PUCRS
Pontifícia Universidade Católica do Rio Grande do Sul

FACULDADE DE ADMINISTRAÇÃO, CONTABILIDADE E ECONOMIA
CURSO DE ADMINISTRAÇÃO DE EMPRESAS

RICARDO DIAS AMÉRICO

PLANO DE IMPLEMENTAÇÃO DE UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO NA ONCOTERÁPICA

Porto Alegre
Novembro 2008

PROGRAD

PONTIFÍCIA UNIVERSIDADE CATÓLICA DO RIO GRANDE DO SUL
FACULDADE DE ADMINISTRAÇÃO, CONTABILIDADE E ECONOMIA
CURSO DE ADMINISTRAÇÃO DE EMPRESAS

RICARDO DIAS AMÉRICO

PLANO DE IMPLEMENTAÇÃO DE UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO NA ONCOTERÁPICA

Porto Alegre
Novembro de 2008

RICARDO DIAS AMÉRICO

PLANO DE IMPLEMENTAÇÃO DE UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO NA ONCOTERÁPICA

Monografia apresentada para obtenção do grau de Bacharel em Administração de Empresas, na Faculdade de Administração, Contabilidade e Economia da Pontifícia Universidade Católica do Rio Grande do Sul.

Professor Orientador: Leonardo Rosa Rohde

Porto Alegre

Novembro de 2008

AGRADECIMENTOS

Agradeço ao professor Leonardo Rosa Rohde, o qual me guiou e me orientou de forma singular, com muita paciência e dedicação.

Agradeço a minha família. Em especial a minha querida e maravilhosa mãe, Eurídice Dias, motivo inspirador e motivacional para a conclusão de todas as etapas da minha vida. Com certeza sem o apoio dessa que foi a pessoa mais importante na minha vida eu não teria alcançado os mais difíceis desafios. Por mais que ela não esteja presente na minha vida eu tenho sempre a terei como um exemplo de vida, tanto para educação de meus futuros filhos quanto para o alcance em seus objetivos de vida.

Agradeço ao meu pai, Marco Aurélio Américo, pois foi este que abriu os meus olhos para o mercado. Sempre ensinando as vantagens que a Administração de Empresas em relação ao mercado, curso que escolhi e estou concluindo, sob influência do meu pai. Por mais distante que a nossa relação foi, hoje, eu tenho certeza que posso contar com o meu pai para as minhas decisões futuras.

Agradeço aos meus irmãos, André e Marco, por estarem sempre presentes nas minhas conquistas e que sem eles a vida não teria tanta graça assim.

A toda a minha família que participaram de todas as conquistas que adquiri até agora. Meus tios, irmãos da minha mãe, Cesar Dias, Ana Beatriz Mesquita (Dinda-Dinda), Maria Berenice Dias e João Daniel Dias. A minha dezena de primos qu
que sempre acompanharam o meu crescimento e que fizeram parte da minha vi
vários momentos especiais.

Agradeço aos meus grandes amigos que fiz durante esses 4 anos de faculdade. Aos inúmeros trabalhos realizados ao lado deles e ao conhecimento e amizade adquiridos durante a faculdade.

A Oncoterápica por proporcionar a realização deste trabalho na empresa. E a todos os funcionários que contribuíram para a viabilização deste plano. Em especial a Sheila e ao Gabriel, por todo o apoio dado para a conclusão do trabalho de conclusão de curso.

E a todos aqueles que um dia acreditaram no meu potencial e que estão presenciando mais esta conquista.

RESUMO

Este plano a ser apresentado é oriundo das falhas de segurança da informação da Oncoterápica. A empresa atua no ramo da saúde, mais especificamente em tratamento de pacientes com câncer. A partir da necessidade encontrada foram traçados objetivos específicos no intuito de atingir um macro objetivo que é o estudo de melhorias para a implementação das normas de segurança da informação, conforme os itens estudados da política de segurança da informação BS 7799.1:2002. Para atingir os escopos determinados foram desenvolvidos no trabalho, além de uma referência bibliográfica, uma metodologia para a coleta de dados e uma posterior análise das falhas de segurança na Oncoterápica. Durante o levantamento dos dados na empresa encontraram-se uma série de erros nos padrões de segurança da empresa. A partir dos dados levantados foram realizadas tomadas de ações para a correção das vulnerabilidades encontradas na organização, sempre se baseando nas melhores práticas inseridas nos padrões internacionais de segurança da informação.

Palavras-chaves: **Segurança da Informação, BS 7799.1:2002.**

LISTAS DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

Cada vez mais as pessoas utilizam “facilitadores” no seu cotidiano. Esses “facilitadores” é a tecnologia, seja para comunicar-se ou para realizar uma compra com o cartão de crédito pela *internet*. Com as organizações não poderia ser diferente, cada vez mais elas encontram-se dependentes de tais “facilitadores”, pois eles oferecem mais agilidade e comodidade para as empresas.

É a informação que “faz o mundo girar”. E a tecnologia trouxe um meio de “transporte” rápido da informação, que é a *internet*. A partir da *internet*, podemos nos conectar com o mundo e em questões de segundos estarmos nos comunicando com qualquer um conectado a rede mundial da *internet.*

Assim sendo, a informação está disponível em qualquer lugar, e pode ser acessada a qualquer momento. Porém existem tipos diferentes de informações, como por exemplo, informações confidenciais, ou seja, informações que nem todos devem ter acesso. E para isso está cada vez mais presente a segurança da informação.

A nomenclatura de segurança da informação é usualmente utilizada para a proteção de informações mantidas em componentes de tecnologia da informação conta a todas as ameaças e vulnerabilidades que estão expostas. A utilização de senhas, por exemplo, é um meio de proteção da informação contida em *e-mails* e contas bancárias.

Clínicas e hospitais também dependem da segurança da informação. E este trabalho será fundamentado, dentro de sete capítulos, em uma clínica de tratamento oncológico: a Oncoterápica.

O terceiro capítulo comprova qual é o tema do trabalho. Através das descrições problemáticas, é determinada a questão problemática a qual deverá ser respondida até a conclusão do trabalho.

O quarto capítulo justifica que o tema escolhido analisando a importância, oportunidade e viabilidade de realizar o assunto desta monografia.

O quinto capítulo é define os objetivos gerais e específicos para a realização e solução da questão determinada no terceiro capítulo.

O sexto capítulo, a era da informação, contem toda a bibliografia consultada no âmbito de sustentar o tema escolhido através de teorias e padrões já conhecidos.

O sétimo capítulo apresenta a maneira com que a questão de pesquisa foi trabalhada na organização. O método determina como será a coleta e análise dos dados da realidade investigada.

O oitavo capítulo apresenta os dados coletados na pesquisa, e propõe melhorias para a problemática questionada no capítulo terceiro.

O nono capítulo e último traz as conclusões e observações finais sobre o trabalho realizado.

2 CARACTERIZAÇÃO DA ORGANIZAÇÃO E DO SEU AMBIENTE

2.1 HISTÓRICO

A Oncoterápica foi fundada em Abril de 1999 e lançou-se no mercado como uma empresa de cunho familiar, trabalhando na prestação de serviços oncológicos, ou seja, no tratamento de pacientes com câncer.

A Clínica começou as suas atividades no ramo de quimioterápicos antineoplásicos, visando estabelecer um atendimento do tipo ambulatorial, ou seja, o paciente é atendido na clínica, faz quimioterapia e retorna para casa, não havendo necessidade de internação, sendo esta uma vantagem em relações aos hospitais que fazem o mesmo tipo de tratamento, internando os pacientes, o que não proporciona ao seu usuário final, o paciente, uma melhora na qualidade de vida, devido as diversas internações que terá que fazer ao longo do seu tratamento. Os serviços são prestados por uma equipe especializada, composta por enfermeiras, farmacêuticas, plantão médico e uma psicóloga.

Na metade de 2006, ocorreu uma mudança de gestão na empresa. A Oncoterápica era composta por três sócios diretores sendo um deles administrador e dois médicos. A mudança ocorreu quando o diretor administrativo saiu da sociedade, deixando os dois médicos como gestores da empresa, uma vez que a organização era de base familiar e tal mudança afetou os familiares envolvidos no negócio, que também foram desligados da empresa.

Em maio de 2007, a nova gestão realizou o desligamento de diversos funcionários e a contratação de novos.

2.2 NEGÓCIO

O negócio para a Oncoterápica é bem claro, uma vez que é focado no usuário final que é o seu paciente. Por sua vez, pode-se analisar qual é o negócio da empresa, em um formato simplificado.

- Atendimento e tratamento a pacientes com câncer.

2.3 MISSÃO

A missão para uma organização é a parte que detalha o negócio da empresa. Uma vez definido o negócio da empresa, parte-se para a missão. A missão da Oncoterápica está citada abaixo.

- Acolher e cuidar da saúde de usuários em terapia antineoplásica.

2.4 VALORES

Os valores utilizados e aplicados na Oncoterápica são de extrema importância, uma vez que todos os funcionários são instruídos a estarem de acordo com os dez "pilares" da empresa, os mesmos estão citados abaixo:

- Coerência: Correspondência entre o que dizemos e o que fazemos;
- Confiança: Confiar em nossa capacidade de protagonizar nosso próprio destino a partir de nossas habilidades, conhecimentos e escolhas;
- Cooperação: Valorização da diversidade e das competências de colaboração horizontal;
- Harmonia: Idéias antagônicas gerando consenso e consciência de que a decisão tomada será melhor para todos;
- Integridade: Combater o tráfico de influência, o suborno e a propina por parte de qualquer pessoa, entidade pública ou privada;
- Interdependência: Nosso sucesso é interdependente com o bem-estar da sociedade;
- Resiliência: Aprender com as crises e lidar com o inconcebível;

- Respeito: Respeito aos direitos de cidadania na relação com toda a pessoa afetada por nossas ações;
- Responsabilidade: Conhecer e cumprir a legislação e as boas práticas;
- Transparência: Acesso as informações e avaliações de desempenho da empresa.

2.5 OBJETIVOS DA ORGANIZAÇÃO

Crescer em média, 5% ao ano, para suprir o custo vegetativo, sempre mantendo a qualidade e o foco principal da empresa, que é paciente/usuário.

2.6 PRODUTOS E/OU SERVIÇOS

A Oncoterápica é uma clínica prestadora de serviços de terapia antineoplásica ambulatorial, para pacientes com câncer, em outras palavras a empresa realiza tratamentos quimioterápicos em seus pacientes. Ela oferece para eles um tratamento diferenciado, pois o paciente recebe o acompanhamento de uma psicóloga especializada para confortar a situação que está passando, assim como, oferece salas de alta qualidade para tratamento e são equipadas com poltronas reclináveis e TV a cabo para melhor comodidade do paciente.

A Oncoterápica possui mais dois consultórios médicos onde os médicos associados atendem a seus respectivos pacientes para ter um maior acompanhamento do tratamento realizado na clínica.

2.7 ESTRUTURA ORGANIZACIONAL E ESTRUTURA FUNCIONAL

A empresa é composta por dois diretores e, basicamente por quatro equipes: o Corpo Clínico (ONCORE), composta por médicos de dois consultórios, responsáveis pelo o tratamento médico dos pacientes; a Equipe Assistencial, composta por enfermeiras, farmacêuticas, psicóloga, médicos plantonistas e recepcionista, que são responsáveis pelo atendimento ao paciente; E o Apoio Operacional, composta pelos funcionários responsáveis pelo Faturamento, Financeiro, Desenvolvimento de Pessoas (RH), Compras/Manutenção (USG) e Tecnologia da Informação. Referente ao organograma abaixo (Figura 1), aonde mostra o apoio operacional da empresa.

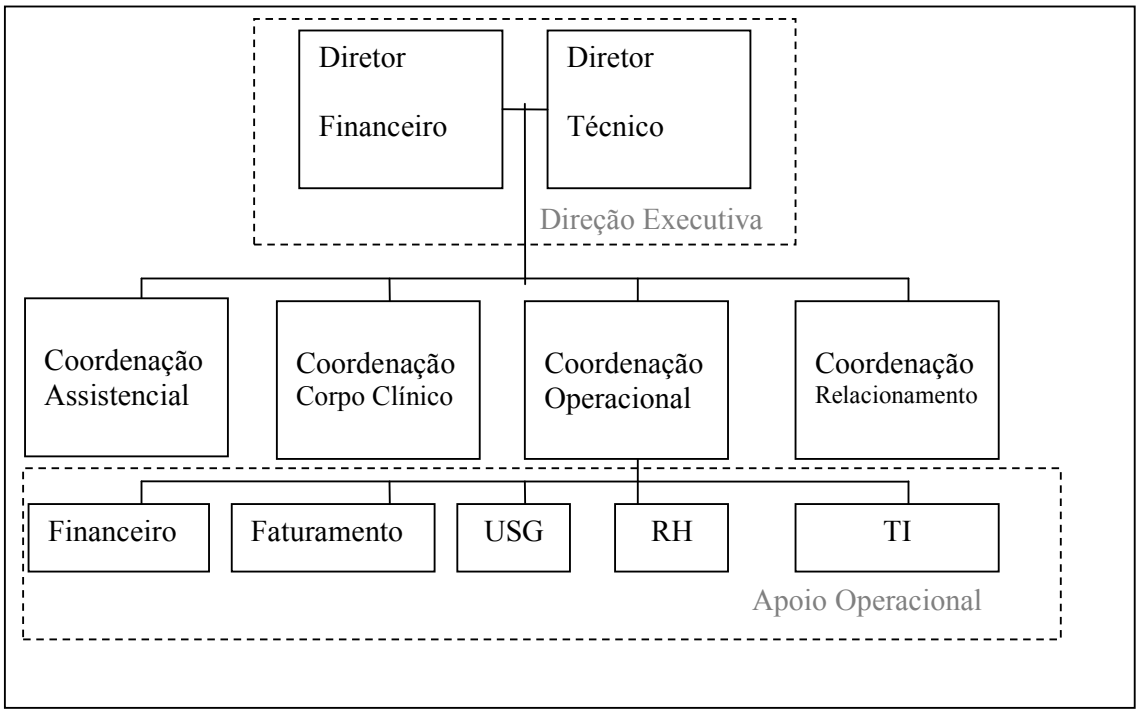


Figura 1 - Organograma da Oncoterápica
Fonte: adaptado de Oncoterápica / O autor (2008).

2.8 MERCADO DE ATUAÇÃO

A empresa atua na área da saúde atendendo a pacientes com câncer. Em sua grande maioria, por ser um tratamento oneroso, os pacientes são conveniados a planos de saúde. Pode-se dizer que os clientes da Oncoterápica, são os planos de saúde, uma vez que eles são os responsáveis por mais de 90% do faturamento da empresa, como abordado no capítulo 2.9. O tratamento do câncer em nível ambulatorial é uma técnica nova, uma vez que os tratamentos sempre ocorreram dentro de hospitais. Os sócios da Oncoterápica visionaram sempre a melhora na qualidade de vida do usuário portador de uma disfunção celular, criando, assim, a Oncoterápica.

Conforme o INCA (Instituto Nacional de Câncer), somente em Porto Alegre nos anos de 1993 a 1997 o número de portadores de câncer entre Homens e Mulheres era de aproximadamente 19.628 pessoas. Esse número foi levantado um ano e meio antes da abertura da empresa.

2.9 PRINCIPAIS CLIENTES

A Oncoterápica possui dois tipos de clientes:

- Clientes conveniados, ou seja, pacientes que possuem convênios de saúde, como Unimed;
- Clientes particulares, que por sua vez não possuem convênio de saúde.

Os dois principais convênios e, grandes responsáveis pelo faturamento da empresa, são a Unimed e o IPERGS (Instituto de Previdência do Estado do Rio Grande do Sul). A Oncoterápica possui outros agentes conveniados como CASSI (Caixa de Assistência dos Funcionários do Banco do Brasil), Golden Cross, Sul América, CABERGS (Caixa de Assistência dos Empregados do Banco do Estado do Rio Grande do Sul), entre outros convênios.

2.10 PRINCIPAIS FORNECEDORES

Os principais fornecedores da Oncoterápica são divididos em: Fornecedores de Medicamentos, Materiais de Enfermagem, Materiais de Escritório e Materiais de Limpeza. Abaixo listados:

- H G Raupp Comercial Ltda – Medicamentos;
- Distribuidora de Medicamentos Paulo Lima Ltda – Medicamentos;
- Dema Medicamentos – Medicamentos;
- Oncoprod Indústria de Comércio de Medicamentos Ltda – Medicamentos;
- BMR Medical Ltda – Materiais de Enfermagem;
- Medicor Produtos Hospitalares Ltda – Materiais de Enfermagem;
- Júnior Materiais de Escritório Ltda – Materiais de Escritório;
- LT Distribuidora Atacadista Ltda – Materiais de Escritório e Limpeza.

2.11 PRINCIPAIS CONCORRENTES

Os principais concorrentes para tratamento ambulatorial são:

- GTTO – Grupo de Tratamento Oncológico Ltda;

- CliniOnco – Clínica de Oncologia de Porto Alegre Ltda.

2.12 ÓRGÃOS REGULAMENTADORES

A Oncoterápica é regulamentada pela ANVISA RDC No. 220 – Regulamento Técnico de funcionamento dos Serviços de Terapia Antineoplásica.

2.13 O SETOR DE TI DA EMPRESA

Como já citado anteriormente, o Apoio Operacional é composto pelos responsáveis dos setores de Faturamento, Financeiro, Desenvolvimento de Pessoas (RH), Compras/Manutenção (USG) e Tecnologia da Informação.

A Tecnologia da Informação é responsável:

- Pela manutenção e atualização de todos os micros em geral na parte de *hardwares* e *softwares;*
- Pelo funcionamento das impressoras;
- Por toda a infra-estrutura de computadores da clínica que é composta por 27 computadores ligados em um servidor;
- Pelo funcionamento do sistema terceirizado pela empresa Interprocess, o qual opera sobre uma plataforma *web* necessitando sempre estar conectado à *internet* para o funcionamento;
- Pela disponibilidade da rede de dados da empresa, fornecendo *internet* a todo e qualquer computador conectado à rede da Oncoterápica.

3 SITUAÇÃO PROBLEMÁTICA

O ambiente corporativo tem sofrido muitas mudanças com a entrada da tecnologia da informação, cada vez mais importante e vital para as empresas uma vez que, a informática foi um "facilitador" nos processos internos e externos de todas as empresas trazendo maior agilidade, precisão, confiabilidade nos dados, troca mais rápida de informações entre usuários/setores, além de muitos outros benefícios às pequenas e grandes empresas.

Com o advento da era da tecnologia as empresas foram adaptando-se a mesma através da compra de computadores, servidores, e logo após os sistemas de gerenciamentos. Esses, por sua vez, tornaram as empresas mais enxutas, uma vez que a demanda de tempo e de pessoal para execução de alguma atividade, foi reduzida.

Por sua vez a Oncoterápica possui também um sistema de gerenciamento de suas informações, o GESCOM, o qual gerencia e armazena dados vitais e confidenciais para a empresa. Além de possuir um servidor dedicado, um computador que é utilizado a fim de fornecer: espaço para armazenamento de dados; manutenção/criação/controle de contas de usuários que acessam a rede; *internet* aos 27 computadores conectados a este servidor.

Caso ocorra algum "ataque" *hacker* a empresa ou o servidor pegue fogo, por exemplo, as chances de a clínica recuperar suas informações é praticamente zero, uma vez que não é aplicada nenhuma política de segurança na empresa.

Já foram constatados alguns fatores relevantes para a falta de segurança da informação na empresa, como, por exemplo:

- Ausência de *backup* dos arquivos mantidos no servidor, o que já proporcionou várias perdas de documentos corrompidos e eles não foram recuperados.

- Qualquer funcionário tem acesso à todas as informações contidas nesse servidor, onde não existe uma política de usuário dentro da empresa com limites de acessos as diversas pastas e a *sites* da *internet*.
- A falta de treinamento/conhecimento dos funcionários da empresa em relação a *e-mails* contendo *malwares* facilita a entrada de *trojans* e *worms* dentro da rede.
- A Oncoterápica não tem controle de todos os bens materiais que possui, assim como todos os componentes de informática, como *mouses, teclados, computadores*, não contém lacres ou cadeados, facilitando assim o furto dos mesmos por qualquer funcionário.
- Nenhuma das salas da clínica possui extintores de incêndios para componentes elétricos.
- Os gabinetes dos computadores e do servidor, não são aterrados, isto é, não possuem um fio-terra para descargas elétricas.

Devido à ausência de segurança da informação pergunta-se: Quais procedimentos devem ser aderidos para que a Oncoterápica esteja em conformidade com a norma de segurança da informação?

4 JUSTIFICATIVA DA ESCOLHA DO TEMA

A segurança está ligada a vários fatores, não apenas da tecnologia, mas do cotidiano. Por sua vez, a mesma está presente nas organizações, visto que as informações estão constantemente vulneráveis e, caso as empresas não possuam nenhuma política de segurança da informação, elas estarão dando margem ao erro, estando sujeitas a furto das informações sem que ninguém perceba.

A Oncoterápica devido as suas fragilidades em sua rede de dados, tanto fisicamente, como virtualmente, necessita de uma política de segurança a fim de, evitar perdas de informações vitais para a organização. Visto que existem informações confidenciais de clientes, fornecedores, faturamento, planejamento estratégico da empresa, a clínica está sujeita a cópias, alterações e até a perda das mesmas.

O trabalho se faz oportuno tendo em vista que a Oncoterápica não se encontra em conformidade com as normas de segurança da informação, portanto caso ocorra qualquer quebra da segurança na empresa, as atividades dos setores poderão ser afetadas e acarretando na demora dos processos internos da clínica, como a “queda” do servidor, por exemplo.

É cabível para o autor deste trabalho, propor um plano de melhorias e a elaboração de um plano de segurança para uma pequena empresa, como a Oncoterápica, uma vez que existem muitas organizações com as suas informações vulneráveis. Após a verificação das não conformidades, a proposta estará mais coerente com a segurança da informação em ambientes corporativos, contribuindo assim para a carreira de auditoria para empresas, na área de segurança da informação.

A viabilidade do trabalho ocorre devido aos possíveis danos envolvidos com uma hipotética invasão na segurança da informação da clínica, pois caso os seus processos

fiquem estagnados a empresa estaria sendo diretamente afetada, visto que seus setores estarão deixando de produzir com a máxima agilidade.

Existem algumas vantagens na padronização e adequação de normas de segurança da informação nas empresas.

A primeira de todas as vantagens seria comodidade e tranqüilidade, pois se a empresa esta em conformidade com métodos pré-estabelecidos, o dono, os funcionários, os sócios, ou seja, o público interno da empresa fica mais sossegado com possíveis ameaças internas e externas para a empresa, uma vez que os padrões internacionais existentes são amplamente estudados e avaliados.

Outra vantagem para uma empresa aplicar normas de segurança da informação seria a possibilidade de avaliação do processo de segurança da organização. Por haver padrões estabelecidos e detalhados para a empresa, eles tornam-se facilmente auditados, uma vez que eles seguem um modelo e, se não estiverem de acordo com o modelo saber-se-á que tal item está fora da política de segurança.

A Oncoterápica, visto o que já foi exposto, só tem a se beneficiar com uma política de segurança da informação, pois estará se protegendo de ameaças futuras, estará se regularizando conforme padrões internacionalmente seguidos por grandes multinacionais.

5 OBJETIVOS

5.1 OBJETIVO GERAL

Elaborar um plano de segurança da informação para a Oncoterápica em conformidade com as normas de segurança da informação.

5.2 OBJETIVOS ESPECÍFICOS

- Verificar os itens em conformidade e não conformidade com a norma BS 17799.1:2002;
- Analisar e propor melhorias para os itens em não conformidade com a norma;
- Implementar uma política de segurança da informação.

6 A ERA DA INFORMAÇÃO

Chiavenato (2004) cita que a Teoria Geral da Administração (TGA) possui aproximadamente cem anos. No decorrer do século XX, ela sofreu diversas mudanças, atravessando a Era da Indústria Clássica, no período que compreende os anos de 1900 a 1950; Era Industrial Neoclássica, que ocorreu a partir do ano de 1950 até 1990 e a partir de 1990 ela ingressou na Era da Informação. O surgimento desta nova era ocorreu devido ao grande impacto do desenvolvimento tecnológico e à Tecnologia da Informação (TI).

Segundo Chiavenato, a Era da Informação está associada a diversos fatores como a TI; globalização; ênfase nos serviços; aceleração da mudança; imprevisibilidade; instabilidade e incerteza, e dentro das organizações, está alinhada à produtividade, qualidade, competitividade, cliente e novamente à globalização.

Uma vez que a Tecnologia da Informação é o escopo da Era da Informação, esta monografia inicia-se abordando sobre a TI com a finalidade de obter maiores informações sobre a tecnologia e associarmos posteriormente tais informações com a Segurança da Informação.

6.1 TECNOLOGIA DA INFORMAÇÃO

A Tecnologia da Informação não abrange somente a informática, ela aborda todo e qualquer assunto referente à tecnologia.

O conceito definido por Laudon e Laudon (1999), é tudo que envolve tecnologia e computadores para a formação e uso da informação. Segundo Rezende e Abreu (2003) ela é disposta pelos seguintes componentes: *hardware*, seus dispositivos e periféricos; *software* e seus recursos; sistemas de telecomunicação; gestão de dados e informação.

Para a tecnologia ter uma funcionalidade e utilidade, Rezende e Abreu enfatizam que é preciso o recurso humano, ora chamado de *peopleware* ora de *humanware*, mesmo que esse componente não esteja inserido na parte de tecnologia de informação.

Segundo Chiavenato (2004), a TI – é a mudança do computador com a televisão e as telecomunicações. Assim sendo a TI vem crescendo cada vez mais na área corporativa e realizando diversas transformações e benefícios, tais como:

- Compressão do espaço: Inovando com um conceito de escritório, o virtual ou não-territorial, assim sendo, prédios comerciais sofreram redução de tamanho significativa devido a tal conceito, uma vez que houve uma eliminação de papéis, ou seja, tudo passou a ser eletrônico, reaproveitando, assim, o espaço usado a mais, com a diminuição do espaço ocorre, diretamente, a diminuição dos custos fixos, pois a criação de um escritório virtual não é preciso uma sala para isso. Assim sendo, para Chiavenato (2004), a miniaturização, a portabilidade e a virtualidade é a nova dimensão espacial que a TI oferece aos seus usuários;
- Compressão do tempo: Conforme já citado no capítulo sobre os benefícios do uso dos sistemas de informação, o mesmo ocorre, é lógico, com a tecnologia de informação, uma vez que as comunicações tornaram-se mais ágeis e em tempo real, possibilitando uma maior dedicação ao cliente. Os processos tornaram-se mais enxutos, uma vez que se passou a uma nova dimensão temporal. Podemos citar como exemplo de compressão de tempo o processo de *just-in-time* (JIT) onde foi o resultado da mudança da redução dos tempos/estoques no processo de produção. (CHIAVENATO, 2004)
- Conectividade: Os *laptops*, *palmtops*, e hoje em dia os *smartphones*, trouxeram uma maior mobilidade e conectividade entre os usuários, através da *internet.* Com o advento da TI, têm-se empresas globais; empresas que trabalham em localidades distantes, mas conectadas em tempo real, realizando as mesmas operações e problemas dentro das empresas, principalmente nas áreas de tomadas de decisões, como setor de Planejamento Estratégico.

6.1.1 **Áreas compreendidas pela Tecnologia da Informação**

Para a gestão total da TI se faz necessária uma análise de viabilidade, através da mensuração dos custos e benefícios aliados ao resultado, sem deixar de lado a situação

real econômica, financeira e político-social da empresa. Na gestão da TI, é preciso focar-se na inteligência da organização e não somente na tecnologia que ela possui. É necessário ter um plano de contingência para suprir qualquer falha no funcionamento, assim como possuir uma política de segurança da informação. (REZENDE E ABREU, 2003)

6.2 SEGURANÇA DA INFORMAÇÃO

Campos (2007) refere-se a segurança da informação baseada em três princípios básicos: Confidencialidade, Integridade e Disponibilidade, conforme figura 2:

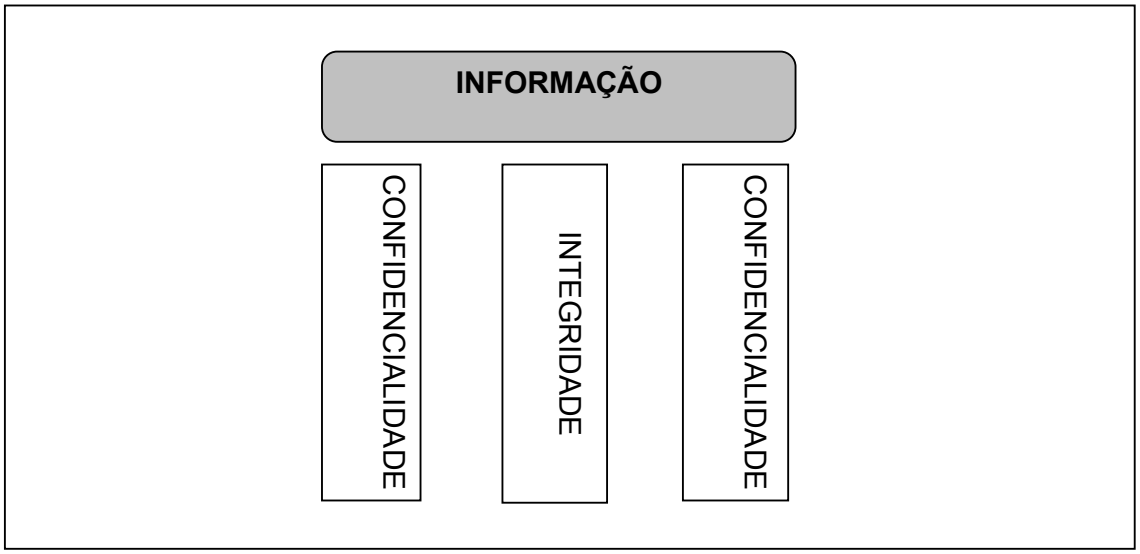


Figura 2 - Os três princípios da informação
Fonte: adaptado de (CAMPOS, 2007) / O autor (2008).

Segundo Sêmola (2003), o princípio da confidencialidade, é que toda e qualquer informação deve ser protegida conforme o sigilo do conteúdo da mesma, visando restringir o seu acesso e liberando acesso somente às pessoas destinadas. Campos (2007) acrescenta que, o acesso a uma informação por um usuário não autorizado, com ou sem dolo, seja ela protegida ou não por senha de acesso, logo se tem um incidente de segurança da informação por quebra de confidencialidade.

Para Sêmola, o princípio da integridade é que toda informação tem que ser armazenada igualmente como foi disponibilizada pelo seu proprietário, pretendendo protegê-las contra qualquer modificação indevida, seja ela intencional ou acidental.

Se porventura uma informação é impropriamente modificada, intencionalmente ou não, seja por uma fraude de um arquivo/documento, alteração de dados armazenados em um banco de dados, ou qualquer modificação indevida em um dado/informação, configura-se uma quebra de integridade referente às seguranças de informação. (CAMPOS, 2007).

Sêmola (2003) enfatiza que o princípio da disponibilidade é que toda informação formada ou obtida por um usuário ou organização deve estar disponível para todos os seus indivíduos a partir do momento em que os mesmos precisarem delas para qualquer fim. Campos (2007) conceitua como quebra de disponibilidade, quando a informação não está acessível para os usuários destinados a tais informações, como a inexistência/perda de documentos, quando os servidores estão "fora do ar", mesmo acidentalmente, ou, se os servidores estão inoperantes devido a invasões de vírus nos mesmos.

Qualquer uma das quebras sejam elas de confidencialidade, integridade ou disponibilidade, geram um incidente de segurança da informação, como todos estão sujeitos a tais falhas, pode haver prejuízos diversos para uma empresa, incluindo financeiros. Para isso analisaremos o que é um ativo de informação, e as ameaças, vulnerabilidades, partindo do princípio da segurança da informação. (CAMPOS, 2007)

6.2.1 **Ativo de Informação**

Para uma organização, a informação é um ativo de grande valor pois, é o elemento essencial de cada negócio, uma vez que toda e qualquer empresa é composta pelas mesmas, como por exemplo, cadastros de clientes, faturamento da empresa, informações bancárias, balanços patrimoniais, planejamento estratégico, e a perda de qualquer tipo de informação corporativa tem um valor bastante significativo.

A informação existe concretamente apenas quando está inserida em diversos meios, como cadernos, enciclopédias, livros, em computadores, entre outros. Logo, pode-se afirmar que mais importante que a informação é o meio onde ela está inserida, armazenada, para que possa existir. (CAMPOS, 2007).

Consideramos aqui a informação como um ativo de uma empresa, assim como ela denomina seus imóveis como ativos devido ao seu valor, usaremos a informação e os meios que armazenam tais ativos, pois a informação de uma empresa vale muito mais

que qualquer imóvel da mesma, até porque sem ela o imóvel não existiria. (CAMPOS, 2007)

Sêmola (2003) diz que o termo ativo possui devida nomenclatura da área financeira, pois é um elemento de valor para as empresas/indivíduos, e logo, necessita de uma proteção devida que é a ISO/IEC-17799, que trataremos no próximo capítulo.

Existem diversas maneiras de dividir e reunir os ativos, mas para Sêmola (2003) ele se divide em: equipamentos, aplicações, usuários, ambientes, informações e processos. Assim sendo, fica viável analisar as fronteiras de cada divisão, manejando-os com especificidade e aumentando as atividades de segurança qualitativamente.

6.2.2 **Aspectos da Segurança da Informação**

Para a prática da segurança da informação, existem dois elementos essenciais, diferentes para o devido objetivo que se queira alcançar, autenticação e legalidade. A primeira é o processo de reconhecimento formal do conjunto de caracteres dos elementos que realizam a comunicação ou estão integrados em uma operação eletrônica que libera o acesso ao dado/informação e seus ativos através de fiscalização de identificação de tais elementos; por sua vez a segunda, legalidade, são as peculiaridades as informações que possuem valor legal em um processo de comunicação, onde todas as informações/ativos estão coerentes com as normas contratuais ou conforme a legislação vigente seja ela institucional, nacional ou internacional. (SÊMOLA, 2003)

A partir desses dois elementos temos os aspectos associados, que são divididos em autorização, auditoria, autenticidade, severidade, relevância do ativo, relevância do processo de negócio, criticidade e irretratabilidade. (SÊMOLA, 2003)

O conceito de autorização é a aprovação ao acesso das informações, operações e sistemas aos usuários envolvidos no processo de câmbio das informações, depois de devido cadastramento e reconhecimento dos mesmos. (SÊMOLA, 2003)

A auditoria é o meio de coleta de provas, com a finalidade de analisar as organizações envolvidas no processo de troca de informações, portanto da origem ao destino e qual o caminho realizado para a troca de informação. (SÊMOLA, 2003)

Autenticidade fica responsável pela a garantia de que as empresas ou usuários envolvidos na troca das informações estejam com a devida certificação, para que não ocorra nenhuma quebra de segurança da informação, como é o caso dos usuários de

home-banking onde consiste que o usuário, dono da conta no banco, acesse a sua conta, sem que as informações entre banco e indivíduo sejam alteradas, pois se necessita ter a garantia da autenticidade. (SÊMOLA, 2003)

Severidade está no grau de impacto do dano de uma determinada informação, no caso ativo, pode ocorrer devido à exposição a qualquer vulnerabilidade por qualquer ameaça que seja. (SÊMOLA, 2003)

Relevância do ativo é a importância dada ao mesmo, em um processo de negócio dentro de uma operação. (SÊMOLA, 2003)

Relevância, para Sêmola (2003), do processo de negócio explica o grau de importância de um tramite de negócio, que visa atingir os objetivos vitais de uma empresa. (SÊMOLA, 2003)

Sêmola aborda a Criticidade como a crítica dada ao impacto causado dentro do negócio, como por exemplo, pela ausência de um ativo ou pelo uso incorreto ou impróprio de um documento.

Irretratabilidade são "característica de informações que possuem uma identificação do seu emissor que o autentica como o autor de informações por ele enviadas e recebidas." (SÊMOLA, 2003, p. 46 e 47).

6.2.3 **Ameaças**

Campos (2007, p.25) faz a análise de que ameaça é um "usuário externo ao ativo de informações", que ao tirar proveito das vulnerabilidade podem realizar qualquer tipo de quebra da segurança da informação referente a esse "ativo de informações".

Sêmola (2003) categoriza as ameaças em três tipos, em conformidade as intenções de cada ameaça, aonde temos as naturais que ocorrem devido a sinistros, como incêndios e acidentes de fenômenos naturais; as involuntárias onde são ameaças inconscientes, normalmente sem causa conhecida, podendo ser por erro humano; e as voluntárias as quais como o próprio nome diz são propositais, ou seja, causada por agentes externos humanos, como *hackers*, espiões, ladrões ou criadores de vírus. Campos (2007) complementa que pouco se pode realizar, a fim de diminuir ou aniquilar as ameaças, uma vez que as mesmas podem ser naturais, involuntárias, ou as que estão fora do nosso controle.

6.2.4 **Vulnerabilidades**

Para Campos (2007, p.23), o conceito de vulnerabilidade "... são as fraquezas presentes nos ativos de informação que poderiam ser exploradas, intencionalmente ou não, resultando na quebra de um ou mais princípios de segurança da informação." Sêmola (2003, p.48) contempla "As vulnerabilidades por si só não provocam incidentes, pois são elementos passivos, necessitando para tanto de um agente causador ou condição favorável, que são as ameaças".

Os exemplos de vulnerabilidades estão divididos em físicos – abrangem instalações prediais fora do padrão, falta de recursos para combate a incêndio, como detectores de fumaça, extintores de incêndios, entre outros; naturais – tudo está suscetível a sinistros, como já citado em ameaças; *hardware* – falha em qualquer componente físico de um computador, dentro de uma Unidade Central de Processamentos (do inglês *Central Processing Unity* – CPU) ou seus periféricos; *software* – falhas em instalações de programas podem acarretar vazamento de informações e acessos indevidos; mídias – qualquer meio portátil que possa conter informações, seja ele uma *pen drive*, CD-ROM, DVD-ROM, Disquete, pode ser perdido, furtado, copiado ou danificados; comunicação – acessos não autorizados, acessos indevidos a redes *wireless*; humanas – uma das vulnerabilidades mais comuns caso não tenha um treinamento adequado, uso correto de senhas, vandalismo (SÊMOLA, 2003; CAMPOS, 2007).

6.2.5 **Medidas de Segurança**

Sêmola (2003) define medidas de segurança como as melhores práticas, métodos e mecanismos utilizados para tentar defender, combater e minimizar o risco envolvido com a informação e seus ativos de quaisquer ameaças e vulnerabilidades. Podemos classificar medidas de seguranças em três categorias:

- Preventivas – Tem como objetivo prevenir incidentes de segurança que possam ocorrer. Visam manter a segurança estabelecida, a fim de que possam ser mantidas as normas de conduta e ética da segurança na empresa. Um exemplo de segurança preventiva são as políticas de segurança dentro de uma empresa, onde fica especificado e documentado que os usuários não podem ultrapassar tais

normas com a finalidade de manter o equilíbrio da segurança da informação (SÊMOLA, 2003);

- Detectáveis – O objetivo é, que através de ferramentas para auxiliar na detecção de infrações das normas de segurança dentro da empresa, através de câmeras de seguranças, sistema de detecção de usuários (SÊMOLA, 2003);
- Corretivas – São ações a serem praticadas para a correção de alguma quebra de segurança, diminuição do impacto, com um plano de contingência para tal, como restauração de *backups*, plano de recuperação de desastres (SÊMOLA, 2003).

Campos (2007) aborda os tópicos de incidente de segurança da informação, probabilidade, impacto e controle, onde:

- Incidente de segurança da informação – "É a ocorrência de um evento que possa causar interrupções ou prejuízos aos processos do negócio, em conseqüência da violação de um dos princípios de segurança da informação" (CAMPOS, 2007, p.25);
- Probabilidade – A probabilidade, conforme a Matemática, trata de um número entre 0 e 1, que indica as chances de algo acontecer. Em segurança, é a probabilidade de ocorrer alguma quebra nas normas de segurança, em relação às ameaças e as vulnerabilidades. É importante citar que podem ocorrer, eventualmente, vulnerabilidades a ativos, mas sem grande um grande potencial de ameaça, como por exemplo, a passagem de um tornado em uma empresa situada no Brasil e nas proximidades de uma empresa, a probabilidade de isto ocorre é praticamente zero, porém, não temos como afirmar com 100% de que isto possa não ocorrer. Campos (2007) faz uma ilustração completa:

> Para ilustrar, imaginemos o seguinte: estamos em agosto de 2001. Alguém nos pergunta sobre a probabilidade de as torres gêmeas do *World Trade Center* caírem no mesmo dia. Sendo um cidadão comum sem acesso a informações privilegiadas, arriscaríamos dizer que isto seria impossível, ou seja, a probabilidade nula. No entanto, por improvável que parecesse, isto infelizmente ocorreu logo no mês posterior. Quer dizer: por menor que seja, não existe probabilidade zero (CAMPOS, 2007, p.27).

- Impacto – O impacto de um incidente está ligado aos futuros prejuízos causado ao negócio, caso ocorra um incidente de quebra de segurança aos ativos da informação;

- Controle – É o modo de evitar a ocorrência de um incidente. Como demonstrado anteriormente, os dois fatores que englobam a probabilidade de um incidente ocorrer é o grau da ameaça e da vulnerabilidade. Assim sendo, devemos nos focar mais para combatermos as ameaças, uma vez que são agentes externos, ou seja, que não estão ao nosso alcance. Para isso devemos programar um controle de segurança da informação, ou seja, é um mecanismo para diminuir a fraqueza, o ponto fraco, de um ativo/informação, sendo eles uma tecnologia, pessoa, processo ou ambiente. Existem alguns tipos de controles como: as senhas de acesso, contratos de responsabilidade, equipamento de *firewall*, entre outros (CAMPOS, 2007).

Para Brasiliano (2002), a segurança da informação está compreendida entre a segurança física da informação e a segurança lógica dos Sistemas de Tecnologia da Informação.

6.2.6 **A segurança física e de pessoal**

A segurança física compreende uma porcentagem importante da segurança global da rede. Sendo assim, qualquer projeto para uma rede de produção deve ser administrado às questões de segurança física como: controle do acesso as salas de máquinas; níveis de acesso as áreas segurança nas salas; registro de acesso e de recuperação de dados; administração de usuários externos; prevenção contra incêndios, relacionadas ao acesso das instalações. (WADLOW, 2000)

Soares *et al* (1995) define segurança física e de pessoal como os meios que garantem a integridade dos recursos físicos de um sistema que são indispensáveis para a segurança geral como um todo. Mecanismos operacionais devem ser delineados para definir responsabilidades dos usuários que utilizam os sistemas. A segurança de qualquer sistema, em último caso, depende da segurança física dos seus meios e da confiabilidade do pessoal que opera tais recursos. Assim sendo, de nada adianta utilizar os melhores *softwares* para a segurança dos sistemas se intrusos podem acessá-los fisicamente.

Nakamura e Geus (2007) lembram que uma das formas de invasão a sistemas empresariais ocorre dentro da própria empresa, caracterizando esta ação como *insiders*, que, conforme "... são os maiores responsáveis pelos incidentes de segurança mais graves nas organizações. Apesar de as pesquisas mostrarem que o número de ataques

pela internet é maior, os maiores prejuízos são causados internamente.” Os autores dizem que a identificação de tais invasores é complicada, mas normalmente são colaboradores insatisfeitos com os seus trabalhos, que querem demonstrar o seu valor para as empresas. Sendo assim, tal tipo de funcionário é facilmente manipulado pela concorrência.

Um exemplo recente foi o caso da a Ferrari®, conhecida equipe de Fórmula 1®, que teve seus documentos técnicos confidenciais repassados para sua rival McLaren®, uma vez que o ex-projetista, Stepney, da equipe vermelha, não conseguiu ascender em sua carreira profissional.

6.2.7 **A segurança lógica da informação**

Atualmente, para Beal (2005), o grande número de ambientes em redes multiplicou o número de problemas com segurança de forma gritante. Sendo assim, qualquer usuário com um computador ou *notebook* torna-se um administrador de sistema, necessitando somente gerenciar em sua máquina procedimentos de segurança, como as ferramentas de antivírus. Sendo assim, caso um usuário não esteja atento com os procedimentos de segurança, ele estará deixando a rede vulnerável à uma invasão, como por exemplo, a contaminação de um vírus. Caso uma rede esteja conectada a *Internet*, a segurança física não garante proteção nenhuma, pois deixa de estar em um local físico e passa a estar em toda a *network*, ou seja, navegando por qualquer provedor conectado a *internet* no mundo inteiro.

Para Beal (2005), a melhor maneira de se compreender as falhas de segurança lógica e, classificar quais as medidas de proteção mais propícias, é dividir as falhas em áreas, tais como: segurança de redes, segurança de aplicativos, segurança de sistemas, segurança do ambiente e usuário final.

6.2.8 **As normas e padrões nacionais e internacionais de segurança da informação**

Para Beal (2005), as normas e padrões são uma importante referência para a qualidade e confiança de qualquer processo. Quando produtos e serviços seguem a normas e padrões internacionalmente reconhecidos, os mesmos passam a ter uma

garantia e maior confiabilidade na hora de escolher algum produto ou solicitar qualquer tipo de serviço.

Na área de TI, existem diversas referências para as empresas implementarem melhores práticas na gestão de tecnologia da informação, como também padrões internacionais que serão citado nos próximos capítulos.

6.2.8.1 BS 7799 e suas variações

A Norma BS7799 foi criada em uma época onde a Inglaterra liderou um movimento da comunidade britânica, que continham as melhores práticas para o gerenciamento de segurança da informação. Devido à falta de segurança nos países da Comunidade Britânica, os mesmos passaram a adotar a norma da BSI – *British Standart Institution*.(SÊMOLA, 2003)

Campos (2007) complementa que o código de prática BS7799 orientava as organizações a concentrar suas ações relacionadas à segurança de informação, mas não era possível verificar se tais ações estavam sendo realizadas corretamente. A partir daí foi criado um *checklist* para a verificação das conformidades da norma com as empresas, logo o novo código levou o nome de BS7799-1 e o *checklist*, de BS 7799-2. Com a criação desta lista de checagem, foi possível criar uma certificação para as empresas que implementavam tais medidas. A partir da ISO – *International Starndartization Organization*, a norma britânica passou a ter uma visibilidade mundial, onde no ano de 2000 analisou a normativa britânica BS 7799-1 e lançou sua versão chamada de ISO 17799:2000. (CAMPOS, 2007)

Porém, a norma BS 7799-2 não foi contemplada pela normativa ISO, que criou uma necessidade mundial que permitisse uma certificação da segurança da informação dentro das organizações. A ISO não chegou a um denominador comum para o lançamento de tal certificação, logo a *British Standart* atualizou e adequou a BS 7799-2 aos padrões da *International Starndartization Organization*, baseados nas famílias dos padrões ISO 9000 e 14000, utilizando o ciclo PDCA (*Plan, Do, Check, Act*). A partir de 2002, passou a ser uma norma de certificação de segurança da informação e tornou-se um instrumento de orientação para a programação de um sistema de gestão de segurança da informação. (CAMPOS, 2007)

Em 2005, foi realizada uma reedição do código de práticas da ISO, com muitas melhorias e identificando os controles de segurança da informação de forma mais clara. Nesta mesma época foi homologada a segunda parte da BS 7799, possibilitando então a certificação, logo a nova norma ISO, passou a ser chamada de ISO 27001, tal qual as famílias 9000 e 14000 (CAMPOS, 2007).

Não demorou muito a ABNT – Associação Brasileira de Normas Técnicas, em conformidade com a ISO 17799:2000, criou o projeto na versão brasileira, onde foram criados comitês de estudos, com grandes nomes das áreas públicas e privadas, que sugeriram melhores adaptações da norma conforme as necessidades do mercado brasileiro e, levando o nome de NBR ISO/IEC 17799-1 tornou-se a primeira norma brasileira da área. (SÊMOLA, 2003)

Assim como a ISO 9000, cada vez mais as certificações de segurança da informação terão valor dentro das organizações, como diferenciais competitivos na Era da Informação. Conforme mostra Nakamura e Geus (2007, *apud* Módulo e-Security, setembro 2002) que no Brasil a importância da política de segurança é a realidade de 39% das empresas; 16% das empresas ainda têm políticas irregulares, por algum motivo, devido a alguns itens em não conformidade com a norma; 30% das organizações a política está em fase de desenvolvimento; e somente 15% das empresas não possuem nem a formalização da política.

Beal (2005) acrescenta que a ISO/IEC 13335 (*Guidelines for the management of* IT *security*) abrange as diretrizes de gestão de segurança focado na área da tecnologia da informação. Ela é composta por cinco partes, que trabalham os conceitos e melhores práticas para a segurança de TI, da administração e planejamento da segurança em TI, a norma tem como objetivo o estabelecimento de uma referência comum de gestão de segurança para toda e qualquer empresa.

6.2.8.2 Estrutura da NBR ISO/IEC 17799

A ISO é organizada em 10 tópicos, conforme Beal (2005), assim como são citados por Menezes (2006):

- Política de segurança: Recomenda a formalização de uma política interna da empresa, com diretrizes, princípios e regras para a devida orientação e base para implementação e manutenção da segurança da informação dentro da empresa.

- Segurança organizacional: Estabelece uma estrutura de gestão da segurança da informação baseada em um PDCA para a empresa;
- Classificação e controle dos ativos de informação: Recomenda realizar inventário dos ativos e classificação de responsabilidades necessárias para o reparo e controles dos mesmos;
- Segurança em pessoas: Aborda para a redução de erro humano, como roubo, fraude ou uso inadequado dos sistemas e informações.
- Segurança física e do ambiente: Aborda sobre questões de proteção dos recursos e as instalações do método de processamento de informações vitais ou variáveis com o negócio.
- Gestão das operações e comunicações: Aborda sobre a garantia a operacionalização correta e segura dos meios de processamento da informação assegurando a integridade de serviços e informações.
- Controle de acesso: Contempla que o acesso a informação recurso de processamento das informações e processos de negócios sejam controlados com base nos requisitos de negócio e segurança da informação. E também que as regras de controle de acesso levem em consideração as políticas para autorização e disseminação da informação.
- Desenvolvimento e manutenção de sistemas: Menezes (2006) abrange os requisitos para o desenvolvimento de sistemas. Recomenda que os requisitos de segurança, junto com os acordos de contingência, sejam classificados na fase de levantamento de requisitos para um projeto e esclarecidos, regulamentados e documentados como parte do estudo de caso para um sistema de informação.
- Gestão da continuidade do negócio: Conforme Beal (2005) é a preparação para as empresas neutralizarem as interrupções das atividades operacionais.
- Conformidade: Uma das diretrizes mais importantes, uma vez que são as diretrizes para o consenso com os requisitos legais, como a proteção de direitos autorais. Descreve também as metodologias a serem adotadas em caso de violação da política de segurança, com punições que os infratores estão sujeitos.

Sendo assim, as empresas que dependem de tais seguranças, uma vez que elas utilizam sistemas de informações gerenciais, para a sua tomada de decisão durante o seu dia-a-dia.

6.2.9 **Política de segurança da informação**

Beal (2006, p.43) "A elaboração de uma política de segurança da informação (PSI) representa um passo fundamental no estabelecimento de um sistema de gestão de segurança da informação eficaz.".

Sêmola (2003) explica que a PSI tem a finalidade de conduzir as ações de gestão de segurança. O autor salienta ainda que guardada as devidas proporções, a PSI tem a mesma importância a constituição federal para um país.

Ferreira e Araújo (2006, p.9) aborda que a PSI "define o conjunto de normas, métodos e procedimentos utilizados para a manutenção da segurança da informação, devendo ser formalizada e divulgada a todos os usuários que fazem uso dos ativos".

Sendo assim, as empresas que dependem de uma política de segurança, pois utilizam sistemas de informações gerenciais, para a sua tomada de decisão durante o seu dia-a-dia.

6.3 SISTEMAS DE INFORMAÇÕES GERENCIAIS

Assim como o corpo humano, as empresas recebem e usufruem de informações que permitem a elas sobreviverem no atual ambiente competitivo. As tomadas de decisões nas empresas ocorrem através das informações disponíveis e, a fim de facilitar as suas decisões, as organizações elaboram sistemas com a finalidade de busca, coleta, armazenamento, classificação e tratamento das informações indispensáveis para o seu perfeito funcionamento. Para esses sistemas de informações gerenciais, a denominação em inglês, é *Management Information System – MIS* (CHIAVENATO, 2004).

Chiavenato (2004) comenta que os SIG (Sistemas de Informações Gerenciais) são formados por sistemas computacionais capacitados para proporcionar todos os tipos de informações, para qualquer tomada de decisão.

Em contra partida os sistemas de informações gerenciais dentro das organizações, Laudon e Laudon (1999, p.5), citam que "um sistema de informação é uma parte integrante de uma organização e é um produto de três componentes: tecnologia, organizações e pessoas" como são demonstradas na figura 3.

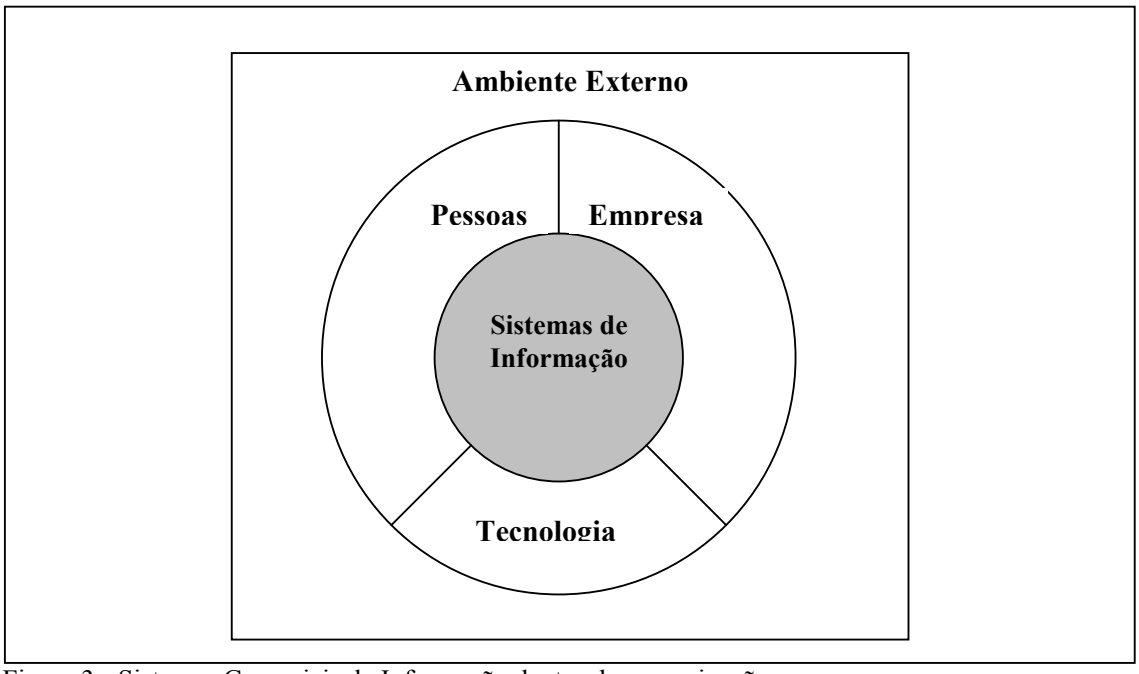


Figura 3 - Sistemas Gerenciais de Informação dentro das organizações.
Fonte: adaptado de (LAUDON e LAUDON, 1999) / O autor (2008).

Laudon e Laudon (1999) definem que, sem o conhecimento das pessoas, das empresas e das tecnologias, uma empresa não consegue utilizar de forma eficiente, os sistemas de informação.

Para os autores, as pessoas fazem parte dos sistemas de informação, ou seja, são os usuários de sistemas baseados em computadores que utilizam dentro de suas empresas e cabe a elas alimentar o banco de dados do sistema.

Conforme Laudon e Laudon (1999) as organizações configuram os sistemas de informação das mais variadas formas, sempre se adequando as suas necessidades, uma vez que elas são organizações formais. Sendo assim, as empresas possuem setores diferentes de trabalho, cada departamento é especializado em uma área da administração, e por conseqüência possui funcionários treinados para as mais variadas funções como vendas, produção, RH e finanças.

Todas as organizações possuem uma hierarquia em sua estrutura, onde sempre um funcionário irá se reportar a outro de nível hierárquico maior que o seu e, os postos de trabalhos mais altos possuem cargos de gerência. Os funcionários de cargos inferiores normalmente alimentam os sistemas através de uma entrada de materiais, por exemplo, os profissionais em cargos mais altos geram relatórios através de tal entrada, podendo tomar a decisão mais correta possível.

O último dos três componentes gira em torno dos sistemas de informações dentro das organizações, a tecnologia, e conforme Laudon e Laudon (1999) são o meio em que os dados são armazenados, organizados, transformados para o usufruto dos funcionários dentro da organização. Laudon e Laudon (1999, p.6) escrevem que: "... um sistema de informação pode ser um sistema manual, usando somente a tecnologia do lápis e papel (um exemplo seria uma pasta de um professor que contém os registros e notas dos seus alunos)". E, complementa com essa transcrição de que, os computadores desapareceram com o sistema manual de processamento de grande volume de operação das informações e é o que será citado no capítulo sobre tecnologia da informação.

Conforme Rezende e Abreu (2003), os sistemas de informação devem ser estruturadores e analisados conforme a perspectiva sociotécnica, onde a tecnologia e a empresa devem ser ajustadas de forma que funcionem em perfeita harmonia. Assim como mostram Laudon e Laudon (1999), as empresas e os usuários passam por processos de aperfeiçoamento, na medida em que os sistemas dentro da empresa, são desenvolvidos a fim de evitar surpresas entre os usuários, ou não ter profissionais treinados para tais, assim como a criação desses sistemas acontecem conforme as necessidades de cada organização.

Oliveira (2002) define que para compreender o conceito de sistemas de informações gerenciais (SIG), primeiro teremos que trabalhar com os conceitos relativos a cada uma de suas partes:

- Sistema;
- Informações;
- Gerenciais.

6.3.1 **Sistema**

Buscando um pouco sobre a onde os sistemas se originaram, Chiavenato (2004) afirma que a Teoria Geral dos Sistemas (TGS) nasceu do trabalho do biólogo *Ludwig Von Bertalanffy*, que consistia em questões científicas, empíricas ou pragmáticas dos sistemas. Os seus esforços concentraram-se na produção de definições que permitiam exercer condições aplicáveis a realidade empírica e pragmática, dentro das questões científicas dos sistemas (REZENDE e ABREU, 2003).

Conforme Laudon e Laudon (1999), uma das definições de sistema é um agrupamento de componentes, interligados e interdependentes com a finalidade de coletar, recuperar, analisar, armazenar e disseminar informação, a fim de auxiliar o planejamento, o controle, coordenação e a tomada da decisão em empresas e organizações.

Chiavenato (2004, p.327) complementa que, após a análise da etimologia da palavra sistema "... (do grego: *sun* = com e *istemi* = colocar junto)..." o mesmo passa a imagem de conexão. "O universo parece estar formado de um conjunto de sistemas, cada qual contido em outro ainda maior como um conjunto de blocos para construção" (CHIAVENATO, 2004 *apud* BEER 1969 p.28).

Já para Rezende e Abreu (2003), "O conceito de sistemas não é uma tecnologia em si, mas é resultante dela."

6.3.1.1 Componentes de Sistema

"Os sistemas de informação essencialmente transformam a informação em uma forma utilizável para a coordenação de fluxo de trabalho de uma empresa, ajudando empregados ou gerentes a tomarem decisões." (LAUDON e LAUDON, 1999, p.4)

Os componentes de um sistema se relacionam através de quatro premissas básicas (ver na Figura 1.1):

- Entrada (*inputs*): Através dos insumos é utilizado qualquer sistema, ou seja, a entrada em um sistema é tudo aquilo que é importado/recebido do mundo exterior para dentro do sistema, como informação, energia, materiais. Através de tais *inputs* o sistema pode trabalhar ou funcionar (CHIAVENATO, 2004);
- Saída (*outputs*): É a resposta/relatório final da operação de um sistema. É através da saída que o sistema exporta para o ambiente o seu resultado, ou seja, é para os usuários que tais resultados são exibidos, para tomar a melhor decisão possível, por exemplo, em um caso de gerenciamento (CHIAVENATO, 2004);
- Processamento: Para Oliveira (2002) é a maneira que os elementos dos sistemas trabalham com as entradas inseridas, a fim de obter as saídas desejadas. Para Chiavenato (2004) ele emprega o termo caixa negra, do inglês, *Black Box,* o qual indaga que um sistema tem o seu interior vendado, ou seja, ninguém pode

desvendar o que há no seu interior, somente "por fora", em meio a alterações externas. A caixa negra processa uma "caixa hermeticamente fechada", com entradas e saídas, citadas acima;

- Retroação (*Feedback*): Chiavenato (2004) comenta que a retroalimentação do sistema, como também pode ser denominada, é uma resposta proporcionado pela saída do sistema conforme a sua entrada no sentido de ser ou não alterada de alguma forma. Oliveira (2002, p.24) diz que "É um instrumento de regulação retroativa ou de controle, em que as informações realimentadas são resultados das divergências verificadas entre as respostas de um sistema e os parâmetros previamente estabelecidos";
- Ambiente: Oliveira (2002) cita que o ambiente de um sistema é o um grupo de elementos que não fazem parte do mesmo, mas alguma mudança feita no sistema pode alterar tais elementos e estes alterados podem mudar o sistema.

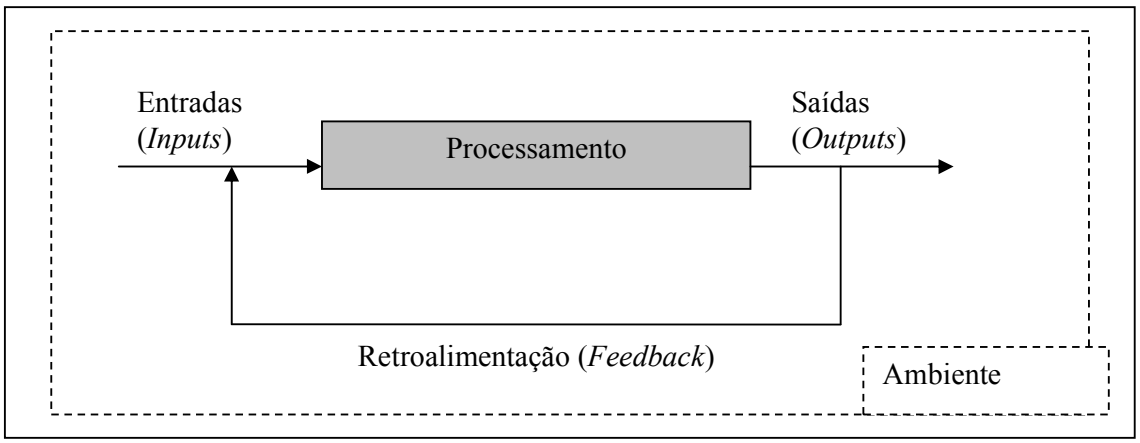


Figura 4 - Relacionamentos entre os componentes de um sistema.
Fonte: adaptado de (CHIAVENATO, 2004) / O autor (2008).

6.3.2 **Informação**

Para Oliveira (2002, p.36), antes de falarmos em informação, devemos diferenciar dado de informação. A diferença que difere dado ou um conjunto de dados de informação "é o conhecimento que ela propicia ao tomador de decisões"

Sendo assim, Oliveira (2002) cita que dado é qualquer tipo de elemento em forma "bruta" que não é compreendido. Chiavenato (2004) informa que é um registro referente a qualquer evento ou ocorrência, como um banco de dados, como o próprio nome já diz, é uma das formas de armazenar a maior quantidade possível de dados para alguma

finalidade de combinação ou processo. Caso tenhamos um dado com significado, como um conjunto de números que formam uma data, temos uma informação.

Laudon e Laudon (1999, p.10) complementam informando que: "... Para Platão, os dados puros eram uma reflexão em uma parede de todas as coisas acontecendo no mundo."

Para Chiavenato (2004, p.332), o conceito de informação "... reduz a incerteza ou que aumento o conhecimento a respeito de algo." Ao contrário de um dado, como citado anteriormente. Ainda o autor cita que é a informação é algo com significado, ou seja, possui sentido, nexo, dentro de um determinado contexto, e, através de tal mensagem, podemos tomar uma ação, uma vez que a informação reduz a probabilidade de erro e até mesmo nos dá mais conhecimento sobre algo.

Oliveira (2004) define a informação como: "quando nós nos comunicamos, escrevemos, a fim de repartir alguns de nossos conhecimentos tácitos, para tentarmos transmitir, como informação, aos demais usuários. O autor lembra que o conhecimento e a informação normalmente são confundidos e que na área de TI, eles podem ser usados como sinônimos. Sendo assim, a informação está associada aos fatos e também à comunidade deles.

Para Campos (2007, p.15), "... informação é ao mesmo tempo composta de dados e componentes do conhecimento, como ilustrado na figura 5 a seguir, que mostra que a informação é a base para o conhecimento."

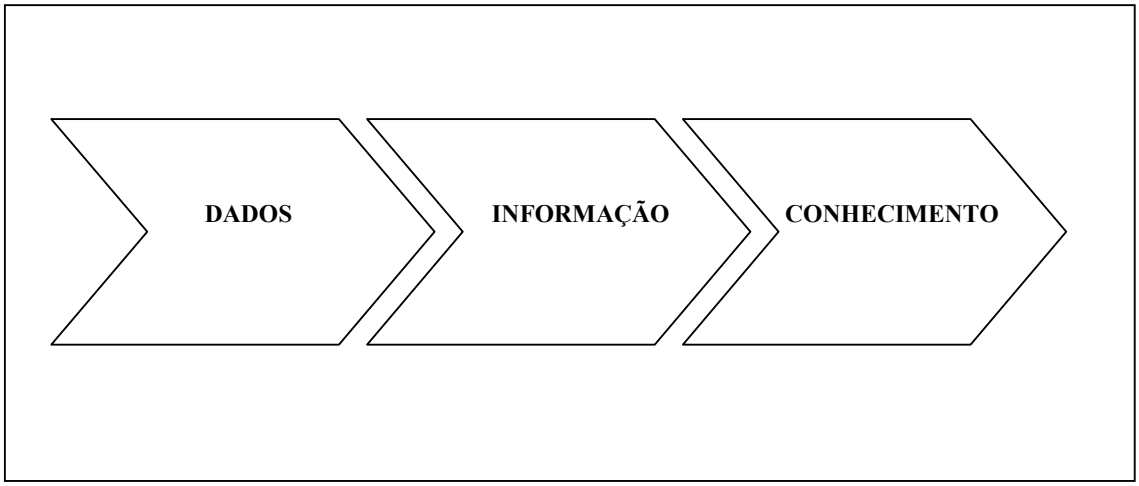


Figura 5 - Composição de informação e conhecimento.
Fonte: Adaptado de (CAMPOS, 2007) / O autor (2008).

6.3.3 **Gerenciais**

Para Oliveira (2003, p.39) "gerencial é o processo administrativo (planejamento, organização, direção e controle) voltado para resultados"

> É importante apresentar o conceito de gerencial de forma inerente ao processo administrativo porque, na maior parte das vezes, os executivos *se esquecem* de percorrer todos os aspectos envolvidos e ficam apenas dirigindo sem qualquer sustentação administrativa, ou seja, não planejam a situação do alcance dos resultados delineados pelo planejamento e, conseqüentemente, não podem controlar e avaliar nada, pois não estabeleceram antecipadamente os resultados a serem alcançados (OLIVEIRA, 2003, p.29).

6.3.4 **Objetivo, foco e características dos sistemas de informação**

O objetivo maior, segundo Rezende e Abreu (2003), é auxiliar, independente do nível do sistema, os processos de tomadas de decisões.

O foco dos sistemas de informação, conforme Rezende e Abreu (2003), tem que estar focado na empresa/negócio, para poder facilitar as tomadas de decisões. Para ilustrar melhor o foco usaremos o exemplo que Rezende e Abreu (2003, p.63) usaram que: "O exemplo pode ser de uma indústria que deve ter seus sistemas de informação direcionados ao processo fabril, efetivamente auxiliando nos processos de produção e comercialização de tais produtos industrializados".

As características, conforme Rezende e Abreu (2003), que os sistemas de informações possuem são – grande volume de dados e informações; complexidade de processamentos; muitos clientes e/ou usuários envolvidos; contexto abrangente, mutável e dinâmico; interligação de diversas técnicas e tecnologias; suporte a tomada de decisões empresariais; auxílio na qualidade, produtividade e competitividade organizacional.

6.3.5 **Benefícios do uso de sistemas de informação**

Um dos benefícios de um sistema de informação eficiente é afetar a estratégia corporativa e o crescimento da empresa, e tal efeito pode ajudar as empresas, clientes, usuários ou indivíduos que interajam com os sistemas de informação (Rezende e Abreu, 2003 *apud* Oliveira, 1988; STAIR, 1998). Analisando também outros benefícios,

conforme Rezende e Abreu, melhor serviço e vantagem competitiva, redução da carga horária de trabalho, uma vez que os sistemas automatizaram vários processos.

Existe também uma maior segurança da informação, uma vez que os sistemas são mais precisos que o ser humano, sendo menos suscetível ao erro. Assim sendo, nota-se que tais benefícios adquiridos com a advinda dos sistemas de informação são muito mais vantajosos tanto para as organizações como para os seus usuários.

7 MÉTODO

Este capítulo trata sobre as metodologias necessárias para elaborar este plano de implementação de segurança da informação na Oncoterápica. Roesch (2006) integra que o estágio de prática profissional é uma ocasião para convencionar teoria e prática. A autora complementa que para o delineamento da pesquisa, usamos na literatura, duas direções principais a pesquisa quantitativa e qualitativa.

Roesch (2006) explica que a técnica quantitativa destaca o uso de dados padronizados que consente ao pesquisador organizar sumários, comparações e generalizações. Sendo assim a análise de dados da pesquisa é norteada por uso de estatística.

Roesch apud Jones (1987) esclarece que a técnica qualitativa trata um interesse teórico que de modo autoconsciente busca suspender suposições descuidadas referente significados divididos.

De acordo com Roesch apud Bryman (1989) o método de pesquisa qualitativa demonstra duas diferenças em comparação à teoria de pesquisa quantitativa. Uma das diferenças é que a distinção entre os dois tipos diferentes de pesquisa não é devido ao fato da presença ou ausência de quantificação. O fato é que o enfoque insinua começar ligado a opiniões amplas cujo teor vai concretizando-se durante o método de coleta. A segunda diferença é a evidência na perspectiva do sujeito pesquisado.

> Enquanto na pesquisa quantitativa o pesquisador parte de conceitos *a priori* sobre a realidade, o pesquisador qualitativo sai a campo não estruturado, justamente para captar as perspectivas e interpretações das pessoas. Neste caso, a reflexão teórica ocorre durante ou quase no final do processo de coleta de dados (ROESCH, 2006 apud BRYMAN 1989, p.125).

Roesch (2006) explica que a pesquisa qualitativa e suas formas de coleta e análise de dados são adequados para uma etapa exploratória da pesquisa. Dessa forma, a teoria qualitativa é adaptada para a avaliação formativa, quando temos de melhorar a efetividade de uma instrução, ou um plano, ou quando temos que formular de normas, bem como temos que selecionar metas de um planejamento e construir uma mediação.

A partir das definições apresentadas a implementação de uma política de segurança da informação foi utilizada uma pesquisa qualitativa que norteou o método de pesquisa deste trabalho. Uma vez que foram sugerido as melhores práticas, ou seja, normas e padrões de um plano já constituído e mediante a isto elaborado o melhor projeto para implementação de um plano de segurança da informação na Oncoterápica.

Dentro de tais perspectivas, Roesch (2006) aborda sobre duas estratégias de pesquisa: o estudo de caso e a pesquisa-ação.

A primeira estratégia para Yin (2001) observa um fato contemporâneo dentro do seu assunto. Difere do método histórico, uma vez que se referem ao presente e não ao passado.

Por sua vez a pesquisa-ação, conforme Roesch (2006) consente em obter conhecimento referente à realidade social empírica. Deste modo, permite ao pesquisador ampliar os itens analíticos conceituais e decisivos de explicação, através dos dados, e não de modos estruturados e altamente quantificados.

O que difere a pesquisa-ação, segundo Roesch (2006, apud Jones 1987), das demais áreas da pesquisa qualitativa é o arrolamento da teoria com a prática. É na pesquisa-ação que o pesquisador alia a teoria com a prática. Assim sendo, o pesquisador é caracterizado como um consultor, pois ele estará participando do processo e analisando o mesmo, verificando os resultados das intervenções. Podendo analisar o modo dos fatos como eles são, pois as pessoas envolvidas no processo têm suas particularidades.

Neste caso, foi utilizado a estratégia de pesquisa-ação como método de colocar em prática a teoria utilizada na BS 7799.1:2002. Uma vez que o autor desta monografia teve facilidade em aplicar na empresa-alvo e assim aliou a teoria, que é a política de segurança da informação, com a prática, ou seja, no ambiente corporativo da Oncoterápica.

Para começar a realizar uma pesquisa qualitativa por meio de uma pesquisa-ação, foi necessário utilizar técnicas de coleta de dados, para que os mesmos foram analisados

e viabilizados de acordo com os padrões. Para isso os meios mais utilizados na pesquisa de caráter qualitativo são as entrevistas e observação participante.

Para Roesch (2006), observação participante é utilizando quando o pesquisador se torna um empregado na empresa.

O levantamento da coleta de dados foi baseado no *checklist* da BS 7799.2, conforme o quadro 2, que mostra todos os itens da norma que foram trabalhados nesta monografia.

Gerenciamento de Informações de Segurança BS 7799.2:2002 *Check List* Auditoria			
Referência		**Área de auditoria, objetivos e questões**	
Checklist	**Norma**	**Seção**	**Questão de Auditoria**
Política de Segurança			
1.1.2	3.1.2	**Revisão e avaliação**	
Classificação e Controle de ativos			
3.1.1	5.1.1	**Inventário de ativos**	
Segurança de pessoal			
4.2.1	6.2.1	**Educando e ensinando segurança da informação**	
4.3.1	6.3.1	**Relatando incidentes na segurança**	
Segurança física e do ambiente			
5.1.1	7.1.1	**Perímetro de segurança física**	
5.1.2	7.1.2	**Controle de entrada física**	
5.1.3	7.1.3	**Segurando escritórios, quartos e facilidades**	
5.2.1	7.2.1	**Implementando equipamentos de proteção**	
5.2.3	7.2.3	**Segurança de cabos**	
5.2.4	7.2.4	**Manutenção de equipamentos**	
5.3.1	7.3.1	**Política de tela e mesa limpa**	
Gestão da comunicação e operacionalização			
6.5.1	8.5.1	***Backup* da informação**	
Controle de Acesso			
7.1.1	9.1.1	**Política de Controle de Acesso**	
7.2.1	9.2.1	**Registro de usuário**	
7.7.3	9.7.3	**Sincronização do relógio**	

Quadro 2 - Gerenciamento de Informações de Segurança BS 7799.2:2002 *Checklist* Auditoria
Fonte: Traduzido mídia CD-ROM de Ferreira e Araújo (2006).

Os itens da *checklist* BS 7799.2 foram todos levantados por métodos de observação participante, uma vez que o autor desta monografia foi funcionário da empresa, facilitando assim o acesso aos itens estudados da *checklist.*

Infelizmente a *checklist* não foi trabalhado em sua total integridade, uma vez que o tempo para a realização deste trabalho é de somente um mês e meio depois de feita a coleta dos dados junto à empresa. Portanto o *checklist* possui 127 itens para serem auditados em empresas, e para este plano de ações foram utilizados somente 15 itens da BS 7799.2:2002, conforme o Quadro 2.

Por sua vez as entrevistas semi-estruturadas, foram realizadas em forma de bate-papo. Pois foram realizadas em reuniões abertas com os responsáveis dos setores dos setores que compõe o administrativo da empresa. Sendo assim não ouve um questionário formulado e sim apresentação de vulnerabilidades na empresa e discutidas em reuniões.

Para finalizar a coleta de dados, foi trabalhada uma tabela de todos os investimentos necessários para implementação das políticas estudadas e analisadas neste trabalho para a Oncoterápica.

8 ANÁLISE DE DADOS

Este capítulo aborda sobre os dados coletados juntamente a empresa e conforme o método de pesquisa citado no capítulo anterior.

Foi realizada juntamente a empresa um cronograma de atividades e ações a serem tomadas em relação à segurança de informação da empresa. Para isso foi criado na empresa um comitê de segurança da informação, conforme o item 3.1.1 da norma BS 7799:2002 como um ponto de partida, para a tomada de ação na empresa. O comitê de segurança da informação é composto pelos responsáveis dos setores de TI, Faturamento, Secretariado e Administrativo. A partir da concepção do comitê foram realizadas reuniões semanais para discutir as vulnerabilidades da informação na Oncoterápica, como apresentado no capítulo da situação problemática desta monografia. E foi compreendida a necessidade de um planejamento de fiscalização e padronização sobre a infra-estrutura de segurança da empresa.

A partir do exposto a Oncoterápica e a criação do comitê de segurança de informação, foram observados os 15 itens compostos no quadro 2 do capítulo 7 deste trabalho. A partir da observação e levantamento de tais dados os mesmos foram analisados e distinguidos entre aqueles que estão em conformidade e os que não estão em conformidade com as normas de segurança da informação. A análise do levantamento está exposta nos dois próximos capítulos.

Mesmo este trabalho sendo uma pesquisa-ação, tiveram itens em que a empresa solicitou orçamento para a implementação, uma vez que é o método utilizado na Oncoterápica, para qualquer tipo de investimento. Sendo assim existem itens observados e analisados neste trabalho que aguardam aprovação de orçamento juntamente a diretoria da Oncoterápica, impossibilitando uma aplicação e avaliação neste trabalho.

8.1 ITENS EM CONFORMIDADE

Os itens em conformidade com a norma de segurança da informação são aqueles que apresentaram similar padrão ao citado na norma, através da análise foi realizada com a análise critica do funcionário de TI da empresa, o autor da monografia, e apresentada em reunião, para avaliação.

Por mais que estivessem em conformidade com a norma, o autor realizou uma análise crítica do item, para que ele se aperfeiçoe, uma vez que os itens estão em constante renovação e reformulação, devido a novas ameaças e novas tecnologias.

Os dados foram apresentados na seguinte ordem:

- O item da *checklist* da BS 7799.2;
- E o que foi encontrado na empresa.

8.1.1 **Relatando incidentes na segurança**

O item 6.3.1 da norma de segurança da informação cita se existe um procedimento de relato formal, para reportar incidentes de segurança, através de canais adequados de segurança, o mais rápido possível.

*Encontrado na empresa***:** Existem três meios de relatar os incidentes ocorridos na Oncoterápica: Por telefone, pelo *Google® Talk®* e por *E-mail*.

Os registros realizados por telefone, não ficam gravados o relato de incidente, para isso o setor de TI solicita ao funcionário que envie um *e-mail* para inclusão do incidente na planilha, para um maior controle, porém nem sempre o mesmo é realizado por parte do funcionário da empresa, por falta de conhecimento da importância do pedido formalizado em forma de texto e não verbalmente.

A planilha de Excel®, conforme Figura 6, ela informa a ordem de registro, o que seria o número de protocolo para o incidente; a data do incidente ocorrido; o usuário que informou; o *hardware*, porém o mesmo não é informado, pois não existe um cadastramento dos ativos de *hardwares* da empresa; a prioridade, conforme a percepção da necessidade da continuidade do processo e o impacto que gera o incidente para a empresa; o tipo de problema, ou seja, o que o funcionário informa; o detalhamento do tipo de problema, ou seja, o que o colaborador de TI entendeu do tipo de problema; e o detalhamento da resolução do problema.

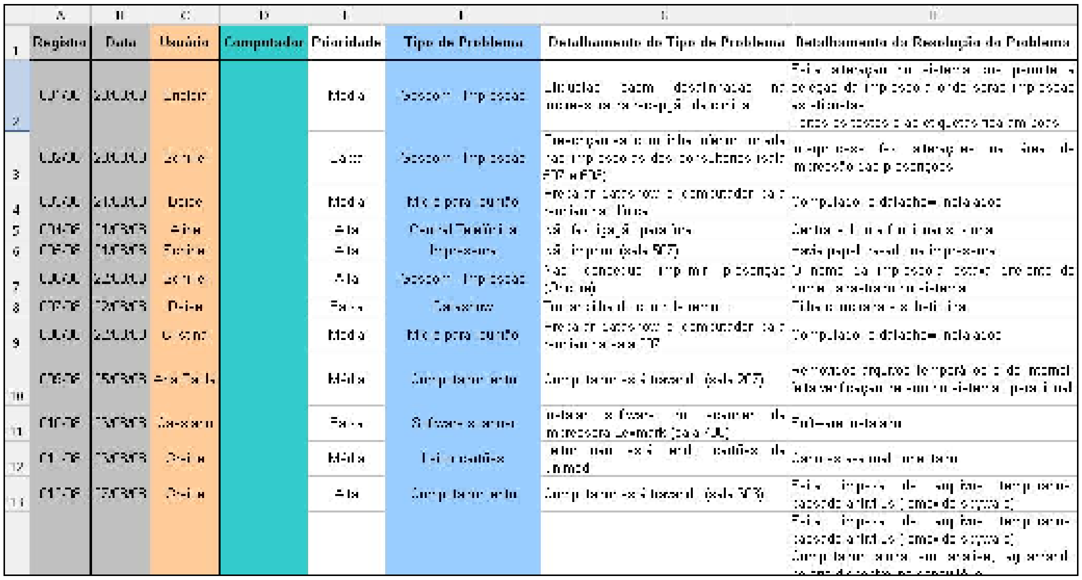


Figura 6 – Planilha de Incidentes da Oncoterápica
Fonte: Oncoterápica (2008).

8.1.2 **Perímetro de segurança física**

No capítulo de Segurança Física do Ambiente, a BS 7799.1, aborda item 7.1.1 (5.1.1 no *checklist*), se as facilidades de segurança das fronteiras físicas foram implementadas para proteger o processo de serviço da informação, ou seja, se existem barreiras que separem e ao mesmo tempo protejam o servidor ou outros ambientes que processem a informação. Alguns exemplos desse tipo de mecanismo, citados na norma: são controles de entrada em portões, paredes, muros, recepção lotada e etc.

Encontrado na empresa: O responsável da TI possui acesso a sala do servidor, uma vez que ele é o único que tem a chave da sala.

A Oncoterápica poderia trabalhar com abertura de porta por fechadura com senha eletrônica, a qual possui um teclado, e a porta só abre mediante a digitação correta da senha. Dependendo do modelo, os valores variam em uma faixa de R$ 200,00 a 655,00 reais.

8.1.3 **Controle de entrada física**

Assim como o item de segurança física, o controle de entrada física. Se o controle de entrada é somente para pessoas autorizadas que tenham acesso a diversas áreas da organização.

Encontrado na empresa: Somente as pessoas autorizadas possuem as chaves para acessar as suas salas. Há apenas duas pessoas que possuem os códigos de segurança dos alarmes de todas as salas, uma delas é a primeira abrir a clínica e a outra é a última pessoa que sai da clínica. O prédio comercial possui uma portaria que utiliza um interfone para comunicar as salas administrativas e os consultórios da Oncoterápica quem está na portaria. Os funcionários da Oncoterápica são os únicos que possuem acesso livre pela portaria, mas acredito que para um maior controle poderia ser utilizado um sistema de catracas, como já existem em outros prédios comerciais de Porto Alegre. Por sua vez a clínica tem a sua própria portaria e utiliza portas escurecidas com vidro fumê, logo as pessoas que olham do lado de fora da recepção, não visualizam nenhuma movimentação, porém, a recepcionista, dentro da clínica, consegue visualizar a circulação de pessoas fora. A recepção é equipada com uma câmera externa, para uma melhor visualização de todos aqueles que se aproximarem da entrada da clínica e, mediante a isso, a recepcionista, através de um mecanismo elétrico, libera a porta para o usuário, seja para sair ou entrar na clínica.

8.1.4 **Sincronização do relógio**

No capítulo da norma que trabalha sobre “Controle de Acesso”, o item da norma 9.7.3 versa sobre se o computador ou dispositivo de comunicação tem a capacidade de operar em tempo real, isso deve ser arrumado para uma norma acordada, como as coordenadas universais ou horário padrão. A definição correta do relógio do computador é importante porque garante a exatidão dos registros da auditoria.

*Encontrado na empresa***:** Os relógios de todos os computadores locais são configurados conforme o relógio do servidor. Por sua vez, o relógio do servidor, é baseado no horário de Brasília, DF (GMT -03h00min), e é atualizado conforme o

horário de verão brasileiro (GMT -02h00min), uma vez que horários de agendamento de pacientes e tratamento dos mesmos são extraídos do horário do computador local.

8.2 ITENS EM NÃO CONFORMIDADE

Os itens em não conformidade com a norma de segurança da informação são aqueles que ou não possuíam nenhuma referência com a norma ou até tinham certa similaridade, porém estava desatualizada ou não funcionava regularmente.

Os itens apresentados nos próximos capítulos foram realizados trabalhos conforme a necessidade da clínica. Logo, os itens podem já estar implementados, ou podem estar aguardando autorização por parte da Oncoterápica, para execução.

A partir de então os onze itens em não conformidades foram abordados da seguinte maneira:

- O item da BS 7799.1:2002;
- O que foi encontrado na empresa;
- Tomada de ação para solução para a conformação da norma BS 7799.1:2002.

8.2.1 **Revisão e Avaliação**

Segundo o item 3.1.2 expõe que se a política de segurança possui um proprietário que seja responsável pela sua manutenção e revisão de acordo com uma revisão de um processo já definido. Se um processo afirma que a revisão tome o lugar em resposta de qualquer mudança que afete a base da avaliação original, exemplo: segurança significativa, incidentes, novas vulnerabilidades ou mudança organizacionais ou técnicas na infra-estrutura.

Encontrado na empresa: A empresa não possuía um responsável ou proprietário pela revisão e avaliação das políticas já praticadas.

Tomada de ação: A partir da primeira reunião que ocorreu na Oncoterápica no dia 12/09/2008, e com a criação do comitê de segurança da informação, ficou designado que o responsável de TI e juntamente com o autor desta monografia, seriam os responsáveis pela manutenção e revisão de toda e qualquer política a ser implementada ou já

implementada na empresa. A partir da já utilização planilha de incidentes pode-se avaliar novas vulneráveis com a norma de segurança da informação.

8.2.2 **Identificação de Ativos**

No capítulo da 5.1 da BS 7799.1:2002 “Classificação e Controle de Ativos” foi trabalho o item 5.1.1 Identificação de Ativos. Esse por sua vez trata se os inventários ou registros são mantidos com os ativos importantes, associando cada informação em um sistema. Se cada ativo identificado tem detalhado o seu proprietário, com definição e classificação de segurança e de acordo com a localização identificada. É um levantamento de patrimônio da empresa, inserindo em cada ativo, uma etiqueta de identificação, e esta etiqueta tem que estar em conformidade com os dados da etiqueta no sistema da empresa, pois esse sistema informa que a etiqueta inserida em um certo ativo, quem é o dono ou responsável pelo ativo, a qual área pertence e a sua específica localização na empresa.

Encontrado na empresa: A empresa tem uma lista, porém a mesma não foi atualizada e revisada desde janeiro do ano de 2007, mas não contempla também uma classificação de segurança sob cada item e proprietário(s) ou responsável do ativo, assim como o ativo não possui um selo de identificação que o mesmo está inserido na listagem.

Tomada de ação: Foi criada uma planilha, conforme a Figura 7, a qual relaciona os ativos da empresa. A mesma é separada em ativos de TI e ativos mobiliários. Cada ativo recebeu uma etiqueta provisória, a qual possui o nome da empresa e um código. O código segue um padrão:

Para ativos da TI da clínica, o código possui os algarismos “729”, uma vez que a clínica está situada na Rua Almirante Barroso 729, seguidos de mais quatro dígitos em ordem crescente por número utilizado. O código para ativos das salas no prédio comercial possuem como algarismos padrão “725” seguidos de quatro dígitos que aumentam conforme o número de ativos.

Todos os ativos de TI possuem no final de cada codificação as letras “ti” juntas. Estes códigos estão alimentados dentro da planilha criada e em funcionamento. Os ativos de TI são contemplam os itens de *Hardwares* que a empresa possui, como monitores, teclados, *mouses*, *desktops*. A planilha mostra a configuração de cada *Hardware*, para isso foi utilizado o programa Everest® (Figura 8), o qual uma vez

instalado em um computador local emite relatórios com informações pertinentes as configurações de cada *Hardware*. A partir de então conseguimos coletar informações os tipos de memórias RAMs utilizadas em cada computador da clínica, para possuir um *backup* deste tipo de *Hardware*. A planilha também contempla fotos das etiquetas, imagens das Placas Mães, assim como imagem dos tipos de monitores. Os ativos de TI foram classificados por localização de sala e por Equipe, conforme o organograma da empresa.

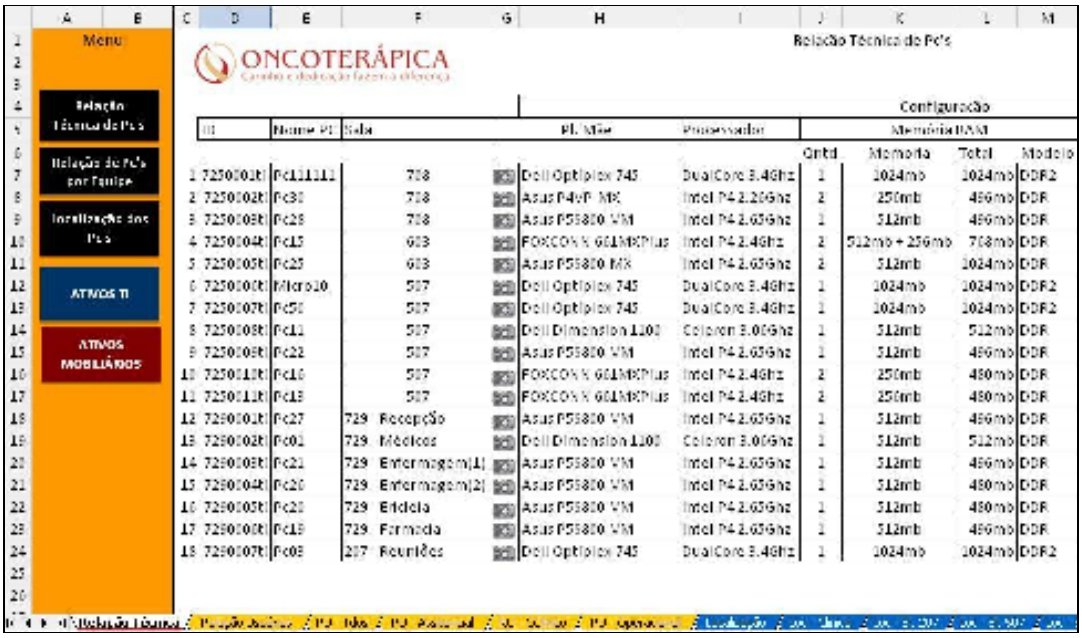


Figura 7 – Planilha de Identificação de Ativos
Fonte: Oncoterápica (2008).

Figura 8 – Informações de *Hardware*
Fonte: Programa Everest® (2008).

8.2.3 **Educando e ensinando segurança da informação**

Entrando na área de Segurança de Pessoas da norma, o item 6.2.1 aborda se todos os funcionários da organização recebem treinamento apropriado de segurança da informação e cursos regulares de políticas e procedimentos da organização.

*Encontrado na empresa***:** Atualmente, no treinamento e informações recebidas a um novo funcionário da empresa não é informado sobre aspectos de segurança e segurança da informação e muito menos políticas e procedimentos a estes processos.

Tomada de ação: A tomada de ações será realizada em duas etapas - para funcionários da empresa e para novos colaboradores.

A tomada de ações para os funcionários da empresa foi realizada uma matriz 5W2H, conforme o quadro 1.

O quê? *What?*	**Quem?** *Who?*	**Quando?** *When?*	**Onde?** *Where?*	**Por que?** *Why?*	**Como?** *How?*	**Quanto ?** *Howmuch?*
Treinamento Funcionários Adm.	Ricardo Américo e Responsável de TI	12/12/2008	Sala de reuniões 203	Para demonstrar aos funcionários as vulnerabilidades que a Oncoterápica possui e instruí-los de como diminuir tais vulnerabilidades.	Através de apresentação de slides e entrega de apostila com os slides apresentados.	R$ 0,00
Treinamento Funcionários Consultórios	Ricardo Américo e Responsável de TI	19/12/2008	Sala de reuniões 203	Para demonstrar aos funcionários dos consultórios as vulnerabilidades que a Oncoterápica possui e instruí-los de como diminuir tais vulnerabilidades.	Através de apresentação de slides e entrega de apostila com os slides apresentados.	R$ 0,00
Treinamento Funcionários Clínica	Ricardo Américo e Responsável de TI	04/01/2008	Sala de reuniões 203	Para demonstrar aos funcionários da clínica as vulnerabilidades que a Oncoterápica possui e instruí-los de como diminuir tais vulnerabilidades.	Através de apresentação de slides e entrega de apostila com os slides apresentados.	R$ 0,00

Quadro 1 – 5W2H para tomada de ação de treinamento de pessoal
Fonte: O autor (2008).

O quadro 1 ilustra todas ações a serem tomadas para os atuais funcionários da Oncoterápica.

Para novos funcionários, ao serem contratados, serão entregues cartilhas referentes a normas e procedimentos internos da empresa. Assim o novo funcionário estará inserindo-se no âmbito de segurança da informação já estabelecido na Oncoterápica.

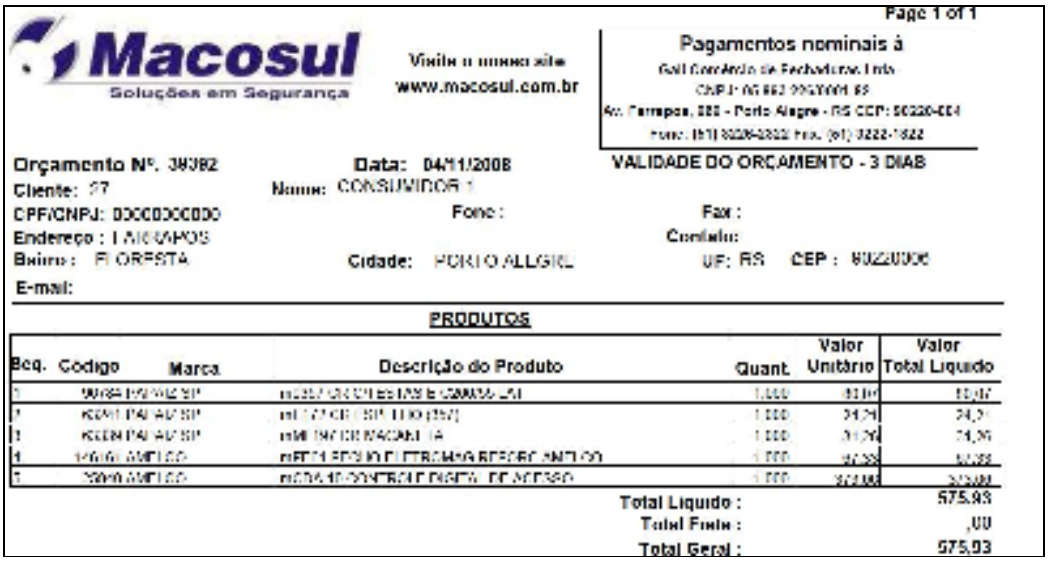
8.2.4 **Segurando escritórios, quartos e facilidades**

O item "Segurando escritórios, quartos e facilidades" é contemplado pelo item 7.1.3 da norma que acerca se as salas que tem a informação dos serviços de processamento estão trancadas ou possuem armários ou cofres fechados. Se os serviços de processamento de informação são protegidos de desastres naturais ou feitos pelo homem. Se existe uma ameaça em potencial de instalações vizinhas.

Encontrado na empresa: Todas as salas da empresa, só são acessadas por intermédio de chaves. Porém as salas não possuem gavetas com chaves e cadeados para reservar as informações de possíveis invasores. O caixa da empresa não fica localizado dentro de um cofre apropriado para abrigar valores e é de fácil acesso de todos, porém possui um responsável ficando vulnerável na falta ou ausência do responsável. Sala do servidor possui uma janela em sua porta de fácil violação, além do que a sala não tem grande circulação de funcionários, facilitando externamente que quiser arrombá-la. Quanto à proteção contra desastres naturais, a sala do servidor, ou seja do processador de informações possui isolamento em casos de descarga elétrica, enchente, pois não está próxima a janelas do prédio e não foi construída abaixo da caixa d'água do prédio. É equipada com detectores de fumaça no caso de incêndio, e um ar-condicionado *split*, o qual refrigera a sala a uma temperatura média de 19 graus centigrados. Somente em casos de terremotos (desastres naturais) a sala conta com a "sorte" da estrutura do prédio, mas como é do conhecimento de todos o Brasil está sob uma grande placa tectônica, o que impossibilita qualquer tremor de terra. Também foi citado no capítulo 8.2.5 os equipamentos de proteção de cada sala da empresa, ou seja, os sensores de movimentos que a empresa possui juntamente com a Siemens® Segurança.

Tomada de ação: Conforme citado no item 8.1.2 desta monografia a empresa poderia utilizar sistemas de codificação para abertura de portas onde contenham informações ou processamento de informações da Oncoterápica, como as salas do

financeiro e a sala do servidor. Para isso foi realizado contato telefônico com a empresa Macosul®, o atendente Milton passou *e-mail* com orçamento do produto, informando que necessitaria a troca da fechadura, a instalação de um contra fecho eletromagnético, que é o que libera a porta após a validação da senha, e o controlador digital de acesso, conforme a Figura 9, a qual mostra o orçamento.



Macosul
Soluções em Segurança

Visite o nosso site
www.macosul.com.br

Pagamentos nominais à

Orçamento Nº. 38382 Data: 04/11/2008
Cliente: 27 Nome: CONSUMIDOR 1
CPF/CNPJ: 00000000000 Fone: Fax:
Endereço : LAVRAPOS Contato:
Bairro : FLORESTA Cidade: PORTO ALEGRE UF: RS CEP :
E-mail:

VALIDADE DO ORÇAMENTO - 3 DIAS

PRODUTOS

Seq.	Codigo	Marca	Descrição do Produto	Quant.	Valor Unitário	Valor Total Liquido
1				1,000		
2				1,000		
3				1,000		
4				1,000		
5				1,000		

Total Liquido : 575,93
Total Frete : ,00
Total Geral : 575,93

Figura 9 – Orçamento fechadura de controle de acesso
Fonte: Macosul (2008).

Para a proteção da janela que possui na porta do servidor, foi sugerida ou a colocação de uma grade, ou a troca do material de vidro, por uma chapa de acrílico. O acrílico é utilizado, por exemplo, no 8.º do prédio da FACE na PUCRS, onde está localizado os *switchs* do prédio. Este material tem uma durabilidade maior que o vidro, pois não é estilhaçado facilmente.

Os valores para uma placa de acrílico nas dimensões 1,20m por 80cm e 4mm de espessura variam de R$ 230,00 a R$ 280,00. Foram solicitados orçamentos, mas as empresas não retornaram os orçamentos a eles ofertados por contato telefônico.

8.2.5 **Implementando equipamentos de proteção**

Conforme o item 7.2.1 da norma de segurança da informação, "implementar equipamentos de proteção" relata que se controles foram adotados para minimizar os riscos de ameaças em potencial, como roubo, fogo, explosivos, fumaça, água, vibração,

efeitos químicos, aparelhos elétricos, radiação eletromagnética, enchentes e etc. Se existe uma política em relação a comer, beber e fumar nas proximidades dos serviços de processamento de informações.

*Encontrado na empresa***:** A empresa possui em todas as salas juntamente com a empresa de Segurança Siemens® sensores de movimentação dentro das salas e na clínica da Oncoterápica. Os sensores são ligados, mediante a digitação de senha e, somente fora do expediente da empresa, com a finalidade de minimizar uma invasão a empresa. O prédio comercial onde estão localizadas as salas administrativas e a clínica possuem *sprinklers*, mais conhecidos como "chuveiros automáticos de prevenção contra incêndio" (Figura 10), porém estes, segundo um técnico em Engenharia Civil contratado pela empresa para vistoria das salas, informou que em um possível incêndio a qualquer sala da Oncoterápica, os *sprinklers* não seriam acionados, já que os equipamentos foram pintados em uma das reformas realizadas. Logo as salas comerciais da empresa estão vulneráveis ao fogo, uma vez que as mesmas, para prevenção de incêndio, só possuem tal equipamento. Todas as salas administrativas, consultórios e a própria clínica possuem áreas próprias para lanches e refeições, porém os mesmo são próximos a serviços de processamento de informações, como os computadores locais.

Tomada de ação: Para o concerto de tais *sprinklers*, seria necessário ativá-los para esvaziar o encanamento deles e assim trocá-los. Porém além de ser um custo muito alto, se torna inviável, pois todo o prédio teria que realizar a esta operação e as atividades teriam que ser cessadas por um tempo muito longo. A única solução para este caso é a compra de equipamentos mais simples, como os extintores de incêndio. Foi orçado juntamente a empresa CR Extintores® cinco extintores de incêndio da classificação ABC (ver Tabela 2). Este tipo de extintor combate a qualquer tipo de incêndio, seja ele em equipamentos elétricos ou materiais sólidos, não havendo a necessidade de comprar dois tipos diferentes de extintores de incêndio.

Criar ambientes para que os funcionários possam realizar lanches ou refeições separadamente de computadores locais ou qualquer equipamento que processe informações.

No capítulo anterior, Segurando escritórios, quartos e facilidades, é um complemento para este capítulo, mas especificamente para proteção de serviços de processamento de informação.

Figura 10 – *Sprinkler* pintado
Fonte: Oncoterápica (2008).

Tabela 2 – Tabela de Orçamento de Equipamentos de Extintores de Incêndio

Tipo de Extintor	Qntd.	Empresa	Custo Instalação	Custo Produto	Custo Total
PQS 04 KG ABC	5	CR Extintores	R$ 0,00	R$ 145,00	R$ 725,00
Total					R$ 725,00

Fonte: CR EXTINTORES (2008).

8.2.6 **Segurança de cabos**

Ainda trabalhando o capítulo de "Segurança Física e do Ambiente" da norma BS 7799.1:2002 ele aborta um item específico que faz referência a "Segurança de cabos" no item 7.2.3 que aborda que se o cabo das telecomunicações que transportam dados e informações de suporte dos serviços estão protegidos de interceptação ou defeito. Se existe algum controle de segurança adicional para substituir informações criticas ou sensíveis.

Encontrado na empresa: Nenhum dos cabos de rede da Oncoterápica possui alguma identificação ou proteção contra interceptação ou defeito. Os cabos de telecomunicações possuem identificação. A infra-estrutura do prédio comercial já não comporta mais cabos *lan*, pois a tubulação feita na construção do mesmo é estreita como está exposto na Figura 12.

A Figura 11 mostra outra situação na clínica. O *switch* principal da empresa, o qual se encontra aos pés aonde uma das enfermeiras trabalha, ao lado de um computador local. Está em contato com o ambiente, sempre com muita sujeira em cima dele. A fonte de alimentação é uma régua, a qual se encontra sobre o *switch*, sem nenhuma isolação e separação da rede lógica com a rede elétrica. O que já ocorreu por várias vezes o desligamento deste equipamento, uma vez que foi retirado da tomada elétrica não intencionalmente.

Tomada de ação: Foi analisado na primeira reunião na Oncoterápica o problema de localização e utilização deste *switch*. O responsável do Administrativo da empresa solicitou um orçamento para o ano de 2009, com a finalidade de que o *switch* esteja em conformidade com os padrões de segurança. Conforme a tabela 3 segue o orçamento realizado, pela empresa S4T® em (www.s4t.com.br), para colocar o *switch* em um *rack* específico para *switches*, porém a maior necessidade seria colocar o equipamento juntamente a sala do servidor localizada no sétimo andar do prédio comercial.

Contratar uma empresa especializada, para identificar todos os cabos em suas duas extremidades, para saber que cabos conectados ao *switch* são ligados em quais computadores, porque somente assim será possível identificar um problema de rede quando o mesmo estiver associado ao cabo RJ-45 conectado ao computador local. Não foi realizado orçamento para este serviço, pois não foi localizado nenhuma empresa em Porto Alegre para realização do mesmo. Mas ainda é necessária a organização dos cabos.

Nos casos de futuras instalações será utilizado um roteador *wireless* em cada uma das salas da empresa, pois não são localizadas no mesmo andar, e será instalado nos computadores placas *wireless* para conectarem-se a rede da Oncoterápica e a eliminação dos fios por conseqüência. Este caso não foi orçado, uma vez que não se tem uma previsão próxima de instalação de novos computadores locais para a empresa.

Figura 11 – *Switch* da Clínica
Fonte: Oncoterápica (2008).

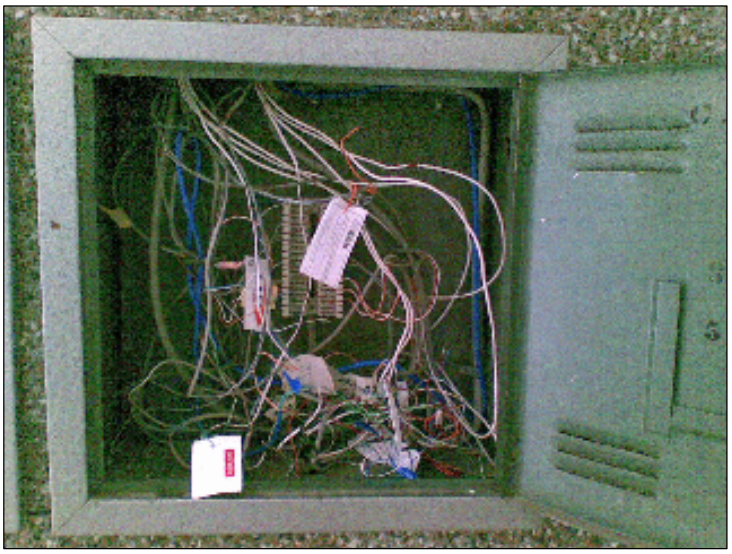


Figura 12 – Cabeamento no prédio comercial
Fonte: Oncoterápica (2008).

Tabela 3 – Orçamento para equipamentos de segurança dos cabos

Item	**Qntd.**	**Custo Total**
Rack para *Switch*	1	R$ 1.537,25
Total		**R$ 1.537,25**

Fonte: O autor (2008).

8.2.7 **Manutenção de equipamentos**

O item 7.2.4 referente à "Manutenção de Equipamentos" informa que se o equipamento é mantido com os intervalos como o fornecedor dos serviços recomendou especificamente. Se a manutenção é realizada apenas por pessoal autorizado. Se todos os registros são mantidos com todas as suspeitas ou falhas reais e todas as medidas de correção e prevenção. Se os controles apropriados são implementados enquanto o equipamento está desligando as instalações. Se o equipamento é coberto por seguro, se as exigências do seguro são satisfatórias.

Encontrado na empresa: Podemos separar a manutenção e atualização de equipamentos em duas etapas:

Hardware: A manutenção de *hardwares* da Oncoterápica não ocorre de forma preventiva, ou seja, ela só é realizada na medida em que ocorrem incidentes nos equipamentos. Foi observado que a empresa possui um servidor desatualizado, pois é um computador normal com a única função de administrar os usuários logados a rede, fornecer a esses usuários conexão com a *internet* e armazenar informações. Porém a configuração deste "servidor" é inferior aos computadores locais dos usuários, uma vez que possui 768Mb de Memória RAM sendo que 16Mb são compartilhados com a memória de vídeo, portanto baixando a memória RAM para 752Mb, processador Intel® Pentium IV® 2.2 GHz e 30Gb de *HardDisk*. Considerando-se que hoje já existem tecnologias mais avançadas que trabalham em nível de processamento com dois núcleos, no caso os Inteis® Core2Duo® e os AMDs® Turionx2®, a Oncoterápica está com um servidor muito desatualizado.

Tomada de ação para Hardwares: Para os computadores locais, não haveria a necessidade de *upgrades* tão drásticos como no servidor da clínica, uma vez que utilizam programas básicos e não necessitam de uma alta velocidade de processamento. Foi apresentado em reunião a necessidade de atualização do servidor, tanto como *Hardware* como em *Sofware* e o mesmo foi solicitado para que o responsável de TI realiza-se um orçamento para um novo servidor. O mesmo está apresentado na tabela 4, conforme orçamento enviado pela Dell Computadores®.

Softwares: A manutenção e atualização de *softwares* ela não ocorre na Oncoterápica. Não possui um controle de licenças de *softwares* adquiridas. Os usuários das máquinas locais, por falta de treinamento, não realizam as atualizações automáticas

para os *softwares*. Sendo assim passa a deixar o sistema vulnerável, uma vez que muitos *softwares*, como os *browsers*, estão em constante atualização, com a finalidade de prevenção de falhas de segurança. O mesmo problema aplica-se ao servidor, o qual possui como sistema operacional o Windows® Server 2000®, que possui algumas limitações, inclusive de seguranças, por isso que já foram lançadas duas novas versões de Windows® Server®, para proteger e oferecer melhores recursos para os sistemas operacionais de servidores. Foi observado também, que o servidor não tem um sistema de *firewall* de toda a rede. Os antivírus das máquinas locais, além de serem *Freewares,* a maioria deles estão na versão mais desatualizada. O número de licenças do pacote *Office* 2007® é inferior ao número instalado nos computadores.

Tomada de ação para Softwares: Foram atualizados todos os antivírus dos computadores para a versão mais atualizada, assim como será realizado um monitoramento semanal referente às atualizações automáticas, tanto para o antivírus como para o do *Windows*® XP® instalado. Por sua vez o servidor, foi realizado um orçamento para *Windows® Server* 2003®, assim como para aquisição de um *firewall*, conforme pode-se observar na tabela 4. E para melhor proteção contra descargas elétricas foi orçado um *Nobreak* com mais capacidade.

Tabela 4 – Orçamento de *Hardwares* e *Softwares* para a Oncoterápica

Equipamento	**Qntd.**	**Configuração**	**Custo Total**
Servidor Dell PowerEdge 840	1	Processador Intel Xeon Quad Core X3220 2.4 GHz	R$ 6.181,55
		2GB de memória RAM DDR-2	
		2 Discos Rígidos 250GB Serial Ata2 de 7200rpm	
		Controladora de array SAS 5IR (PCI-Express)	
		1 Interface de rede 10/100/1000 UTP Onboard	
		DVD-RW, Mouse Ótico, Teclado USB	
		3 anos de garantia *ProSupport End User* com atendimento on-site 7x24 com 4 horas de tempo de resposta	
		Sem Monitor	
Dell UPS 1.5 KVA 127V	1	No-Break APC Smart de 1500VA - 120V	R$ 1.260,73
Windows Server Standard 2003	1	32 bits OEM em inglês - Service Pack 2	Incluso servidor
Microsoft Cal de acesso	13	Acessos das máquinas locais ao servidor	R$ 1.005,55
Firewall	1	Aguarda orçamento	Aguarda Orçamento
Total			**R$ 8.447,83**

Fonte: O autor (2008).

A Dell Computadores® incluiu no orçamento uma prestação de serviço 24/7, ou seja, caso alguma peça do servidor dê algum defeito, eles cobrem o atendimento 24 horas por dia, 7 dias da semana, chegando ao local em no máximo 4 horas para a solução do problema.

8.2.8 **Política de Mesa Limpa e Tela Limpa**

Um dos itens mais simples da norma e mais fáceis de ser controlado, não está em conformidade na Oncoterápica, segundo o item 7.3.1, se a tela de bloqueio automática do computador é ativada pelo usuário. Ou a tela pode ser bloqueada quando o computador não é usado por um período. Se os funcionários foram avisados para deixar qualquer material confidencial em forma de documentos em papel, mídia e etc. trancados quando estão ausentes.

*Encontrado na empresa***:** Os funcionários da área administrativa, os quais manejam materiais de informações privilegiadas da empresa, quando ausentes, deixam tais informações sob as suas mesas ou dentro de gavetas sem nenhuma proteção, como mostra a Figura 13. As telas do sistema do operacional não são bloqueadas nem pelo usuário, nem pelo sistema quando esse não é utilizado por um determinado período. Os funcionários não recebem nenhuma instrução quanto a proteção de documentos em papel, mídia e etc.

Tomada de ação: Com a realização do treinamento, citado no capítulo 8.2.3, os usuários estarão aptos para tomar maiores prevenções quanto à política de mesa limpa e tela limpa.

Figura 13 – Mesa do setor financeiro
Fonte: Oncoterápica (2008).

A Figura 13 ilustra a mesa de um funcionário do administrativo. A mesa contem as agendas do funcionário, papéis de relatórios do sistema de gestão da empresa, informações sobre fornecedores entre outros materiais.

8.2.9 ***Backup* da informação**

O item 8.5.1 aborda se o *backup* de informações empresarias importantes, como servidor de produção, componentes críticos de rede, configuração de *backup* etc., foram feitos regularmente. Exemplo: Segunda-Quinta: incrementar o backup e sexta: backup completo.

Se a mídia de *backup* junto com o procedimento para restaurar o *backup* são guardados com segurança e bem longe do site atual. Se o *backup* de mídia é regularmente testado para garantir que eles podem ser restaurados no prazo colocado no procedimento operacional de recuperação.

Encontrado na empresa: O *backup* da empresa é realizado por um computador local, o do funcionário de TI, através de um *software* de *backup* o Cobian® *Backup*. Este computador está localizado a 3,5 metros da sala do servidor. Ele realiza a cópia das pastas do servidor para dentro de uma partição do *HardDisk* do computador local, compactando os arquivos copiados. O *Backup* é realizado no formato que a norma cita como exemplo, é um *backup* incremental de segunda a quinta e sexta-feira é realizado

um *backup* completo. A gravação em mídia de DVD é realizada pelo o funcionário de TI, mas normalmente ela não é realizada.

Com a realização de *backup* pelo programa já utilizado pela a empresa, o mesmo comprime os arquivos copiados, porém os arquivos eles não são testados para saber se eles estão realmente disponíveis e funcionando.

Tomada de decisão: Para realizar um *backup* padrão de segurança em informação, continuará sendo utilizado o Cobian *Backup*® e mais disco virtual na *internet*. O serviço é realizado pela Locaweb® a qual disponibiliza diversos serviços via *internet* para pessoas físicas e jurídicas. Os serviços são os mais variados, como registro de domínios para a *internet*, como a virtualização de servidores para empresas. Este é um recurso interessante da Locaweb® a qual nomeia o serviço como *Clouding Server* que seria o servidor em nuvem (*na internet*).

Para a Oncoterápica será necessário contratar o serviço de disco virtual locaweb® o qual proporciona aluga um espaço virtual, conforme a necessidade do cliente. No caso da Oncoterápica o orçamento realizado, tabela 5, a necessidade seria ter um espaço de 10GB, uma vez que os *backups* da empresa estão aproximadamente em 4GB. E através de um programa, da própria Locaweb®, ele realiza o agendamento da pasta de *backup* do servidor, com o servidor da Locaweb®.

Com a realização de *backup* pelo programa já utilizado pela a empresa será realizado no dia posterior ao do *backup* um teste para avaliar se o arquivo comprimido está em perfeito funcionamento e para que o mesmo não seja rompido.

Tabela 5 – Orçamento de hospedagem de *backup*

Plano	**Disco Virtual**	**Taxa de transferência**	**Custo Mensal**	**Custo Anual**
Disco Virtual III	10GB	500GB	R$ 29,00	R$ 348,00
Total				R$ 348,00

Fonte: O autor (2008).

8.2.10 **Política de Controle de Acesso**

A Política de Controle de Acesso é tratada na norma no item 9.1.1 e relata que se os requisitos de negócios para controle de acesso foram definidos e documentados. Se a política de controle de acesso abrange as regras e direito para cada usuário do grupo. Se

os usuários e serviços receberam uma afirmação clara da empresa dos requisitos de negócio para ser cumprida pelo controle de acessos.

*Encontrado na empresa***:** Os médicos da Oncoterápica acessam a rede com um usuário padrão. O usuário padrão dos médicos não possui senha, além do que o padrão de segurança do nome do usuário dos médicos é facilmente deduzido. Os outros usuários da empresa não possuem regras e direitos de acesso, todos os usuários possuem acesso total a todas as pastas do servidor, desde que os mesmos consigam realizar o mapeamento da rede através de sua máquina local. Não existe uma documentação dos controles de acessos definidos para cada usuário ou grupo.

Tomada de ação: Levantamento de todos os usuários e seus respectivos grupos. Através de reunião com os gestores de cada setor, realizar um cadastro padrão, para que o gestor indique o que o usuário poderá ter acesso. A partir do modelo apresentado na Figura 14, será realizado a cadastro de controle de acesso de cada usuário. E tal documentação será anexada em uma pasta suspensa na sala da TI.

No caso dos usuários médicos, serão criadas senhas de fácil acesso, porém as mesmas terão 30 dias de expiração. Sendo assim, as senhas não poderão se repetir, e pelo menos, haverá uma senha de acesso ao sistema, diminuindo o risco que a empresa possui hoje.

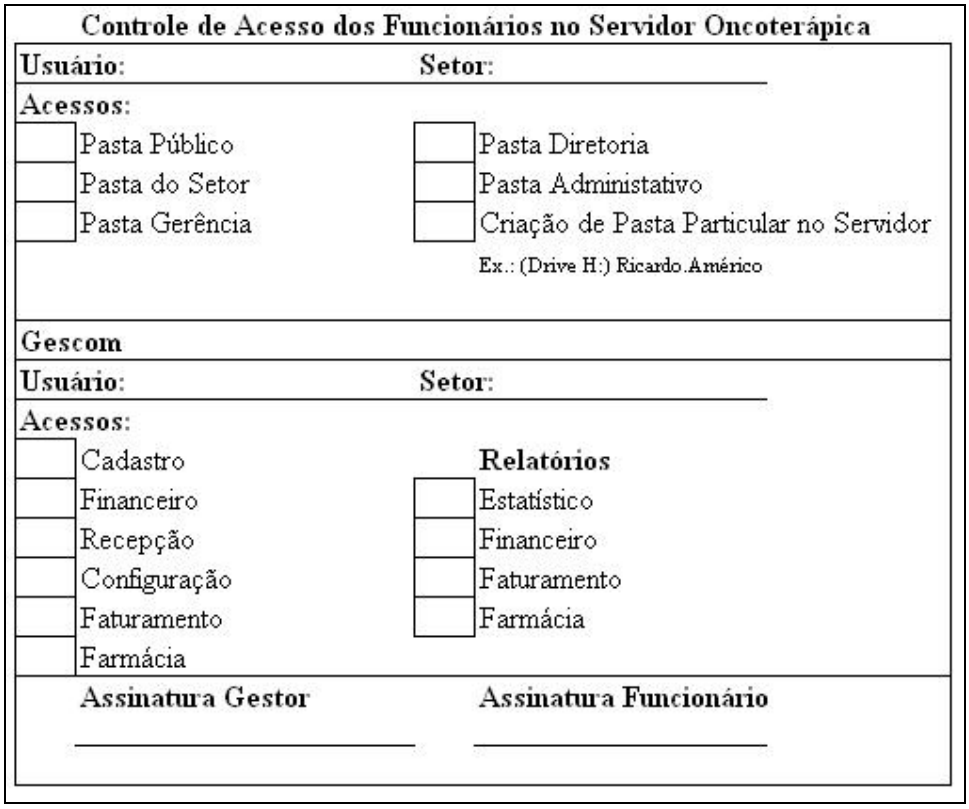


Figura 14 – Cadastro de Controle de Acesso do Funcionário Oncoterápica
Fonte: O autor (2008).

8.2.11 **Registro de usuário**

Como complemento do capítulo 8.2.10, o item da Política de Controle de Acesso da norma, no capítulo 9.2.1 trata se existe um processo de registro ou desregistro formal de usuários garantindo o acesso para multiusuários do sistema de informações e serviços.

Encontrado na empresa: A política de usuários da Oncoterápica nunca foi revisada, ou seja, na troca de funcionários de TI, nunca foi realizado nenhum controle dos usuários ativos e os que já foram desativados. Logo, existem usuários ativos no "Ad" do Windows® Server® que já foram desligados da empresa.

Tomada de ação: A partir do capítulo 8.2.10 desta monografia, todos os itens que tratam sobre restrição, manutenção e revisão dos usuários será contemplada.

Logo os novos funcionários da Oncoterápica terão seus cadastros realizados de maneira padrão, conforme a documentação apresentada pelo o gestor de sua área. Uma vez que com a documentação padrão dos usuários de cada setor, ter-se-á um perfil de cada usuário dentro de cada setor, facilitando o cadastramento de novos funcionários. E os funcionários que forem se desligando da empresa serão excluídos os registros dos usuários do sistema, conforme solicitação por *e-mail* do gestor da área.

8.3 QUADRO GERAL DE TOMADA DE AÇÃO

Depois de tudo analisado, orçado, para a Oncoterápica conseguir implementar e ficar em conformidade com a norma de segurança da informação, foi realizado uma tabela 6 geral a qual descrimina custo total em relação a implementação de todas as políticas de seguranças neste trabalho apresentadas.

Os custos apresentados na tabela 6 foram levantados no dia 04/11/2008 e, todos podem sofrer alterações sem aviso prévio do fornecedor. Eles são utilizados nesta tabela em nível de analise de viabilização, para a Oncoterápica, para a conformação com a norma BS 7799.1:2002.

Este orçamento será apresentado a Oncoterápica dia 14/11/2008, a fim de estudo, por parte da empresa, da implementação daqueles itens que possuem um custo.

Tabela 6 – Orçamento Geral de Implementação conforme as Políticas de Segurança da Informação do *Checklist* BS 7799.2:2002

Referencia			**Área de auditoria,**	**Conformidade / Não Conformidade**	**Orçamento**	
Checklist	**Norma**	**TCC**	**Questões de Auditorias**		**O que?**	**Quanto?**
Política de Segurança						
1.1.2	3.1.2	8.2.1	Revisão e avaliação	Não Conformidade	-	R$ 0,00
SUBTOTAL POLÍTICA DE SEGURANÇA						**R$ 0,00**
Classificação e Controle de ativos						
3.1.1	5.1.1	8.2.2	Inventário de ativos	Não Conformidade	-	R$ 0,00
SUBTOTAL CLASSIFICAÇÃO E CONTROLE DE ATIVOS						**R$ 0,00**
Segurança de pessoal						
4.2.1	6.2.1	8.2.3	Educando e ensinando segurança da informação	Não Conformidade	-	R$ 0,00
4.3.1	6.3.1	8.1.1	Relatando incidentes na segurança	Conformidade	-	R$ 0,00
SUBTOTAL SEGURANÇA DE PESSOAL						**R$ 0,00**

Segurança física e do ambiente						
5.1.1	7.1.1	8.1.2	Perímetro de segurança física	Conformidade	-	R$ 0,00
5.1.2	7.1.2	8.1.3	Controle de entrada física	Conformidade	-	R$ 0,00
5.1.3	7.1.3	8.2.4	Segurando escritórios, quartos e facilidades	Não Conformidade	CR C/TESTAS	R$ 80,07
					CR ESPELHO	R$ 24,21
					MAÇANETA	R$ 31,26
					FECHO ELETROMAGNETICO	R$ 67,33
					CDA	R$ 373,06
5.2.1	7.2.1	8.2.5	Implementando equipamentos de proteção	Não Conformidade	5 Extintores de Incêndio de 4 KG do tipo ABC	R$ 725,00
5.2.3	7.2.3	8.2.6	Segurança de cabos	Não Conformidade	Rack para *Switch*	R$ 1.537,25
5.2.4	7.2.4	8.2.7	Manutenção de equipamentos	Não Conformidade	1 Servidor Dell PowerEdge 840	R$ 6.181,55
					1 Del UPS *NoBreak*	R$ 1.260,73
					13 Microsoft Cal de acesso	R$ 1.005,55
					Firewall	Aguarda orçamento
5.3.1	7.3.1	8.2.8	Política de tela e mesa limpa	Não Conformidade	-	R$ 0,00
SUBTOTAL SEGURANÇA FÍSICA E DO AMBIENTE						**R$ 11.286,01**
Gestão da comunicação e operacionalização						
6.5.1	8.5.1	8.2.9	*Backup* da informação	Não Conformidade	Contratação de 1 ano de Disco Virtual Locaweb	R$ 348,00
SUBTOTAL GESTÃO DA COMUNICAÇÃO E OPERACIONALIZAÇÃO						**R$ 348,00**
Controle de Acesso						
7.1.1	9.1.1	8.2.10	Política de Controle de Acesso	Não Conformidade	-	R$ 0,00
7.2.1	9.2.1	8.2.11	Registro de usuário	Não Conformidade	-	R$ 0,00
7.7.3	9.7.3	8.1.4	Sincronização do relógio	Conformidade	-	R$ 0,00
SUBTOTAL CONTROLE DE ACESSO						R$ 0,00
TOTAL DA IMPLEMENTAÇÃO DE UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO						**R$ 11.634,01**

Fonte: O autor (2008).

9 CONCLUSÕES

Este capítulo é o qual o autor da obra traça conclusões, considerações finais e análise de novas propostas para a empresa referentes ao trabalho realizado.

Para muitas empresas é muito importante um sistema de proteção de suas informações, pois a inteligência competitiva entre as empresas concorrentes esta cada vez mais acirrada.

Cada vez mais a tecnologia da informação está presente nas organizações. Técnicas de melhores práticas como ITIL®, CoBiT®, ISO® estão cada vez mais desenvolvidas e atualizadas. Assim sendo, as melhores práticas para a T.I. seriam equivalentes a jurisprudência para o setor judiciário.

Focado nas constantes atualizações do mercado tecnológico para organizações e a inexistência de tais práticas na Oncoterápica, aliado as diversas vulnerabilidades existentes contra sistemas de informações gerenciais, o autor conseguiu realizar um trabalho atrelando esses três fatores.

Para isso foram traçados 3 objetivos específicos, os quais juntos, resultariam em um objetivo geral.

O primeiro objetivo específico para o trabalho foi: "Verificar os itens em conformidade e não conformidade com a norma BS 7799.1:2002". Para isso foi utilizado um *checklist*, em língua inglesa, disponível em mídia de CD-ROM por (Ferreira e Araújo, 2006). Assim foram primeiramente traduzidos todos os 127 itens existentes na *checklist* e verificados, observados, somente 15 itens do *checklist* da norma BS 7799.1.

O segundo objetivo foi: "Analisar e propor melhorias para os itens em não conformidade com a norma". Dos 15 itens verificados conforme a *checklist*, foram encontrados 11 em não conformidade. A partir do conhecimento de que 11 itens não estavam em conformidade foram estudados e orçados e proposto tomadas de ação para que a Oncoterápica estivesse de acordo com a BS 7799.1:2002.

O terceiro e último objetivo que compõe o objetivo geral é “Implementar uma política de segurança da informação”. Este objetivo ele foi atingido em sua totalidade. Já que dos 11 itens em não conformidade, apenas 18,18% estão já implementados na empresa, o que representa somente 2 itens. Os demais itens estão dependentes de avaliação de custos com a empresa, devido a políticas do financeiro e da diretoria da Oncoterápica. Outros itens estão agendados para serem trabalhados na empresa, como foi apresentado no capítulo 8 deste trabalho.

Logo, o objetivo geral deste trabalho não conseguiu ser aplicado em sua totalidade, uma vez que a falta de tempo para a realização de todo o projeto e depois a coleta de dados demandaram um tempo maior do que o imaginado pelo o autor e até pela a empresa. Porém ele está sendo aplicado a um médio prazo. Os responsáveis que participam do comitê de segurança da informação da empresa estão mais conscientes das vulnerabilidades existentes na empresa.

O fácil acesso a informação na empresa, uma vez que o autor da monografia era funcionário da empresa. E o livre acesso a qualquer setor da empresa, facilitou a observação de todos os itens do *checklist*. A escolha dos 15 itens trabalhados ao longo do trabalho foi de escolha do autor da monografia, conforme uma pré-análise baseada na BS 7799.1:2002.

Um próximo objetivo a ser tratado após a conclusão e conformação dos 11 itens em não conformidade apresentados neste trabalho seriam:

- Aprimorar os 15 itens em conformidade com a Oncoterápica, ou seja, os 15 itens aqui estudados e todos implementados, sofrerem constantes atualizações e avaliações para a diminuição do risco de incidentes na empresa;
- Criar um plano de contingência para a Oncoterápica.

Por fim, o trabalho de conclusão realizado pelo autor desta monografia teve uma grande influência para o seu crescimento profissional. Uma vez que o autor esta se graduando em Administração de Empresas, sem nenhuma ênfase. Logo o Plano de Implementação de Normas de Segurança da Informação na Oncoterápica, teve uma grande contribuição para a definição de atuação profissional para o autor devido a abrangência de áreas para um administrador de empresas atuar. A Oncoterápica beneficiou-se juntamente com o autor desta monografia, pois a empresa descobriu falhas que não cogitava a hipótese de existirem.

REFERÊNCIAS

BEAL, Adriana. **Segurança da Informação: Princípios e Melhores Práticas para a Proteção dos Ativos de Informação nas Organizações.** 1ª ed. São Paulo: Atlas, 2005.

BRASILIANO, Antonio Celso R. **A (in)Segurança nas Redes Empresariais: A Inteligência Competitiva e a fuga involuntária das informações.** 1ª ed. São Paulo: Sicurezza, 2002.

CAMPOS, André. **Sistema de segurança da informação.** 2ª ed. Florianópolis: Visual Books, 2007.

CHIAVENATO, Idalberto. **Introdução a Teoria Geral da Administração.** 3ª ed. Rio de Janeiro: Elsevier, 2004.

FERREIRA, Fernando Nicolau Freitas, ARAÚJO, Márcio Tadeu. **Política de Segurança da Informação: Guia Prático para Elaboração e Implementação.** 1ª ed. Rio de Janeiro: Ciência Moderna Ltda, 2006.

INCA - Instituto Nacional de Câncer. **Dados dos Registros de Base Populacional**. Porto Alegre: Disponível em: <http://www.inca.gov.br/regpop/2003/>. Acessado em: 10 nov. 2008.

LAUDON, Kenneth C, LAUDON, Jane P. **Sistemas de informação: com internet.** 4ª ed. Rio de Janeiro: LTC, 1999.

MENEZES, Josué das Chagas. **Gestão da Segurança da Informação.** 1ª ed. Leme: Mizuno, 2006.

NAKAMURA, Emilio Tissato, GEUS, Paulo Lício. **Segurança de Redes, em ambientes cooperativos.** 1ª ed. São Paulo: Novatec, 2007.

OLIVEIRA, Djalma de Pinho R. **Sistemas de informações gerenciais: estratégicas, táticas operacionais.** 8ª ed. São Paulo: Atlas, 2002.

OLIVEIRA, Jayr Figueiredo. **Sistemas de informação versus Tecnologias da informação: Um impasse empresarial.** 2ª ed. São Paulo: Érica, 2004.

REZENDE, Denis Alcides, ABREU, Aline França. **Tecnologia da Informação aplicada a sistemas de informações empresariais: o papel estratégico da informação e dos sistemas de informação nas empresas.** 3ª ed. São Paulo: Atlas, 2003.

ROESCH, Sylvia Maria A. **Projetos de estágio do curso de administração.** 3ª ed. São Paulo: Atlas, 2006.

SÊMOLA, Marcos. **Gestão da Segurança da Informação: Uma visão executiva.** 1ª ed. Rio de Janeiro: Campus, 2003

SOARES, Luiz Fernando G. FILHO, Guido Lemos de S. COLCHER, Sérgio. **Redes de computadores, das LANs MANs e WANs às Redes ATM.** 2ª ed. Rio de Janeiro: Campus, 1995.

YIN, Robert K. **Estudo de Caso: planejamento e método.** Trad. Daniel Grassi. 2ª ed. Porto Alegre: Bookman, 2001.

APÊNDICE A - DADOS DE IDENTIFICAÇÃO

DADOS DE IDENTIFICAÇÃO DO ALUNO

Nome: Ricardo Dias Américo

Endereço: R. Vasco da Gama, 19 apartamento 13.

Data de Nascimento: 22/07/1987

Fone p/ Contato: (51) 9157.6894

E-Mail: rdamerico@gmail.com

Empresa atual: G2M Recuperação de Crédito.

Endereço: R. do Andradas, 1001 conj. 1204.

Fone p/ Contato: 3076.3230

E-Mail: ti.suporte.oncoterapica@gmail.com

Experiência Profissional (mais relevantes)

Empresa: Portocred S/A

Ramo de Atividade: Financeira

Período: março 2006 – julho 2007.

Cargo: Cobrança Administrativa

Cursos de aperfeiçoamento

Curso: BSC, Itil e Cobit, Governança de TI.

Entidade: Alfamída

Período: abril – 2008.

Carga horária: 100 horas

DADOS DE IDENTIFICAÇÃO DO SUPERVISOR

Nome: Sheila Souza da Silva
Empresa atual: Oncoterápica Ltda.
Endereço: R. Almirante Barroso, 735 conj. 501.
Fone p/ Contato: 3076.3218
E-Mail: sheilasouza.oncoterapica@gmail.com

Experiência Profissional (mais relevantes)

Empresa: Oncoterápica Ltda
Ramo de Atividade: Saúde
Período: outubro 1999 – atual.
Cargo: Supervisora Administrativo.

Cursos de aperfeiçoamento

Curso: MBA em Gestão Financeira e Controladoria
Entidade: FGV – Fundação Getúlio Vargas
Período: Abril 2008 - atual.

ANEXO A – ORÇAMENTO DELL

A seguir é demonstrado o orçamento realizado juntamente a Dell® Computadores.