES DE SEGURANCA (CAIS)       #                      *
* # Rede Nacional de Ensino e Pesquisa (RNP)                     #                      *
* #                                                            #                        *
* # cais@cais.rnp.br    http://www.cais.rnp.br                 #                        *
* # Chave PGP disponivel http://www.rnp.br/cais/cais-pgp.key     #                      *
* ############################################################                          *
*****************************************************************************************

Prezado Cliente,
Acreditamos que tenha ocorrido algum imprevisto com o pagamento de sua conta, pois identificamos
em nosso sistema que hÃ¡ valores em aberto relacionado ao seu CPF/CNPJ.

MÃªs Referente: MarÃ§o/2018
Vencimento da conta: 03/2018
Encargos devidos: 182,40

ObservaÃ§Ã£o: Se necessario efetuaremos a cobranÃ§a via dÃ©bito automÃ¡tico DDA,
em sua conta, para evitar o bloqueio de sua linha/serviÃ§os.


CobranÃ§a Vivo: Demonstrativo Fat. 03/2018

Para mais detalhes: Acesse aqui os detalhes de sua PendÃªncia.

ATENÃ‡ÃƒO: Para melhor visualizaÃ§Ã£o abrir a partir de um computador (Windows).

Central de Relacionamento com o Cliente Vivo
```

Fonte: Catálogo de fraudes RNP[5]

2.2.4 Vulnerabilidades

Vulnerabilidades representam pontos de potenciais falhas em um sistema, sabendo que nenhum ambiente computacional é totalmente seguro e, com isto, é comum que sejam encontradas vulnerabilidades nas medidas de segurança implantadas nas organizações.

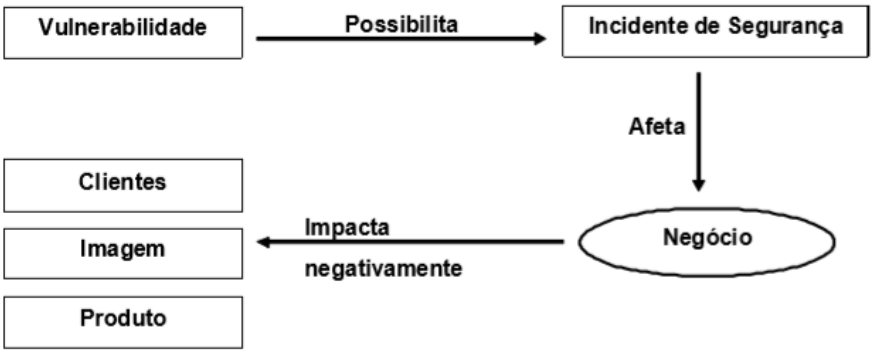
De acordo com MARCIANO (2001):

> "Uma vulnerabilidade representa um ponto potencial de falha, ou seja, um elemento relacionado à informação que é passível de ser explorado por alguma ameaça - pode ser um servidor ou sistema computacional, uma instalação física ou, ainda, um usuário ou um gestor de informações consideradas sensíveis."

E LAUREANO (2005) destaca que a vulnerabilidade acaba sendo a causa maior dos incidentes de segurança, "cada vulnerabilidade existente pode permitir a ocorrência de determinados incidentes de segurança. Desta forma, podemos concluir que são as vulnerabilidades as principais causas das ocorrências de incidentes de segurança". Veja o exemplo na figura 7:

[5] https://www.rnp.br/servicos/seguranca/catalogo-fraudes

Figura 7. Relação vulnerabilidade e incidente de segurança



Fonte: (LAUREANO, 2005)

Como podemos observar na figura 7, as vulnerabilidade possibilitam a ocorrência de incidentes da segurança que, consequentemente, afetam os negócios da empresa, reduzindo a credibilidade da empresa e de seus produtos perante o cliente.

2.2.5 Incidente de Segurança

A Superintendência de Tecnologia da Informação e Comunicação da Universidade Federal do Rio de Janeiro - (TIC-UFRJ) (2018) define um incidente de segurança deste modo:

> "Um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação levando a perda de um ou mais princípios básicos de Segurança da Informação: Confidencialidade, Integridade e Disponibilidade."

Podemos exemplificar alguns incidentes como:

- Ataques *DDoS* e *DoS*;
- Acessos não autorizados a dados ou sistemas;
- Falhas em sistemas computacionais.

Segundo o CERT.br (Grupo de Resposta a Incidentes de Segurança para a Internet no Brasil) o ano de 2017 apresentou crescimento em incidentes da segurança em relação a 2016. Esses incidentes foram divididos por categoria, onde as notificações de páginas falsas que não envolvem bancos nem comercio eletrônico subiram 6%, ataques a servidores web tiverem um aumento de 10% e propagação de worms apresentou um aumento de 60%.

Segundo o AVAST (2018), é importante informar que esses worms se disseminam através de anexos de e-mail, compartilhamento de arquivos e links a sites maliciosos e todas estas formas de disseminação destes worms acabam sendo executadas por pessoas, evidenciando assim a vulnerabilidade causada pelo fator humano.

2.2.6 Fator Humano

Para o Diretor Geral da SearchInform no Brasil, Vladimir Prestes, a proteção dos dados das empresas são baseadas em componentes técnicos e o fator humano. Ele afirma que há uma tendência cada vez maior de focar no indivíduo e isto é evidenciado pela criação de diversas ferramentas de análise de comportamento de usuários, como por exemplo o UEBA, que em tradução literal significa Análise Comportamental de Usuários e Entidade. As UEBAs basicamente utilizam algoritmos e estatísticas de análises para detectar anomalias no comportamento humano, que podem oferecer ameaças à segurança da informação.

De acordo com o texto de Vladimir Prestes (2018), as ameaças estão divididas em ameaças tecnológicas e ameaças humanas, estas ameaças podem ser combatidas de forma automatizada por proteção antivirus, proteção contra ataques direcionados, dentre outras soluções especializadas. Estas ameaças tecnológicas são menos complexas de se combater, pois elas seguem um determinado padrão que a lógica do computador reconhece e pode tomar decisões automaticamente para bloquear tais ameaças. Já contra as ameaças humanas em TI não existem proteções totalmente automatizadas, comumente estas ameaças tem de ser enfrentadas utilizando a combinação de soluções especializadas e medidas administrativas, como por exemplo capacitação técnica para os colaboradores e regulamentos específicos para a manipulação de informações críticas para os negócios da empresa.

Investir grandes quantias de dinheiro apenas em soluções especializadas, para prevenir ameaças tecnológicas não garante a segurança completa, na verdade não existem nenhum método que seja totalmente eficiente que assegure total segurança, contudo a melhor opção é de fato investir em soluções para combater tanto ameaças humanas, quando as tecnológicas reduzindo assim ao máximo os riscos a informações.

MITNICK (2003) diz que é natural achar que é improvável ser vítima de alguma trapaça até que se tenha algum motivo para pensar de forma diferente. Comumente, apesar de fazemos uma análise da situação para termos uma noção dos riscos, acabamos em muitas situações dando o benefício da dúvida. Ainda segundo ele, deveríamos seguir o conselho de nossos pais e não confiar em estranhos principalmente em locais de trabalho.

É explorando esse benefício da dúvida, oferecido geralmente por pessoas que nunca passaram por experiências negativas com situações onde elas tenham sido lesadas, principalmente financeiramente, é que os engenheiros sociais agem, vejamos um exemplo que pode ocorrer dentro de uma empresa que não possui procedimentos de segurança focados no usuário: Um engenheiro social faz uma ligação para algum departamento de uma empresa, solicitando quaisquer que sejam as informações afirmando que se trata de um pedido de um membro da gerência, informando o nome deste tal membro, normalmente por uma questão de hierarquia e também por ser normal a troca de determinadas informações entre setores distintos, estas informações acabam caindo em mãos erradas e nestas situações é que entendemos a importância da classificação da informação e do treinamento dos colaboradores em relação a segurança da informação.

A ameaça humana é evidenciada por MITNICK (2003) quando diz que nenhum sistema computacional é totalmente automatizado e deve haver pelo menos um humano que tem acesso a ele, com isto caso o atacante (entende-se como atacante aquele indivíduo que pretende invadir um sistema ou manipular alguém que possua acesso ao sistema ou a informações especificas para utilização indevida e não autorizada) possua métodos para manipular esta pessoa é fato que nenhuma forma de segurança automatizada será capaz de detê-lo. Seja lá qual for a forma com que o atacante faça uso, o fator humano sempre acaba sendo o elo mais fraco da segurança tornando-se o alvo principal.

Por mais que existam diversos mecanismos de segurança, sem a existência de treinamentos e planos de conscientização, o colaborador ver tudo relacionado a segurança da informação apenas como mais burocracias que atrasam seu trabalho e torna-se um colaborador desmotivado que continuará realizando suas tarefas de forma que ofereça riscos para a segurança da informação daquela empresa.

Podemos associar a vulnerabilidade humana diretamente aos sentimentos do indivíduo. Em seu livro “Segredos do Hacker Ético” ASSUNÇÃO (2008) afirma que o

engenheiro social tem a capacidade de manipular sentimentos para que assim seus alvos causem falhas no sistema, abram brechas na segurança ou simplesmente acabem disponibilizando informações de forma involuntária, sem ter conhecimento de sua importância. Ele ainda cita alguns destes sentimentos, vejamos:

- Curiosidade – Existem inúmeros golpes possíveis que podem ser aplicados aproveitando da curiosidade humana, esta curiosidade é natural e muito comum, pois boa parte de nós é curioso porém nem sempre ela nos ajuda. Por exemplo, um golpe muito utilizado até hoje são *e-mails* ou mensagens de texto informando que a pessoa ganhou determinado prêmio e para resgatar esse prêmio é necessário ligar para um determinado número ou acessar um *link* específico, onde a vítima acaba abrindo os *links* e, caso sejam abertos na empresa que esta vítima trabalha certamente esta empresa ficará vulnerável, pois nesses *links* encontram-se vírus, *trojans, keyloggers* e etc. Por telefone, as vítimas acabam entregando informações que podem ser desde informações pessoais, até as informações das empresas que trabalham, dependendo apenas da criatividade do engenheiro social de desenvolver o golpe;
- Confiança – A confiança acaba sendo utilizada para aplicar golpes do seguinte modo: o engenheiro social pode se passar por um funcionário da empresa, bastando ter conhecimentos específicos sobre procedimentos internos e assuntos que deveriam estar restritos apenas ao ambiente da empresa, gerando assim uma sensação de segurança na vítima. O engenheiro social pode por exemplo utilizar ferramentas como e-mails, ligações ou mensagens expressas se passando por um gerente, dizendo que trocou de número de telefone por algum motivo e necessita de uma determinada informação, se tratando de uma pessoa de um cargo importante dificilmente será questionado e receberá as informações que necessita;
- Simpatia – Engenheiros sociais possuem facilidade com relações interpessoais, de modo que ganham a simpatia de qualquer um. Oferecem ajuda, são prestativos e, assim, deixam suas vítimas com a guarda baixa, pois quem iria suspeitar de alguém tão simpático, não é mesmo? Um exemplo poderia ser uma ligação de um engenheiro social se passando por um colega de trabalho de outro setor da empresa ou de uma filial, informando um possível erro nos dados recebidos pela vítima, sendo necessária uma

confirmação de quais dados teriam sido enviados, para ‘garantir’ que tudo estivesse bem;

- Culpa – Fazer com que alguém se sinta culpado geralmente faz com que a mesma tente de algum modo compensar sua culpa. Um engenheiro social tendo conhecimento sobre clientes de uma determinada empresa pode mandar e-mails falsos informando sobre dados errados de determinado produto que foram enviados, em anexo um falso documento que supostamente foi enviado pela vítima para a tal empresa do cliente. Certamente a vítima irá abrir os anexos para ver do que se trata, para tentar corrigir seu suposto erro antes de causar consequências mais graves para ela;
- Medo – A manipulação do medo tem retorno para o engenheiro social, bem mais rápido que a manipulação dos demais sentimentos, pois as ameaças feitas nesta abordagem parecem vir de alguém de um nível hierárquico bem maior que o da vítima, dentro da empresa. Deixando a vítima com um nível de estresse alto, sem raciocinar muito bem em frente a uma eminente situação em que pode perder seu emprego.

Estes sentimentos que citou-se até o momento são alguns dos que podem ser explorados pela engenharia social, mas outros autores identificam tantos outros sentimentos que podem fazer com que o próprio colaborador realize ataques aos bancos de dados, cause erros nos sistemas, altere dados sem permissão ou simplesmente façam uso inapropriado dos dados. O próprio colaborador insatisfeito, desmotivado ou desvalorizado pela empresa pode ser causador de ameaças que podem ser classificadas como voluntárias ou involuntárias.

2.2.7 Engenharia Social

Mas afinal, o que seria a tal engenharia social de que tanto falamos até aqui? Na visão da segurança da informação MITNICK (2003) diz que:

> “A engenharia social usa a influência e a persuasão para enganar as pessoas e convencê-las de que o engenheiro social é alguém que na verdade ele não e, ou pela manipulação. Como resultado, o engenheiro social pode aproveitar-se das pessoas para obter as informações com ou sem o uso da tecnologia”.

Já para a Central de Proteção e Segurança da *Microsoft* a engenharia social é definida da seguinte forma:

> “A engenharia social é uma forma pela qual os criminosos ganham acesso ao seu computador. O objetivo da engenharia social é, geralmente,

> instalar spyware ou outro software mal-intencionado ou induzi-lo a entregar suas senhas ou outras informações confidenciais pessoais ou financeiras”

Em outras palavras, o engenheiro social nem sempre se dá ao trabalho de fazer uso de tecnologias avançadas para quebrar criptografias, invadir bancos de dados, sistemas ou bloquear serviços, ele simplesmente usa sua persuasão e capacidade de manipular suas vítimas para conseguir as informações valiosas. MITNICK (2003) afirma que:

> “Na maioria dos casos, os engenheiros sociais bem-sucedidos têm uma habilidade muito boa em lidar com as pessoas. Eles são charmosos, educados e agradam facilmente — os traços sociais necessários para estabelecer a afinidade e confiança.”

Na figura 9 a seguir, vemos uma representação das características de um engenheiro social, de acordo com o livro Governança da Segurança da Informação:

Figura 8. Perfil do Engenheiro Social

Fonte: Governança da Segurança da Informação 1ª edição[6]

Uma pessoa com características apresentadas na Figura 8, quase nunca levantará suspeitas e, muitas vezes, alcançará seu objetivo, coletando informações sem que a vítima nem ao menos se dê conta que foi manipulada.

Existe uma infinidade de técnicas que podem ser utilizadas pelo engenheiro social e ao longo dos anos elas vão sendo aprimoradas e moldadas para cada situação. Podemos listar algumas destas técnicas que são amplamente utilizadas, vejamos:

[6] http://mauriciolyra.pro.br/site/wp-content/uploads/2016/02/Livro-Completo-v4-para-impressão-com-ISBN.pdf

- *Spoofing* – Esta técnica se apresenta em diversas formas distintas, existe o *spoofing* de número de telefone, *spoofing* de *IP*, *spoofing* de *e-mail*, *spoofing* de *DNS*, esses são os mais conhecidos e todos eles tem o mesmo objetivo, se passar por alguém ou algo que não são para disseminar *malwares* ou contornar controles de acesso;
- *Phishing* (Pescaria) – Normalmente esta técnica é utilizada na forma de e-mails ou mensagens expressas, como *Whatsapp* onde o atacante envia mensagens que aparentam ser verdadeiras, solicitando acessar um determinado *site* com *link* na própria mensagem, quando a pessoa acessa esses links, ela é direcionada a um *site* falso bem semelhante com o original, com algum tipo de cadastro a ser realizado. Assim é possível obter senhas, dados pessoais e etc.;
- *Shoulder Surfing* (Espiar sobre os ombros) **–** Esta técnica consiste simplesmente em colher informações que a vítima está acessando na tela de um computador, *tablet*, entre outros dispositivos ou até mesmo em documentos em formato físico que se encontram nas mãos da vítima;
- *Dumpster Diving* – É técnica que busca encontrar informações valiosas no lixo físico, tendo conhecimento que nem sempre documentos, anotações e coisas do tipo são descartados de modo inadequado o engenheiro social pode fazer uso desta técnica;
- *Eavesdropping* – Engenheiros sociais são observadores, esta técnica consiste em reunir informações de forma não autorizada a partir de telefonemas, vídeos, ouvir conversas, ler e-mails.

Ataques de engenheiros sociais podem ter seu nível de sucesso reduzido, mas não anulado com o desenvolvimento de programas, planos ou campanhas de conscientização e treinamentos de pessoal para que assim seu conhecimento técnico seja elevado, possibilitando o reconhecimento não apenas das técnicas utilizadas na engenharia social apresentadas aqui, mas um conjunto bem mais extenso e diversificado.

2.2.8 ISO/IEC 27001

A ISO 27001 faz parte da família ISO 27000 e é a mais conhecida delas. Esta família possui mais de 40 normas internacionais que são relacionadas com a segurança da informação, a primeira versão da ISO 27001 foi criada em 2005 sendo

baseada na norma britânica BS 7799-2, sua versão mais atual é de 2013 deste modo seu título completo agora é ISO/IEC 27001:2013.

Esta ISO tem por finalidade prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um sistema de gestão da segurança da informação (SGSI) em uma organização, isto permite uma proteção mais eficiente dos dados da organização, minimizando as possibilidades dos mesmos serem acessados de forma não autorizada.

A ISO 27001 pode ser implementada em qualquer organização, pública ou privada, comerciais ou sem fins lucrativos adaptando-se a realidade da organização. Ela adota o modelo PDCA que é utilizado para estruturar os processos do SGSI, pois a SGSI é abrangente tendo que gerir segurança em TI, recursos humanos, proteção física dentre outros. Quando esta ISO é implementada em uma organização existe a possibilidade de obter certificação e esta certificação significa que um organismo certificador independente confirmou que a organização está em conformidade com a ISO 27001. A Advisera pontua algumas das vantagens de se implantar a ISO 27001:

- Conformidade com requisitos legais – Com a implementação da ISO 27001, a organização consequentemente atende a requisitos contratuais, leis e regulamentações relacionadas à segurança da informação;
- Obter vantagens de marketing – Possuir a certificação ISO 27001, pode representar um diferencial de mercado em relação aos concorrentes;
- Reduzir custos – A filosofia desta ISO é prevenir incidentes da informação, se os incidentes são prevenidos, consequentemente não são gerados custos. Independente se os incidentes são grandes ou pequenos, sempre geram custos;
- Melhor organização – Com frequência as organizações crescem, mas seus processos e procedimentos acabam não sendo definidos o que torna o trabalho do colaborador mais complicado, pois muitas vezes não se sabe o que necessita ser executado, quando, nem por quem. A implementação da ISO 27001 faz com que os principais processos da organização sejam descritos em documentos, que tornando os processos mais claros, facilitando a compreensão do colaborador sobre quais tarefas devem ser realizadas por ele e quando estas tarefas devem ser executadas, assim reduzindo seu tempo ocioso.

A ISO 27001 possui 11 seções e Anexo A, estas seções são: introdução, escopo, referência normativa, termos e definições, contexto da organização, liderança, planejamento, apoio, operação, avaliação do desempenho, melhorias e o Anexo A que disponibiliza 114 controles distribuídos em 14 seções. Para esse trabalho é levado em conta que não temos por finalidade uma certificação para a empresa nesse momento, então faremos uso principalmente da seção 7 Apoio, mais especificamente 7.3 Conscientização que apresenta o seguinte:

> Pessoas que realizam trabalho sob o controle da organização devem estar cientes da:
>
> a) política de segurança da informação;
>
> b) suas contribuições para a eficácia do sistema de gestão da segurança da informação, incluindo os benefícios da melhoria do desempenho da segurança da informação; e
>
> c) implicações da não conformidade com os requisitos do sistema de gestão da segurança da informação.

2.2.9 ISO/IEC 27002

A ISO 27002 é o antigo padrão 17799:2005 que, por sua vez, tem por base a norma britânica BS 7799-1, a ISO 27002 assim como a 27001 também faz parte da família da 27000 que é um conjunto de diversas normas relacionadas ao escopo da segurança da informação. A ISO 27002 é a única da família 27000 que possibilita a certificação de um profissional e não de uma organização; observando o título da mesma podemos logo notar qual o seu objetivo, ISO/IEC 27002:2013 Boas práticas para gestão de segurança da informação. Recomenda-se utilizar a ISO 27001 em conjunto com a 27002, porém mesmo se a organização não possuir interesse em ser auditada na ISO 27001, pode seguir as boas práticas apresentadas na 27002.

De acordo com a própria ABNT NBR ISO 27002:2013:

> Esta Norma é projetada para as organizações usarem como uma referência na seleção de controles dentro do processo de implementação de um sistema de gestão da segurança da informação (SGSI), baseado na ABNT NBR ISO/IEC 27001 ou como um documento de orientação para as organizações implementarem controles de segurança da informação comumente aceitos. Organizações de todos os tipos e tamanhos (incluindo o setor privado e público, organizações comerciais e sem fins lucrativos), coletam, processam, armazenam e transmitem informações em diferentes formatos, incluindo o eletrônico, físico e verbal (por exemplo, conversações e apresentações).

Nesta monografia será utilizada uma das 14 seções desta norma, a seção 7, em especifico a 7.2.2 Conscientização, educação e treinamento em segurança da informação:

Controle

Convém que todos os funcionários da organização e, onde pertinente, partes externas devem recebam treinamento, educação e conscientização apropriados, e as atualizações regulares das políticas e procedimentos organizacionais relevantes para as suas funções.

3 METODOLOGIA DE PESQUISA

A metodologia utilizada é a pesquisa exploratória definida por (SELLTIZ et al., 1967, p.63, apud GIL, 2002) da seguinte forma:

> "Estas pesquisas têm como objetivo proporcionar maior familiaridade com o problema, com vistas a torná-lo mais explícito ou a constituir hipóteses. Pode-se dizer que estas pesquisas têm como objetivo principal o aprimoramento de ideias ou a descoberta de intuições. Seu planejamento é, portanto, bastante flexível, de modo que possibilite a consideração dos mais variados aspectos relativos ao fato estudado. Na maioria dos casos, essas pesquisas envolvem: (a) levantamento bibliográfico; (b) entrevistas com pessoas que tiveram experiências práticas com o problema pesquisado; e (c) análise de exemplos que "estimulem a compreensão""

Considerando a metodologia aplicada nesta pesquisa, realizou-se entrevistas com colaboradores da Ômega S.A., o que possibilitou identificar as falhas na segurança da informação da indústria e, deste modo, propor um plano de conscientização para os colaboradores desta indústria com foco ao elo mais fraco da segurança, o fator humano.

Foram realizadas entrevistas semiestruturadas seguindo o modelo do Apêndice A com 40 colaboradores de diferentes setores da empresa e uma entrevista com o gestor de T.I. utilizando o modelo de questionário do Apêndice B, na semana do dia 5 ao dia 9 do mês de Fevereiro de 2018. As perguntas utilizadas nas entrevistas foram elaboradas com base nos objetivos de controles estabelecidos na ISO 27001. Esta ferramenta foi utilizada para que fosse possível visualizar quais eram de fato os problemas mais pertinentes na segurança da informação daquela indústria e até mesmo analisar se os colaboradores teriam conhecimento de tais problemas. Possibilitando assim apresentar uma proposta de plano de conscientização coerente com a realidade daquela indústria.

3.1 Estudo de caso

Esta seção falará sobre a empresa à qual será apresentada a proposta de um plano de conscientização para a melhoria da segurança da informação na mesma; por motivos de confidencialidade seu verdadeiro nome será omitido e vamos chama-la de "Ômega S.A.".

A Ômega é uma empresa do setor industrial do estado do Pará que cultiva sua própria matéria prima há mais de 35 anos e vem se reinventando a cada ano, buscando a partir de pesquisas, desenvolver novos produtos para assim alcançar

novos mercados. Hoje ela conta com uma gama relativamente grande de produtos que são vendidos para empresas do ramo alimentício, cosmético, dentre outros, tanto no mercado nacional quanto internacional. Atualmente, a Ômega conta com uma sede onde todos os produtos passam por diversos processos de beneficiamento, de onde esses produtos são enviados para os clientes, uma filial em outra cidade do estado e o escritório do setor financeiro na capital. Para realização das tarefas, a empresa conta com mais de 130 colaboradores apenas em sua sede, que são distribuídos por turno e setores, de modo que os setores de produção funcionam 24 horas por dia e setores como o administrativo funcionam em horário comercial.

Bem como muitas outras empresas, a Ômega S.A. cresceu e expandiu seus negócios, tornando necessária a sua informatização. Há 10 anos a empresa possui seu próprio sistema, que armazena diversas informações de todos os setores da empresa, como cargas que entram e saem da empresa com horário de entrada e saída, peso da carga, placa do veículo, nome do motorista. O tipo de carga pode variar desde embalagens até produtos vendido pela Ômega S.A., insumos, material de limpeza para a higienização da própria indústria, saída de material reciclável, entrada de matéria prima, notas fiscais, laudos para liberação de cargas, entrada e saída de itens do almoxarifado, entrada de alimento para que os colaboradores se alimentem e etc.

Esse sistema possui funcionalidades diferenciadas para cada setor onde é utilizado, sendo assim, apesar de ser um sistema que abrange todos os setores é necessário que o colaborador aprenda a parte específica que ele utilizará para exercer sua função utilizando o sistema, porém, a Ômega S.A. não possui treinamentos específicos para que o colaborador se familiarize com o sistema, em vez disto, o que ocorre com frequência é que um colaborador com mais conhecimento passe informações para outro colaborador de modo informal para que quando necessário aquele segundo colaborador “quebre um galho” para o primeiro. Desta forma, os riscos de ocorrer erros humanos devido à ausência de treinamento adequado são acentuados.

Um exemplo é que em diversas situações dados são inseridos de forma incorreta, isto representa uma falha na segurança da informação pois estão sendo gerados dados inconsistentes que não representam de fato a realidade e acabam comprometendo a integridade da informação. Outro problema da empresa é que,

apesar de ter preocupações com firewall, antivirus e apresentar algumas orientações sobre segurança da informação para seus colaboradores de maneira informal dentre outros, a organização não possui um sistema de gerenciamento de segurança da informação consolidado, o que dificulta identificar de onde surgem as ameaças, onde há mais riscos e quais os dados mais sensíveis. Também não existem documentos que comprovem a existência de uma política de segurança da informação que tem papel fundamental não somente, mas principalmente, em relação aos fatores humanos da segurança da informação.

A partir das entrevistas realizadas na Ômega com colaboradores de todos os setores além do gestor de T.I., obteve-se os resultados que podem ser verificados na seção 4. A empresa apresenta diversos problemas graves em relação a segurança da informação e aqui são apresentados os principais problemas relacionados aos fatores humanos que ela enfrenta atualmente e que comprometem fortemente a segurança da informação:

- Política de mesa/tela limpa – Muitos dos colaboradores que tem acesso a computadores de mesa e documentos impressos não seguem a política de mesa/tela limpa por alguns motivos, o primeiro é pela falta de conhecimento dos colaboradores sobre tal política, a segunda é que por não existir nenhuma punição definida para quem não fizer uso de tal política e alguns colaboradores acreditam ser apenas um empecilho na realização de suas tarefas, sem compreender seu real papel que é manter informações importantes longe riscos;
- Identificação de funcionários/estagiários/visitantes por meio de crachás – Na Ômega S.A. não há a utilização de crachás por parte dos colaboradores e estagiários, também não há exigências em relação ao uso crachás para visitantes e colaboradores terceirizados, o que torna a empresa muito mais suscetível invasões físicas por engenheiros sociais. Num passado recente, a empresa contava com um sistema de monitoramento que inibia esse tipo de ação e também era útil na identificação destes intrusos, porém com a falta de manutenção adequada esse sistema de monitoramento foi desativado e com a crise financeira pela qual o país vem passando, a revitalização deste monitoramento foi adiado mesmo tendo conhecimento do risco que estava sendo assumido, pois um engenheiro social pode se aproveitar desta falta de identificação para se passar por um investidor, fornecedor ou coisa do tipo e

conseguir informações deixadas expostas pelos colaboradores que não praticam a política de mesa/tela limpa, citada anteriormente;

- Senhas – Não há orientação para os colaboradores sobre a importância de criação de senhas fortes, com letras maiúsculas, minúsculas, caracteres especiais, números, quantidade mínima de caracteres e evitar a utilização de números de documentos, data de aniversários de pessoas próximas ou coisas muito óbvias deste tipo. Os colaboradores tem autonomia para criarem senhas como por exemplo: MINHASENHA ou 123senha, tanto no e-mail corporativo, quanto no sistema informacional da empresa. Um agravante para esta situação é que não há também regras sobre mudança de senhas com tempo pré-definido;
- Usar um único perfil de *e-mail*/sistema por várias pessoas – Pode parece algo óbvio que não se deve compartilhar *login* e senha com outras pessoas, mas esta prática é recorrente na Ômega S.A., onde muitos dos funcionários acessam o sistema informacional da empresa com *login* de terceiros. O mesmo ocorre em relação ao *e-mail* empresarial, onde por muitas vezes um único *login* e senha é compartilhado por uma equipe toda, assim caso exista alguma informação vazada ou com sua confiabilidade comprometida, torna a identificação do responsável muito mais complexa;
- Utilização de dispositivos móveis com acesso à internet disponibilizada na empresa – Na Ômega S.A. todos os funcionários tem acesso a internet via *wi-fi* com seus celulares de uso pessoal, para fins diversos geralmente sem relação com suas funções. Apenas alguns funcionários tem algum tipo de restrição de uso de celular, unicamente por conta da função que exerce para evitar possíveis acidentes. Os colaboradores em sua maioria usam seus celulares mesmo durante a execução de suas funções e todos que levam celulares para a empresa usam eles conectados à rede antes de iniciar suas funções, durante o café da manhã e outras refeições e em momentos de lazer. Vale ressaltar que são pouquíssimos os sites bloqueados ao acesso por meio da rede da empresa, e-mails, redes sociais e uma infinidades de outros sites podem ser acessados sem problemas. Outro fato que fragiliza ainda mais a situação atual da segurança da informação é que existe uma rede aberta para visitantes, que pode ser acessada mesmo do lado de fora do muro da empresa e não é difícil encontrar pessoas que não são

colaboradores, acessando a internet por meio da rede da empresa o que representa uma ameaça enorme para a empresa, uma vez que quanto maior o número de pessoas sem conhecimento técnico utilizando a rede, maiores são as chances de eventuais contaminações da rede por vírus e similares, sem contar possíveis *crackers* que não teriam problema algum para coletar dados da empresa;

- Softwares sem licença – De acordo com um estudo apresentado pela *Microsoft* no ano de 2012, 37% dos *softwares* encontrados nas empresas não eram genuínos. Na Ômega S.A. não são todos os computadores que possuem bloqueio de instalação de softwares, o que torna extremamente simples o computador ou ainda toda a rede da empresa ser afetada por vírus, *keyloggers*, *spywares*, *malwares* dentre outras ameaças que podem excluir e corromper arquivos, além de diversos outros riscos, isto aliado a falta de treinamento e da possibilidade de acessar sites não confiáveis a partir dos computadores da empresa acaba tornando a empresa e suas informações alvos extremamente vulneráveis;
- Ausência de backup – Esta ausência de backup na empresa representa mais um enorme risco, uma vez que algumas informações do processo de produção, loteamento, laudos, dentre outros arquivos importantes que são armazenados em apenas um computador. Assim, se, por exemplo, um funcionário insatisfeito com a empresa quiser causar prejuízos para a empresa, ele pode muito bem alterar as informações contidas naquele computador que, vale salientar, não é utilizado apenas por uma pessoa, mas sim por pelo menos duas equipes;
- Mídias removíveis – O uso de *pendrive* e *HD* externo nos computadores da empresa são frequentes por não existirem restrições em relação ao uso destas ferramentas. Estas ferramentas são uma via de mão dupla, pois além de representarem um potencial vetor de vírus e similares, ainda podem ser utilizadas para roubar informações confidenciais da empresa.

4 RESULTADOS

Nessa seção serão apresentados os resultados obtidos a partir da análise dos dados coletados através da aplicação dos questionários de segurança da informação dentro da empresa, para que fosse possível identificar quais os problemas presentes na Ômega. Vale ressaltar que a sede da empresa onde os questionários foram aplicados possui 130 colaboradores, destes, participaram da pesquisa 40 colaboradores de setores diversos da empresa mais o gestor de T.I.

As perguntas presentes nos questionários foram baseadas nos controles apresentados na ISO 27001 que possuem alguma relação com fatores humanos. Analisando as respostas obtidas é possível identificar as não conformidades com a segurança da informação.

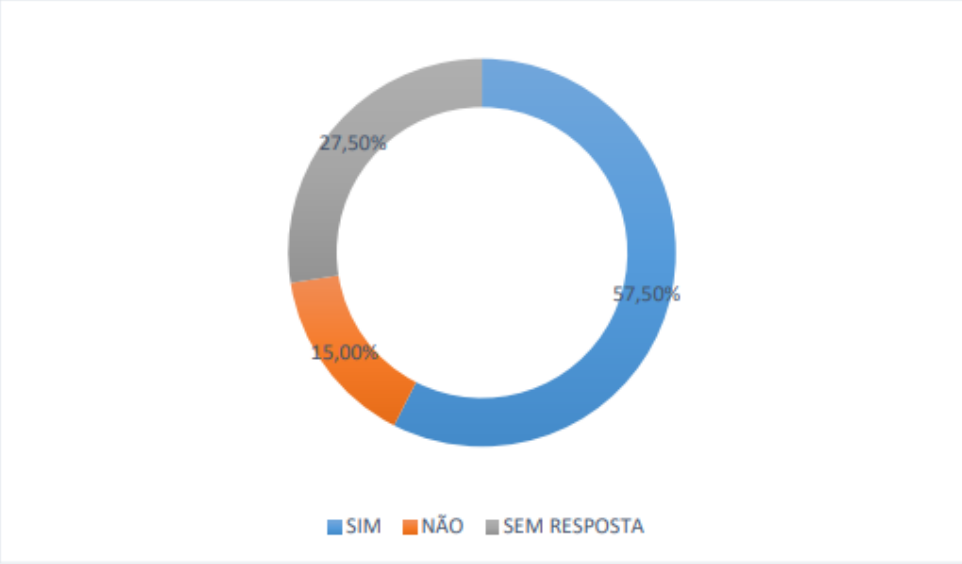
4.1 Questionário aplicado aos colaboradores

O questionário foi aplicado a 40 colaboradores. Tal questionário é constituído de 20 perguntas que poderiam ser respondidas com SIM ou NÃO e o colaborador entrevistado poderia optar ainda por não responder alguma pergunta caso não se sentisse à vontade. Após a aplicação do questionário foram feitas observações sobre algumas experiências presenciadas pelo colaborador dentro da empresa que pudessem ter relação com as vulnerabilidades humanas.

Abaixo são apresentados os gráficos desenvolvidos a partir das respostas dos participantes das entrevistas realizadas para a visualização dos dados obtidos.

Como representado na Figura 9, 23 dos 40 entrevistados na Ômega concordam que a segurança da informação é importante para a empresa. É um dado positivo, pois mesmo sem compreender muito bem o papel da segurança da informações, esses colaboradores acreditam que essa segurança é importante. Os demais colaboradores entrevistados não souberam ou não quiseram responder a pergunta.

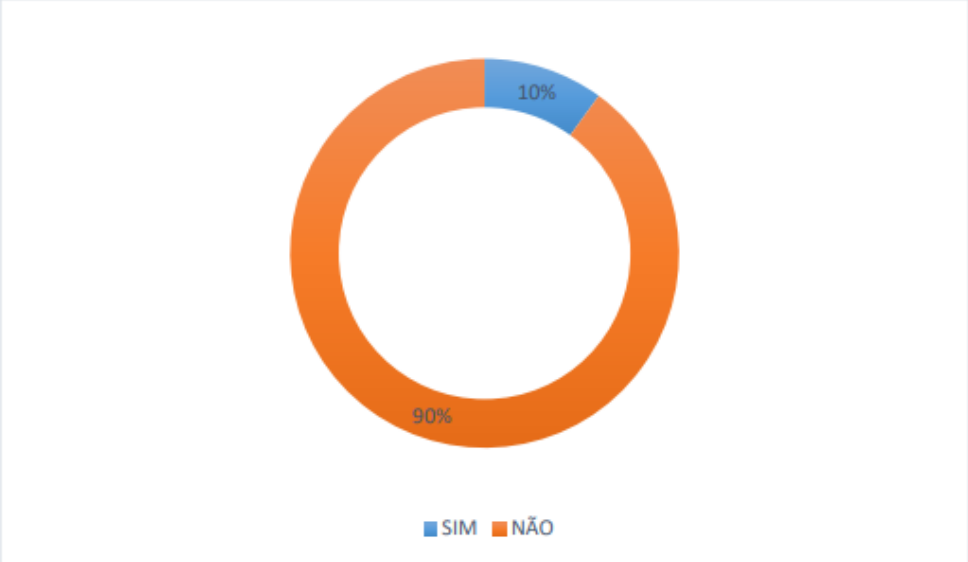
Figura 9. Respostas a pergunta 1



Fonte: O Próprio Autor (2018)

A Figura 10 apresenta uma situação muito grave, onde 36 dos colaboradores entrevistados nunca passaram por treinamento de segurança da informação, os outros 4 entrevistados, participaram de treinamentos ou participaram de cursos relacionados à segurança da informação em empresas onde eles trabalhavam no passado. Isso torna visível que a Ômega não se preocupou em tomar medidas preventivas em relação às vulnerabilidades humanas.

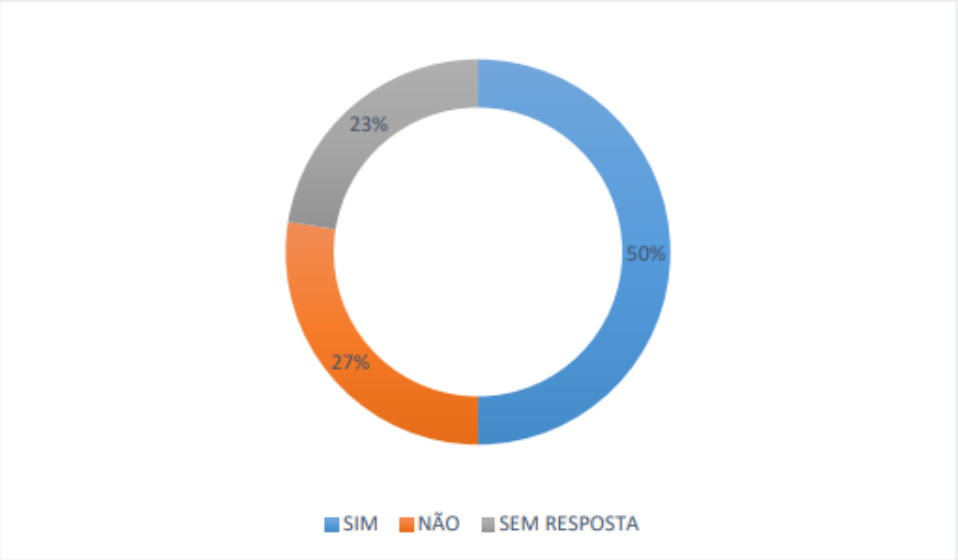
Figura 10. Respostas a pergunta 2



Fonte: O Próprio Autor (2018)

De acordo com o gráfico da Figura 11, dos 40 entrevistados, 20 afirmaram que a segurança da informação é de total responsabilidade da equipe de T.I. Essa mentalidade é reflexo da ausência de uma política de segurança da informação consolidada, bem como ausência de campanhas de conscientização na empresa.

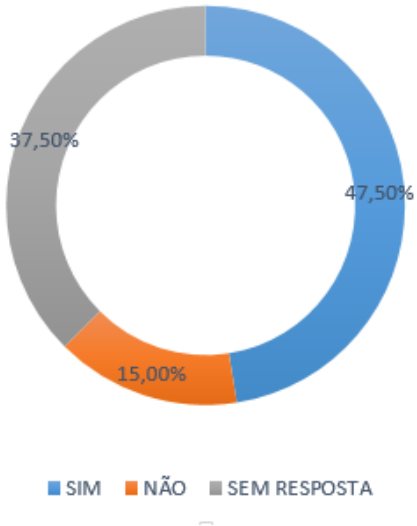
Figura 11. Respostas a pergunta 3



Fonte: O Próprio Autor (2018)

A Figura 12 é referente à pergunta relacionada ao controle da ISO 27001 que recomenda a política de tela/mesa limpa, 19 dos colaboradores que participaram da pesquisa reconheceram que deixam arquivos na área de trabalho dos seus computadores e deixam documentos, agendas e anotações importantes em suas mesas durante e após seu expediente, práticas inaceitáveis, pois expõem de forma desnecessária as informações às ameaças presentes no ambiente.

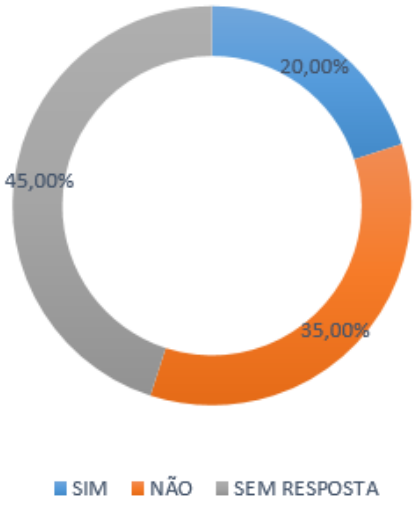
Figura 12. Respostas a pergunta 4



Fonte: O Próprio Autor (2018)

A Figura 13 é referente à pergunta de número 5 do questionário, que pergunta aos colaboradores se é possível instalar *softwares* nos computadores da empresa. 8 entrevistados apenas afirmaram ser possível, isso graças aos bloqueios que a equipe de T.I. implantou em computadores que armazenam informações mais sensíveis. Contudo, não deveria ser possível a instalação de nenhum *software* em nenhum computador da empresa a não ser pelo pessoal autorizado, para evitar que programas maliciosos sejam inseridos nos computadores da empresa. 18 dos 40 entrevistados não quiseram responder a pergunta e não justificaram o motivo pelo qual não responderam.

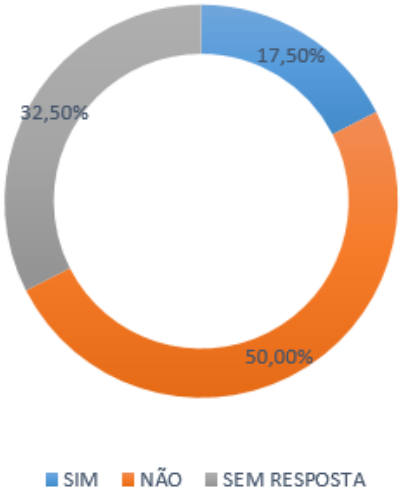
Figura 13. Respostas a pergunta 5



Fonte: O Próprio Autor (2018)

A Figura 14 mostra que apenas 7 dos entrevistados tem o costume de bloquear a tela do computador ao deixar seu ambiente de trabalho por algum motivo. Uma prática simples que pode evitar grandes prejuízos à empresa, uma vez que podem existir nesse ambiente colaboradores mal intencionados que podem se aproveitar da ausência do colega para fazer uso indevido dos dados que ali se encontram. Por outro lado 20 entrevistados afirmaram não se importar com isso, pois acreditam que esse procedimento é desnecessário e atrasa o serviço.

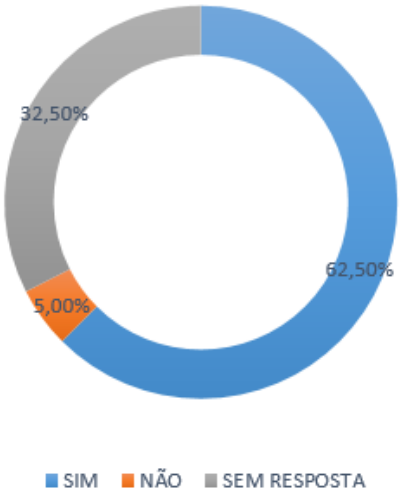
Figura 14. Respostas a pergunta 6



Fonte: O Próprio Autor (2018)

A Figura 15 tem dados positivos em relação aos demais até aqui. Segundo 25 dos entrevistados, os computadores da empresa possuem antivírus. Levando em consideração a pouca afinidade que os colaboradores apresentaram até aqui em relação à segurança da informação, possuir um antivirus é de fundamental importância reduzindo minimamente os riscos aos ativos da informação.

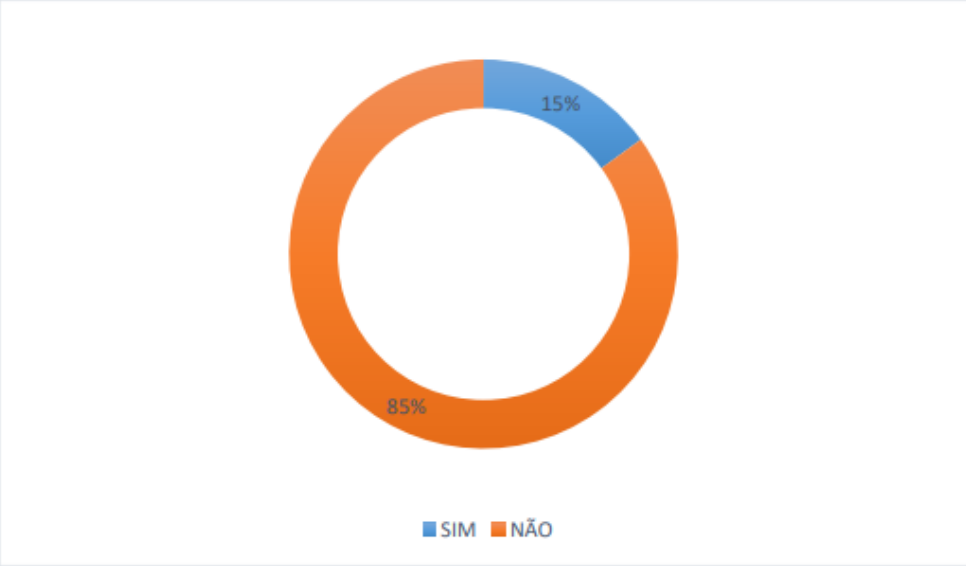
Figura 15. Respostas a pergunta 7



Fonte: O Próprio Autor (2018)

A Figura 16 apresenta mais uma informação positiva em meio a problemas tão grandes. Apenas 6 dos colaboradores confirmam que já utilizaram seu computador pessoal para acessar informações relativas à suas funções na empresa. Apesar de ser uma porcentagem baixa esse tipo de prática não deve ser encorajada, uma vez que controlar a segurança dos ativos da empresa fora da mesma se torna mais complexo.

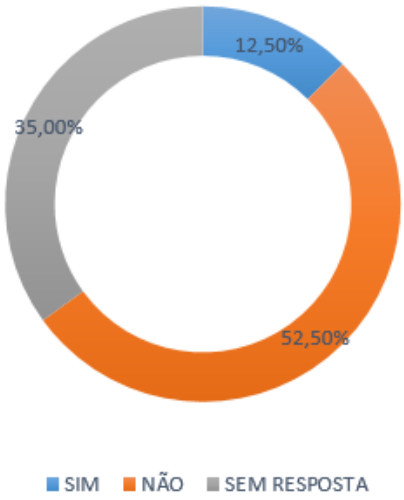
Figura 16. Respostas a pergunta 8



Fonte: O Próprio Autor (2018)

Na Figura 17 apenas 12% do colaboradores afirma que existem recomendações para a realização de cópias de segurança dos arquivos que eles manipulam. Quando questionados sobre de quem era a recomendação os entrevistados informaram que se tratava do seu superior imediato, o que evidencia que os setores não estão trabalhando juntos para tornar o ambiente mais seguro.

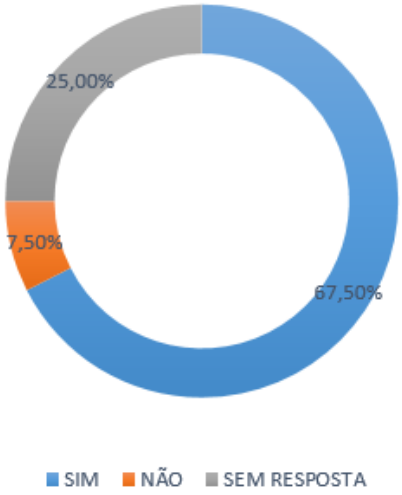
Figura 17. Respostas a pergunta 9



Fonte: O Próprio Autor (2018)

Analisando os dados da Figura 18, é possível notar que 27 entrevistados reconhecem a utilização de mídias removíveis dentro da Ômega e 10 preferiram não responder. Alguns colaboradores relataram que existem pessoas que levam *HD* para baixar filmes, uma prática perigosa já que muitos sites que disponibilizam *downloads* de vídeos, jogos e outros *softwares* são grandes disseminadores de pragas virtuais, além de que com essa prática a banda de *internet* da empresa é comprometida.

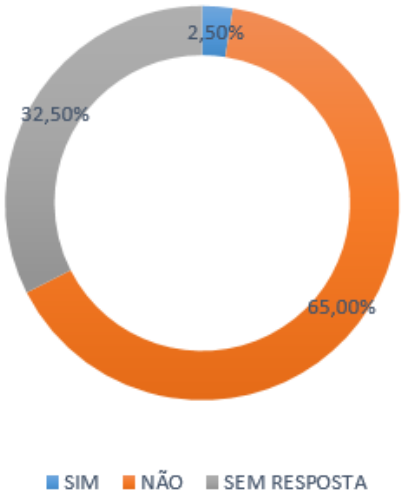
Figura 18. Respostas a pergunta 10



Fonte: O Próprio Autor (2018)

A Figura 19 representa o resultado para a pergunta sobre a existência de recomendações de criação de senhas fortes. 26 dos entrevistados responderam que não. Os colaboradores foram questionados se tinham o hábito de trocar as senhas com uma determinada frequência e as respostas, no geral, também foram negativas, o que os torna alvos fáceis para engenheiros sociais e *Keyloggers*. A disseminação de boas práticas da segurança da informação pode reverter facilmente essa situação, informando sobre os riscos causados pela não utilização de boas senhas e trocas frequente das mesmas.

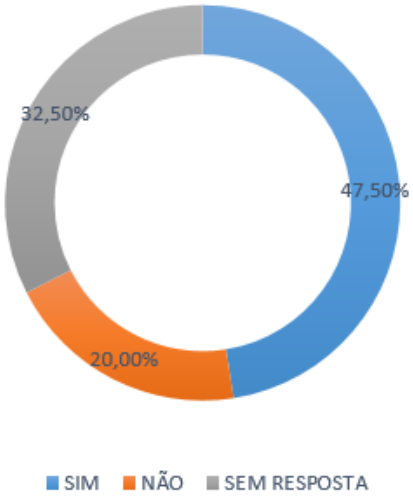
Figura 19. Respostas a pergunta 11



Fonte: O Próprio Autor (2018)

A Figura 20 refere-se à prática de utilização de nome de usuário e/ou senhas de colegas de trabalho. 19 disseram que sim, utilizam *login* e senha de seus colegas, e alguns ainda completaram afirmando que essa seria uma prática rotineira na empresa. Com essa prática não há como identificar quem realmente realizou uma modificação nos dados, danificou ou copiou arquivos.

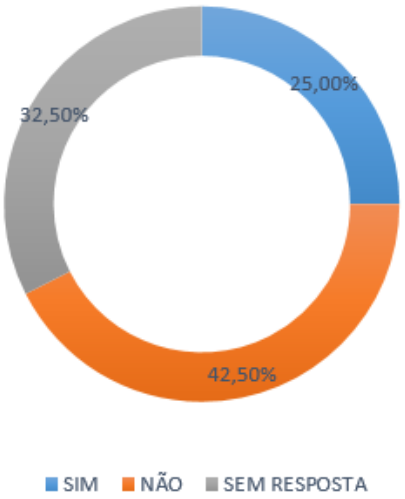
Figura 20. Respostas a pergunta 12



Fonte: O Próprio Autor (2018)

Na Figura 21, 17 dos entrevistados afirmaram que não buscam os arquivos impressos imediatamente e alegam que concluem suas tarefas antes de buscarem os documentos. Um detalhe é que boa parte dos documentos são enviados para a impressora que fica localizada na recepção, onde há circulação de funcionários terceirizados, clientes, visitantes e colaboradores de todos os setores que podem aproveitar a oportunidade para extrair alguma informação interessante dos documentos.

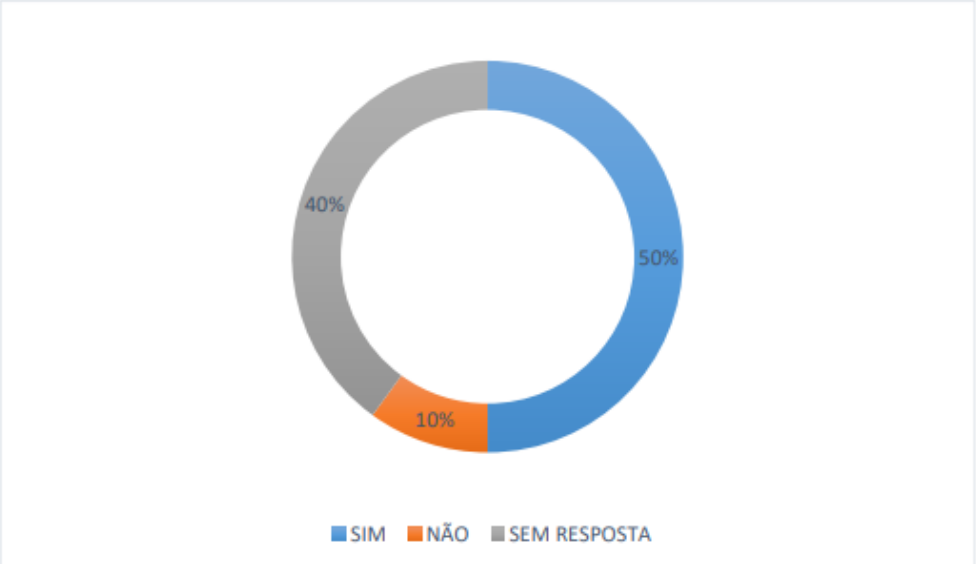
Figura 21. Respostas a pergunta 13



Fonte: O Próprio Autor (2018)

A Figura 22 apresenta que 20 dos colaboradores entrevistados afirmam existir procedimento para descarte de documentos. Estes colaboradores afirmam que antes de descartar esses documentos, eles picam o papel em pequenos pedaços, evitando assim o acesso aos dados ali presentes, sendo uma ótima prática que já faz parte da cultura da organização.

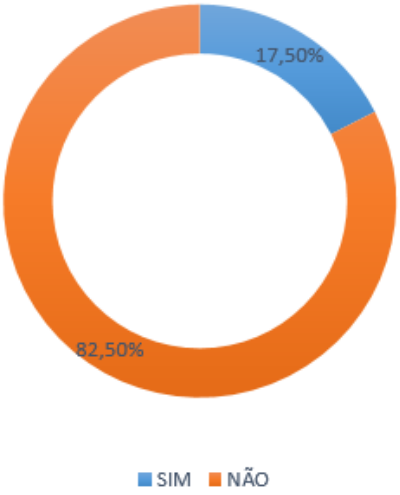
Figura 22. Respostas a pergunta 14



Fonte: O Próprio Autor (2018)

A Figura 23 diz respeito ao conhecimento dos colaboradores em relação à engenharia social. 33 dos participantes afirmou não ter conhecimento sobre o que é engenharia social. Logo, boa parte desses colaboradores são potenciais vítimas, uma vez que sem conhecimento da existência desses engenheiros sociais torna-se impossível se prevenir contra as técnicas utilizadas por eles.

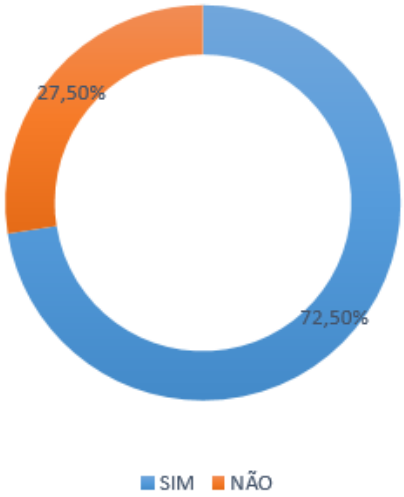
Figura 23. Respostas a pergunta 15



Fonte: O Próprio Autor (2018)

Na Figura 24 são apresentados dados sobre a utilização de telefone celular dentro da empresa, 29 dos participantes admitiram utilizar celulares dentro da empresa. Quando questionados qual a finalidade do uso, boa parte afirmou que utilizava para acessar redes sociais e outros fins pessoais sem ligação com suas funções.

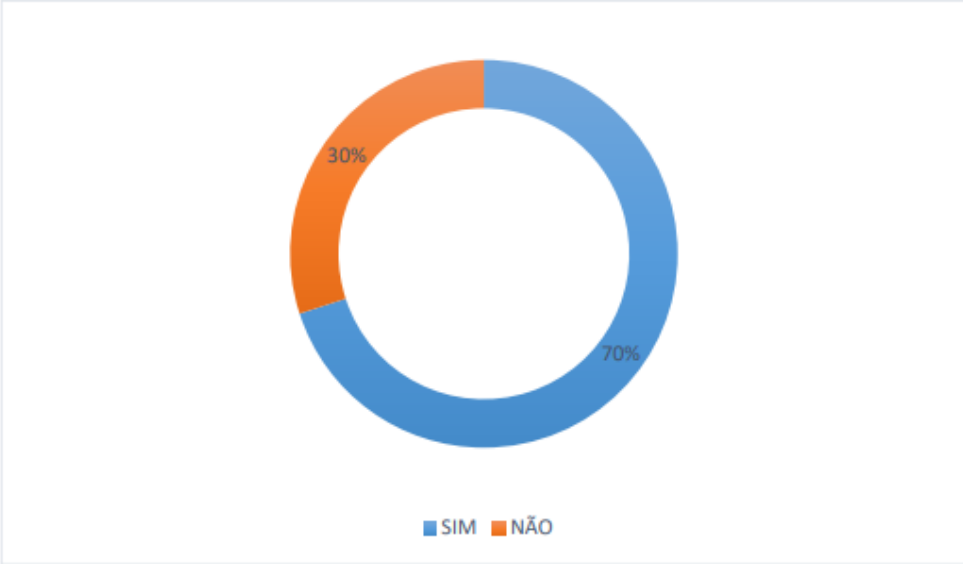
Figura 24. Respostas a pergunta 16



Fonte: O Próprio Autor (2018)

A Figura 25 diz respeito a prática de transmissão de informações relativas a empresa por meio de aparelhos telefônicos, seja celular ou telefone fixo. Podemos notar que a prática é amplamente utilizada dentro da empresa. 28 dos colaboradores entrevistados já trocaram informações deste modo ou ainda trocam. A utilização das tecnologias para facilitar o trabalho é ótimo, contudo devem haver recomendações a serem seguidas para evitar golpes, como ataques de engenheiros sociais por meio de ligações.

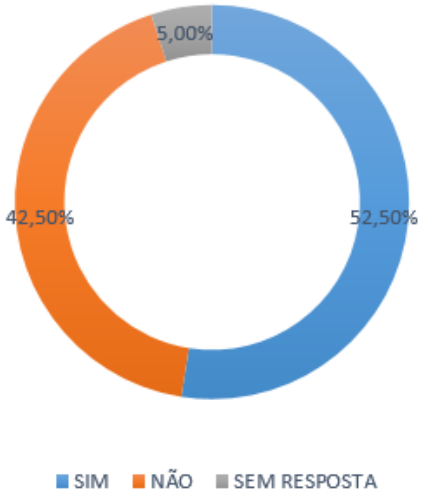
Figura 25. Respostas a pergunta 17



Fonte: O Próprio Autor (2018)

De acordo com os dados da Figura 26, 21 dos entrevistados admitiram já ter realizado *download* de algum arquivo por meio da rede da empresa. Como já dito antes, esse tipo de atitude além de ser antiética, pois estão fazendo uso inadequado de ativos, ainda oferece uma série de riscos à segurança da informação.

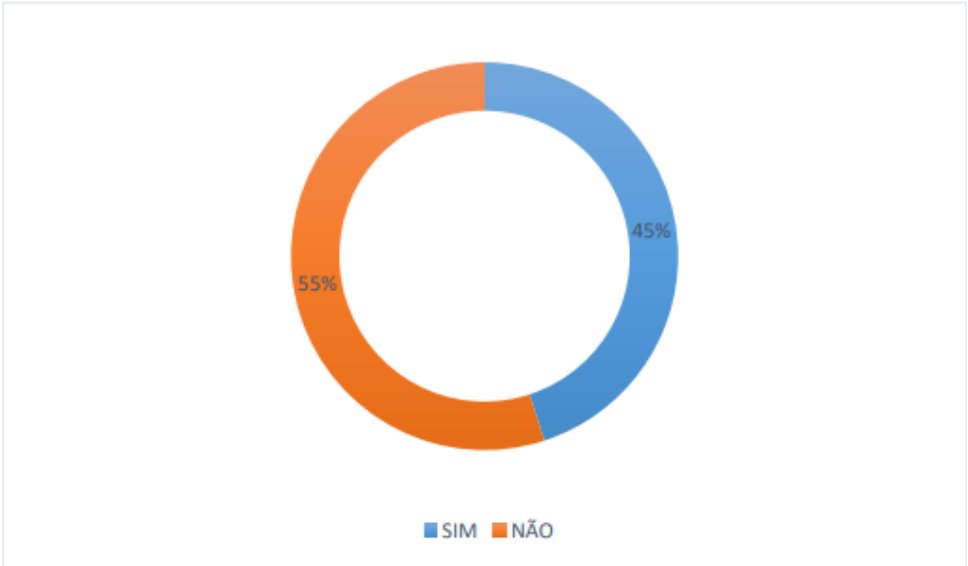
Figura 26. Respostas a pergunta 18



Fonte: O Próprio Autor (2018)

Os dados da Figura 27 indicam que 22 dos colaboradores entrevistados evitam falar sobre assuntos relacionados a suas funções em ambientes públicos ou em áreas comuns, como refeitório e recepção. Mesmo sem conhecimento técnico, esses entrevistados estão contribuindo com a segurança da informação, evitando assuntos que podem conter informações valiosas para a empresa.

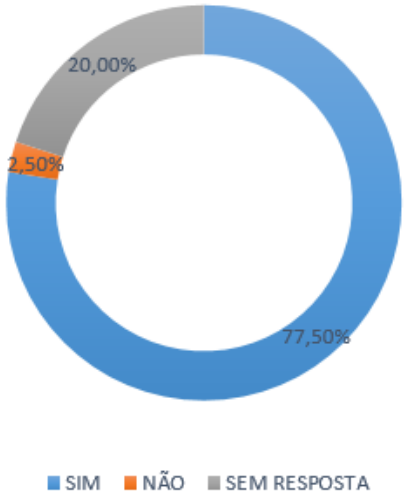
Figura 27. Respostas a pergunta 19



Fonte: O Próprio Autor (2018)

Na Figura 28 o resultado da pergunta 20, se existem locais dentro da empresa que só podem ser acessados por grupos determinados de funcionários. 31 entrevistados afirmaram que sim, isso é importante uma vez que muitos ativos devem ser mantidos longe do alcance principalmente de funcionários terceirizados e visitantes. Mais um ponto positivo que deve ser mantido quando a empresa implementar uma futura PSI bem estruturada e funcional.

Figura 28. Respostas a pergunta 20



Fonte: O Próprio Autor (2018)

Como foi constatado pelas respostas dadas pelos colaboradores da Ômega, ela vive hoje um momento extremamente delicado em relação às boas práticas de segurança da informação, grande maioria das perguntas realizadas obteve um grau negativo muito alto, tornando-se inaceitável mesmo para padrões mínimos de segurança.

4.2 Questionário aplicado ao gestor de T.I.

O questionário aplicado ao gestor de T.I. [Apêndice B] é composto por 2 perguntas e um pedido para que o mesmo cite um problema encontrado na empresa relacionado a fatores humanos que comprometem a segurança da informação diferente dos que tinham sidos abordados no questionário aplicado aos demais colaboradores.

A primeira pergunta questionava a existência de um inventário de ativos, a resposta do gestor foi não. O gestor afirmou reconhecer a importância dessa medida, uma vez que isso tornaria mais fácil, por exemplo, a manutenção preventiva dos equipamentos, tornaria as ações contra incidentes da informação mais rápidas e isso seria possível a partir do momento que se pode delegar responsabilidades em relação à segurança dos ativo a quem os manipula.

A segunda pergunta era sobre a existência da classificação e rotulação de informações contidas em arquivos de texto, planilhas e similares. Ele afirma que houve uma tentativa de implementação dessa classificação, mas por algum motivo que ele não relatou, a implementação não seguiu em frente e por conta disso ele mesmo tem uma parcela de culpa em relação a falta de cuidados com as informações que os colaboradores possuem.

Para o gestor de T.I. algo que também é importante ser pontuado é o fato da inexistência da utilização de Crachás na empresa, além dos colaboradores não possuírem tal identificação, esse tipo de identificação não é exigido de funcionários terceirizados e visitantes o que torna o acesso ao interior da empresa extremamente simples, de modo que um engenheiro social pode realizar ataques sem ao menos deixar pistas. Ainda estendeu-se a comentar sobre uma seleção de novos colaboradores mais criteriosa e a adoção de medidas punitivas.

Analisando de modo geral os resultados das entrevistas foi possível constatar a quase inexistência de qualquer mecanismo de segurança da informação que não sejam os automatizados, como antivirus, *firewall*, solicitação de senhas de administradores para instalação de *softwares* e outros que foram relatados pelo gestor de T.I.

As informações obtidas atrás das entrevistas foram enviadas para a alta administração da empresa pelo gestor de T.I. para que todos tivessem o conhecimento da preocupante situação da empresa, para que dessa forma a alta administração declarasse apoio ao desenvolvimento do plano de conscientização, tornando a iniciativa mais palpável.

4.3 Proposta para a implementação do plano de conscientização

Os problemas que possuem relação com os fatores humanos na Ômega, como pudemos notar, são numerosos e graves. Buscando amenizar esses problemas, esta monografia tem como missão apresentar uma proposta de plano de

conscientização que envolva todos os setores da empresa de modo que esses colaboradores possam entrar em conformidade com as boas práticas de segurança da informação sugeridas pelas ISO's 27001 e 27002, afim de que esses colaboradores entendam que eles são peças fundamentais para que os dados da empresa sejam mantidos em segurança e compreendam que as boas práticas na segurança da informação existem para reduzir vulnerabilidades e não para criar burocracias desnecessárias.

4.3.1 Orientação para PSI

Como pôde-se constatar até o dado momento, uma política de segurança da informação bem estruturada é a base para que qualquer instituição mantenha suas informações íntegras, com sua confidencialidade inócuas e acessíveis. Para orientar um futuro desenvolvimento de uma PSI para a Ômega, apresenta-se alguns tópicos fundamentais, tópicos esses que são baseados nos controles apresentados na ISO 27001, que devem estar contidos nesta PSI, pois são formas de combater os problemas mais visíveis enfrentados hoje pela empresa de acordo com os questionários respondidos pelos colaboradores e conversas com o gerente de TI da empresa.

- Classificação da Informação – Todas as informações devem ser classificadas de acordo com sua importância para a organização (secretas, confidenciais, particulares e públicas) deste modo será possível aplicar a proteção adequada para cada tipo de informação uma vez que esta classificação deve considerar o valor, sensibilidade e criticidade destas informações para que sejam evitadas perdas, divulgações ou modificações não autorizadas destas;
- Inventário dos ativos – Para que seja possível ter conhecimento do que se deve proteger é necessário o inventário dos ativos, esses ativos podem ser classificados como ativos de informação, ativos de *softwares*, ativos físicos, reputação da empresa, pessoas e suas habilidades, experiência, qualificações. Com isto é possível definir os responsáveis por cada ativo;
- Gerenciamento de mídias removíveis – É conveniente a implementação de procedimentos relacionados a mídias removíveis, é possível bloquear o acesso a portas *USB*, unidades ópticas e leitores de cartão tanto de forma física, quanto pela utilização de softwares que gerenciam transferências de dados para mídias removíveis, alguns destes softwares possuem ferramentas que não permitem

que dados sejam transferidos para as mídias, deste modo tais mídias funcionam apenas no modo leitura;

- Política de Senha – Alguns requisitos devem ser obedecidos em relação a senhas, as senhas devem ser de uso pessoal de modo que o uso compartilhado deve ser punido; senhas não devem ser repetidas, por exemplo, a senha do terminal de trabalho deve ser diferente da senha do e-mail, que também deve ser diferente de senhas utilizadas em outras plataformas disponíveis na empresa; não utilizar número de documentos, data de aniversários, nome de parentes ou bichinhos de estimação como senha; as senhas devem ter um número mínimo de caracteres, mesclando números, letras maiúsculas e minúsculas, caracteres especiais, deste modo: Okk8D4x4a100km. É recomendado que tais senhas possuam um prazo de validade pré-definido, deste modo estas senhas são redefinidas com frequência;
- Política de mesa limpa e tela limpa – É comum na Ômega que os colaboradores mantenham documentos como laudos de qualidade, notas fiscais, cronograma de produção semanal, agendas com senhas, contato de fornecedores e clientes em suas mesas de forma exposta é recorrente também se ausentarem de suas estações de trabalho e deixarem seus *e-mails* logados, assim como o sistema da empresa; frequentemente documentos são impressos e ficam por vários minutos na impressora, as vezes horas sem que quem os imprimiu os procure, é válido frisar que boa parte do documentos é enviado para a impressora que se encontra na recepção, onde se encontram clientes, visitantes, motoristas terceirizados e outros. Esse comportamento pode se mostrar danoso uma vez que não há como sabermos quais as verdadeiras intenções dos colegas de trabalho e demais pessoas que se encontram naquele ambiente. Recomenda-se que documentos, senhas, contato de fornecedores e clientes sejam mantidos em gavetas com chave, computadores devem ser bloqueados, sempre que o colaborador se ausente de sua estação de trabalho, documentos impressos devem ser recolhidos por quem os imprimiu o mais rápido possível estas recomendações devem impedir o comprometimento de ativos e interrupções das operações da empresa;
- Cópias de segurança das informações – Existem informações que só são salvas em computadores específicos da empresa como relatórios de produção, relatórios de monitoramento de processos, relatório de entrada de matéria prima

e laudos de qualidade porém estas informações não possuem *backup* se por alguma eventualidade alguém que tenha acesso as esses dados altere ou delete de forma acidental ou intencional a inexistência de copias de segurança destas informações podem causar inconsistências nas informações de lotes de produção, atraso no envio para clientes e outros problemas que se traduzem em prejuízos, perca de credibilidade com clientes causando impactos diretos a imagem da empresa;

- Instalação de software nos sistemas operacionais – Para que a integridade do sistema operacional seja preservada é necessário a implantação de procedimentos que não permitam que sejam executadas instalações de softwares por pessoas não autorizadas;
- Política para o uso de dispositivo móvel – No cenário tecnológico em que vivemos é comum que as empresas liberem o uso de dispositivos moveis para seus colaboradores, na Ômega o acesso à internet é liberado sem restrições e esse é o grande problema, sites que disponibilizam downloads de filmes, softwares, música e diversos outros conteúdos inadequados, além de acesso a redes sociais, e-mails pessoais. É interessante adotar medidas para bloquear o acesso a esses sites citados acima, restrição de uso de dispositivos moveis em alguns locais da empresa, para evitar que sejam fotografados documentos que possam apresentar informações importantes, limitar o uso de dispositivos moveis para fins sem relação com os negócios da empresa apenas nos intervalos para alimentação ou fora de seus expedientes;
- Seleção – Para reduzir as chances de estagiários ou candidatos à vagas na empresa representarem potenciais riscos à segurança da informação, deve-se fazer levantamentos sobre a pessoa, analisando suas redes sociais, entrando em contato com empresas onde a pessoa já trabalhou anteriormente para assegurar que mesmo não oferece riscos aparentes as políticas de segurança da informação;
- Processo disciplinar – É fundamental para o bom funcionamento das políticas de segurança da informação, que sejam desenvolvidos processos disciplinares e que esses processos sejam informados a partes internas e externas onde for pertinente, para que assim seja possível aplicar ações disciplinares contra colaboradores que violem a segurança da informação, estas ações variam de

acordo com a gravidade, podem ir desde orientações verbais até a demissão por justa causa;

- Conscientização, educação e treinamento em segurança da informação – Para o bom funcionamento da segurança da informação, faz-se necessário que os colaboradores e a quem mais ser pertinente compreendam que a tecnologia por si só não representa segurança de forma integral, na realidade a segurança completa é uma ilusão, é necessário que todos sejam envolvidos e comprometidos com a segurança da informação e não apenas a equipe de TI para que os riscos sejam minimizados ao máximo, é necessário que sejam realizados treinamentos regulares de acordo com as funções exercidas por cada funcionário.

4.3.2 Plano de Conscientização

Neste plano de conscientização são definidos objetivos para estabelecer e manter o foco do mesmo, assim são listados tais objetivos: Convencer a diretoria sobre a importância da conscientização dos colaboradores, informar os colaboradores sobre ameaças à segurança da informação, tornar o colaborador capaz de identificar e relatar problemas de segurança da informação.

Para que o plano de conscientização obtenha êxito é fundamental o apoio da alta administração da empresa, esse apoio pode ser expresso na forma de um comunicado [Apêndice C] e para que haja esse apoio por parte da diretoria, os dados coletados com realização de diálogos informais e questionários devem ser apresentados. Com o aval da diretoria o plano de conscientização ganha mais visibilidade e credibilidade entre os colaboradores e partes externas.

Informar os colaboradores sobre ameaças à segurança da informação é pertinente uma vez que tendo conhecimento de como estão expostos a esses ataques e a forma como tais ataques são efetuados, tornam esses colaboradores menos vulneráveis.

Tornar o colaborador capaz de identificar e relatar problemas de segurança da informação, deste modo pode-se agilizar e otimizar o tratamento das vulnerabilidades que surgem em sua própria fonte.

4.3.3 Nível atual de conscientização do colaboradores

É notável que os colaboradores em sua maior parcela não compreendem o real valor das informações que estão em suas responsabilidades e não se atém ao

fato que, por exemplo, um vazamento de informação é capaz de levar a empresa a falência e, consequentemente, fazer com que o colaborador perca seu emprego. Além disso, os prejuízos não são causados apenas por vazamentos de informações, existindo uma série de outros riscos à segurança da informação.

Um exemplo da falta de conscientização na empresa é um caso relatado por um colaborador da Ômega durante a realização das entrevistas. Segundo ele, no segundo semestre de 2017, um outro colaborador que era responsável pela análise de qualidade de produção deveria realizar análises especificas a cada 30 minutos durante seu turno noturno, entretanto este estava apenas replicando analises e inserindo os dados em tabelas. Com o tempo houveram muitas reclamações de clientes referentes a qualidade do produto entregue a eles, então foram realizados cruzamento de dados, novas análises e assim foi possível identificar qual a origem das inconsistências nas informações. Essa atitude do colaborador de replicar as análises resultou em muitos prejuízos para a empresa, uma vez que ela deixou de vender alguns lotes que já haviam sido produzidos, teve que reprocessar outros lotes e perdeu credibilidade com alguns clientes, tudo por conta deste colaborador que não compreendia o valor dos dados que manipulava.

4.3.4 O papel do colaborador a partir de sua conscientização

A partir do conhecimento adquirido com a campanha de conscientização o colaborador deve compreender que seu papel em relação à segurança da informação consiste em evitar expor os ativos que se encontram em responsabilidade a riscos, identificar ameaças à segurança da informação e ser capaz de reportar incidentes da informação.

4.3.2 Conteúdo da campanha de conscientização

O conteúdo da campanha deve contemplar os pontos onde existem mais vulnerabilidades dentro da Ômega, uma vez que não é possível em uma única campanha trabalhar todos os problemas atuais, aqui são pontuados os assuntos que devem ser abordados com os colaboradores na campanha proposta:

- Engenharia social – Referente a exposição de documentos impressos e na tela do computador, descarte de documentos impressos, conversas sobre assuntos empresariais em ambientes públicos, anexos de *e-mails*, informações confidenciais passadas por meio de ligações telefônicas;

- Contas e Senhas – Referente a prática de compartilhamento de senhas e *logins* de acesso entre os funcionários, senhas fracas;
- Uso seguro da *internet* – Referente ao uso inadequado da rede corporativa, para fins pessoais;
- Segurança em dispositivos moveis – Referente ao uso de *smartphones* para registrar imagens de ambientes internos, acesso a redes sociais e mensagens expressas, uso de e-mail pessoal;

4.3.3 Divulgação de conteúdo

Para a obtenção de bons resultados com um plano de conscientização é também indispensável a utilização dos meios corretos para sua divulgação, atendendo as limitações da organização e sendo capaz de alcançar a diversidade de públicos que são alvos desse plano, uma vez que existem colaboradores que não tem acesso a computadores por exemplo. Elencaremos alguns dos possíveis meios de divulgação na sequência.

- E-mail – A divulgação por meio de e-mail pode ser realizada de forma diária apresentado situações cotidianas que podem elevar os riscos à segurança da informação ou pequenas dicas sobre as boas práticas da segurança da informação;
- Informativos nos quadros de avisos – Os quadros de avisos na Ômega possuem muita visibilidade entre os colaboradores, cada setor possui seu próprio quadro de aviso bem como as áreas comuns a todos, desse modo todos os colaboradores tem acesso ao conteúdo de conscientização sobre a segurança da informação, nesse meio de divulgação é interessante apresentar a “Dica da Semana” um informativo com alguma recomendação apresentada de forma simples para todos os colaboradores;
- Palestras – Palestras regulares com especialistas em segurança da informação dentro da empresa, para que os assuntos sejam abordados de modo minucioso. Nesta forma de divulgação é muito importante a participação de gerentes e supervisores uma vez que com maior volume de conhecimento obtido eles podem colaborar com a disseminação das boas práticas em segurança da informação;
- Cartilhas – Cartilhas com recomendações e dicas de como o colaborador deve se portar para proteger os ativos de possíveis ameaças devem ser

elaboradas e distribuídas de forma digital ou impressa. Há também a possibilidade de adquirir esse tipo de material de empresas especializadas em segurança da informação ou ainda parcerias com instituições como o Cert.br que disponibiliza a “Cartilha de Segurança para Internet” que aborda temas como: Golpes na internet, segurança na internet, spam, Contas e Senhas dentre outros temas. Vale ressaltar que o Cert.br disponibiliza esse material sob a licença “*Creative Commons* Atribuição- Uso não comercial- Vedada a criação de obras derivadas 3.0 Brasil”, ou seja, ela pode ser copiada e distribuída dentro da empresa, desde que seja dado os créditos cabíveis ao autor da obra, não é permitido a comercialização dessa cartilha e não é permitido alterar ou criar novas versões baseando-se na obra original;

- Campanhas de conscientização – As campanhas possibilitam abordar o tema de diversas maneiras. Por exemplo com vídeos educativos, encenações de situações recorrentes dentro da empresa que acentuam as vulnerabilidades, gincanas com perguntas sobre as boas práticas de segurança da informação com premiação para quem acertar mais respostas e outros. É interessante realizar pelos menos uma vez ao ano a semana de conscientização para que os colaboradores não acabem deixando as boas práticas caírem no esquecimento.

4.3.4 Manter campanha ativa

A campanha de conscientização deve ser um processo continuo, buscando melhorias frequentemente do contrário os esforços para que ela fosse desenvolvida se tornam inúteis. Uma vez que se não houver continuação, transmite a ideia de que a segurança da informação não tão importante e assim e os conhecimentos transmitidos são deixados de lado ao passar do tempo.

5 CONCLUSÃO

Com o levantamento bibliográfico que realizou-se acerca das implicações dos fatores humanos, bem como, com entrevistas na Ômega constatou-se que o ser humano dentro de um ambiente empresarial é, de fato, o elo mais fraco da segurança da informação, tornando mais evidente a necessidade de investimentos no desenvolvimento de treinamentos e capacitação dos colaboradores que visem evitar danos irreversíveis para a reputação da empresa, assim como perda de ativos por meios de técnicas maliciosas que explorem as vulnerabilidades humanas.

Esta monografia evidenciou que, mesmo investindo em tecnologias para proteger ativos, sem que haja o entendimento que os fatores humanos devem ser considerados um pilar da segurança da informação, esses ativos permanecem vulneráveis a ameaças. Uma política de segurança da informação que não negligência esses fatores humanos tem papel essencial, uma vez que a partir do desenvolvimento da mesma é possível implementar programas de conscientização para que todos dentro da organização sejam conhecedores de seus deveres em relação aos ativos.

No desenvolvimento deste trabalho houveram dificuldades em obter obras cientificas atuais, sendo que boa parte dos materiais relevantes obtidos foram publicados entre os anos 2000 e 2010, isso especificamente sobre obras referentes aos fatores humanos na segurança da informação.

O tempo disponibilizado pela empresa para o desenvolvimento do trabalho também foi uma dificuldade pois limitou-se a uma semana, caso o tempo disponibilizado pela empresa fosse maior, as observações sobre os problemas de segurança da informação poderiam ser analisados de forma mais minuciosa, deste modo, o trabalho poderia apresentar resultados mais detalhados.

Para futuros estudos, há a possibilidade de analisar quais foram os impactos para a Ômega após a consolidação de sua PSI, bem como, analisar os resultados obtidos com as campanhas de conscientização na empresa, após alguns ciclos de melhorias do mesmo.

Obteve-se sucesso no que foi proposto nessa monografia. Fez-se o levantamento bibliográfico, possibilitando assim desenvolver entrevistas almejando

analisar quais eram as problemas relativos aos fatores humanos, com esses resultados foi possível apresentar uma proposta de plano de conscientização detalhado, com técnicas para facilitar a absorção do conteúdo proposto, para ser apresentado aos colaboradores da empresa.

6 REFERÊNCIAS BIBLIOGRÁFICAS

ABNT NBR ISO IEC 27001:2013, Tecnologia da Informação – Técnicas de Segurança – Sistemas de gestão da segurança da informação – Requisitos

ABNT NBR ISO IEC 27002:2013, Tecnologia da Informação-Técnicas de Segurança – Código de Prática para controles de segurança da informação

ASSUNÇÃO, F. **Segredos do Hacker Ético**. 1 ed. Florianópolis: Visual Books, 2002.

ASSUNÇÃO, F. **Segredos do Hacker Ético**. 2 ed. Florianópolis: Visual Books, 2008.

AVAST. **Worm de computador**. Disponível < https://www.avast.com/pt-br/c-computer-worm > Acesso em: 01 abril 2018

CAMPOS, A. **Sistemas de segurança da informação**. 2 ed. Florianópolis: Visual Books, 2007.

CERT.br- Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil- **Cartilha de Segurança para Internet**. Disponível em: < http://www.cert.br/sobre/ > Acesso em: 04 abr. 2018

Cicco – UFRN. 2016. Disponível em: < http://www.lbd.dcc.ufmg.br/colecoes/eise/2016/007.pdf > Acesso em: 08 mai 2018.

DIAS, C. **Segurança e auditoria da tecnologia da informação**. Rio de Janeiro: Axcel, 2000.

Dicio, Dicionário Online de Português. Disponível em: < https://www.dicio.com.br/ > Acesso em: 20 mar 2018

Dicionário Aurélio de Português Online. Disponível em: < https://www.dicio.com.br/aurelio-2/ > Acesso em: 20 mar 2018

GIL, A. **Como Elaborar Projetos de Pesquisa.** Edição 4. São Paulo. 2002.

LAUREANO, M. **Gestão de Segurança da Informação**. 2005 Disponível em: < http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf > Acesso: 05 fev 2018.

MARCIANO, J. **Segurança da Informação - uma abordagem social**. 2006. Disponível em: < http://www.enancib.ppgci.ufba.br/premio/UnB_Marciano.pdf > Acesso em: 09 mar 2018.

MICROSOFT. **O que é engenharia social?** Disponível < https://www.microsoft.com/pt-br/security/resources/socialengineering-whatis.aspx > Acesso: 10 mai 2018

MICROSOFT. **O spam?.** Disponível < https://www.microsoft.com/pt-br/security/resources/spam-whatis.aspx > Acesso: 3 mai 2018

MICROSOFT. **Os riscos do software pirata.** Disponível < https://answers.microsoft.com/pt-br/windows/forum/windows_7-windows_install/os-riscos-do-software-pirata/f5622291-f4ac-461b-88cb-643ddf41807f > Acesso: 26 mai. 2018

MITNICK, D.; SIMON, L. **A Arte de Enganar:** ataques de hackers – controlando o fator humano na segurança da Informação. São Paulo: Pearson Makron Books, 2003.

O GLOBO. **Investimentos em segurança da informação cresce mais no país**. Disponível em < https://oglobo.globo.com/economia/negocios/investimento-em-seguranca-da-informacao-cresce-mais-no-pais-17645471 > Acesso em: 12 jul 2018

PRESTES, V. **Fator humano:** o principal componente da segurança da informação. 2018. Disponível em: < http://computerworld.com.br/fator-humano-o-principal-componente-da-seguranca-da-informacao > Acesso em: 09 jun 2018.

SANTOS, C.; BRAGA, B. **Orientações para implantação de um Plano de Conscientização de Segurança da Informação na Maternidade Escola Januário**

SÊMOLA, M. **Gestão da Segurança da Informação**. Uma visão executiva. 1. Ed. Rio de Janeiro: Elsevier, 2003.

SOUSA, R. **Gestão de Ativos – A organização nas mãos da TI - Revista Infra Magazine 11**. 2013. Disponível em: < https://www.devmedia.com.br/gestao-de-ativos-a-organizacao-nas-maos-da-ti-revista-infra-magazine-11/27895 > Acesso em: 15 mar 2018.

Superintendência de Tecnologia da Informação e Comunicação da Universidade Federal do Rio de Janeiro (TIC-UFRJ). Disponível em < www.tic.ufrj.br/index.php/o-que-sao-incidentes > Acesso em: 15 mar. 2018.

WADLOW, T. **Segurança de Redes**. Editora Campus. Rio de Janeiro, 2000.

WURMAN, R. S. **Ansiedade de informação**: como transformar informação em compreensão. 5.ed. São Paulo: Cultura Editores, 1995. 380p.

7 APÊNDICE

Apêndice A

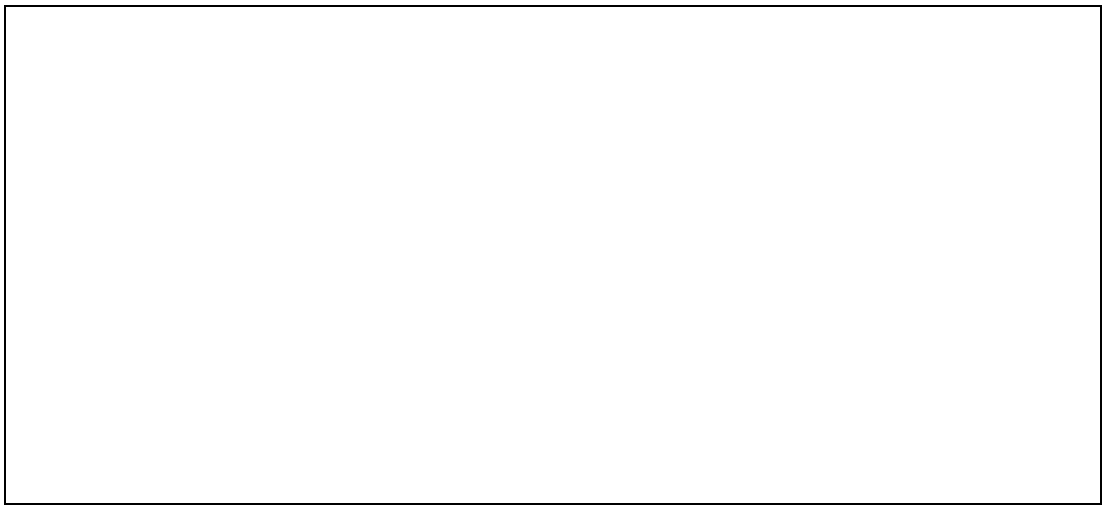
QUESTIONÁRIO DE SEGURANÇA DA INFORMAÇÃO				
Nº	PERGUNTAS	SIM	NÃO	S/R*
1	A segurança da informação é importante para a empresa?			
2	Você já passou por algum treinamento ou fez curso sobre segurança da informação?			
3	Você concorda que a segurança da informação é responsabilidade exclusiva da equipe de TI?			
4	Você salva documento na área de trabalho do computador ou costuma deixar documentos, agendas, anotações em cima da sua mesa de trabalho?			
5	É possível instalar softwares (programas) nos computadores da empresa?			
6	Quando você se ausenta do seu local de trabalho, costuma bloquear o computador?			

7	Os computadores da empresa possuem antivirus?			
8	Já utilizou computador pessoal para acessar informações da empresa para realizar alguma tarefa?			
9	Existem recomendações sobre a realização cópias de segurança de arquivos?			
10	É comum o uso de mídias removíveis (*pendrive*, HD, cartão de memória e etc.) pelos funcionários na empresa?			
11	Existe alguma recomendação em relação a criação de senhas, quando se faz necessário?			
12	Já utilizou nome de usuário e/ou senhas de e-mail corporativo ou similar de colega de trabalho?			
13	Quando faz-se necessário a impressão de algum arquivo de texto ou tabela contendo informações relacionadas a função que você exerce na empresa, você busca-os rapidamente?			
14	Existe algum procedimento padrão para descarte de documentos (Relatórios, Análises de Produção)?			

15	Você já ouviu falar em Engenharia Social?			
16	Você faz uso de telefone celular dentro da empresa?			
17	Utiliza o telefone para receber ou transmitir informações da empresa?			
18	Já utilizou a rede da empresa para realizar downloads que não possuem relação com sua função?			
19	Você conversa sobre informações relativas a sua função em ambientes públicos e/ou áreas comuns a todos os colaboradores (recepção, refeitório, banheiro)?			
20	Existem locais dentro da empresa onde o acesso é restrito a um determinado grupo de funcionários?			
*Sem resposta				
OUTRAS PERGUNTAS E OBSERVAÇÕES				

Apêndice B

QUESTIONÁRIO DIRECIONADO AO GESTOR DE TI			
Nº	PERGUNTAS	S	N
1	A empresa possui inventário de ativos?		
2	A empresa classifica e rotula com (públicas, internas, confidenciais e sigilosas) as informações contidas em todos os seus documentos (texto em pdf ou .txt e planilhas e etc), de forma que os colaboradores tomem ciência e tenham o comportamento condizente com o nível instituído pela empresa?		
3	Cite dois problemas atuais da empresa relacionados ao fator humano que comprometem a segurança da informação.		
ESPAÇO RESERVADO A OBSERVAÇÕES			



Apêndice C

COMUNICADO DA DIRETORIA

As tecnologias da informação nas últimas décadas tem alavancado o desenvolvimento empresarial de todos os ramos uma vez que tornam os acessos a informação mais rápidos e precisos, nossa empresa também se beneficia destes recursos tecnológicos, toda via estas tecnologias possuem vulnerabilidades, para auxiliar na redução destas é que existe a segurança da informação.

Senhores colaboradores, é para evitar exposição, furtos e roubos de dados sensíveis, dentre outras razões que destaco a importância da segurança da informação para a nossa empresa. Com base nisto, reforço a importância da criação da Política de Segurança da Informação em nossa empresa, para que com ela e com os senhores possam seguir apoiando a empresa, melhorando o nível de segurança tornando-a mais competitiva e dinâmica.

Desde já agradeço,

_____

Diretor Geral da Empresa Ômega S.A.