INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO SERTÃO PERNAMBUCANO – CAMPUS FLORESTA

AILSON KELVY NUNES CALAÇA

POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO: FASES PLANEJAMENTO, DESENVOLVIMENTO E IMPLEMENTAÇÃO - UMA REVISÃO BIBLIOGRÁFICA

FLORESTA-PE

2015

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO SERTÃO PERNAMBUCANO – CAMPUS FLORESTA

AILSON KELVY NUNES CALAÇA

POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO: FASES PLANEJAMENTO, DESENVOLVIMENTO E IMPLEMENTAÇÃO - UMA REVISÃO BIBLIOGRÁFICA

Orientador: Lincoln Tavares dos Santos

Monografia orientada pelo prof. Esp. Lincoln Tavares dos Santos a ser apresentada à banca examinadora do IF Sertão-PE como requisito parcial para obtenção do título de Tecnólogo em Gestão da Tecnologia da Informação

FLORESTA-PE

2015

FICHA CATALOGRÁFICA

Calaça, Ailson Kelvy Nunes.

Políticas de Segurança da Informação: fases planejamento, desenvolvimento e implementação - uma revisão bibliográfica. / Ailson Kelvy Nunes Calaça. – Floresta, 2015.
62 p. : il.

TCC (Graduação) – Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano – Campus Floresta. Gestão de Tecnologia da Informação.

Orientador: Prof. Lincoln Tavares dos Santos.

1. Segurança da Informação. 2. Dados (Informática). 3. Política de Segurança da Informação. I. Título. II.Santos, Lincoln Tavares dos.

CDD 658.472

AILSON KELVY NUNES CALAÇA

POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO: FASES PLANEJAMENTO, DESENVOLVIMENTO E IMPLEMENTAÇÃO – UMA REVISÃO BIBLIOGRÁFICA

Esta monografia foi julgada e aprovada para obtenção do título de Tecnólogo, no curso de Gestão da Tecnologia da Informação, no Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano.

Floresta, 13 de Março de 2015.

Cassiano Henrique de Albuquerque
Coordenador do Curso de Gestão de Tecnologia da Informação

BANCA EXAMINADORA

_____
Prof. Esp. Lincoln Tavares dos Santos (IF SERTÃO-PE Orientador)

_____
Prof. Esp. Elismar Moraes dos Santos (IF SERTÃO-PE)

_____
Prof. MSc. Cassiano Henrique de Albuquerque (IF SERTÃO-PE)

Dedico este trabalho aos meus pais pelo apoio e incentivo

Primeiramente agradeço a Deus por mais essa conquista. Agradeço a meus pais que sempre me incentivaram nos estudos, a todo o corpo de funcionários do IF Sertão PE Campus Floresta pela amizade e palavras de incentivo. Ao meu orientador Lincoln Tavares dos Santos que sempre esteve ao meu lado nessa caminhada. Por fim, a todos meus amigos e todos aqueles que expressaram apoio.

“Não sabendo que era impossível, ele foi lá e fez”

Jean Cocteau

Resumo

Nos dias de hoje têm se em quase todas as empresas, governos, universidades, lares e outros tipos de usuários em geral integrados na *World Wide Web* (WWW), a Internet. Nessa grande rede circula uma quantidade muito grande de informações e dados. Alguns desses muito importantes e que tem um alto valor para emissores e receptores dessas informações. Nos meios de comunicação (TV, jornais, Internet) nota-se quase todos os dias notícias sobre extravios de dados e informações. Hoje as tecnologias estão se desenvolvendo a uma velocidade muito grande e é sabido que as tecnologias usadas por pessoas mal intencionadas são equivalentes às que usuários honestos usam, percebe-se então que é muito perigoso manter e armazenar dados e informações de uma maneira que tenham nenhuma ou pouca segurança. A organização que deseja ter suas informações seguras de qualquer tipo de ameaça precisa desenvolver regras e normas que organizem e regulem a criação, organização, armazenamento, transmissão, recebimento e descarte de dados e informações. O conjunto dessas normas e procedimentos é denominado “Políticas de Segurança da informação (PSI)”. As empresas estão aplicando uma política de segurança que normatize o trato com a informação? Quais são alguns dos desafios encontrados no processo de implementação da PSI? O presente trabalho tem como foco mostrar os objetivos da PSI, dar uma visão geral de como se dá o planejamento, a criação, a implementação, dar uma visão aprofundada de sua importância em um mundo perigoso para o armazenamento e transmissão da informação.

Palavras-chave: Dados. Informação. Segurança da Informação. Política de Segurança da Informação.

Abstract

Nowadays almost all businesses, governments, universities, nursing homes and other general users are integrated into the World Wide Web (WWW), the Internet. In this large network circulates a large amount of information and data. Some of these are very important and that has a high value for senders and receivers of information. In the media (TV, newspapers, Internet) announces almost every day news about misplacement of data and information. Today technologies are developed at a very high speed and it is known that the technologies used by dishonest people are equivalent to the ones honest users have. It is clear then that it is very dangerous to maintain and store data and information in a manner that have little or no security. Companies who wish to have their information safe from any kind of threat needs to develop rules and regulations that organize and regulate the creation, organization, storage, transmission, receipt and disposal of data and information. This set of rules and procedures is called "Information Security Policy (ISP)." Are companies applying a security policy that will regulate the dealings with the information? What are some of the challenges encountered in the ISP implementation process? This paper focuses on the objectives of the ISP present an overview of how is the planning, creation, and implementation; give a thorough view of its importance in a dangerous world for the storage and transmission of information.

Keywords: Data, Information, Information Security. Information Security Policy

SUMÁRIO

Lista de Figuras

Lista de abreviaturas e siglas

BS - *British Standard*

COBIT - *Control Objectives for information and related Technology*

DOS - *Denial of Service* (negação de serviço)

ISSO - *International Organization for Standardization*

ITIL® - *Information Technology Infrastructure Library*

IEC - *International Electrotechnical Commission*

NBR - Norma Brasileira

PDF - *Portable Document Format*

PSI - Política de Segurança da Informação

SGBD - Sistema de Gerenciamento de Banco de Dados

SWOT - Acrônimo para *Strenghts, Weakness, Oportunities, Threats*.

TI - Tecnologia da Informação

WWW - *World Wide Web*

INTRODUÇÃO

As tecnologias da informática avançaram muito em desenvolvimento e hoje estão em praticamente todas as residências, microempresas e grandes empresas. Essas tecnologias são usadas para inúmeros fins, que sejam: processamento de dados, telecomunicações, comunicação interna e externa à empresa, transporte e armazenamento de dados entre outros fins.

A tecnologia mudou. Se antes da era digital as empresas podiam armazenar suas informações com segurança em gavetas e trancadas em cofres, hoje isso deve ser analisado de outra forma, pois grande parte das informações migraram para o meio eletrônico (SILVA, 2012, pág. 1), portanto vulnerabilidades de ataques surgiram. Se antes praticamente só era possível um ataque físico, hoje um atacante pode roubar informações de muito longe do alvo, através dos meios de comunicação atuais. O transporte e o armazenamento dos dados é uma questão crítica nas organizações visto que a maior parte das empresas tratam essas informações como confidenciais, e estas são ativos que têm um valor agregado grande em empresas que prezam pela eficiência, produtividade e resguardo das informações dos clientes. Com frequência são noticiados casos de vazamentos de informações de clientes, números de cartões de créditos, senhas entre outros casos. Nakamura (2007, pág. 27) explica que:

> Alguns incidentes mostram que os prejuízos com a falta de segurança podem ser grandes. O roubo de 5,6 milhões de números de cartões de crédito da Visa e da MasterCard de uma administradora de cartões americana, em fevereiro de 2003 [JT03], por exemplo, pode sugerir grandes problemas e inconvenientes para as vítimas [...].

O canal Corporate (2014) enumera os maiores vazamentos de informações do ano de 2013. Segundo o canal alguns dos maiores vazamentos de 2013 foram:

– Adobe: 152 milhões de senhas e nomes de usuários foram disponibilizados na Internet com 2,8 milhões de dados adicionais.

– Target: Vazamento de 70 milhões de dados de clientes e 40 milhões de informações bancárias como números de senhas e cartões de crédito e débito (a empresa afirmou que usava sistemas de segurança de acordo com as normas regulatórias, após uma investigação concluiu-se que a única proteção usada era uma cópia gratuita do antivírus Malware-bytes).

– Ubisoft: *Hacker*s tiveram acesso a um banco de dados de 58 milhões de usuários, com informações como *e-mail*, nomes e senhas.

– Evernote: 50 milhões de usuários tiveram de resetar suas senhas após um acesso não-autorizado aos servidores do aplicativo de compartilhamento de anotações.

Notícias como essas são frequentes e mostram que o perigo de se ter informações vazadas e, principalmente, informações de terceiros e de clientes divulgadas sem autorização são problemas que todas as empresas estão sujeitas e que precisam trabalhar para evitá-los. Precisam investir na Segurança da Informação para que estas sejam resguardadas e garantam os três princípios básicos da segurança da informação: a integridade, a confidencialidade e a disponibilidade. Para que a organização tenha êxito no resguardo dessas informações é necessário que se criem normas e procedimentos bem estabelecidos onde todas as pessoas que possam ter acesso às informações seguirão cuidadosamente rotinas e procedimentos evitando assim o acesso de estranhos a esses dados. Esse conjunto de normas e procedimentos tem como objetivo a proteção dos dados e informações da empresa e de clientes e normatizar todo o trato com a informação, este processo é denominado “Política de Segurança da Informação” (PSI).

Nakamura (2007, pág. 188) define a PSI como “a base para todas as questões relacionadas à proteção da informação, desempenhando um papel importante em todas as organizações”. Campos (2007, pág. 129) dá uma definição de Política de Segurança de Informação com mais detalhes: “a política é um conjunto de regras, normas e procedimentos que determina qual deve ser o comportamento das pessoas que se relacionam com a organização no que se refere ao tratamento

da informação”. Portanto segundo o autor, a PSI é um conjunto de normas que definem regras para as pessoas que tenham acesso a informações da organização em questão saibam o que podem e o que não podem fazer com elas, se podem revelá-las a estranhos à organização ou mantê-las em sigilo.

Segundo a norma ABNT NBR ISO IEC 27001 (2006, pág. 14) a PSI é um controle da segurança da informação que tem como objetivo “prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes (ABNT, 2006). A organização deve saber o momento de criar uma PSI, saber o porquê de sua criação, os desafios encontrados em sua implementação, de quanto em quanto tempo deverá atualizá-la.

Uma empresa ao decidir implantar uma PSI seguramente encontrará vários desafios em sua implementação. Alguns desses desafios de implementação são, de acordo com Nakamura (2007, pág. 200): Recursos financeiros insuficientes e prioridades diferentes entre a PSI, incompreensão da importância da PSI para o resguardo das informações, desinteresse em trabalhar continuamente com a PSI, percepção de complexidade do uso da Política, falsa percepção de ameaça ao poder dos diretores, inexistência de um processo disciplinar. Todos esses desafios podem ser transpostos se forem seguidos alguns pontos. Silva (2012, pág. 64) coloca alguns pontos para que essa Política tenha sucesso e não caia no esquecimento como por exemplo: Ser verdadeira, ter o apoio da direção, não ser um manual, não ser um documento técnico, ser simples. Seguindo esses procedimentos a PSI irá contribuir para ajudar a organização a manter suas informações em uma margem de segurança aceitável e a transpor os desafios de implementação da melhor forma.

Conceitua-se a PSI como um documento com diretrizes, normas e procedimentos em que são trabalhados os princípios da segurança da informação nas organizações. Percebe-se que a PSI é um documento de grande importância, visto alguns autores considerá-la o primeiro passo de uma organização rumo à cultura de segurança, num mundo repleto de ameaças como o de hoje.

1.1 TEMA E PROBLEMA

O tema desse trabalho é a segurança da informação e a implementação de PSIs. O problema a qual o trabalho se propõe a solucionar é o seguinte: “Como são desenvolvidas as abordagens dos processos de planejamento, desenvolvimento e implementação de uma PSI?”

1.2 OBJETIVOS

1.2.1 Objetivo geral

 Desenvolver uma revisão bibliográfica abordando o tema “PSI” com abordagem direcionada às fases de planejamento, desenvolvimento e implementação em empresas.

1.2.2 Objetivos específicos

 Desenvolver uma revisão da literatura relativa ao tema PSI.

 Desenvolver uma análise direcionada a alguns dos desafios de implementação de PSI.

 Abordar os processos de planejamento, desenvolvimento e implementação de PSIs.

1.3 JUSTIFICATIVA

A segurança da informação é um fator importante para qualquer organização. A garantia de que as informações dos clientes estão seguras é uma obrigação de qualquer empresa. As empresas devem garantir segurança para as informações de seus clientes e isto está previsto na lei brasileira e internacional. Por exemplo, o Código Penal brasileiro nos artigos 153 e 154 dá a previsão aos crimes por Divulgação de Segredo e Violação do Segredo (SILVA, 2012, pág. 63). No campo internacional a mais famosa das leis é a Sarbanes-Oxley, também conhecida como Sox ou Sarbox, é uma lei americana que “prevê a criação, nas empresas, de mecanismos de auditoria e segurança confiáveis, definindo regras para a criação de comitês encarregados de supervisionar suas atividades e operações, formados em boa parte por membros independentes” (PORTAL DE AUDITORIA).

Esse é um tópico que ocupa constantemente o noticiário da tecnologia ou até mesmo criminal. Uma PSI bem implementada dará a empresa que a aplica coerência e facilidade para se tomar diversas decisões relativas à segurança da informação. As decisões são reconhecidas como justas porque se baseiam num documento conhecido (quando bem divulgado na etapa de implementação) por todos e não pela vontade daquele que decide. Segundo Nakamura (2007, pág. 188), a PSI é o marco inicial para que sejam adotados os primeiros e mais importantes passos em direção à consolidação da segurança da informação em qualquer organização. Silva (2012, pág. 60) também traz o mesmo discurso ao afirmar que a PSI é o primeiro passo efetivo para se disciplinar a questão da segurança da informação dentro das organizações. Segundo Nakamura (2007, pág. 198) o procedimento mais complicado dentre o planejamento, o desenvolvimento e a implementação é este último devido a alguns fatores, alguns desses fatores de acordo com o autor são recursos financeiros insuficientes, incompreensão da importância da PSI para o resguardo das informações, desinteresse em trabalhar continuamente com a PSI, percepção de complexidade do uso da Política, falsa percepção de ameaça ao poder dos diretores. É importante que sejam esclarecidos esses fatores à luz da literatura da área para que a implementação da PSI seja efetiva. O presente trabalho escrito como revisão bibliográfica dará subsídios importantes para que sejam conhecidos os preceitos

mais importantes da questão da segurança da informação aplicadas nas empresas trabalhadas nessas três fases: planejamento, desenvolvimento e implementação.

2 REFERENCIAL TEÓRICO

2.1 Breve histórico da Segurança da Informação

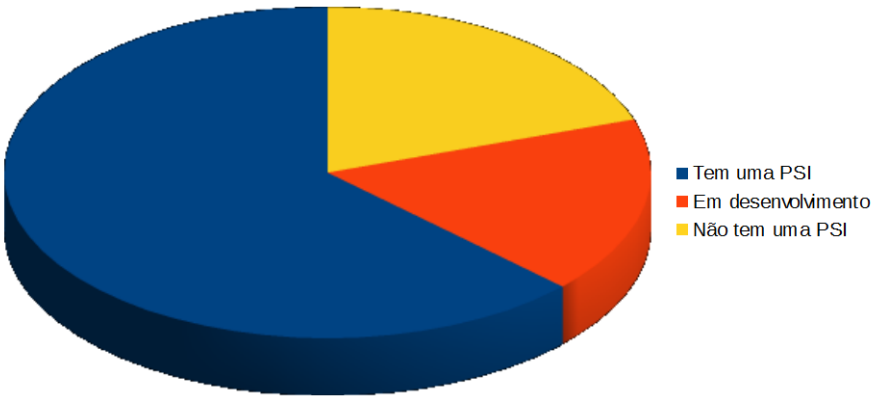
Segundo Lago a segurança da informação começa no Antigo Egito quando escribas e sacerdotes mediavam a vontade do faraó. O acesso às informações era restrito, os hieróglifos, as inscrições sagradas, dificilmente alguém conseguia decodificar quanto maior complexidade. Posteriormente, segundo o mesmo autor temos evoluções na segurança como a Cifra de César onde ele alterava as posições das letras e até reforçava essa segurança trocando letras latinas por gregas, temos também vários outros modos de proteger a informação como métodos hebreus, evitando que pessoas não autorizadas tenham acesso a essas informações. Já Von Solms (1996) *apud* Al-Awadi e Renaud (Pág. 2), explica que a questão da segurança da informação evoluiu em três estágios. No primeiro desses estágios nos anos sessenta a maior preocupação entre todas era com a segurança física da informação. A segurança da informação se preocupava com as instalações físicas e documentos físicos. A exemplo disso, as impressões naquela época circulavam em modo protegido. O segundo estágio iniciou-se em meados dos anos setenta quando a segurança da informação foi adaptada a necessidades individuais de cada organização, isso mesmo a importância e escopo da segurança da informação tendo aumentado radicalmente. No terceiro estágio com o advento da tecnologia avançada as organizações tiveram a necessidade de interligar seus serviços de TI e evoluir de um ambiente de trabalho fechado para ambientes complexos onde suas máquinas passariam a trabalhar em rede de forma interligada adicionando assim, mais complexidade ao tema.

2.2 O estado atual do trabalho com Políticas de Segurança no Brasil

O atual estado do trabalho com Políticas de Segurança no Brasil está melhorando dia após dia. Pesquisa citada por Nakamura (2007, pág. 191) mostra que a política de segurança da informação no Brasil era realidade em apenas 39% das

organizações. Segundo a pesquisa citada por esse autor, 16% das organizações possuíam uma política não atualizada, 30% possuíam uma política ainda em desenvolvimento e 15% não possuíam uma política formalizada. Levantamento do TCU em 2012 constatou que 45% das entidades da administração pública federal possuíam uma Política de Segurança da Informação (TCU, 2012). Pesquisa mais recente, realizada pela Daryus dá conta que em relação a anos anteriores, o aspecto do uso de PSIs está bem melhor. Segundo essa pesquisa, realizada de Junho a Agosto de 2014 no Brasil 63,11% das empresas no Brasil tem uma Política de Segurança da Informação e 17,21% está com uma em desenvolvimento (DARYUS, 2014). Abaixo tem-se o gráfico da pesquisa realizada pela Daryus:

Figura 1 - O uso de PSIs no Brasil



Fonte: Daryus, 2014.

2.3 Conceitos

O tema desse trabalho, a segurança da informação e implementação de PSI refletem alguns conceitos que para seu entendimento devem ser bem explicados. Num primeiro momento lê-se palavras como, segurança, política. Além dessas palavras existem duas outras que dizem respeito ao trabalho: *dado e informação*. Existe um consenso entre os autores que explica que o conjunto de dados são o

componente da informação. O que seriam dados? O que seria informação? Qual o significado de política? O que é segurança?

Política, na visão de Ferreira (2009, pág. 1592) é a "*habilidade no trato das relações humanas, com vista à obtenção dos resultados desejados".* Ou seja para esse autor o termo política significa o trabalho das relações humanas com o intuito de alcançar objetivos / resultados que se deseje. Sobre segurança*,* Mitnick (1963, pág. 4) diz que *"c*omo observou o consultor de segurança Bruce Schneier, ' a segurança não é um produto, ela é um processo'. Além disso ela não é um problema para a tecnologia – ela é um problema para as pessoas e para a direção".

Chiavenato (2000) *apud* Lanverly *et al.* (2014, pág. 2) diz que os dados são os elementos que servem de base para a formação de juízos ou para a resolução de problemas, ainda segundo o autor o dado é apenas um índice, registro que é passível de uma análise subjetiva sendo necessário de alguém para sua manipulação (e consequente transformação em informação). Somasundaram e Shrivastava (2011, Pág. 27) definem dado como um conjunto de fatos que estão em estado bruto a partir dos quais conclusões podem ser tiradas. Os autores também dão uma classificação aos dados. Segundo eles, os dados podem ser classificados como sendo do tipo estruturados e não estruturados. Os dados estruturados seriam dados que estão armazenados de uma forma que possam ser facilmente encontrados por meio de aplicativos empresariais de relacionamento com o cliente a exemplo de um SGBD. Os dados não estruturados seriam dados que não poderiam ser consultados rapidamente por meio de aplicativos empresariais. A exemplo disso pode-se citar números de telefones armazenados na extensão PDF (SOMASUNDARAM & SHRIVASTAVA, 2011, pág 29). Tanto em Somasundaram e Shrivastava quanto Lanverly *et al*, percebe-se a necessidade de uma análise dos dados para que possa se obter a informação. Lanverly *et al.* (2014, pág. 2) define a informação como sendo o conjunto de dados classificados, armazenados e relacionados entre si. Somasundaram & Shrivastava (2011, pág. 29) definem a informação como a inteligência e o conhecimento derivados dos dados.

Figura 2 - A segurança da informação deve ser encarada como um processo contínuo, nunca como um produto

Fonte: disponível em: < http://pixabay.com/pt/leitura-homem-lendo-revista-385059/> . Acesso em 09 Nov. 2014.

A segurança da informação de acordo com a norma ABNT NBR ISO IEC 27001 (ABNT, 2006) é a “Preservação da confidencialidade, integridade e disponibilidade da informação; adicionalmente outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade podem estar envolvidas”. Com base nas definições apresentadas anteriormente, a segurança da informação poderá ser definida como um processo contínuo baseado em métodos, pessoas capacitadas e na gestão da organização com a ajuda, ou não, de tecnologias apropriadas que visam garantir no mínimo os três princípios básicos (CAMPOS, 2007, p.17) para o trato com a informação: a confidencialidade , a integridade, e a disponibilidade dessas informações.

O princípio da confidencialidade é garantido quando somente pessoas autorizadas tem acesso as informações em questão, quando pessoas não autorizadas tem acesso a essas informações então tem-se um incidente de

segurança da informação em virtude da quebra de confidencialidade. O princípio da integridade tem como objetivo garantir que as informações estão íntegras e não foram alteradas, pelo menos não quando não houver autorização para isso. Pessoas podem intencionalmente ou não acessar arquivos em sistemas de computadores e apagá-los ou alterá-los. Quando se tem um caso a exemplo desse, em que a partir disso as informações não estão mais confiáveis então há um incidente de segurança da informação por quebra de integridade (CAMPOS, 2007, p.18). A disponibilidade se dá pela garantia de que a informação estará disponível no momento exato em que for solicitada, requerida. Se uma informação ou mesmo dados simples são apagados ou não estão nos lugares exatos quando temos necessidade deles, então temos um incidente de segurança por quebra de disponibilidade. Quando a organização/instituição se empenha para garantir esses três princípios fundamentais, pode se afirmar que ela está no caminho certo para que a proteção de seus dados e informações sejam garantidos.

2.4 Ativos de Informação

Ativos de informação são os componentes dos processos de criação, transmissão, armazenamento, recebimento e descarte da informação. Segundo Campos (2007, pág. 22), os ativos da informação são: a Informação, as tecnologias, as pessoas, os processos e os ambientes.

A informação é um bem de inestimável valor para qualquer organização, como se sabe, mas a informação é um bem abstrato que depende de meios para se fazer existir, a exemplo de papéis, discos rígidos, disquetes, fitas magnéticas, arquivos de aço, ondas de rádio e até mesmo no conhecimento das pessoas. A partir disso, pode se perceber que o meio que a mantém é tão importante quanto ela própria. Sem esses meios não haveria qualquer tipo de informação. A informação em si consiste de um conjunto de dados devidamente organizados e compreensíveis, da qual a partir desses pode se tirar conclusões válidas. Exemplos de informação: mensagens, dados de sistema, ideias.

O ativo de informação denominado tecnologia consiste no meio que suporta

a informação a exemplo da mente humana, papel, correio eletrônico, sistemas de informação entre outros. As pessoas são ativos tão importantes quanto a própria informação, são as pessoas que geram, consomem e se utilizam da informação para os mais diversos fins. Exemplos: gerente de vendas, contador, diretor financeiro, entre outros. Segundo Campos (2007, pág. 80) as pessoas são os ativos mais importantes, pois são elas que geram e consomem informações, utilizam os ambientes, executam os processos e utilizam as tecnologias podendo também serem considerados os que mais oferecem riscos. Os processos são os métodos trabalhados no trato com a informação a exemplo das normas para uso do correio eletrônico, métodos de descarte da informação, entre outros processos. Os ambientes são locais físicos que possuem informações que precisam serem protegidas. Exemplos: sala de arquivos, sala de servidores, espaços para armazenamento de mídias digitais, entre outros. (CAMPOS, 2007, pág. 22). Para que a segurança da informação esteja, pelo menos em tese, garantida, a política de dados a ser elaborada precisa contemplar todos esses ativos.

2.5 Metodologias atuais na segurança da informação

Existem várias ferramentas das quais pode-se trabalhar nos processos em torno da PSI e da segurança da informação, o COBIT e o ITIL[1]® são algumas dessas principais *frameworks* usadas (normas da ISO também são amplamente utilizadas, mas serão comentadas posteriormente). Segundo Freitas (2010, pág. 56) as práticas de TI mais utilizadas atualmente são essas, o COBIT e o ITIL®. Pesquisa da Daryus (2014, Pág. 24) dá conta que a certificação ITIL® foi a mais requisitada entre os pesquisados, segundo a mesma pesquisa a certificação COBIT foi a terceira mais requisitada. O ITIL® aborda no processo do Ciclo do Desenho do Serviço chamado Gerenciamento de Segurança da Informação a problemática das PSIs. Já o COBIT inclui guias de implementação, detalhes dos facilitadores e utilização do COBIT na área de segurança da informação.

[1] [1] "ITIL® é uma marca registrada do The Cabinet Office no Reino Unido e em outros países"

2.6 **As normas ISO**

A Política de Segurança da Informação pode ser desenvolvida tendo como base o conjunto de normas ISO relacionadas à Segurança da Informação. O padrão BS 7799 parte 1 foi o primeiro padrão da área desenvolvido pela ISO, esse padrão foi desenvolvido em 1995 e se referia a o conjunto de práticas relativas ao gerenciamento da Segurança da Informação. Já o BS 7799 parte 2 foi desenvolvido em 1998 e se referia a especificação para sistemas de Gestão de Segurança da Informação. Esses padrões foram atualizados para a norma ISO/IEC 17799, uma norma internacional em relação aqueles padrões desenvolvidos pelos britânicos. Esses padrões foram atualizados para os atuais ISO/IEC 27001 e ISO/IEC 27002 (NAKAMURA, 2007, pág. 190).

3 METODOLOGIA

Metodologia é a descrição com detalhes dos métodos, técnicas e processos seguidos na pesquisa explicando as hipóteses ou os pressupostos, a população ou amostra, os instrumentos e também a coleta de dados (UFMG, 2014). A metodologia usada nesse trabalho foi a pesquisa bibliográfica que tem como finalidade colocar o autor em contato direto com tudo o que foi escrito, dito ou filmado sobre determinado tema, inclusive conferências seguidas de debates, que tenham sido transcritos de alguma forma, quer publicadas, quer gravadas (MARCONI, 2010, pág. 166). Koche (2012, pág. 122) define a pesquisa bibliográfica como “a que se desenvolve tentando explicar um problema utilizando o conhecimento disponível a partir das teorias publicadas em livros ou obras congêneres”.

Sendo assim, a pesquisa foi feita baseada em documentos, impressos e digitais que de alguma forma continham contribuições para o tema. Portais, teses, normas, trabalhos acadêmicos, monografias, textos em outros idiomas que não o português também foram trabalhados, visto que determinados temas são mais difíceis de serem encontrados em português. A técnica utilizada na pesquisa foi a pesquisa bibliográfica com caráter exploratório e qualitativo, com levantamento de informações e literatura relativas à segurança da informação e implementação de PSI, visando fomentar um debate com esse tema.

Marconi (2010, pág. 166) afirma que “a pesquisa bibliográfica não é mera repetição do que já foi dito ou escrito sobre certo assunto, mas propicia o exame de um tema sob novo enfoque ou abordagem, chegando a conclusões inovadoras.” Esse trabalho segue essa colocação, a pesquisa não é apenas repetição de outros trabalhos, foram consultadas obras, textos, teses, artigos, monografias, artigos. Feita a leitura desses trabalhos foi elaborado uma análise: o presente trabalho. Outros trabalhos são citados mas existe um ponto de vista com relação ao tema e com base nessas citações são tiradas conclusões e é dada assim uma contribuição ao tema.

4 O PLANEJAMENTO PARA A CRIAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Tendo conhecimento do que são os ativos da informação, o passo seguinte no trabalho com a PSI é o seu planejamento. A política de segurança trata de todos os aspectos que podem de alguma forma afetar a segurança da informação na empresa. Ao se falar sobre a importância de políticas de segurança em ambientes informatizados, pode-se pensar somente na parte tecnológica da empresa, mas um ataque vem quase sempre de um ser humano que de alguma forma usou de seu conhecimento para cometer uma atitude maliciosa. Uma política de segurança eficaz "trata dos aspectos humanos, culturais e tecnológicos de uma organização, levando também em consideração os processos e os negócios, além da legislação local." (Nakamura 2007, pág. 189). Dessa forma as pessoas encarregadas do planejamento e elaboração da política de segurança devem abordar a engenharia social, os aspectos tecnológicos, a cultura dos funcionários, processos e negócios e também, muito importante, a legislação local e a dos âmbitos superiores que de alguma forma digam respeito a ela. Durante a fase de planejamento é necessário fazer um inventário de ativos e desenvolver uma análise de risco.

O inventário de ativos, segundo é ABNT ISO IEC 27001 (Pág. 24) é um controle em que "todos os ativos devem ser claramente identificados e um inventário de todos os ativos importantes deve ser estruturado e mantido."

A análise de riscos (AR) segundo a ABNT ISO IEC 27001 (Pág.11) é " o uso sistemático de informações para identificar fontes e estimar o risco". Essa análise tem um papel fundamental na segurança da informação, visto que sabendo onde estão os maiores riscos, pode-se alocar recursos suficientes para tratá-lo.

A equipe encarregada da elaboração da política deve se ater num ponto importante: não permitir que a política de segurança seja apenas reativa, só procurar a solução do um problema a partir da sua ocorrência mas sim trabalhar em torno da pró-atividade. Segundo a norma ABNT NBR ISO IEC 27001 (pág. 13), " ações para prevenir não conformidades frequentemente tem melhor custo-benefício que ações corretivas." Tendo isso em mente, a equipe de planejamento deve sempre trabalhar procurando brechas em que problemas possam aparecer de alguma forma e

também na prevenção desses possíveis problemas para que não ocorram novamente.

Figura 3 - A PSI deve ter como características o caráter preventivo e não apenas o reativo.

Fonte: disponível em: <http://pixabay.com/pt/pol%C3%ADtica-de-privacidade-445153/ >. Acesso em: 01 out. 2014

Trabalhando com esse princípio preventivo, uma empresa em sua fase de planejamento para a criação da PSI pode pensar na contratação de um *hacker* ético, um profissional que, devidamente capacitado na área de segurança, irá trabalhar para descobrir possíveis brechas nos sistemas de informação de seu posto de trabalho, sua empresa, organização e a partir daí procurar sua solução ou, se não for autorizado a isso, encaminhar o problema para os responsáveis na área de segurança (CONVERGÊNCIA DIGITAL, 2014)**.** Existe uma demanda por certificações em muitas áreas de negócio (NAKAMURA, 2007, pág. 191), um investidor que deseje um boa implementação para seu investimento poderá solicitar uma certificação para garantir que não tenha problemas futuros com a segurança, e com a PSI não é diferente. Devido à crescente demanda da segurança da

informação, as certificações na área de política de segurança irão crescer continuamente como um diferencial competitivo na Era da Informação. As normas ISO IEC 27001 e ISO IEC 27002 indicam que as PSIs são um controle essencial, que tem um grande impacto para que a informação seja protegida.

Com o uso determinado pelo pessoal ou comissão competente da PSI, as decisões relacionadas à Segurança da Informação serão aceitas com mais facilidade, porque serão determinadas por um grupo ou pessoal capacitado para ser aplicada a todo o pessoal da organização inclusive os próprios desenvolvedores dessa Política e também porque será conhecida por todos e amplamente divulgada. Esta dificilmente seria aceita, ou seria aceita com receios se fosse aplicada ou desenvolvida pelo critério pessoal daquele que toma as decisões e não por pessoas capacitadas.

Nakamura, (2007, pág. 191) sugere que no planejamento de uma política de segurança, a mesma seja dividida em vários níveis, como um nível genérico, um nível dos usuários e um nível técnico. O nível genérico se aplicaria a equipe gerencial da empresa, visto que existe a possibilidade de os gerentes possivelmente não dominarem os termos técnicos e procedimentos mais específicos, assim o nível genérico seria apropriado para que os administradores soubessem o que está se passando na empresa. O nível dos usuários se aplicaria para que estes tenham consciência dos seus papéis e responsabilidades para a manutenção da segurança da informação dentro da empresa chegando até o nível técnico que se aplicaria a tópicos bem específicos como a implementação de regras num firewall (NAKAMURA, 2007, pág. 191).

Para que o planejamento da PSI dê resultados, além de outros itens, é necessário que a mesma tenha o aval dos diretores da empresa, o pessoal encarregado dessa tarefa terá de elaborá-la de uma forma que ela de fato dê resultados no sentido de aumentar a produtividade e os ganhos na empresa e que não atrapalhe de forma nenhuma o conjunto de processos da empresa. Um conjunto de normas e procedimentos como a PSI não pode ser um documento burocrático que atrapalhe ou diminua o ritmo de produção da empresa, se essa Política não fizer exatamente o contrário disso, poderá ser extirpada da empresa por seus diretores (CAMPOS, 2007, pág. 130). Mitnick (1963, pág. 8) também confirma essa colocação

quando diz que

> Pouca ou nenhuma segurança deixa a empresa vulnerável, mas uma ênfase exagerada atrapalha a realização dos negócios e inibe o crescimento e a prosperidade da empresa. O desafio é atingir um equilíbrio entre a segurança e a produtividade.

Uma empresa que deseja ter uma política de segurança eficaz precisa que sua elaboração seja unânime e de conhecimento de todos. Precisa também que tenha o aval e assinatura de seus diretores para que possa ser aplicada de forma legal e reconhecida. Depois de elaborada a Política, esta precisa ser divulgada ao máximo e é necessário que esteja sempre acessível a todo e qualquer funcionário da empresa para que possa ser aceita por todos.

5 O DESENVOLVIMENTO DA PSI

Lourenço (2009, pág. 29) afirma que o primeiro passo para firmar uma Política de Segurança da Informação é a correta classificação de ativos a serem protegidos, a partir daí a equipe de desenvolvimento irá alocar os recursos conforme o grau de importância de cada um dos ativos, Ugerman (2005) corrobora dessa afirmação quando explica que o primeiro passo no desenvolvimento da PSI é a avaliação dos ativos de informação e identificação das ameaças para esses ativos (UGERMAN, 2005). Existe uma ferramenta que pode ser útil no desenvolvimento da PSI, essa ferramenta é a matriz SWOT. Segundo Chiavenato (2014, pág. 175) “trata-se de uma tabela de dupla entrada na qual nas linhas estão as forças e fraquezas organizacionais e nas colunas as oportunidades e ameaças ambientais”. A utilização da matriz SWOT (TCU, 2010) pode ser útil no desenvolvimento da PSI, a partir da qual serão listados:

→ As forças (*strengths*): Ex.: um bom orçamento, cultura organizacional amigável com relação à segurança da informação implementação de PSI entre outros;

→ As fraquezas (*weaknesses*): Ex.: pessoal interno descontente, infraestrutura inadequada, orçamento limitado, pessoal não capacitado, não uso e observância de normas de segurança entre outros;

→ As oportunidades (*opportunities*): Ex.: obtenção de certificações na área de segurança da informação com consequente aumento da credibilidade da empresa e oportunidades de negócio com organizações que prezam pela Segurança da Informação entre outros;

→ Ameaças (*threats*): Ex.: contaminação por vírus e *trojans,* engenharia social, invasões a sistemas entre outros. Whitman (2003) *et al apud* Al-awadi e Renaud classifica essas ameaças como externas e internas como sendo:

Ameaças internas: instalação ou uso de *hardware* não autorizado, periféricos;

abuso de controle de acesso a computadores; roubo físico de *hardware* ou *software*; erros humanos; danos causados por empregados descontentes; uso dos recursos da organização atividades ou comunicações ilegais (pornografia, perseguição virtual) e instalação ou uso de *software* não autorizado.

Ameaças externas: vírus, desastres naturais, *spams* e incidentes de *hacking*.

Feita a avaliação dos ativos de informação e identificação das ameaças para esses ativos o segundo passo é o desenvolvimento de uma avaliação de risco. Essa avaliação de risco permite que a organização tenha uma noção do que está desprotegido, com um nível de proteção aceitável e muito protegido, desnecessariamente. O objetivo dessa avaliação é determinar a correta alocação de recursos, alocando mais recursos para o que está menos protegido e evitando gastos desnecessários com o que está desnecessariamente protegido (UGERMAN, 2005).

A PSI deve ser um documento de fácil entendimento por todos da organização já que será um documento a ser lido por todos os servidores da organização, de todos os níveis da hierarquia da empresa. É recomendável que a mesma seja estruturada em procedimentos, normas e diretrizes para que essa política seja de fácil entendimento por todos. Por exemplo, pode se desenvolver a diretriz para uso de informações digitais, dentro dessa diretriz, pode se colocar a norma para uso de *desktops* e finalmente, dentro dessa norma estaria o procedimento para o envio de *e-mails*, todas essas colocações tendo em vista os objetivos da PSI.

É necessário que esses tópicos estejam fielmente interligados entre si. Um procedimento precisa estar alinhado com uma norma, que por sua vez precisa estar de acordo com uma diretriz. Se alguma das partes inferiores não estiver contida em uma parte superior entre esses três itens, então algo deve estar errado e precisa ser revisto (CAMPOS, 2007, pág. 135). Esse documento pode ser um conjunto único composto pelas diretrizes, normas e procedimentos ou separados em documentos diferentes, um para as diretrizes, outro para as normas e outro para os procedimentos como destaca Campos (2007, pág. 134). O mesmo autor destaca

ainda que esses três tópicos devem existir de forma documentada (escrita) e que é necessário haver um controle de versão e revisão desses documentos para garantir a relevância e a organização dos mesmos. Nakamura (2007, pág. 190) sugere apenas normas e procedimentos como sendo parte da PSI, excluindo o tópico *diretrizes*. As ideias de Campos (2007) sobre a organização de diretrizes, normas e procedimentos são expressas na figura seguinte:

Figura 4 – Segundo Campos (2007, pág. 134) a estrutura da PSI deve seguir a organização mostrada pela figura

Fonte: disponível em: <http:\\claudiododt.files.wordpress.com2011\06\cia1.com>.

O mesmo autor sugere ainda, que um documento inicial denominado PSI seja criado e contenha as diretrizes e outras informações importantes, a qual seria amplamente conhecida e divulgada. Outros documentos seriam criados exclusivamente para conter as normas e os procedimentos, estes seriam criados de acordo com a necessidade da organização mas sempre alinhados com os outros documentos da Politica de Segurança da Informação.

Campos (2007, pág. 135) sugere a seguinte agenda de trabalho para o

desenvolvimento da PSI:

→ Estabelecer o método de trabalho: Documento contendo as definições gerais, os objetivos e metas, as diretrizes, as responsabilidades, as definições de registro de incidente e a frequência de revisão;

→ Avaliar as questões de negócio, legais e contratuais: legislação, regulamento interno e contratos;

→ Definir o contexto estratégico e de risco: Os critérios de risco, os riscos aceitáveis;

→ Construir a política;

→ Aprovar a política;

e por fim divulgar, amplamente, essa política.

A norma NBR ISO 27002 (2013) estabelece que o documento da PSI contenha declarações relativas a:

a) Uma definição de segurança da informação, suas metas globais, escopo e importância da segurança da informação como um mecanismo que habilita o compartilhamento da informação;

b) Uma declaração de comprometimento da direção, apoiando as metas e princípios de segurança da informação, alinhada com os objetivos e estratégias do negócio;

c) Uma estrutura para estabelecer os objetivos de controle e os controles, incluindo a estrutura de análise/avaliação e gerenciamento de risco;

d) Breve explanação das políticas, princípios, normas e requisitos de conformidade de segurança da informação específicos para a organização, incluindo:

1) Conformidade com a legislação e com requisitos regulamentares e contratuais;
2) Requisitos de conscientização, treinamento e educação em segurança da informação;

3) Gestão da continuidade do negócio;

4) Consequências das violações na Política de Segurança da Informação;

e) Definição das responsabilidades gerais e específicas na gestão da segurança da informação, incluindo o registro dos incidentes de segurança da informação;

f) Referências à documentação que possam apoiar a política, por exemplo, políticas e procedimentos de segurança mais detalhados de sistemas de informação específicos e regras de segurança que os usuários devem seguir.

É recomendável que o desenvolvimento da PSI seja baseado em padrões de normas internacionais relacionadas a Segurança da Informação que são amplamente usados e aceitos mundialmente. Temos as atualizadas normas ISO da série 27000 que foram baseadas nas BS (*British Standard*) 7799 parte 1 e parte 2, e na ISO IEC 17799. A BS 7799 é um padrão internacional e mundialmente aceito para a implementação de controles de segurança e foi publicado pela primeira vez em 1995, sendo atualizado em 1999 com o objetivo de incorporar normas relativas ao uso do comércio eletrônico. O padrão da *British Standard* foi desenvolvido por um conjunto de empresas privadas e órgãos do governo e é dividido em duas partes:

- **BS 7799** parte 1 (1995): Conjunto de práticas relativas ao gerenciamento da Segurança da Informação;

- **BS 7799** Parte 2 (1998): Especificação para sistemas de Gestão de Segurança da Informação.

A *ISO* adotou o *ISO/IEC* 17799, uma versão internacional da *BS* 7799, o mesmo padrão foi adotado também pelo *IEC.* Atualmente temos uma versão atualizada da ISO/IEC 17799, essa atualização é A ISO/IEC 27002, e foi atualizada a partir de 2007 já com o novo esquema de numeração da ISO. A ISO 27001 também é mais recente. A PSI pode ser definida com base nas referências desses dois padrões mas sempre levando em conta as particularidades de cada empresa, visto que cada uma possui métodos e característica próprias (NAKAMURA, 2007, pág. 190). Para visualizar com mais detalhes e ter mais compreensão de uma PSI vide o Anexo 1 – Política de Segurança da Informação no final desse trabalho.

6 IMPLEMENTAÇÃO DA PSI E SEUS DESAFIOS

De acordo com Nakamura (2007, pág. 198) a implementação da PSI é a parte mais difícil entre os processos de planejamento, desenvolvimento e implementação. No processo de sua implementação serão aplicadas as mudanças e essa é a parte que torna o processo complicado. É necessário considerar a educação dos funcionários como um fator primordial nesse ponto, visto que o desconhecimento desse documento pode tornar a política inoperante e reduzir sua eficácia (NAKAMURA, 2007, pág. 199). Trabalhos como *workshops*, cursos, palestras devem ser considerados para o trabalho de conscientização do pessoal na qual a PSI irá abranger. Oliveira (2013) destaca que para que a implementação e aceitação da política de segurança seja eficaz, todos os profissionais deverão estar cientes das vulnerabilidades e ameaças que existem ao trabalhar com a informação. Campanol (2012) defende que, além de apresentar a PSI aos funcionários da organização, os responsáveis precisam recolher declarações de comprometimento dos funcionários e assegurar que a mesma estará sempre disponível para todos.

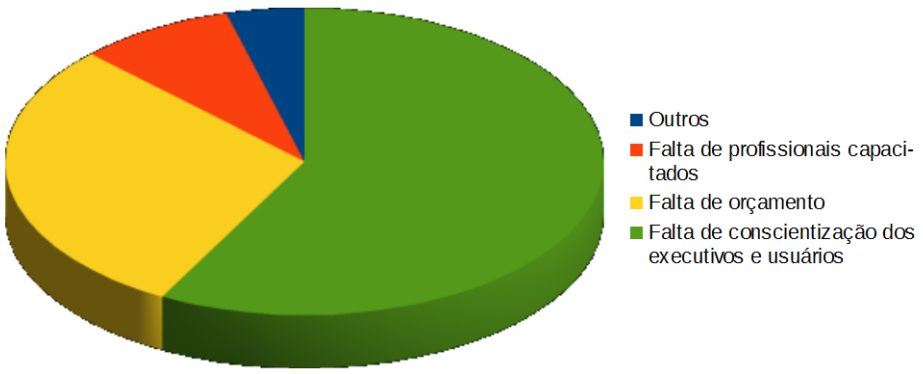
Além do comprometimento da direção com relação ao apoio a essa política, faz se necessário avaliações periódicas da mesma. Essas avaliações tem como objetivo melhorar constantemente a PSI, observando se ela está regulando o tratamento com a informação e mantendo a mesma atualizada com relação a novas vulnerabilidades, permissões e mudanças em processos gerenciais ou infraestrutura (CAMPANOL, 2012). Basto (2013) observa que essa política deve sempre ser revista, com vistas a nunca ficar ultrapassada. Freitas e Araújo (2008) *apud* Oliveira (2013) estabelecem um prazo de 6 meses a um ano entre uma avaliação e outra da PSI e sempre que surgirem novas tecnologias ou atualização das atuais que possam de alguma forma causar algum impacto na segurança das informações da organização essa PSI deve ser atualizada. O mesmo autor citando a NBR ISO/IEC 27002 recomenda que a PSI “seja revisada periodicamente e de forma planejada ou quando ocorrerem mudanças significativas, para assegurar a sua continua pertinência, adequação e eficácia” (OLIVEIRA, 2013). O portal NCES aborda essa questão da revisão da Política de Segurança da Informação quando comenta que a

revisão depende das necessidades da organização e do seu conhecimento tecnológico e concorda com Freitas e Araújo (2008) *apud* Oliveira (2013) quando diz que a mesma deve ser revisada sempre que ocorrer alguma mudança na tecnologia. O portal avisa que essa PSI deve ser revisada no mínimo uma vez por ano.

Tendo em vista essas colocações, pode-se estabelecer um prazo de um a um ano e meio para que as revisões na PSI sejam feitas ou todas as vezes que chegarem à organização equipamentos ou tecnologias relevantes que possam de alguma forma causar impacto na segurança da empresa.

No gráfico abaixo, pesquisa da Módulo *apud* Silva (2012, pág. 67) mostra alguns dos principais obstáculos para a implementação da segurança nas organizações, percebemos que os dois maiores problemas são a falta de orçamento e a falta de conscientização dos executivos e usuários. A falta de conscientização pode ser resolvida com o treinamento e falta de orçamento muitas vezes provém da falta de conhecimento por parte da gestão a respeito da importância da segurança da informação. Nos itens seguintes serão abordados a questão do orçamento e do treinamento e suas relações com a PSI.

Figura 5: Os quatro principais obstáculos para a implementação da segurança



Fonte: Silva, 2012.

6.1 Orçamento insuficiente

O orçamento direcionado à PSI é um desafio que a equipe responsável pela sua criação e implantação deve se ater para que se consiga planejá-la, desenvolvê-la e implementá-la de acordo com a legislação vigente. A falta de orçamento é o obstáculo mais comum na implantação da PSI (NAKAMURA, 2007, pág. 201). Como consequência da alegação pela administração de falta de orçamento, um setor de TI poderá implantar apenas o primeiro passo de um processo, em vez de implantá-lo completamente como seria o correto. Como exemplo, um setor poderá solicitar apenas a compra de um novo *software* e treinamento apenas para a equipe de operações. Nesse caso o correto seria, além desses itens, as correções, os *patches* frequentes, os encargos de manutenção do *software*, o treinamento do usuário final (WOOD, 2011, tradução nossa).

É necessário empenho para convencer a administração de que o investimento em segurança é de fato um investimento e não um gasto, quando não existe esse empenho fico complicado convencer a gestão sobre a importância dos investimentos em segurança. Nakamura (2007, pág. 201) afirma que muitas vezes isso se deve à falha de convencer os administradores sobre os valores inerentes aos dados e informações e que portanto, devem ser protegidos. Uma maneira de mostrar à administração o valor e o perigo de não alocar os recursos necessários à PSI é simulando um ataque (esse ataque só deve ser simulado após comunicação prévia e por escrito). Após o ataque a administração perceberá que os negócios podem ser interrompidos e com isso dará mais atenção a alocação de recursos à PSI (NAKAMURA, 2007, pág. 201).

Figura 6 - A "falta" de orçamento para a segurança da informação e da PSI muitas vezes é consequência de uma gerência desinformada sobre sua importância.

Fonte: Disponível em: <http://pixabay.com/pt/homem-silhueta-flipchart-parede-318584>. Acesso em 02 Jan. 2014

O orçamento é um dos desafios a serem transpostos pela equipe que planejará, desenvolverá e implementará a PSI. Muitas vezes essa “falta” de orçamento vem do desconhecimento por parte da administração de que os dados e informações são ativos e tem um valor inestimável para a organização, sendo assim, devem ser protegidos. A PSI surge como o ponto de partida para a segurança dos dados. Uma capacitação e demonstração à equipe administrativa de que investir em segurança é um investimento e não um gasto, com certeza fará a direção da empresa ver o investimento na implementação da PSI com bons olhos e assim, direcionar recursos suficientes para sua implementação.

6.2 Treinamento de usuário

O treinamento visa promover o conhecimento do funcionário, tanto teórico como prático: segundo Chiavenato (1985, pág. 288) *apud* Administradores (2008), “treinamento é o processo educacional, aplicado de maneira sistêmica, através do qual as pessoas aprendem conhecimentos, atitudes e habilidades em função de objetivos definidos.” Pesquisa feita por Al-awadi e Renaud (pág. 4) assegura que a maioria dos incidentes que as organizações enfrentam provém dos seus próprios usuários. Diz a pesquisa:

> Isto confirma o que Katz (2005) conclui, que os funcionários são a maior ameaça à segurança da informação. "[...] Não enfrentamos quaisquer ataques de *hackers*, a única coisa que enfrentamos é vírus e spam. Os vírus foram instalados quando empregados abriram *e-mails* de spam ou arquivos anexados que tinham vírus que então afetaram o sistema da organização (AL-AWADI & RENAUD, pág. 4, tradução nossa).

Portanto a organização precisa trabalhar com programas de treinamento e conscientização contínuos, pois o treinamento quando não levado a sério, nem implementado corretamente pode se transformar em um problema na implementação da PSI. Espírito Santo sugere que a parte de treinamento seja feita em parceria com o setor de recursos humanos da organização, com a realização das seguintes diretrizes:

> a realização de análises de idoneidade pessoal e profissional das pessoas que pleiteiam uma vaga na empresa; definir uma política de confidencialidade ou código de ética entre trabalhadores e organização; realizar treinamentos em segurança da informação para todos os funcionários e não apenas para os profissionais de tecnologia da informação; definir uma política que dê acesso a funcionários ativos e que solicite a remoção de profissionais desligados da empresa (ESPÍRITO SANTO, Pág. 6).

Para que o treinamento seja aproveitado da melhor forma, que tenha sucesso e

tenha os melhores resultados, nada melhor que ter na equipe de desenvolvimento dos treinamentos representantes da comunidade a qual esse treinamento se aplicará (WOOD, 2011). O treinamento deve ser teórico e também prático, incluindo simulações no seu rol de atividades. O processo de conscientização pode ser feito com a distribuição de folhetos, panfletos, palestras informativas e de conscientização. Um programa de educação contínua que faça com que as pessoas sintam-se parte ativa do processo é a melhor maneira de alcançar o sucesso (TCU, 2007, pág. 36).

Figura 7 - O treinamento, quando não implementado, pode se transformar em um problema na implantação da Política de Segurança da Informação

Fonte: Disponível em https://pixabay.com/pt/alto-falantes-alto-falante-414560/. Acesso em 15 Mar. 2015.

7 CONCLUSÃO

A segurança da informação é uma questão importante no dia-a-dia das empresas nos dias de hoje. Por uma questão até de valorização, as empresas precisam focar nos aspectos de segurança da informação, pois com os sistemas de informações interligados, essas organizações estão sujeitas a vários perigos. Como consequência desses perigos podem ocorrer o vazamento de informações. Tendo em vista esses problemas, as organizações precisam buscar soluções para resguardar suas informações. Segundo o estudo, os maiores perigos à informação estão no interior das organizações, com os funcionários.

Pelo exposto no trabalho, a PSI é a base para todas as questões relacionadas à proteção da informação, desempenhando um papel importante em todas as organizações. Um bom planejamento e desenvolvimento dessa ferramenta ajudarão a empresa a conseguir aplicar a mesma da melhor forma, seguindo as normas recomendadas para esse fim. Na fase de planejamento é necessário que sejam abordados os aspectos humanos, culturais e tecnológicos de uma organização, levando também em consideração os processos e os negócios, além da legislação local. Necessário é também que essa PSI tenham um caráter preventivo e não apenas reativo e que seja pensada em três níveis: nível genérico, nível de usuários e nível técnico com o objetivo de ser inteligível a todos da organização. Para o desenvolvimento da mesma é necessário observar as normas que tratam da questão da segurança da informação: a ISO/IEC 17799, ISO/IEC 27001 e a ISO/IEC 27002, as BS 7799 parte 1 e BS 7799 parte 2 ou as metodologias de governança que contemplem a PSI como o COBIT e o ITIL®. A fase de implementação da PSI é a mais complicada devido a vários desafios inerentes a essa fase como recursos financeiros insuficientes, incompreensão da importância da PSI para o resguardo das informações, desinteresse em trabalhar continuamente com a PSI, percepção de complexidade do uso da Política, falsa percepção de ameaça ao poder dos diretores, comunicação entre a equipe operacional e a gestão, treinamento de usuário.

Foi elaborado um trabalho que aborda o tema do uso das PSI, suas três

fases de desenvolvimento e alguns dos desafios de implementação. Com esse trabalho, percebe-se que as políticas de segurança da informação, apesar de sua importância, não estão sendo trabalhadas pela maioria das empresas no Brasil e no mundo, mas estão sendo utilizadas cada vez mais. Percebe-se também que o maior perigo para toda e qualquer organização é o seu próprio funcionário. Funcionários despreparados concorrem para aumentar as estatísticas de problemas de segurança da informação nas empresas, razão pela qual pontua-se a importância do treinamento e programas de conscientização. Como diferencial desse trabalho pode-se citar o aprofundamento e o enfoque em relação às três fases de elaboração da PSI, nos vários trabalhos pesquisados vê-se pouco aprofundamento nesses tópicos. Conclue-se com esse trabalho que as PSIs tem papel fundamental nas empresas e devem ser trabalhados continuamente, mesmo não sendo tão amplamente utilizadas estão com seu uso aumentando cada dia mais.

7.1 Trabalhos futuros

A partir das ideias resultantes desse trabalho cogita-se a realização de uma pesquisa específica à Microrregião de Itaparica na qual serão pesquisados o uso e a eficiência das PSIs nas empresas dessa Microrregião. O resultado dessa pesquisa poderá resultar num artigo que será apresentado em simpósios e/ou encontros da área de segurança. Essa pesquisa também poderá ser feita como resultado de uma monografia de um curso de pós-graduação lato-sensu na área de segurança, sempre tendo como base o presente trabalho.

7.2 Dificuldades encontradas

Uma das maiores dificuldades encontradas nesse trabalho foi a falta de um material sólido no idioma português, quase todo o material estava no idioma inglês, tendo assim que o autor se debruçasse na tradução de artigos e materiais de outros idiomas para o português. Dificuldade essa que de forma nenhuma diminuiu a importância do trabalho, mas sim, o fez mais rico.

REFERÊNCIAS

ABNT. **ABNT NBR ISO/IEC 27001: Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de Segurança da Informação**. 2006. Disponível em: http://professor.ufabc.edu.br/~joao.kleinschmidt/aulas/seg2013/norma1.pdf. Acesso em: 13 de Out. 2014.

ABNT. **NBR ISO 27002.** 2013. Disponível em: http://www.abntcatalogo.com.br/norma.aspx?ID=306582. Acesso em 15 Jan. 2015.

ADMINISTRADORES. **Definição de treinamento.** Disponível em: http://www.administradores.com.br/artigos/carreira/definicao-de-treinamento/22212/. Acesso em: 04 de Dez. 2014.

AL-AWADI, Maryam; RENAUD, Karen. **Success factors in information security implementation in organizations.** 8 pág. Disponível em : <http://www.dcs.gla.ac.uk/~karen/Papers/sucessFactors2.pdf>. Acesso em: 20 de Set. 2014.

BASTO, Fabrício. **Política da Segurança da Informação – Como fazer?** . Analistati, Dezembro, 2012. Disponível em: <http://analistati.com/politica-de-seguranca-da-informacao-como-fazer/>. Acesso em: 26 de Ago.2014.

CAMPOS, André; **Sistema de Segurança da Informação: Controlando os Riscos**. 2. ed. Florianópolis: Visual Books, 2007. 218 P.

CAMPANOL, Octavio. **Implantação de uma PSI.** TI Especialistas, Agosto, 2012. Disponível em: http://www.tiespecialistas.com.br/2012/08/implantacao-de-uma-politica-de-seguranca. Acesso em: 27 de Ago. 2014.

CHIAVENATO, Idalberto. **Administração: teoria: processo e prática**. 5º Ed. Barueri: Manole, 2014.

CONVERGÊNCIA DIGITAL. **Curso prepara *hacker* ético no Brasil**. Convergência digital, Maio, 2014. Disponível em:< http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=36652#.VGyi5DTF81Y>. Acesso em: 27 de Out. 2014.

CORPORATE, **Relembre os maiores vazamentos de informação de 2013**. Canaltech Corporate, Março, 2014. Disponível em: http://corporate.canaltech.com.br/materia/seguranca/Relembre-os-maiores-vazamentos-de-informacao-de-2013. Acesso em :26 de Nov. 2014.

DARYUS. **Pesquisa nacional de segurança da informação 2014**. Disponível em: <http://www.daryus.com.br/view/pdf/DARYUS_Pesquisa_ISM.pdf>. Acesso em 11 Jan. 2015.

ESPÍRITO SANTO, Adrielle Fernanda Silva do. **Segurança da informação**. Disponível em: http://www.ice.edu.br/TNX/encontrocomputacao/artigos-internos/aluno_adrielle_fernanda_seguranca_da_informacao.pdf. Acesso em 03 de jan. 2015.

FAUSTINI, Rodrigo. **Política de Segurança da Informação.** Disonível em: <http://www.faustiniconsulting.com/artigo05.htm>. Acesso em 08 Fev. 2015.

FERREIRA, Aurfélio Buarque de Holanda. **Novo dicionário da língua portuguesa. 4° Ed. Curitiba: Ed. Positivo, 2009.** 2120 P.

FREITAS, Marcos André do Santos. **Fundamentos do gerenciamento de serviços de TI: preparação para a certificação ITIL® V3 Foundation**. Rio de Janeiro: Ed. Brasport, 2010. 351 P.

KOCHE, José Carlos. **Fundamentos de metodologia científica: teoria da ciência e iniciação à pesquisa.** 30° Ed. Petrópolis: Ed. Vozes, 2012. 182 P.

LAGO, Davi Guimarães do; GUIMARÃES, Ênio Bemfica. **Segurança da informação e sua história.** Disponível em : <http://www.viajus.com.br/viajus.php?pagina=artigos&id=2202&idAreaSel=20&seeArt=yes> Acesso em: 22 de Jul. 2015.

LANVERLY, Byron de M. Jr.; Silva, É. Da S.; SOUZA, J. H.; NEVES, R. P.; NASCIMENTO, F. A. ; GUIMARÃES, A. P.; NASCIMENTO. H. M. JR. **Proteja o maior bem da sua empresa, a *informação,* com: Política de segurança da informação.** Maceió. 13 pág. Disponível em: <http://www.fatec.edu.br/html/fatecam/images/stories/dspti_ii/asti_ii_material_apoio_4_seguranca_informacao_politicas.pdf>. Acesso em: 10 de Nov. 2014.

LOURENÇO, S. P. ***Aspectos jurídicos da segurança da informação na empresa.*** 2009. 92 f. Dissertação (Mestrado na área de concentração direito empresarial junto a Faculdade de Direito Milton Campos), Faculdade de Direito Milton Campos, Nova Lima Disponível em: http://www.mcampos.br/posgraduacao/mestrado/dissertacoes/2011/shandorportellaaspectosjuridicossegurancainformacaoempresa.pdf. Acesso em: 03 de Jan. 2015.

MARCONI, Marina de Andrade. **Fundamentos de metodologia científica**. São Paulo: Atlas, 2010. 297 P.

MITNICK, Kevin D. **A arte de enganar.** São Paulo: Pearson Makron Books, 2003. 284 P.

MODULO. 10° pesquisa nacional de segurança da informação. 2006. Disponível em: <https://www.modulo.com.br/media/10a_pesquisa_nacional.pdf>. Acesso em: 08 de Fev. 2015.

NAKAMURA, Emílio Tissato. **Segurança de redes em ambientes cooperativos.** São Paulo: Novatec Editora, 2007. 483 P.

NCES. **Security policy: development and Implementation.** Disponível em: <http://nces.ed.gov/pubs98/safetech/chapter3.asp#df--/>. Acesso em 10 de Dez. 2014.

OLIVEIRA, Paulo César. **Política de segurança da informação: definição, importância, elaboração e implementação**. Junho, 2013. Disponível em:<http://www.profissionaisti.com.br/2013/06/politica-de-seguranca-da-informacao-definicao-importancia-elaboracao-e-implementacao/>. Acesso em 25 de Ago. 2014.

PORTAL DE AUDITORIA. **Introdução à Lei Sarbanes-Oxley**. Disponível em: <http://www.portaldeauditoria.com.br/auditoria-interna/Introducao-a-lei-Sarbanes-Oxley-Sox.asp>. Acesso em: 07 de Jan. 2015.

SILVA, Antônio Everardo Nunes da. **Segurança da informação – Vazamento de informações:** as informações estão realmente seguras em sua empresa? Rio de Janeiro: Editora Ciência Moderna LTDA, 2012. 104 P.

SOMASUNDARAM, G; SHRIVASTAVA, A. **Armazenamento e gerenciamento de informações**: **como armazenar, gerenciar e proteger informações digitais**. Porto Alegre: Bookman, 2011. 480 P.

TCU. **Análise SWOT e Diagrama de Verificação de Risco Aplicados em Auditoria:** PORTARIA-SEGECEX Nº 31, DE 9 DE DEZEMBRO DE 2010. Brasília, Dezembro, 2010. Disponível em: **<**http://portal2.tcu.gov.br/portal/page/portal/TCU/comunidades/programas_governo/tecnicas_anop/BTCU_ESPECIAL_30_de_14_12_2010_An%C3%A1lise_SWOT_e_Diagrama_.pdf> Acesso em: 07 de Dez. 2014.

—— **Boas práticas em segurança da informação**. Brasília, 2007, 70 p., disponível em <http://portal2.tcu.gov.br/portal/pls/portal/docs/2059162.PDF>. Acesso em: 03 de Dez. 2014.

—— **Boas práticas em segurança da informação**. Brasília, 2012, 108 p., disponível

em <http://portal2.tcu.gov.br/portal/pls/portal/docs/2511466.PDF>. Acesso em: 08 de Jane. 2015.

UFMG. **Manual de normalização para o NITEG e o PPGCI da ECI-UFMG.** 2011. Disponível em <http://normalizacao.eci.ufmg.br/?Reda%E7%E3o_e_Estilo:Metodologia>. Acesso em: 04 de Jan. 2015.

UGERMAN, Mark. **Creating and enforcing an effective information security policy**. ISACA ® , 2005. Disponível em: <http://www.isaca.org/Journal/Past-Issues/2005/Volume-6/Pages/JOnline-Creating-and-Enforcing-an-Effective-Information-Security-Policy1.aspx>. Acesso em: 12 de Nov. 2014.

WOOD, Charles Cresson. **Five reasons why security policies don't get implemented**. Information Shield, 2011. Disponível em: <http://www.informationshield.com/security-policy/2011/01/five-reasons-why-security-policies-don%E2%80%99t-get-implemented/> Acesso em: 10 de Set. 2014.

ANEXO 1 – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (MODELO)[2]

A Política de segurança da informação, na A EMPRESA, aplica-se a todos os funcionários, prestadores de serviços, sistemas e serviços, incluindo trabalhos executados externamente ou por terceiros, que utilizem o ambiente de processamento da Companhia, ou acesso a informações pertencentes à A EMPRESA. Todo e qualquer usuário de recursos computadorizados da Companhia tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática. A violação desta política de segurança é qualquer ato que:

- Exponha a Companhia a uma perda monetária efetiva ou potencial por meio do comprometimento da segurança dos dados /ou de informações ou ainda da perda de equipamento.

- Envolva a revelação de dados confidenciais, direitos autorais, negociações, patentes ou uso não autorizado de dados corporativos.

- Envolva o uso de dados para propósitos ilícitos, que venham a incluir a violação de qualquer lei, regulamento ou qualquer outro dispositivo governamental.

Missão do Setor de Informática:

Ser o gestor do processo de segurança e proteger as informações da organização, catalisando, coordenando, desenvolvendo e/ou implementando ações para esta finalidade.

---

[2] E-SERVICES. **Política de Segurança da Informação (Modelo).** Fonte: <http://www.e-services.com.br/portal/artigos/politica_seguranca.pdf/>. Acesso em: 4 de Dez. 2014.

Objetivo da Política de Segurança da Informação:

Garantir a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade da informação necessária para a realização do negócio da A EMPRESA.

É Dever de todos dentro da A EMPRESA:

Considerar a informação como sendo um bem da organização, um dos recursos críticos para a realização do negócio, que possui grande valor para a A EMPRESA e deve sempre ser tratada profissionalmente.

01 – CLASSIFICAÇÃO DA INFORMAÇÃO

É de responsabilidade do Gerente/Supervisor de cada área estabelecer critérios relativos ao nível de confidencialidade da informação (relatórios e/ou mídias) gerada por sua área de acordo com a tabela abaixo:

1 – Pública

2 – Interna

3 – Confidencial

4 – Restrita

Conceitos: Informação Pública: É toda informação que pode ser acessada por usuários da organização, clientes, fornecedores, prestadores de serviços e público em geral.

Informação Interna: É toda informação que só pode ser acessada por funcionários da organização. São informações que possuem um grau de confidencialidade que pode comprometer a imagem da organização.

Informação Confidencial: É toda informação que pode ser acessada por usuários da organização e por parceiros da organização. A divulgação não autorizada dessa

informação pode causar impacto (financeiro, de imagem ou operacional) ao negócio da organização ou ao negócio do parceiro.

Informação Restrita: É toda informação que pode ser acessada somente por usuários da organização explicitamente indicado pelo nome ou por área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da organização.

Todo Gerente/Supervisor deve orientar seus subordinados a não circularem informações e/ou mídias consideradas confidenciais e/ou restritas, como também não deixar relatórios nas impressoras, e mídias em locais de fácil acesso, tendo sempre em mente o conceito “mesa limpa”, ou seja, ao terminar o trabalho não

deixar nenhum relatório e/ou mídia confidencial e/ou restrito sobre suas mesas.

02 – DADOS PESSOAIS DE FUNCIONÁRIOS

A A EMPRESA se compromete em não acumular ou manter intencionalmente Dados Pessoais de Funcionários alem daqueles relevantes na condução do seu negócio.

Todos os Dados Pessoais de Funcionários serão considerados dados confidenciais.

Dados Pessoais de Funcionários sob a responsabilidade da A EMPRESA não serão usados para fins diferentes daqueles para os quais foram coletados.

Dados Pessoais de Funcionários não serão transferidos para terceiros, exceto quando exigido pelo nosso negócio, e desde que tais terceiros mantenham a confidencialidade dos referidos dados, incluindo-se, neste caso a lista de endereços eletrônicos (e-mails) usados pelos funcionários da A EMPRESA.

03 – PROGRAMAS ILEGAIS

É terminantemente proibido o uso de programas ilegais (PIRATAS) na A EMPRESA. Os usuários não podem, em hipótese alguma, instalar este tipo de "*software*" (programa) nos equipamentos da Companhia.

Periodicamente, o Setor de Informática fará verificações nos dados dos servidores e/ou nos computadores dos usuários, visando garantir a correta aplicação desta diretriz.

04 – PERMISSÕES E SENHAS

Quando da necessidade de cadastramento de um novo usuário para utilização da "rede", sistemas ou equipamentos de informática da Companhia, o setor de origem do novo usuário deverá comunicar esta necessidade ao setor de Informática, por meio de memorando ou e-mail, informando a que tipo de rotinas e programas o novo usuário terá direito de acesso e quais serão restritos. A Informática fará o cadastramento e informará ao novo usuário qual será a sua primeira senha, a qual deverá, obrigatoriamente, ser alterada a cada 45 (quarenta e cinco) dias.

Por segurança, a Informática recomenda que as senhas tenham sempre um mínimo de 8 (oito) caracteres alfanuméricos.

Todos os usuários responsáveis pela aprovação eletrônica de documentos (exemplo: pedidos de compra, solicitações e etc) deverão comunicar ao Setor de Informática qual será o seu substituto quando de sua ausência da A EMPRESA, para que as permissões possam ser alteradas (delegação de poderes).

05 – COMPARTILHAMENTO DE PASTAS E DADOS

É de obrigação dos usuários rever periodicamente todos os compartilhamentos existentes em suas estações de trabalho e garantir que dados considerados confidenciais e/ou restritos não estejam disponíveis a acessos indevidos.

06 – CÓPIA DE SEGURANÇA (BACKUP) DO SISTEMA INTEGRADO E SERVIDORES DE REDE

Cópias de segurança do sistema integrado e servidores de rede são de responsabilidade da Informática e deverão ser feitas diariamente.

Ao final de cada mês também deverá ser feita uma cópia de segurança com os dados de fechamento do mês, do Sistema Integrado. Esta cópia será feita imediatamente após a comunicação formal da Contabilidade, por meio de memorando, que o referido mês foi encerrado.

Nos meses pares, a Informática enviará 1 (uma) cópia extra da fita do "backup" de fechamento do referido mês, para ser arquivada na Contabilidade.

07 – SEGURANÇA E INTEGRIDADE DO BANCO DE DADOS

O gerenciamento do(s) banco(s) de dados é responsabilidade exclusiva do Setor de Informática, assim como a manutenção, alteração e atualização de equipamentos e programas.

08 – ADMISSÃO/DEMISSÃO DE FUNCIONÁRIOS/TEMPORÁRIOS/ESTAGIÁRIOS

O setor de Recrutamento e Seleção de Pessoal da Companhia deverá informar ao setor de Informática, toda e qualquer movimentação de temporários e/ou estagiários, e admissão/demissão de funcionários, para que os mesmos possam ser cadastrados ou excluídos no sistema da Companhia. Isto inclui o fornecimento de sua senha ("password") e registro do seu nome como usuário no sistema (user-id), pelo setor de Informática.

Cabe ao setor solicitante da contratação a comunicação ao setor de Informática sobre as rotinas a que o novo contratado terá direito de acesso. No caso de temporários e/ou estagiários deverá também ser informado o tempo em que o mesmo prestará serviço á Companhia, para que na data de seu desligamento possam também ser encerradas as atividades relacionadas ao direito de seu acesso ao sistema.

No caso de demissão, o setor de Recursos Humanos deverá comunicar o fato o mais rapidamente possível à Informática, para que o funcionário demitido seja excluído do sistema.

Cabe ao setor de Recursos Humanos dar conhecimento e obter as devidas assinaturas de concordância dos novos contratados em relação à Política de Segurança da Informação da A EMPRESA.

Nenhum funcionário, estagiário ou temporário, poderá ser contratado, sem ter expressamente concordado com esta política.

09 – TRANSFERÊNCIA DE FUNCIONÁRIOS

Quando um funcionário for promovido ou transferido de seção ou gerência, o setor de cargos e salários deverá comunicar o fato ao Setor de Informática, para que sejam feitas as adequações necessárias para o acesso do referido funcionário ao sistema informatizado da Companhia.

10 – CÓPIAS DE SEGURANÇA DE ARQUIVOS INDIVIDUAIS

É responsabilidade dos próprios usuários a elaboração de cópias de segurança ("backups") de textos, planilhas, mensagens eletrônicas, desenhos e outros arquivos ou documentos, desenvolvidos pelos funcionários, em suas estações de trabalho, e que não sejam considerados de fundamental importância para a continuidade dos negócios da A EMPRESA.

No caso das informações consideradas de fundamental importância para a continuidade dos negócios da A EMPRESA o Setor de Informática disponibilizará um espaço nos servidores onde cada usuário deverá manter estas informações. Estas informações serão incluídas na rotina diária de backup da Informática.

11 – PROPRIEDADE INTELECTUAL

É de propriedade da A EMPRESA, todos os “designs”, criações ou procedimentos desenvolvidos por qualquer funcionário durante o curso de seu vínculo empregatício com a A EMPRESA.

12 – USO DO AMBIENTE WEB (Internet)

O acesso à Internet será autorizado para os usuários que necessitarem da mesma para o desempenho das suas atividades profissionais na A EMPRESA. Sites que não contenham informações que agreguem conhecimento profissional e/ou para o negócio não devem ser acessados.

O uso da Internet será monitorado pelo Setor de Informática, inclusive através de “logs” (arquivos gerados no servidor) que informam qual usuário está conectado, o tempo que usou a Internet e qual página acessou.

A definição dos funcionários que terão permissão para uso (navegação) da Internet é atribuição da Direção da Companhia, com base em recomendação do Supervisor de Informática.

Não é permitido instalar programas provenientes da Internet nos microcomputadores da A EMPRESA, sem expressa anuência do setor de Informática, exceto os programas oferecidos por órgãos públicos federais, estaduais e/ou municipais.

Os usuários devem se assegurar de que não estão executando ações que possam infringir direitos autorais, marcas, licença de uso ou patentes de terceiros.

Quando navegando na Internet, é proibido a visualização, transferência (downloads), cópia ou qualquer outro tipo de acesso a sites:

• De estações de rádio;

• De conteúdo pornográfico ou relacionados a sexo;

• Que defendam atividades ilegais;

• Que menosprezem, depreciem ou incitem o preconceito a determinadas classes;

•Que promovam a participação em salas de discussão de assuntos não relacionados aos negócios da EMPRESA;

• Que promovam discussão pública sobre os negócios da A EMPRESA, a menos que autorizado pela Diretoria;

• Que possibilitem a distribuição de informações de nível “Confidencial”.

• Que permitam a transferência (downloads) de arquivos e/ou programas ilegais. 13

– USO DO CORREIO ELETRÔNICO – ("e-mail")

O correio eletrônico fornecido pela A EMPRESA é um instrumento de comunicação interna e externa para a realização do negócio da A EMPRESA.

As mensagens devem ser escritas em linguagem profissional, não devem comprometer a imagem da A EMPRESA, não podem ser contrárias à legislação vigente e nem aos princípios éticos da A EMPRESA. O uso do correio eletrônico é pessoal e o usuário é responsável por toda mensagem enviada pelo seu endereço.

É terminantemente proibido o envio de mensagens que:

• Contenham declarações difamatórias e linguagem ofensiva;

• Possam trazer prejuízos a outras pessoas;

• Sejam hostis e inúteis;

• Sejam relativas a “correntes”, de conteúdos pornográficos ou equivalentes;

• Possam prejudicar a imagem da organização;

• Possam prejudicar a imagem de outras empresas;

• Sejam incoerentes com as políticas da A EMPRESA

Para incluir um novo usuário no correio eletrônico, a respectiva Gerência deverá fazer um pedido formal ao Setor de Informática, que providenciará a inclusão do mesmo. A utilização do "e-mail" deve ser criteriosa, evitando que o sistema fique congestionado. Em caso de congestionamento no Sistema de correio eletrônico o

Setor de Informática fará auditorias no servidor de correio e/ou nas estações de trabalho dos usuários, visando identificar o motivo que ocasionou o

mesmo. Não será permitido o uso de e-mail gratuitos (liberados em alguns sites da web), nos computadores da A EMPRESA. O Setor de Informática poderá, visando evitar a entrada de vírus na A EMPRESA, bloquear o recebimento de

e-mails provenientes de sites gratuitos.

14 – NECESSIDADES DE NOVOS SISTEMAS , APLICATIVOS E/OU EQUIPAMENTOS

O Setor de Informática é responsável pela aplicação da Política da A EMPRESA em relação a definição de compra e substituição de “*software*” e “*hardware*”.

Qualquer necessidade de novos programas ("*softwares*") ou de novos equipamentos de informática (hardware) deverá ser discutida com o responsável pelo setor de Informática.

Não é permitido a compra ou o desenvolvimento de "*softwares*" ou "*hardwares*" diretamente pelos usuários.

15 – USO DE COMPUTADORES PESSOAIS (LAP TOP) DE PROPIEDADE DA A EMPRESA

Os usuários que tiverem direito ao uso de computadores pessoais (laptop ou notebook), ou qualquer outro equipamento computacional, de propriedade da A EMPRESA, devem estar cientes de que:

• Os recursos de tecnologia da informação, disponibilizados para os usuários, têm como objetivo a realização de atividades profissionais.

• A proteção do recurso computacional de uso individual é de responsabilidade do próprio usuário.

• É de responsabilidade de cada usuário assegurar a integridade do equipamento, a confidencialidade e disponibilidade da informação contida no mesmo.

• O usuário não deve alterar a configuração do equipamento recebido.

Alguns cuidados que devem ser observados: Fora do trabalho:

• Mantenha o equipamento sempre com você;

• Atenção em hall de hotéis, aeroportos, aviões, táxi e etc.

• Quando transportar o equipamento em automóvel utilize sempre o porta malas ou lugar não visível;

• Atenção ao transportar o equipamento na rua.

Em caso de furto:

• Registre a ocorrência em uma delegacia de polícia;

• Comunique ao seu superior imediato e ao Setor de Informática;

• Envie uma cópia da ocorrência para o Setor de Informática.

16 – RESPONSABILIDADES DOS GERENTES/SUPERVISORES

Os gerentes e supervisores são responsáveis pelas definições dos direitos de acesso de seus funcionários aos sistemas e informações da Companhia, cabendo a eles verificarem se os mesmos estão acessando exatamente as rotinas compatíveis com as suas respectivas funções, usando e conservando adequadamente os

equipamentos, e mantendo cópias de segurança de seus arquivos individuais, conforme estabelecido nesta política.

O Setor de Informática fará auditorias periódicas do acesso dos usuários às informações, verificando:

• Que tipo de informação o usuário pode acessar;

• Quem está autorizado a acessar determinada rotina e/ou informação;

• Quem acessou determinada rotina e informação;

• Quem autorizou o usuário a ter permissão de acesso à determinada rotina ou informação;

• Que informação ou rotina determinado usuário acessou;

• Quem tentou acessar qualquer rotina ou informação sem estar autorizado.

17 – SISTEMA DE TELECOMUNICAÇÕES

O controle de uso, a concessão de permissões e a aplicação de restrições em relação aos ramais telefônicos da A EMPRESA, assim como, o uso de eventuais ramais virtuais instalados nos computadores, é responsabilidade do setor de Informática, de acordo com as definições da Diretoria da A EMPRESA.

Ao final de cada mês, para controle, serão enviados relatórios informando a cada gerência quanto foi gasto por cada ramal.

18 – USO DE ANTI-VÍRUS

Todo arquivo em mídia proveniente de entidade externa a A EMPRESA deve ser verificado por programa antivírus.

Todo arquivo recebido / obtido através do ambiente Internet deve ser verificado por programa antivírus. Todas as estações de trabalho devem ter um antivírus instalado. A atualização do antivírus será automática, agendada pelo setor de Informática, via rede. O usuário não pode em hipótese alguma, desabilitar o programa antivírus instalado nas estações de trabalho.

19 – PENALIDADES

O não cumprimento desta Política de Segurança da Informação implica em falta grave e poderá resultar nas seguintes ações: advertência formal, suspensão, rescisão do contrato de trabalho, outra ação disciplinar e/ou processo civil ou criminal.

Rio de Janeiro, 08 de Agosto de 2006.

Presidente Diretor Vice Presidente Adm./Financeiro

Nome:_____

Supervisor de Informática·

Número:_____

_____

Funcionário