UNIVERSIDADE ESTADUAL DO NORTE DO PARANÁ

FACULDADES LUIZ MENEGHEL

KENION CÉSAR MICHELATO COLAÇO

AUDITORIA DA TECNOLOGIA DA INFORMAÇÃO EVIDENCIANDO SEGURANÇA FÍSICA E LÓGICA EM AMBIENTE COMPUTACIONAL

Bandeirantes

2008

KENION CÉSAR MICHELATO COLAÇO

AUDITORIA DA TECNOLOGIA DA INFORMAÇÃO EVIDENCIANDO SEGURANÇA FÍSICA E LÓGICA EM AMBIENTE COMPUTACIONAL

Trabalho de Conclusão de Curso submetido à Universidade Estadual do Norte do Paraná campus Luiz Meneghel, como requisito parcial para a obtenção do grau de Bacharel em Sistemas de Informação.

Orientador: Prof. Carlos Eduardo Ribeiro.

Bandeirantes

2008

KENION CÉSAR MICHELATO COLAÇO

AUDITORIA DA TECNOLOGIA DA INFORMAÇÃO EVIDENCIANDO SEGURANÇA FÍSICA E LÓGICA EM AMBIENTE COMPUTACIONAL

Trabalho de Conclusão de Curso submetido à Universidade Estadual do Norte do Paraná campus Luiz Meneghel, como requisito parcial para a obtenção do grau de Bacharel em Sistemas de Informação.

COMISSÃO EXAMINADORA

_____
Prof.Carlos Eduardo Ribeiro (orientador)
Faculdades Luiz Meneghel

_____
Prof. MSc.Ederson Marcos Sgarbi
Faculdades Luiz Meneghel

_____
Prof. Luiz Fernando Legore do Nascimento
Faculdades Luiz Meneghel

Bandeirantes, __ de_____ de 2008.

Dedico a Deus por mais essa etapa. A minha amada esposa Cirjilene. A minha querida filha Mariana

AGRADECIMENTOS

Agradeço primeiramente a Deus e a Nossa Senhora Aparecida.

A meus pais razão e cumplicidade da minha vida.

Ao meu orientador Carlos (Biluka), pela paciência e determinação durante o desenvolvimento do trabalho.

A professora Daniela pelas dicas e por se mostrar sempre disposta a ajudar.

A todos os professores do Departamento de Informática, que contribuíram para o meu aprendizado e dinâmica.

A Indústria e Comércio de Móveis Santos Andirá que permitiu o acesso ao ambiente computacional para que eu concluísse a auditoria.

Aos grandes parceiros Fernando e Rodrigo, pelo acompanhamento e dicas durante a auditoria.

Aos verdadeiros amigos Emmanuel e Flaviana que sempre estiveram ao meu lado me apoiando e me incentivando nos melhores e piores momentos vividos nestes quatro anos e em toda a minha vida.

Aos grandes amigos da VIII Turma de Sistema de Informação.

Enfim, agradeço a todos aqueles que direta ou indiretamente participaram e contribuíram para transformar dificuldade em objetivamente e dinâmica.

“O sucesso nasce do querer,
da determinação e persistência
em chegar a um objetivo.
Mesmo não atingindo o alvo,
quem busca e vence obstáculos,
no mínimo fará coisas admiráveis”.

José de Alencar

MICHELATO, Kenion. **Auditoria da Tecnologia da Informação evidenciando Segurança Física e Lógica em Ambiente Computacional.** 2008. 97 p. Monografia (Graduação em Sistemas de Informação) – Universidade Estadual do Norte do Paraná.

RESUMO

Está cada vez mais difícil manter em segurança as informações referentes a empresas ou pessoas. O descuido nessa área pode causar prejuízos significativos, e muitas vezes irreversíveis. Mas felizmente a maior parte das empresas está consciente do perigo e estamos vivendo um momento em que praticamente todas elas mantêm alguma política de segurança. A Segurança da Informação refere-se à proteção requerida para proteger as informações de empresas ou de pessoas, ou seja, o conceito se aplica tanto as informações corporativas quanto às pessoais. Ela pode estar guardada para uso restrito ou exposta ao público para consulta ou aquisição. Podem ser estabelecidas métricas para definição do nível de segurança existente e requerido. Dessa forma, são estabelecidas as bases para análise da melhoria da situação de segurança existentes. A segurança de uma determinada informação pode ser afetada por fatores comportamentais e de uso de quem se utiliza dela, pelo ambiente ou infra-estrutura que a cerca ou por pessoas mal intencionadas que têm o objetivo de furtar, destruir ou modificar tal informação. Este trabalho tem como objetivo principal avaliar por meio da auditoria da TI, a segurança física e lógica da informação de uma Indústria Moveleira.

Palavras-chave: TI (Tecnologia da Informação), Métricas, Segurança da Informação, informações corporativas,

MICHELATO, Kenion. **Audit of Information Technology showing the physical and logical security in Computational Environment.** 2008. p. 97 Monograph (Diploma in Information Systems) - University of Northern Parana.

ABSTRACT

It is increasingly difficult to maintain security in the information relating to companies or individuals. The neglect in this area can cause significant losses, and often irreversible. But fortunately most of the companies is aware of the danger and we are living a moment that almost all of them retain some security policy. The Information Security refers to the protection required to protect information from companies or persons, namely, the concept applies to both the corporate information regarding personal. It can be stored for use restricted or exposed to the public for consultation or acquisition. May be established metrics for defining the level of security available and requested. Thus, the foundations are laid for improving the situation analysis of existing security. The safety of a particular information may be affected by behavioral factors and use of those who use it for the environment and infrastructure that the fence or by malicious people that are designed to steal, destroy or modify such information. This study aims to evaluate through the main audit of IT, physical security and rationality of information from a furniture industry.

Keywords: IT (Information Technology), Metrics, Information Security, corporate information,

LISTA DE FIGURA

LISTA DE QUADROS

LISTA DE SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
BSI	*Britsh Standards Institute*
B2B	*Business to Business*
B2C	*Business to Consumer*
CPD	Controle de Processamento de Dados
DTI	Departamento de Tecnologia da Informação
DVIN	Divisão de Informática
ERP	Enterprise Resource Planning
IPL	Inicial do Sistema Operacional (Initial Program Load)
ISO	International Organization For Standardization (Organização Internacional de Normalização).
IT AUDIT	Information Tecnology Audit
PA	Procedimento de Auditoria
PED	Processamento de Dados Eletrônicos
ROI	*Return of Investiment*
SI	Sistemas de Informação
TCU	Tribunal de Contas da União
TI	Tecnologia da Informação
WITSA	Word Information Technology and Services Alliance

SUMÁRIO

1 INTRODUÇÃO

Segundo Dias (2000), a auditoria é uma atividade que engloba o exame das operações, processos, sistemas responsabilidades gerenciais de uma determinada entidade, com intuito de verificar sua conformidade com certos objetivos e políticas institucionais, orçamentos, regras normas ou padrões. A atividade de auditoria pode ser dividida em três partes: planejamento, execução e relatório.

Neste projeto serão abordadas as principais técnicas e práticas de auditoria em tecnologia da informação, onde o âmbito da auditoria constitui-se da amplitude e exaustão dos processos de auditoria, incluindo uma limitação racional dos trabalhos a serem executados. Definir, então, até que ponto será aprofundado as tarefas de auditoria e seu grau de abrangência.

De acordo com o Tribunal de Contas da União (TCU), 1998)), grande parte das empresas se utiliza maciçamente da tecnologia da informação para automatizar sua operação e registrar, processar, manter e apresentar informações. Por isso, cada vez mais as equipes de auditoria terão que usar como evidência dados provenientes de sistemas informatizados.

Não se deve partir do princípio de que dados extraídos de computadores são confiáveis. Embora ofereçam vantagens para as organizações, os sistemas informatizados podem também representar grandes riscos. É possível que erros e fraudes não sejam detectados por causa da enorme quantidade de dados controlados pelos sistemas, da possível discrepância entre o que está armazenado e o que é efetivamente apresentado em relatórios de saída, e da mínima necessidade de intervenção humana nos processos.

A auditoria da Tecnologia da Informação (TI) possibilitará avaliar se o ambiente computacional da empresa, servirá de evidência para os achados de auditoria, se são confiáveis, e exatos, conforme os requisitos em segurança da informação, evidenciando acesso físico e lógico de dados, fator decorrido da crescente evolução tecnológica, trazendo a preocupação com a questão de guarda e manuseio de dados e informações. Desse patamar, surge a importância da Gestão da Segurança da Informação, com a finalidade de adotar controles físicos,

tecnológicos e humanos personalizados, que viabilizem a redução e administração de riscos, levando a instituição a atingir o nível de segurança adequado ao seu negocio. Tendo em vista a necessidade da Internet e do computador para realizar simples tarefas, antes efetuadas pessoalmente (fisicamente), o numero de usuários só tende a crescer. O aumento na inserção e manuseio de dados em pequenas, médias e grandes empresas, faz com que surja ainda mais a necessidade de proteção, de se gerir a segurança da informação.

1.1 Objetivos

1.1.1 Objetivo Geral

O objetivo deste trabalho é efetuar a auditoria da TI em uma indústria moveleira, devendo-se avaliar o grau de segurança da informação, evidenciando a segurança física e lógica de um ambiente computacional. Para tanto usar-se-ão técnicas pesquisadas que integra os conceitos de um programa de auditoria da TI, para assegurar a disponibilidade e segurança dos computadores e a confiança e integridade da guarda e manipulação de informações envolvidas no sistema da entidade.

1.1.2 Objetivos Específicos

Os objetivos específicos deste projeto é planejar, executar e emitir relatório final, utilizando-se da técnica de **‘Entrevista’** de auditoria de TI, a fim de verificar e proporcionar possíveis melhorias no ambiente computacional da entidade. Podemos citar:

- Escolher para o planejamento, uma lista de verificação específica evidenciando segurança física e lógica para aplicação da auditoria de TI (*apresentação).*
- Executar a auditoria de TI por meio de um *checklist* específico (entrevistas).

- Elaborar um relatório final com todos os erros encontrados e propor melhorias (*encerramento).*

1.1.3 Justificativa

O campo de Sistemas de Informação (SI) é relativamente novo comparando as outras áreas do conhecimento. A importância crescente de seu papel desempenhado nas empresas modernas permitiu que o processo de auditagem computacional se tornasse essencial devido sua preocupação em relação à segurança. Propõe-se planejar, executar e relatar em uma indústria moveleira, uma auditoria da TI que compreenda terminologia, conceituação e técnicas das áreas de auditoria, sistemas de informação e processamento eletrônico de dados. Isto se justifica devido ao complexo sistema computacional que engloba processos, sistemas e responsabilidades gerenciais da entidade, que tem o intuito de verificar a conformidade de certos objetivos e políticas institucionais, orçamentos, regras, normas e padrões. Essas organizações estão cada vez mais dependentes dos sistemas de informação e das redes de computadores, por ser um ambiente heterogêneo e complexo, difícil de ser mantido, protegido e controlado.

Para que a proposta de auditoria da TI em segurança de acesso físico e lógico, possa ser efetivada com sucesso, é necessária a negociação com a alta gerência para que se evitem falsas expectativas, discuta e defina claramente o campo da auditoria, seu grau de profundidade de suas verificações e o nível de capacitação técnica e profissional necessário para auditar às subáreas escolhidas. Permitir à equipe definir as metodologias a serem utilizadas, os objetivos de controle a serem atingidos e os procedimentos de auditorias mais desejados.

1.1.4 Organização do Trabalho

Este trabalho encontra-se estruturado da seguinte maneira: no capítulo 2 e 3 é apresentado um conceito sobre tecnologia da informação e sistemas de informação. O capítulo 4 é referente a auditoria em tecnologia da informação. O

capitulo 5 é apresentado um estudo sobre segurança da informação. O capítulo 6 descreve as principais técnicas de auditoria em tecnologia da informação. O capítulo 7 diz respeito a *Avaliação Proposta*, onde apresentam-se Lista de Verificação (planejamento), *Checklist* (execução), Relatório final (encerramento) para efetuar a Auditoria de TI. No capítulo 8 é feita uma *Análise de Resultados.* O capítulo 9 é apresentado a gerência o *Relatório Final da Auditoria de TI* e por fim, no capítulo 10, é apresentada a conclusão e trabalhos futuros.

2 TECNOLOGIA DA INFORMAÇÃO

O termo Tecnologia de Informação (TI) muitas vezes é confundido ou tem-se como sinônimo de Sistema de Informação. Segundo Alter (1996), a TI vem a ser um conjunto de hardwares e softwares que possibilitam a geração, armazenamento, veiculação, processamento e reprodução dos Sistemas de Informação.

Conforme Beuren (1998), tecnologia de informação corresponde ao conjunto de componentes necessários para o tratamento das informações, como *hardware* (equipamento), *software* (programa ou conjunto de programas), telecomunicações, redes e outros meios disponíveis. A questão da TI envolve tanto aspectos técnicos como organizacionais que incluem recursos humanos, negócios e metas e, principalmente, uma postura administrativa ampla e bem elaborada.

A implementação da TI nas empresas resulta em benefícios, tanto para a estrutura organizacional como também para trabalhos específicos. Considera-se que estes benefícios resultam da transformação do escopo dos negócios, das mudanças nos processos internos (estrutura e processos organizacionais), das mudanças da plataforma de TI e na arquitetura dos sistemas de informação (BRITO, 1996).

A mudança organizacional, nas últimas décadas, tem sido dirigida pela Tecnologia da Informação e este ligeiro e desenfreado movimento, ainda mais percebido com o advento da Internet, têm levantado questões relacionadas à capacidade das organizações atuais em administrar a introdução da TI de forma organizada.

3 SISTEMAS DE INFORMAÇÃO

Um sistema de informação tem a função de coletar, manipular, armazenar e disseminar dados e informações pela empresa. Segundo Polloni (2000) é qualquer sistema (incluindo seu processamento) que seja utilizado para prover informações.

Estes sistemas são chamados de informatizados quando utilizam computadores para a execução das tarefas diárias da empresa, onde seus componentes mais comuns são o *hardware* (terminais, impressoras, unidades de disco, etc.), o *software* (programas de sistemas operacionais, de banco de dados, de telecomunicações e de sistemas aplicativos), dados (registros que o sistema conserva por um período de tempo) e os procedimentos (instruções formais para a operação do sistema) (STAIR, 1998).

Os sistemas de informação possuem as seguintes características (GIL, 1999):

- Distribuição do processamento em computadores independentes ou através de redes locais ou de tele processamento;
- Unicidade da informação com a estruturação em banco de dados;
- Independência na concepção e implantação de novos usos da tecnologia de processamento eletrônico de dados no ambiente de trabalho;

Segundo Mañas (1999), o sistema de informação – SI – pode ser definido como o conjunto interdependente das pessoas, das estruturas da organização, da TI, dos procedimentos e métodos que deveria permitir à empresa dispor, no tempo desejado, das informações que necessita (ou necessitará) para seu funcionamento atual e para a sua evolução.

Dependendo do porte e da área de atuação, a forma e a intensidade da informatização é diferente de uma empresa para outra. Por exemplo, temos instituições financeiras que devem manter seus sistemas de informação ativos o tempo todo e, neste sentido, efetuam grandes investimentos em segurança e tecnologia.

Cada vez mais é aceita a idéia de que o verdadeiro patrimônio de uma entidade a sua tecnologia, que compõe seus sistemas, processos e informações. Instituições financeiras caminham para dispêndios da ordem de 5% em computação em relação a sua receita operacional e um sem-número de entidades seguem patamares superiores a 2% com informatização versus faturamento (GIL, 1999).

A utilização de sistemas aplicativos, como suporte a negócios, requer ainda a utilização de tecnologia sofisticada, envolvendo interfaces com diferentes sistemas, transações que atualizam arquivos em “real-time”, transferência eletrônica de dados com clientes, fornecedores e instituições financeiras. Atender a normas e legislação complexa, variada e alterada com freqüência, também são exigências comuns dos sistemas.

Surgem aí novas técnicas de controle, para assegurar a integridade dos dados que trafegam pelos sistemas. Portanto, um sistema de informação designa a logística indispensável para a realização do processo de informação, não se reduzindo somente à informática.

4 AUDITORIA DA TECNOLOGIA DA INFORMAÇÃO

De acordo com Dias (2000), o termo tecnologia da informação surgiu inicialmente como uma classificação do Departamento de Comércio dos EUA para indústrias cujos serviços e/ou produtos correspondem a hardware, software, serviços de informática, equipamentos e serviços de comunicação. A Word Information Technology and Services Alliances (WITSA) também utiliza essa mesma denominação. Na verdade, a nomenclatura mais completa seria tecnologia da informação e comunicação (TIC), porém sua forma simplificada, sem a palavra comunicação, foi à denominação que mais se difundiu nos últimos anos. Pode-se dizer, então, que tecnologia da informação engloba termos, mais conhecidos no jargão brasileiro, como informática, sistemas, telecomunicações, ciência da computação, processamento de dados, engenharia de sistemas e de software.

Segundo Ferreira (*et al* 2006), a utilização dos recursos da TI, pelos colaboradores deve ocorrer apenas no desempenho de atividade diretamente relacionadas aos negócios da organização. As políticas da organização não devem admitir o uso dos recursos para a discriminação ou provocação em razão do sexo, raça, cor, religião, nacionalidade, idade, porte de deficiência física, condição de saúde, estado civil ou qualquer outra condição prevista por lei. Adicionalmente em nenhuma hipótese, os colaboradores poderão utilizar meios que seja discriminatória, difamatória ou provocativa (material pornográfico, mensagens racistas, piadas, desenhos etc.).

Como conseqüência, a nomenclatura auditoria da tecnologia da informação, ou auditoria da TI, passou a ser utilizada mais recentemente, como uma tradução do termo em inglês IT *Audit (Information Tecnology Audit).* Atualmente, os termos auditoria de sistemas (nome pelo qual esse tipo de auditoria era conhecido anteriormente) e auditoria da tecnologia da informação têm sido usados como sinônimos.

Na auditoria da TI é analisado um conjunto de controles gerenciais e procedimentos que afetam todo o ambiente de informática e, conseqüentemente, todos os sistemas aplicativos.

Neste tipo de auditoria são verificados os padrões e políticas

adotados pela organização, a operação sobre sistemas e dados, a disponibilidade e a manutenção do ambiente computacional, a utilização de recursos computacionais, a gerência de banco de dados e de rede, além de todos os aspectos relacionados à segurança de informações, como segurança física, lógica e ambiental e continuidade dos serviços de informática.

Esses controles relacionam-se, então, com a infra–estrutura do departamento de informática, seus procedimentos, políticas e práticas. Oferecem uma estrutura básica de controle de todas as atividades relacionadas com a gerência de informática e de segurança de informações, servindo como sustentação para os controles mais específicos sobre os aplicativos. Normalmente, em uma auditoria cujo objeto é os controles de infra-estrutura de informática da organização, os trabalhos de investigação se concentram no departamento de informática.

De acordo com o TCU (1998), controles gerais consistem na estrutura, políticas e procedimentos que se aplicam às operações do sistema computacional de uma organização como um todo. Eles criam o ambiente em que os sistemas aplicativos e os controles irão operar. Durante uma auditoria em que seja necessário avaliar algum sistema informatizado, seja ele financeiro, contábil, de pagamento de pessoal etc., é preciso inicialmente avaliar os controles gerais que atuam sobre o sistema computacional da organização. Controles gerais deficientes acarretam uma diminuição da confiabilidade a ser atribuída aos controles das aplicações individuais. Por essa razão, os controles gerais são normalmente avaliados separadamente, e antes da avaliação dos controles dos aplicativos que venham a ser examinados em uma auditoria de sistemas informatizados. Quando o objetivo da auditoria de sistemas informatizados é a avaliação de um aplicativo específico (por exemplo, sistema de processamento da folha de pagamento de uma entidade, ou de controle de empréstimos de uma instituição bancária), a equipe de auditoria pode muitas vezes economizar tempo, antecipando atividades de auditoria, ao planejar testes que avaliem controles tanto do ambiente geral quanto do aplicativo. Por exemplo, como parte da avaliação dos controles gerais, a equipe irá testar controles que abrangem alterações de programas.

Existem seis categorias de controles gerais que devem ser consideradas em auditoria:

- controles organizacionais*:* políticas, procedimentos e estrutura organizacional estabelecidos para organizar as responsabilidades de todos os envolvidos nas atividades relacionadas à área da informática;
- programa geral de segurança: oferece a estrutura para: (1) gerência do risco, (2) desenvolvimento de políticas de segurança, (3) atribuição das responsabilidades de segurança, e (3) supervisão da adequação dos controles gerais da entidade;
- continuidade do serviço: controles que garantem que, na ocorrência de eventos inesperados, as operações críticas não sejam interrompidas, ou seja, imediatamente retomadas, e os dados críticos sejam protegidos.
- controles de *software* de sistema**:** limitam e supervisionam o acesso aos programas e arquivos críticos para o sistema, que controlam o *hardware* do sistema computacional e protegem as aplicações presentes;
- controles de acesso: limitam ou detectam o acesso a recursos computacionais (dados, programas, equipamentos e instalações), protegendo esses recursos contra modificação não autorizada, perda e divulgação de informações confidenciais;
- controles de desenvolvimento e alteração de *softwares* aplicativos: previnem a implementação ou modificação não autorizada de programas.

4.1 Controles Organizacionais

O termo "Departamento de Tecnologia da Informação" (ou DTI) será utilizado para substituir o antigo CPD (Centro de Processamento de Dados), representando o departamento responsável por todos os serviços relacionados à área de informática, (redes de computadores, centrais de telecomunicação etc.).

O DTI precisa ter uma estrutura organizacional bem definida, com as responsabilidades de suas unidades organizacionais claramente estabelecidas, documentadas e divulgadas, e políticas de pessoal adequadas, quanto à seleção, segregação de funções, treinamento e avaliação de desempenho. Essa estrutura deve gerenciar racionalmente os recursos computacionais da organização, de modo

a suprir as necessidades de informação de forma eficiente e econômica.

Segundo Dias (2000), é necessário que o auditor, durante o planejamento da auditoria, analise a estrutura adotada pela entidade auditada, seus diversos componentes e o relacionamento do departamento com outros setores da organização. De acordo com a estrutura, o auditor deve adaptar os objetivos de controle e os procedimentos a serem adotados e, posteriormente, verificar se os controles organizacionais são adequados.

É importante que o auditor determine se as medidas administrativas estabelecidas pelo auditado são suficientes para garantir o controle adequado das atividades do departamento de informática e se essas atividades satisfazem os objetivos de negócios da organização.

4.2 Segregação de Funções

A segregação de funções tem como objetivo evitar que um indivíduo venha a controlar todos os estágios críticos de um processo (por exemplo, um programador com permissão para independentemente escrever, testar e aprovar alterações de programa).

Segundo Ferreira (*et al* 2006), a segregação de funções é uma forma de aumentar significativamente a segurança de um processo. Seu objetivo é separar responsabilidades e atividades, sejam elas executadas por áreas, sejam pessoas. Segregar funções minimiza a probabilidade de ocorrência de atos de má fé ou erros operacionais.

Freqüentemente, a segregação de funções é alcançada pela divisão de responsabilidades entre dois ou mais grupos organizacionais. Com essa divisão, a probabilidade de que erros e ações indevidas sejam detectados aumenta sensivelmente, visto que as atividades de um grupo ou indivíduo irão servir para checar as atividades do outro.

A ausência ou inadequação da segregação de funções de informática aumenta o risco de ocorrência de transações errôneas ou fraudulentas, alterações impróprias de programa e danos em recursos computacionais.

A extensão da segregação de funções a ser aplicada em uma organização irá depender do seu tamanho e do risco associado às suas instalações e atividades. Uma organização de grande porte terá mais flexibilidade em separar funções-chave que organizações pequenas, que dependem de poucos indivíduos para executar suas operações. Da mesma forma, atividades que envolvem transações financeiras de alto valor, ou que de alguma outra forma são bastante arriscadas, devem ser divididas entre diversos indivíduos e sujeitas a uma supervisão mais rigorosa.

Na prática, no entanto, com os constantes cortes de investimentos nas organizações, o quadro de pessoal do departamento de informática tem sido cada vez mais reduzido. Em algumas organizações, devido à diminuição do quadro, pode ser difícil implementar a segregação de funções. Se o auditor se deparar com um caso semelhante, é aconselhável adaptar sua análise e suas recomendações de acordo com a problemática da organização e buscar outros controles que possam compensar os riscos da falta de segregação de funções.

Por causa da natureza da operação dos computadores, a segregação de funções por si só não garante que somente atividades autorizadas sejam executadas pelos funcionários, especialmente operadores de computador. Para auxiliar na prevenção e detecção de ações não autorizadas ou incorretas, é também necessária uma supervisão gerencial efetiva e procedimentos formais de operação.

Os elementos críticos para a avaliação dos controles organizacionais são:

- Unidades organizacionais bem definidas, com níveis claros de autoridade, responsabilidades e habilidades técnicas necessárias para exercer os cargos;
- Atividades dos funcionários controladas através de procedimentos de operação e supervisão documentados e políticas claras de seleção, treinamento e avaliação de desempenho;
- Política de segregação de funções e controles de acesso para garantir na prática a segregação de funções;

- Recursos computacionais gerenciados de forma a suprir as necessidades de informação de forma eficiente e econômica.

4.3 Unidades Organizacionais bem Definidas

São definidas, para cada unidade organizacional do DTI:

- Seus principais objetivos e padrões de desempenho
- Os diversos níveis de autoridade, as responsabilidades de cada cargo e as habilidades técnicas necessárias para exercê-los.

Os funcionários do DTI:

- Exercem atividades compatíveis com as estabelecidas formalmente pela organização;
- Possuem capacitação técnica compatível com o previsto no respectivo plano de cargo.

4.4 Atividades dos Funcionários Controladas e Políticas Claras de Seleção, Treinamento e Avaliação de Desempenho

Pontos a serem verificados:

- Existem instruções documentadas para o desempenho das atividades dentro do DTI, que são seguidas pelos funcionários;
- Manuais de instrução indicam como operar softwares de sistema e aplicativos;
- O pessoal deve ter supervisão adequada, inclusive nas trocas de turno de operação de computadores;
- Todas as atividades dos operadores do sistema computacional são automaticamente armazenadas no registro histórico de operação;
- Supervisores revisam periodicamente o registro histórico de operação, e

investigam qualquer anormalidade;

- A inicialização do sistema é supervisionada e executada por pessoal autorizado e os parâmetros informados durante o carregamento inicial do sistema operacional (*initial program load* – IPL), estão de acordo com os procedimentos estabelecidos;
- É feito um planejamento das necessidades de pessoal especializado e existem políticas definidas, métodos e critérios para o preenchimento de vagas que permitem aferir as reais habilidades técnicas dos pretendentes,
- Existem um programa de treinamento de pessoal na área de tecnologia da informação, com recursos suficientes para capacitar o pessoal técnico,
- Existe um programa de avaliação de desempenho eficaz.

4.5 Recursos Computacionais Gerenciados de Forma Eficiente e Econômica

As tarefas executadas pelo DTI obedecem a um cronograma adequado, de forma a permitir que os recursos computacionais sejam utilizados com eficiência e que as solicitações dos usuários possam ser atendidas. Entrevistar usuários e proprietários de recursos computacionais para detectar eventuais distorções na alocação de recursos e/ou conflitos causados por falhas no planejamento da distribuição da carga de trabalho.

A capacidade do hardware instalado deve ser suficiente para atender a demanda nos horários de pico e manter a qualidade do serviço para os usuários. Entrevistar usuários e analisar os registros de utilização do hardware - *log accounting* – para detectar desbalanceamento da configuração do sistema, pela caracterização de dispositivos - unidades de disco, impressoras, terminais, etc.. que estejam com folga ou sobrecarregados.

Existe um plano definido ou um acordo entre o DTI e os grupos de usuários, quanto à disponibilidade dos recursos computacionais, com prioridades de processamento adequadas às necessidades da organização.

Foram estabelecidas metas pela alta administração quanto à

disponibilidade de processamento de dados e serviços on-line.

A alta administração periodicamente avalia e compara os desempenhos de serviço com as metas previstas e pesquisa junto aos departamentos usuário para saber se as necessidades de disponibilidade dos sistemas estão sendo atendidas.

5 SEGURANÇA DA INFORMAÇÃO

A evolução da segurança da informação faz parte de nossas vidas e o homem é o maior resultado desta evolução. No meio tecnológico, talvez a maior evolução já ocorrida seja a internet. Desde o seu advento, incentivou a mudança de paradigmas e possibilitou uma explosão de conectividade e acessibilidade, onde influenciam consideravelmente a forma como as empresas gerem seus negócios.

Segundo Sêmola (2003), sita a mudança e o crescimento da TI “os computadores tomam conta dos ambientes de escritório, quebram o paradigma e acesso local à informação, e chegam a qualquer lugar do mundo através de portáveis e *notebooks* e da rede mundial de computadores: a *internet*”.

A segurança da informação protege as informações contra uma ampla gama de ameaças, para assegurar a continuidade dos negócios, minimizar prejuízos e maximizar o retorno de investimentos e oportunidades comerciais.

Conforme Neto (2004) nos traz a seguinte observação: “Quanto mais tempo você passar conectado a Internet, maiores serão as chances de você ser invadido!”

> É fácil ter-se um sistema de computação seguro. Você meramente tem que desconectar o seu sistema de qualquer rede externa, e permitir somente terminais ligados diretamente a ele. Pôr a máquina e seus terminais em uma sala fechada, e um guarda na porta. (GRAMP & MORRIS *apud* FRAZÃO, 1998).

Como na *internet*, a segurança da informação também evolui. Saiu do nível puramente técnico e restrito à área da TI, onde se preocupava em ter um sistema de antivírus, um *firewall* bem configurado, para um nível de gestão, que alem de pensar em tecnologia, precisa investir e desenvolver também os processos e pessoas.

Segundo Gabbay (2003) na sua tese, expõe claramente a evolução da segurança da informação, dizendo que:

> Os aspectos relativos à implantação de uma eficiente Política de Segurança de Informação vem evoluindo significativamente ao longo dos anos. Os procedimentos de segurança da informação têm se alterado bastante desde seus dias iniciais, quando a segurança física, junto comum conjunto de back-up, compunha os controles de segurança de informação, sendo que atualmente a segurança da informação é composta de políticas, padrões, programas de conscientização, estratégias de segurança, etc.

5.1 Princípios da Segurança da Informação.

A segurança da informação é um conjunto de software, hardware, procedimentos e padrões implementados para proteger as informações dasameaças que possam explorar as vulnerabilidades do ambiente e impactar no seu negócio da organização.

A norma NBR ISO/IEC 17799 (2005) define segurança da informação como ‘é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio’.

As informações podem existir sob muitas formas. Podem ser impressas ou escritas em papel, armazenadas eletronicamente, enviadas pelo correio ou usando meios eletrônicos, mostradas em filmes, ou faladas em conversas. Qualquer que seja a forma que as informações assumam, ou os meios pelos quais sejam compartilhadas ou armazenadas, elas devem ser sempre protegidas adequadamente.

Os princípios da informação são:

- **Confidencialidade:** garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso;
- **Integridade:** a informação é alterada somente pelas pessoas autorizadas;
- **Disponibilidade:** garantia de que as pessoas autorizadas obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

De acordo com a figura 1 abaixo, é demonstratado o ciclo da segurança da informação.

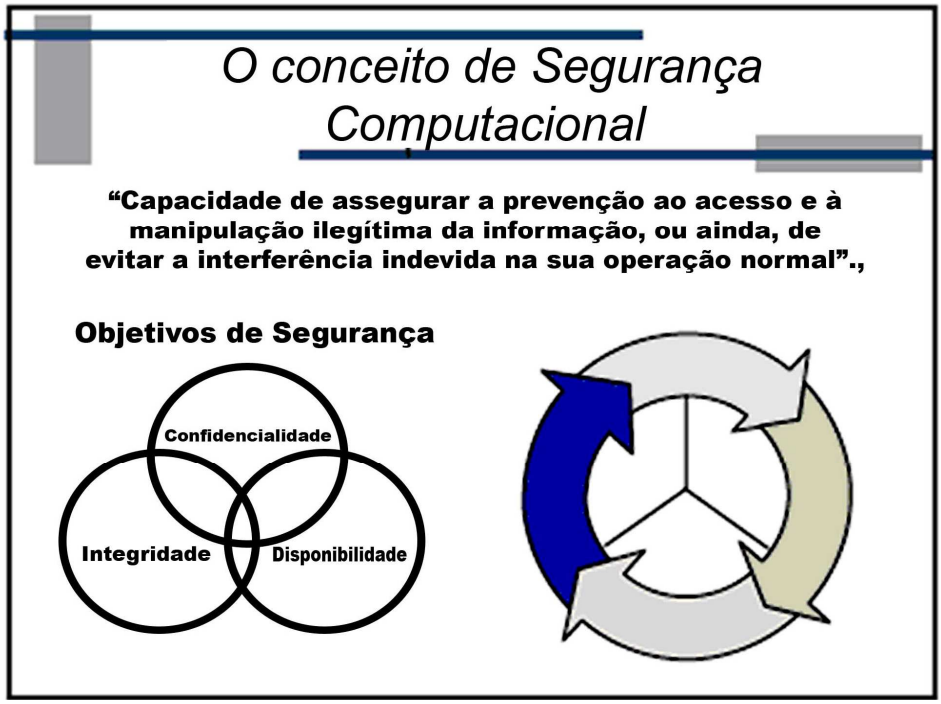


Figura 1: Ciclo do Conceito de Segurança Computacional.

Para assegurar a integridade e confidencialidade das informações, tornam-se necessárias medidas de controle e segurança de sistemas de informação em operação. Cabe à auditoria de sistemas validarem e avaliar os resultados gerados pelos sistemas informatizados, a eficiência dos processos concluídos e a segurança e confiabilidade das informações.

Segundo Dias (2000), a auditoria é uma das principais ferramentas que objetivam proteger os sistemas contra erros e atos maliciosos cometidos por usuários autorizados. Para identificar os autores e suas ações, são utilizadas trilhas de auditoria e *logs*, que registram tudo que foi executado no sistema, por quem e quando. Em algumas aplicações críticas, as trilhas de auditoria podem incluir operações de restauração ao estado inicial, auxiliando o trabalho de reconstrução do sistema original. A maioria dos objetivos de segurança se preocupa em evitar eventos indesejados. Na prática, no entanto, nem todas as ações impróprias podem ser evitadas. Para lidar com essas situações, é necessário monitorar as ações dos usuários, detectarem falhas de segurança e ser capaz de responsabilizar os culpados.

Esclarecendo melhor, quando se fala em investir em segurança da informação, é o mesmo que investir para que as informações permaneçam confidenciais, integras e disponíveis para a pessoa certa na hora certa.

5.2 Ameaças a Segurança da Informação

As ameaças à segurança da informação sempre vão existir, porém as vulnerabilidades podem ser tratadas. Um fator preocupante em relação às ameaças está na falta de consciência dos executivos de TI. Desde o faxineiro mal intencionado com acesso a sala do gerente depois do expediente até um aplicativo adquirido, o qual não foi devidamente testado, são ameaças que as organizações se deparam no cotidiano.

Segundo Sêmola (2003) conceitua ameaça como sendo agentes ou condições que causam incidentes que comprometem as informações e seus ativos por meio de exploração de vulnerabilidades, provocando perdas de confidencialidade, integridade e disponibilidade, conseqüentemente, causando impactos aos negócios de uma organização.

As ameaças de seguranças podem ser divididas em: ameaças humanas e naturais causadas por desastres da natureza conforme ilustrado na figura 2 abaixo:

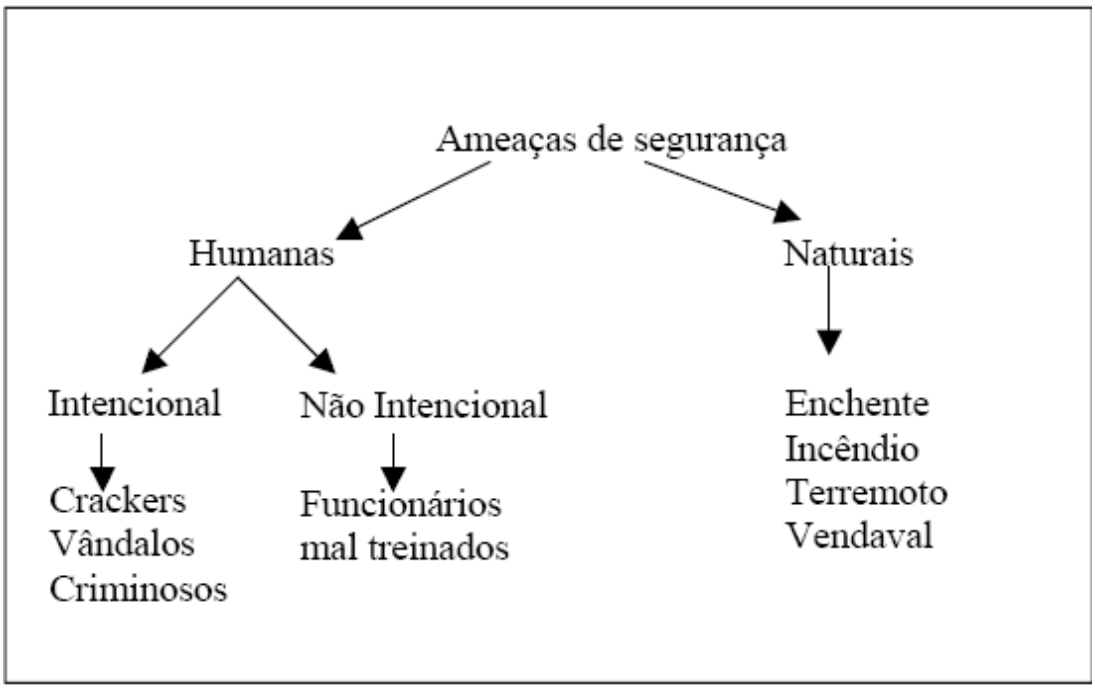


Figura 2: Ciclo de Ameaças.

Conforme Gabbay (2003) cita ‘as ameaças existem tanto no ambiente externo quanto no ambiente interno, sendo fundamental entende-las para que seja possível propor medidas de segurança voltadas a eliminar a causa do problema’. Entretanto alguns exemplos de ameaças internas são a contaminação por vírus de computador, funcionários mal treinados para a utilização de sistemas críticos, pirataria de software, fraude cometida por funcionários, roubo de informações e erros humanos.

As ameaças exploram as vulnerabilidades resultando no risco, logo o vírus de computador é uma ameaça externa, pois não se consegue controla-lo, sempre vai existir, enquanto a ameaça interna, funcionário mal treinado, por exemplo, pode-se treiná-lo. No entanto, não se elimina a ameaça do funcionário, por acidente, efetuar algum dano.

O que se pode fazer é reduzir as vulnerabilidades, ou seja, as fraquezas. Por exemplo, no caso de um ambiente restrito, como um Data Center, pode-se implementar mecanismos de segurança como controle de acesso biométrico, dessa forma está reduzido a vulnerabilidade de acesso indevido, porém a ameaça de alguém mal intencionado tentar entrar no ambiente, continuará existindo.

5.3 A Necessidade de se ter a Segurança de Informações

As informações e os processos, sistemas e redes que lhes dão suporte são ativos importantes para os negócios. A confidencialidade, a integridade e a disponibilidade das informações podem ser essenciais para manter a competitividade, o fluxo de caixa, a rentabilidade, o atendimento à legislação e a imagem comercial.

Cada vez mais, as organizações e seus sistemas de informação e redes enfrentam ameaças de segurança vindas das mais diversas fontes, incluindo fraudes através de computadores, espionagem, sabotagem, vandalismo, incêndio ou enchentes. Fontes de prejuízos tais como vírus de computador, *hackers* e ataques de negação de serviços têm se tornado mais comuns, mais ambiciosos e cada vez mais sofisticados.

Devido à dependência de sistemas e serviços de informação, as organizações estão mais vulneráveis às ameaças contra a segurança. A interconexão de redes públicas e privadas e o compartilhamento de recursos de informação aumentam a dificuldade de se conseguir controle de acesso. A tendência ao processamento distribuído vem enfraquecendo a efetividade do controle central especializado.

Muitos sistemas de informação não foram projetados para serem seguros. A segurança que pode ser obtida através de meios técnicos é limitada, e deveria ser apoiada por procedimentos e gestão adequados. Identificar quais controles deve ser implementado exige um planejamento cuidadoso e atenção aos detalhes. A gestão da segurança de informações precisa, no mínimo, da participação de todos os empregados da organização. Também pode exigir a participação de fornecedores, clientes ou acionistas. Consultoria especializada de organizações externas também pode ser necessária.

Os controles para segurança das informações são consideravelmente mais baratos e mais eficazes se incorporados no estágio de especificação de necessidades e projeto.

5.4 Definindo uma Política de Segurança de Informações.

Segundo Dias (2000), a política de segurança é um mecanismo preventivo de proteção de dados e processos importantes de uma organização que define um padrão de segurança a ser seguido pela área técnica e gerencial de TI, e pelos usuários internos.

A política de segurança de informações deve estabelecer princípios institucionais de como a organização irá proteger, controlar e monitorar seus recursos computacionais e, conseqüentemente, as informações por eles manipuladas. É importante que a política estabeleça ainda as responsabilidades das funções relacionadas com a segurança e discrimine as principais ameaças, riscos e impactos envolvidos.

Apesar de muitos aspectos serem relacionados especificamente com sistemas de informação e recursos computacionais, a política de segurança de informações deve ir alem desses aspectos, integrando-se às políticas institucionais relativas à segurança em geral, às metas de negócios da organização e ao plano estratégico de informática. Uma boa ou má política de segurança de informações gera impactos sobre todos os envolvidos na área computacional da empresa. É importante lembrar que essa política não envolve apenas a área de informática, mas todas as informações da organização, que talvez sejam seus recursos patrimoniais mais críticos hoje em dia.

Como toda política institucional, deve ser aprovada e apoiada pela alta gerência e divulgada a todos os funcionários envolvidos com segurança de informações e usuários de informática. A partir de então, todos os controles devem ser basear nessa política de segurança, aprovada pela alta gerência e difundida pela organização.

De acordo com o Padrão Internacional ISO/IEC 17799 (2005), um documento com a política de segurança de informações deverá ser aprovado pela gerência, publicado e divulgado, conforme apropriado, para todos os empregados. Deve-se declarar o comprometimento da gerência e estabelecer a abordagem da organização quanto à gestão da segurança de informações. No mínimo, a seguinte orientação deve ser incluída:

- Uma definição de segurança de informações, seus objetivos gerais e escopo e a importância da segurança como um mecanismo capacitado para compartilhamento de informações;
- Uma declaração de intenção da gerência, apoiando os objetivos e princípios da segurança de informações;
- Uma breve explanação das políticas, princípios e padrões de segurança e das exigências a serem obedecidas que são de particular importância para a organização, por exemplo:
    - Obediência às exigências legislativas e contratuais;
    - Necessidades de educação (treinamento) para segurança;
    - Prevenção e detecção de vírus e outros softwares prejudiciais;

- Conseqüências das violações da política de segurança;

- Uma definição das responsabilidades gerais e especificas pela gestão da segurança das informações, incluindo relatórios de incidentes de segurança;

- Referências a documentos que podem apoiar a política, por exemplo: políticas de segurança mais detalhadas e procedimentos para sistemas de informação, específicos ou regras de segurança que os usuários devem obedecer.

Esta política deve ser comunicada em toda a organização para os usuários de uma forma que seja relevante, acessível e entendível para o leitor-alvo.

5.5 NBR ISO/IEC 17799: Código de Prática para a Gestão da Segurança da Informação

Com a necessidade de padronização e a ausência de referências globais em modelos, ferramentas e padrões operacionais, surgiram os institutos centenários *British Standards Institute* (BSI) e o *International Organization for Standardization* (ISO).

Atualmente o dinamismo e a facilidade do acesso às informações somada a grande concorrência, tem fomentado a busca de um modelo ideal para agregar aos processos organizacionais, visto que o maior ativo de uma IES são seus alunos, e conseqüentemente suas informações. O objetivo e o propósito de definir padrões, regras e ferramentas de controle é a uniformidade de um processo, produto ou serviço. Segundo Alves (2006), “entre os diversos benefícios da adoção de normas e padrões reconhecidos pelo mercado, está o acesso a casos de sucessos e fracassos, que servirão de referência para projeções futuras”. Uma das primeiras normas sobre a Segurança da Informação, foi criada em 1995 pelo Instituto Britânico de Padronizações, e catalogada como BS 7799 – *Code of Practice for Information Security Management*. Com sua rápida aceitação na Inglaterra, passou a ser explorada por outros países da comunidade britânica, tais como: África do Sul, Austrália e Nova Zelândia.

No Brasil, em 1999 a ISO formou um comitê com mais de 120 países convidados, adotando nos meses seguintes a primeira parte das normas inglesas, denominada de ISO/IEC 17799:2000. A primeira parte da BS7799 se resume ao conjunto de Código de Práticas para o Gerenciamento da Segurança da Informação, e a segunda em: Sistema de Gerenciamento da Segurança da Informação (MENEZES, 2006). No ano de 2001, a norma ISO/IEC 17799:2000, fora traduzida pela Associação Brasileira de Normas Técnicas (ABNT) como NBR 17799 – Código de Prática para a Gestão da Segurança da Informação. (ALVES, 2006).

> A proposta da norma é “estabelecer diretrizes e princípios para iniciar, implementar, manter e melhorar a gestão da segurança da informação em uma organização”, atrelada ao objetivo da segurança da informação que é garantir o funcionamento da organização frente às ameaças a que ela esteja sujeita. A informação pode existir de diversas formas, ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou através de meio eletrônico, mostrada em filmes ou falada em conversas. Seja qual for a forma apresentada ou meio através do qual a informação é compartilhada ou armazenada, é recomendado que seja sempre protegida adequadamente. (NBR ISO/IEC 17799, 2001).

Em 2005, houve uma atualização e revisão técnica da NBR ISO/IEC 17799, assumindo uma nova nomenclatura NBR ISO/IEC 17799:2005. A diferença entre ambas as versões, pode ser resumida na ênfase dos resultados da implantação de um ambiente de segurança da informação, diminuir o risco, aumentar o ROI (*Return of Investiment*) e as oportunidades de negócios.

Conforme Sêmola (2003),

> É notório que uma norma não ganha respeito e adesão automática pelo simples fato de existir. O processo é lento, mas pode se tornar rápido, sobretudo quando temos em mente que, a exemplo da ISO 9001, aderir pode significar um importante diferencial competitivo para as organizações.

Os fatores críticos para o sucesso de uma implantação bem sucedida numa organização, de acordo a NBR ISO/IEC 17799, é a aplicação de:

a) política, atividades de segurança e objetivos que reflitam no negócio;

b) uma metodologia eficaz para implantar a política de segurança que consista com a cultura organizacional;

c) compromisso por parte da alta direção, e um suporte visível e eficiente;
d) um esclarecimento das necessidades de segurança, um bom entendimento na avaliação e gerenciamento de riscos;
e) uma campanha de *marketing* eficaz para todos os funcionários, independente de cargo;
f) um canal de distribuição de orientação sobre a política e os padrões de segurança para funcionários e contratados;
g) treinamentos e educação apropriados;
h) um sistema para medição do nível de desempenho na gestão da segurança da informação e sugestões de melhorias com foco na maturidade dos processos.

Diferentemente da ISO 9001:2000, e “por se tratar de um código de prática, esta parte não é um objeto de certificação, mas recomenda um amplo conjunto de controles que subsidiam os responsáveis pela gestão corporativa de segurança da informação”. (SÊMOLA, 2003).

Investir e aplicar em melhores práticas ou até mesmo em uma certificação de Segurança da Informação, agrega benefícios e melhorias nos relacionamentos entre B2B (business to business) e B2C (business to consumer), além de impulsionar um valor público à instituição, como também um diferencial competitivo e de compromisso com a segurança da informação dos clientes, investidores e colaboradores.

5.6 Avaliação dos Riscos.

Conhecer os riscos de TI é o ponto de partida para entender as ameaças e fraquezas que a empresa está exposta, além de também possibilitar desenhar uma política de segurança adequada à organização, ou seja, que contemple os riscos. Conforme Gabbay (2003) ”um risco existe quando uma ameaça, com potencial para causar algum dano, possui uma vulnerabilidade correspondente com alto nível de proteção”.

Porém discorda-se da citação acima feita pelo autor, pois uma vulnerabilidade faz parte de um ativo, mas não do risco ou da ameaça. Por exemplo, em uma sala destrancada, são guardados *notebooks*. Neste caso uma das vulnerabilidades é a porta não estar devidamente trancada e a ameaça é o ladrão, logo o risco é a probabilidade do ladrão entrar na sala e sair com o *notebook*.

Considerando que o *notebook* possui informação confidencial e que o disco rígido não esteja criptografado, os três princípios da segurança: **Confidencialidade, Integridade e Disponibilidade** foram afetados.

Segundo Sêmola (2003), riscos é “probabilidades de ameaças explorarem vulnerabilidades, provocando perdas de **Confidencialidade, Integridade e Disponibilidade** causando, possivelmente, impactos nos negócios”.

Um entendimento melhor sobre a composição do risco pode ser visto na figura 3 abaixo:

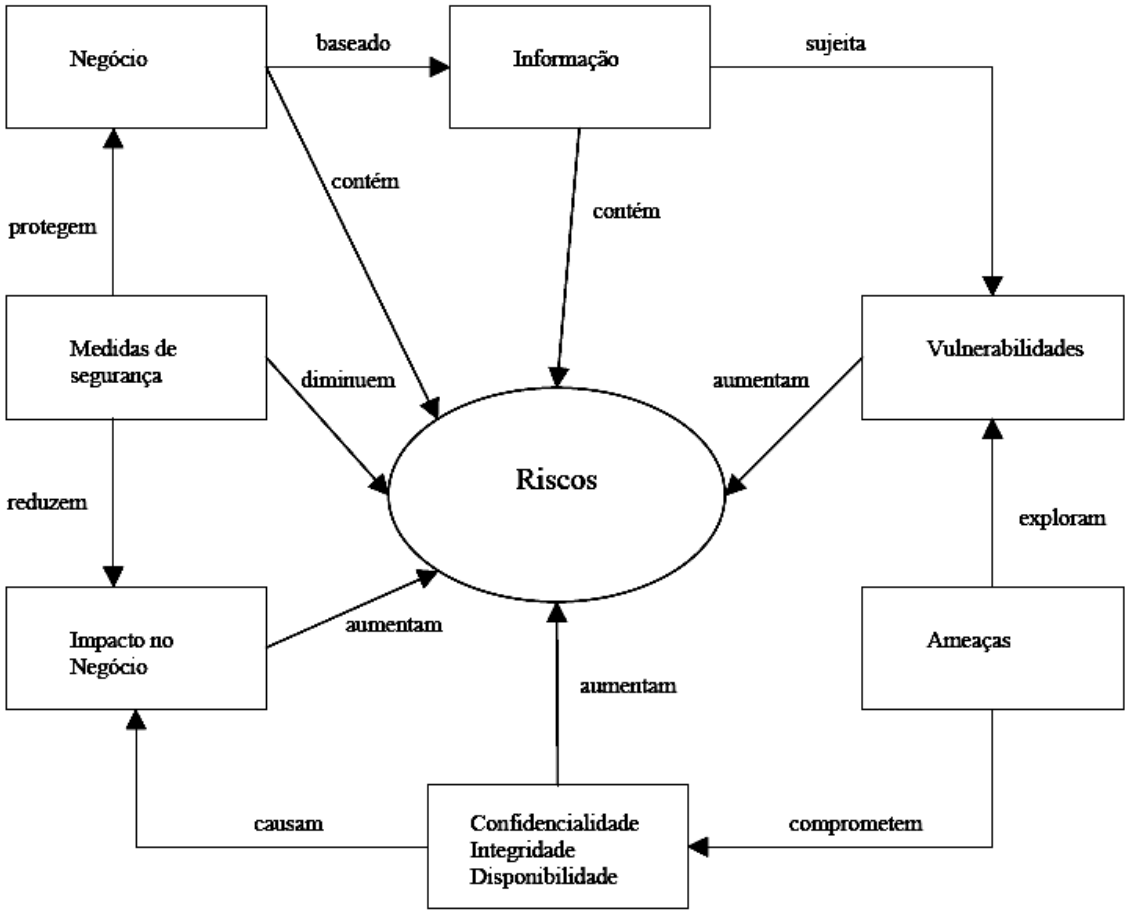


Figura 3: Composição do Risco.

Considerar a construção de uma sistemática de analise de risco, definindo, os níveis de risco que a empresa ou o gestor de TI pode aceitar, controlar

ou transferir, como um seguro, por exemplo. Além de uma periodicidade definida, a composição de um comitê de riscos pode ajudar no direcionamento dos investimentos dos controles.

5.7 Controle de Acesso Físico.

A segurança física é tão importante quanto a segurança lógica. Pessoas mal intencionadas com acesso às áreas criticas como um Data Center, podem causar grandes danos à informação e consequentemente à continuidade do negocio da organização

De acordo com a NBR ISO/IEC 17799 (2005), o objetivo da segurança física é “prevenir o acesso não autorizado, danos e interferências com as instalações e informações da organização”.

Talvez por se tratar de um produto tangível, a segurança física é mais bem entendida pelo alto escalão. É mais fácil para o gestor de segurança justificar um investimento como, por exemplo, a compra de portas corta-fogo, de um sistema de detecção e extinção de incêndio do que propor a aquisição de um sistema de detecção de intrusos, no qual é um equipamento com software. No entanto vale ressaltar, que uma análise de risco auxilia na identificação de vulnerabilidades do ambiente e consequentemente na priorização dos investimentos.

5.8 Controle de Acesso Lógico.

Os controles de acesso lógico são um conjunto de procedimentos e medidas com o objetivo de proteger dados, programas e sistemas contra tentativas de acesso não autorizadas feitas por pessoas ou por outros programas de computador.

O controle de acesso lógico pode ser encarado de duas formas diferentes: a partir do usuário a quem serão concedidos certos privilégios e acessos aos recursos.

A proteção aos recursos computacionais baseia-se nas necessidades de acesso de cada usuário, enquanto que a identificação e autenticação do usuário (confirmação de que o usuário realmente é quem ele diz ser), é feita normalmente por meio de um identificador de usuário (ID) e por uma senha durante o processo de *logon* no sistema.

5.8.1 Que Recursos devem ser Protegidos?

A proteção aos recursos computacionais inclui desde aplicativos e arquivos de dados até utilitários e o próprio sistema operacional. Abaixo serão apresentados os motivos pelos quais esses recursos devem ser protegidos:

- Aplicativos (programas fonte e objeto): O acesso não autorizado ao código fonte dos aplicativos pode ser usado para alterar suas funções e a lógica do programa. Por exemplo, em um aplicativo bancário, pode-se zerar os centavos de todas as contas-correntes e transferir o total dos centavos para uma determinada conta, beneficiando ilegalmente esse correntista.
- Arquivo de dados: Bases de dados, arquivos ou transações de bancos de dados devem ser protegidos para evitar que os dados sejam apagados ou alterados sem autorização, como, por exemplo, arquivos com a configuração do sistema, dados da folha de pagamento, dados estratégicos da empresa.
- Utilitários e sistema operacional: O acesso a utilitários, como editores, compiladores, softwares de manutenção, monitoração e diagnóstico deve ser usadas para alterar aplicativos, arquivos de dados e de configuração do sistema operacional, por exemplo. O sistema operacional é sempre alvo bastante visado, pois sua configuração é o ponto-chave de todo o esquema de segurança. A fragilidade do sistema operacional compromete a segurança de todo o conjunto de aplicativos, utilitários e arquivos.
- Arquivos de senha: A falta de proteção adequada aos arquivos que armazenam as senhas pode comprometer todo o sistema, pois uma pessoa não autorizada, ao obter identificador (ID) e senha de um usuário privilegiado, pode, intencionalmente, causar danos ao sistema. Essa pessoa dificilmente

será barrada por qualquer controle de segurança instalado, já que se faz passar por um usuário autorizado.

- Arquivos de *log:* Os arquivos de *log* são usados para registrar ações dos usuários, constituindo-se em ótimas fontes de informação para auditorias futuras. Os *logs* registram quem acessou os recursos computacionais, aplicativos, arquivos de dados e utilitários, quando foi feito o acesos e que tipo de operações foram efetuadas. Um invasor ou usuário não autorizado pode tentar acessar o sistema, apagar ou alterar dados, acessar aplicativos, alterar a configuração do sistema operacional para facilitar futuras invasões, e depois alterar os arquivos de *log* para que suas ações não possam ser identificadas. Dessa forma, o administrador do sistema não ficará sabendo que houve uma invasão.

5.8.2 O que os controles de acesso lógico pretendem garantir em relação à segurança de informações.

Os controles de acesso lógico são implantados com o objetivo de garantir que:

- Apenas usuários autorizados tenham acesso aos recursos;
- Os usuários tenham acesso apenas aos recursos realmente necessários para a execução de suas tarefas;
- O acesso a recursos críticos seja bem monitorado e restrito a poucas pessoas;
- Os usuários estejam impedidos de executar transações incompatíveis com sua função ou alem de suas responsabilidades.

5.9 *Enterprise Resource Planning* (ERP)

O sistema de informação, composto de vários módulos que integram fortemente as áreas financeira, industrial, comercial, administrativa e contábil da empresa e que tem tratamento das informações indispensáveis à gestão das rotinas

e das mudanças aceleradas no ambiente empresarial, é conhecido comercialmente como *Enterprise Resource Planning* (ERP) e a sua característica principal é a parametrização do fluxo de trabalho, onde os usuários conseguem fazer ajustes de forma rápida e sem perder o controle ou a perspectiva histórica das atividades (WOOD *et al*, 2000), como demonstra a figura 4 abaixo:

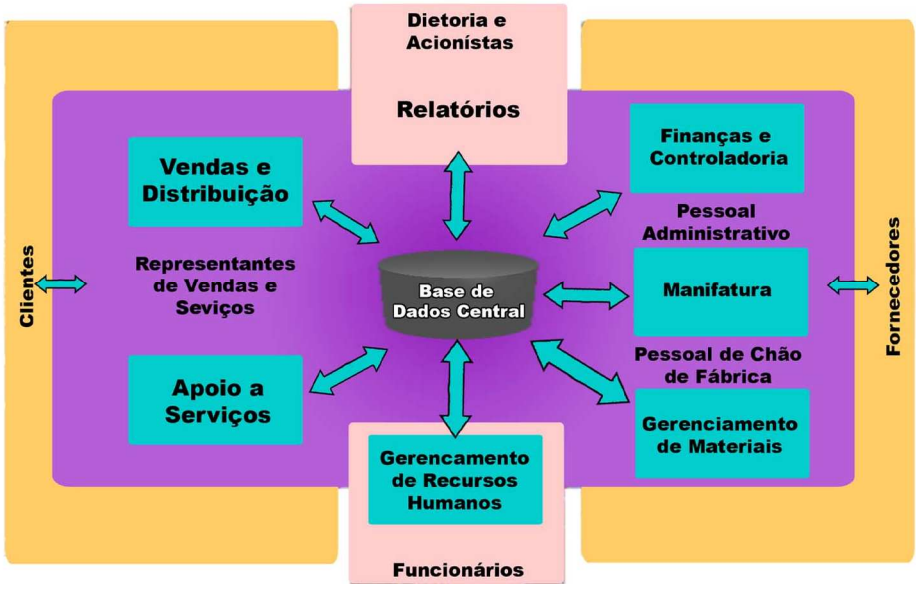


Figura 4: Implantação de Sistemas de Gestão Integrada (ERP, Davenport).

Para a implantação de um sistema ERP ou Sistema de Gestão Empresarial , as empresas devem considerar alguns tópicos (AMOR, 2000):

- Processos de negócio: o sistema deve suportar todos os processos do negócio;
- Integração de componente: o sistema deve ser altamente integrável entre as rotinas;
- Flexibilidade: deve ser ajustável às necessidades da empresa;
- Conectividade com a Internet: deve estar integrado aos negócios on-line da empresa;
- Implementação rápida: reduzindo a espera do retorno sobre o investimento;
- Facilidade de uso: gerenciado por todos as pessoas da empresa, em diversos níveis;

Existem, no mercado, diversos ERPs ou Sistemas de Gestão Empresarial, possuindo características específicas que os direcionam a determinados tipos e portes de empresa. Um dos pontos que influencia na hora da escolha de um ERP é o tamanho da organização.

Com a evolução da Internet, empresas desenvolvedoras desse tipo de sistema devem adaptá-lo às exigências do mercado, pois essa conectividade permite o auto-atendimento. Com isso, os clientes e fornecedores interagem com as empresas, sem a necessidade de contato com um representante. Sistemas ERP que não possuírem esta conectividade não serão mais aceitos.

6 TÉCNICAS DE AUDITORIAS PARA A SEGURANÇA DA INFORMAÇÃO.

Segundo Gil (2000), a auditoria é a validação e avaliação do controle interno de informações em processamento eletrônico de dados, relacionado à fidelidade da informação em relação aos dados, à segurança física e lógica, à confidencialidade, à segurança ambiental, à obediência a legislação em vigor, à eficiência e eficácia e ainda relacionado à obediência das políticas da alta direção da empresa. O termo validação exprime a idéia de teste e a avaliação exprime a idéia de julgamento e emissão de opinião. A seguir será descrito algumas técnicas de auditoria para a segurança da informação.

Algumas técnicas são de difícil aplicação e adaptação às condições especificas de cada sistema analisado. Cabe ao auditor conhece-las e avaliar custos e benefícios efetivos para sua utilização. A seguir, as técnicas que podem ser utilizadas, levando-se em consideração os parâmetros do controle interno, o momento da aplicação da técnica, o ambiente tecnológico de computação e os processos ou resultados do sistema de informação a ser auditado.

6.1 Massa de Teste ou *Test-Deck*

Esta técnica consiste em preparar dados de entrada com as mais diversas condições e variáveis diferentes para testar. Estes dados são alimentados e processados pelas rotinas e programas normais de produção, em processamento separado, mas simulando um ambiente real, permitindo avaliar sua exatidão e os controles existentes.

A referida técnica pode ser usada para rotinas específicas de um sistema e possibilita verificar:

- Rotinas de validação de dados de entrada, detecção de erros e consistência das transações ou processos;
- Lógica de processamento e controles relacionados à criação e manutenção de arquivos;
- Adequação da atualização da documentação dos programas e dos sistemas.

Esta técnica permite identificar e avaliar os controles, políticas, normas e procedimentos definidos, o auditor não necessita de assistência ou ajuda para preparar os dados de entrada e avaliar os resultados esperados e não se exige um profundo conhecimento de informática. Como desvantagens desta técnica, é possível que não sejam consideradas todas as possibilidades e situações geradoras de transações e ainda, dependendo do escopo do teste, pode tornar-se bastante complexa e demorada.

6.2 *Integrated Test Facility- Itf*

A técnica ITF, ou Simulação Paralela, é uma variante da Massa de Teste e consiste em gerar uma entidade fictícia dentro do sistema e gerar transações para esta entidade, as quais serão processadas dentro do ciclo normal de processamento do sistema.

É chamada de integrada porque as transações fictícias, que serão auditadas, são processadas junto com as transações normais e registradas nos mesmos arquivos. Utiliza-se esta técnica para testar e verificar sistemas complexos e de grande porte, onde não é possível separar o processamento num outro ambiente.

Como vantagens desta técnica, pode-se constatar um exame bastante abrangente, sem a necessidade de processamento especial e separado, além do custo operacional bastante reduzido, pois não perde-se tempo criando um ambiente de testes. Porém, como desvantagens, existe a necessidade de se estabelecer procedimentos de separação e retirada dos dados de auditoria das transações normais. Também existe a possibilidade de inclusão de dados não íntegros nos registros normais da empresa e distorções de resultados em relatórios de análise.

6.3 *Software* de Auditoria

Esta técnica permite que o auditor faça uma análise independente sobre os dados de um arquivo de um sistema em operação. É composto de um grupo de programas adquiridos (pacotes) ou preparados pelo auditor, com o objetivo de avaliar e validar dados de arquivos mediante parâmetros e condições definidas.

Sua característica básica é que diferencia-se de outras técnicas no sentido de que não integra as rotinas normais de processamento e são executadas no momento em que o auditor julgar conveniente.

Existem duas grandes vantagens com o uso desta técnica: permite grande abrangência na execução de avaliações, segundo a criatividade do auditor; possibilita independência à auditoria na determinação e execução dos trabalhos, inclusive fora do ambiente da empresa.

As desvantagens consistem na necessidade de conhecimento e treinamento em linguagem de programação e/ou aprendizado do software adquirido, por parte do auditor e também um alto custo e limitações do software de auditoria adquirido.

6.4 Módulos de Auditoria Inserido

Esta técnica baseia-se em incorporar ao sistema aplicativo um programa ou rotina específica desenvolvida pela área de informática com o objetivo de analisar as transações e selecioná-las mediante critérios predeterminados, para posterior exame pela Auditoria.

A grande vantagem desta técnica é que ela possibilita que as transações sejam selecionadas e examinadas no momento em que efetivamente ocorreram e também permite o exame de todas as transações consideradas de interesse da auditoria, de forma automática.

Como desvantagem podemos citar que esta técnica exige conhecimento e esforço de programação, para os módulos da auditoria,

necessitando definições e ajustes do sistema e, como conseqüência, que estes módulos sejam revistos e atualizados continuamente, para que seus resultados sejam efetivos.

6.5 Técnicas de Monitoração e Rastreamento

Estas técnicas, utilizadas por profissionais de informática, são extremamente úteis para a Auditoria. Ferramentas como o *Mapping*, *Tracing* e Snapshot permitem analisar os resultados de um programa de computador durante a sua execução.

O *Mapping* é um *software* de monitoração, que indica o número de vezes que cada instrução foi executada num processamento, os segmentos não utilizados e o tempo de processamento. Estas informações permitem a identificação de segmentos pouco utilizados nos programas, que têm a maior probabilidade de estar associados a rotinas não autorizadas.

A técnica de *Tracing* detalha instrução por instrução executada pelo programa e em que seqüência estas instruções são executadas. Esta técnica permite que o auditor obtenha conhecimento das instruções executadas durante o processamento de transações específicas.

Isto revela porque alguns resultados foram obtidos no processamento de determinada transação e então ser comparados com as políticas e procedimentos definidos na empresa.

O *Snapshot* fornece um quadro dos dados, extraído em determinados pontos do processamento. Esta técnica permite que o auditor veja as chaves de arquivos, valores acumulados, áreas de armazenamento (memória), códigos e identificação de computadores e usuários e qualquer outra informação disponível no programa. Dessa forma é possível acompanhar transações específicas e determinar o seu caminho lógico, condições de controle e seqüência de processamento.

6.6 Análise e Comparação de Código Fonte

Técnica pouco utilizada, que consiste na análise visual das instruções do programa (código fonte) e/ou na guarda de uma cópia dos principais programas em linguagem fonte e objeto, para posterior comparação com as versões dos mesmos programas que estão em operação. Esta comparação é executada pelo auditor utilizando um software que, após verificar instrução por instrução, indica as diferenças encontradas.

Esta técnica pode ser útil para auxiliar na avaliação de procedimentos de manutenção de software, bibliotecas de programas, códigos fonte e controle de versões de programas e sistemas. Entretanto, convém ressaltar que esta técnica exige profundos conhecimentos de processamento eletrônico de dados por parte do auditor de sistemas.

6.7 Verificação *"In-Loco"*

Esta técnica baseia-se na observação pessoal do auditor de sistemas sobre os processos e funções inerentes ao sistema. Implica no cumprimento da seguinte seqüência de procedimentos:

- Marcar antecipadamente a data e à hora com o responsável pelo sistema, que acompanhará as verificações ou convoca-las no momento da verificação, caso o fator surpresa for necessário;
- Anotar os procedimentos e acontecimentos e coletar documentos. Caso necessário, elaborar uma representação gráfica das rotinas do sistema;
- Anotar o nome completo das pessoas que prestaram depoimentos e respectivas data e hora;
- Analisar os resultados obtidos e emitir opinião via relatório de fraquezas de controle interno. Caso necessário, voltar ao início deste procedimento.

6.8 Análise de *"Job Accouting" / "Log"*

Os arquivos de *Log/Accounting* são gerados por uma rotina componente do sistema operacional, que contém registros de utilização do hardware e software que compõe o ambiente computacional. A tabulação deste arquivo permite a verificação da intensidade de uso do software aplicativo e de apoio vigente.

Existem dois tipos de arquivos de interesse do auditor: os que possuem os registros de contabilização e os que possuem os registros de atividade do *"data set"*. Os registros de contabilização mostram quais usuários usaram quais programas, quantas vezes e por quanto tempo.

Além disso, incluem identificação do usuário, características do hardware com desempenho do "*job*" e como foi completado. Os registros de atividade do "*data set*" providenciam informações acerca de quais arquivos de dados foram usados durante o processamento e quem solicitou o uso do "*data set*".

Esta técnica permite a identificação da ineficiência do sistema auditado, a apuração do desbalanceamento da configuração do computador, pela caracterização de dispositivos de entrada e saída (disco, fitas, terminais, impressoras) que estão com folga ou sobrecarregados, a determinação de erros de programas ou de operação, o uso de programas fraudulentos ou utilização indevida e ainda a identificação de tentativas de acesso a arquivos ou ao sistema por senhas não autorizadas.

Esta técnica de auditoria é um instrumento poderoso, porém sua aplicação requer grande conhecimento de computação. Observa-se, entretanto, que o emprego desta técnica no ambiente de microcomputadores, muitas vezes é inviável, pela inexistência de um software que grave os arquivos de "Log".

6.9 Análise de Relatórios / Telas

Esta técnica visa a análise de documentos, relatórios e telas do sistema para determinar o nível de utilização pelo usuário, esquemas de distribuição

e número de vias emitido, grau de confidencialidade de seu conteúdo, forma de utilização e integração e distribuição das informações, segundo o layout vigente.

As etapas a serem seguidas para a aplicação desta técnica consistem em relacionar, por usuário, e classificar, por prioridade, todos os relatórios/telas/documentos que pertençam ao ponto de controle analisado, obter um modelo ou cópia destes, elaborar um *checklist* ou questionário para a realização dos levantamentos relacionados, realizar entrevistas com as pessoas que os utilizam e analisar as respostas, formar e emitir opinião acerca do nível de controle interno.

As principais fraquezas identificadas com esta técnica são:

- Relatórios, telas e documentos não mais utilizados;
- *Layout* inadequado;
- Distribuição indevida de vias;
- Confidencialidade não estabelecida ou não respeitada.

Esta técnica é primordial para a avaliação do parâmetro eficácia do sistema. A conclusão do trabalho freqüentemente possibilita a redução de custos com a desativação total ou parcial de relatórios, telas e documentos. No tocante a telas, a aplicação desta técnica pode ser dificultada, pela facilidade que os usuários têm na criação e descarte das mesmas.

6.10 Questionários

Corresponde à elaboração de um conjunto de perguntas objetivando a verificação de um determinado ponto de controle. Buscam adequar o ponto de controle aos parâmetros do controle interno, tais como segurança física e lógica, controle de acesso, confidencialidade, obediência à legislação, eficiência e eficácia (GIL, 1999).

Para a elaboração do questionário, deve-se primeiramente analisar o ponto de controle a ser auditado; em seguida, selecionar as pessoas que deverão responder o questionário; depois, elaborar um conjunto de instruções de como

responder as questões; distribuir o questionário para as pessoas selecionadas; controlar o recebimento ou não dos questionários respondidos e, finalmente, analisar e avaliar os resultados obtidos (ARIMA, 1994).

A técnica do questionário é aplicada normalmente de forma casada a outras, como Entrevista, Verificação “In Loco”, etc. O quadro 1 apresenta um modelo de questionário, aplicável na auditoria de sistemas de informação em operação.

QUESTIONÁRIO PARA AVALIAÇÃO DE CONTROLE INTERNO					
N.	PONTO DE CONTROLE: 2.Controle de acesso ao sistema	SIM ou N/A	NÃO	REF.	OBSERVAÇÕES
01	O sistema de informação está preparado para não permitir o acesso indevido de pessoas não habilitadas?				
02	Existe no sistema um esquema especial de senhas e “password” de forma hierarquisada de acesso as suas bases de dados?				
03	Existe rotinas e procedimentos estabelecidos para atribuição ou modificação do nível de acesso?				
04	Na medida do possível, senhas únicas são atribuídas a usuários individuais?				

Quadro 1 – Modelo de Questionário de Auditoria.

A vantagem desta técnica é a possibilidade de interrogar várias pessoas ao mesmo tempo e sem o deslocamento do auditor. Além disso, permite diagnosticar pontos relevantes, para serem validados com maior profundidade posteriormente.

Como desvantagem, existe a possibilidade de interpretações subjetivas, tanto para as questões quanto para as respostas.

Estes questionários objetivam esclarecer situações de operação do sistema, tais como: plano diretor de informática; sistemas aplicativos *batch* em operações; sistemas aplicativos *online* em operação; microinformática no ambiente

do usuário; segurança física ambiental; segurança lógica dos sistemas em operação; ambiente de banco de dados; ambiente de auditoria interna (MAGALHÃES, 2001).

6.11 Entrevistas

A técnica de entrevista consiste em realizar reuniões entre o auditor e os auditados – pessoas envolvidas no ponto de controle do sistema a ser auditado.

Os procedimentos a seguir podem ser adotados para a revisão e avaliação do grau de controle interno existente:

- Analisar o ponto de controle a ser auditado e identificar as pessoas envolvidas;
- Elaborar um "*checklist*" ou roteiro para a realização da entrevista;
- Marcar, antecipadamente, a data, hora e local com as pessoas que serão entrevistadas, bem como comunicar a natureza do trabalho a ser desenvolvido;
- Realizar a reunião e anotar as respostas dos entrevistados a cada questão efetuada;
- Elaborar uma ata da reunião, com o registro dos principais pontos discutidos, e distribuir uma cópia da ata para cada participante da entrevista;
- Analisar as respostas, avaliar os resultados para a formação de opinião, acerca do nível de controle interno do ponto de controle;
- Emitir o relatório de fraquezas de controle interno;

Esta técnica pode ser aplicada em qualquer ponto de controle como um complemento à aplicação das demais técnicas, ou seja, é freqüentemente casada com as técnicas verificação "in loco", questionários, *test-deck*, entre outras.

Além disso, a entrevista permite maior rapidez na avaliação do ponto de controle e possibilita esclarecimentos de pontos duvidosos ou polêmicos.

Vale ressaltar, ainda, que a opinião do auditor é expressa com base na palavra do auditado, possibilitando interpretações subjetivas, tanto nas questões como nas respostas.

7 PROPOSTA DE AUDITORIA DA TECNOLOGIA DA INFORMAÇÃO

O presente trabalho consiste em efetuar a auditoria da Tecnologia da Informação em uma indústria moveleira, avaliando o grau de segurança da informação, evidenciando a segurança física e lógica de um ambiente computacional. Para que a auditoria da TI seja efetivada, optou-se em usar técnicas pesquisadas que integram os conceitos de um programa de auditoria da TI, para garantir e assegurar a disponibilidade e segurança dos computadores e a confiança e integridade da guarda e manipulação de informações envolvidas no ambiente computacional da entidade.

A motivação para o desenvolvimento deste trabalho deve-se ao grande número de processos envolvidos no ambiente computacional, envolvendo a segurança física e lógica da informação, vulneráveis com relação à segurança de dados não atendendo as expectativas exigidas por uma política de segurança da informação (*ISO 17799).* Para que os mesmos erros não ocorram consideravelmente no ambiente computacional da entidade, optou-se em efetivar uma auditoria de TI: **Planejar, Executar e emitir Relatório final propondo melhorias**, para mostrar que, se ambientes computacionais desconsiderarem estes métodos estão expostos a vulnerabilidades inesperadas.

Com base no levantamento bibliográfico foi selecionada a técnica mais apropriada, neste caso, a técnica selecionada foi a de **Entrevista**. Isto deve-se ao fato de não haver a necessidade da auditoria ser aplicada por um especialista, aplicando técnicas de auditorias em TI seguindo normas certificadas, e por possuir um custo benefício baixo, além de garantir resultados abrangentes e satisfatórios, uma vez que o conhecimento encontra-se embutido em políticas de segurança da informação certificadas.

As técnicas para efetuar esta auditoria, trata-se de **Planejar** os trabalhos por intermédio de uma lista de verificação, a **Execução** será efetuada através de um *checklist* específico para a área de segurança física e lógica do ambiente computacional, e por fim emitir **Relatórios** com possíveis dados levantados no decorrer da auditoria, demonstrando as conformidades dos processos, sugerindo melhorias se erros forem encontrados. Com um estudo mais

abrangente sobre esta técnica descobriu-se que a auditoria poderá ser conduzida por um único auditor, por tratar-se de uma auditoria não oficial.

7.1 Planejamento

A fase de planejamento de uma auditoria identifica os instrumentos indispensáveis à sua realização. Além de estabelecer os recursos necessários à execução dos trabalhos de auditoria, a área de verificação, as metodologias, os objetivos de controle e os procedimentos a serem adotados, o auditor realiza um trabalho de pesquisa de fontes de informação sobre o objeto a ser auditado e negocia todos esses aspectos com sua gerência.

7.1.1 Pesquisa de Fontes de Informações

Na fase de planejamento da auditoria, a equipe deve reunir a maior quantidade possível de informações sobre a entidade auditada e seu ambiente de informática (plataforma de hardware, sistemas operacionais, tipo de processamento, metodologia de desenvolvimento, principais sistemas, etc.). Com essas informações poderá esboçar seu plano de auditoria e partir para a fase de delimitação dos trabalhos.

Esse conhecimento prévio do ambiente de informática da entidade auditado permite ao auditor ter uma noção do grau de complexidade de seus sistemas e, então, estabelecer os recursos e os conhecimentos técnicos necessários à equipe da auditoria.

Saber com antecedência o tipo de ambiente computacional com o qual o auditor vai se deparar é, sem dúvida, bastante vantajoso, já que haverá mais tempo para se preparar tecnicamente ou para incluir um especialista na equipe. A equipe precisará manter contato e entrevistar pessoas-chaves da entidade.

As principais fontes de informações sobre a entidade auditada são relatórios de auditorias anteriores, base de dados, documentos ou páginas da entidade na Internet, notícias veiculadas na imprensa, visitas anteriores à entidade e

relatórios da auditoria interna.

7.1.2 Definindo Campo, Âmbito e Sub-Áreas

A partir do momento em que foi decidida a realização de uma auditoria e já existem informações suficientes sobre a entidade e seu ambiente computacional, a equipe delimita sua atuação, definindo o campo, o âmbito e as sub-áreas a serem auditadas. O campo da auditoria é composto por objeto, período de fiscalização e natureza.

No caso de auditorias de informática, a natureza é auditoria da tecnologia da informação, quase sempre com enfoque operacional (exame dos aspectos econômicos, de eficiência e eficácia). O objeto auditado pode englobar um sistema computacional específico; uma, várias ou todas as seções do departamento de informática; ou até mesmo toda a organização (em termos de políticas de informática e segurança de informações ou nos casos em que o negócio da organização resume-se à prestação de serviços computacionais). O período de uma auditoria da TI depende diretamente do âmbito (grau de profundidade das verificações) e das sub-áreas de sistemas escolhidas pela equipe.

Além da definição do campo, são determinadas a amplitude e a exaustão dos processos de auditoria, incluindo uma limitação racional dos trabalhos a serem executados.

Tendo sido definido o conjunto campo e âmbito da auditoria, é fixada, então, a área de verificação. Essa área delimita de modo muito preciso os temas da auditoria e, em função do objeto a ser fiscalizado e da natureza da auditoria, pode ser subdividida em sub-áreas, como mostra a figura 5 abaixo:

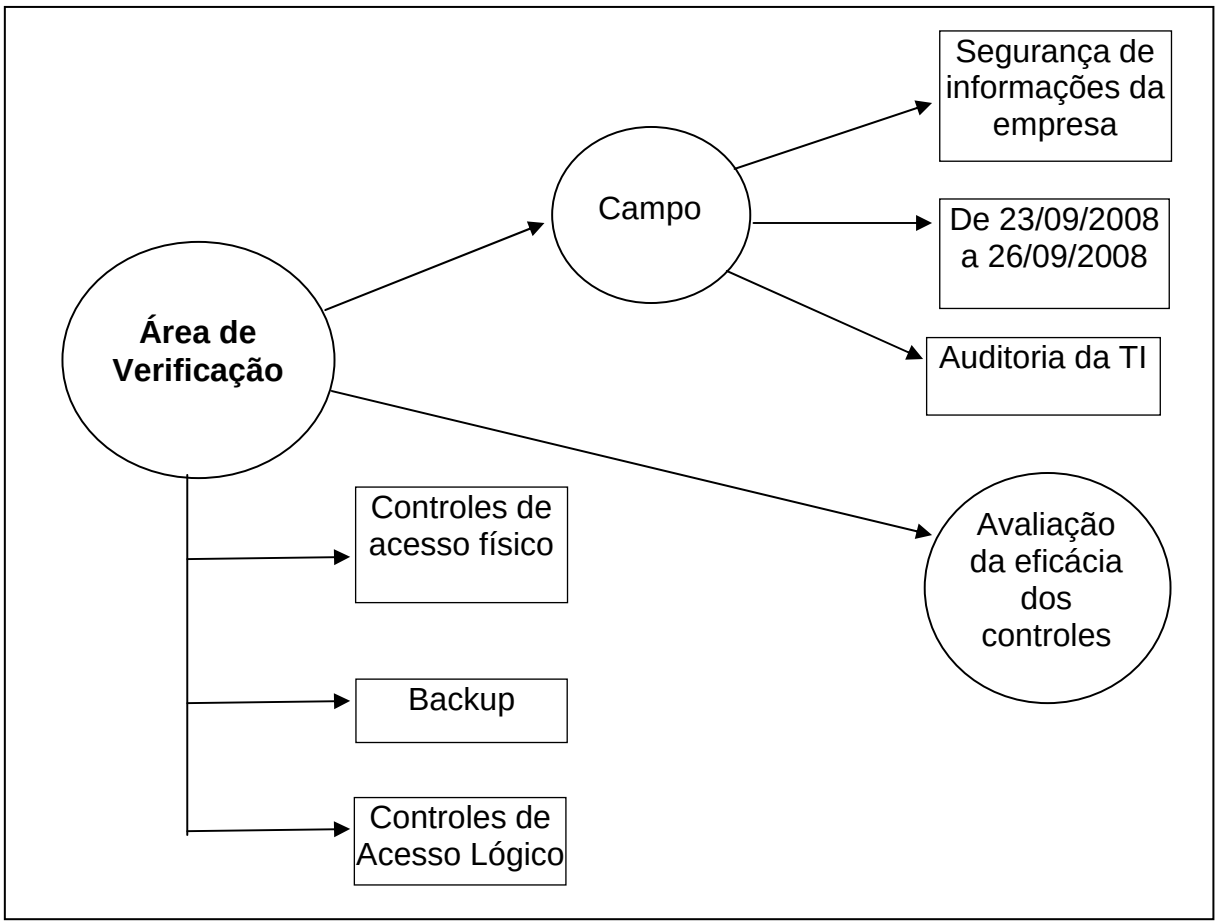


Figura 5: Área de Verificação

É aconselhável coordenar o número de sub-áreas a serem auditadas com a magnitude ou complexidade do objeto da auditoria, isto é, para ambientes extensos ou de grande complexidade, convém limitar a quantidade de controles a serem verificados para que a equipe realize um trabalho de qualidade.

Após a definição das áreas e sub-áreas a serem auditadas, o auditor retorna à fase de pesquisa para relacionar as fontes de consulta especializadas necessárias durante a auditoria, tais como livros técnicos, manuais de auditoria, artigos especializados, sites na Internet especializados em segurança ou outras áreas específicas de informática.

Para levantar as principais questões relacionadas ao ambiente computacional evidenciando controle de acesso físico e lógico, avaliando se todos os aspectos importantes para analise dos resultados e/ou continuidade para etapa(s) posterior(es), foram considerados, com isto elaborou-se uma Lista de Verificação demonstrando itens em **C** (Conformidade) e ou **NC** (Não Conformidade) em cada item relacionado, de acordo com os quadros 2 (ANEXO A) e 3 (ANEXO B) abaixo relacionados:

Lista de Verificação para Auditoria da Tecnologia da Informação

ÁREA:	
TIPO DE AUDITORIA:	
DATA DA AUDITORIA:	
EQUIPE DA AUDITORIA (NOME / FUNÇÃO NA EQUIPE)	

Controles de Acesso Físico	**C**	**NC**
A) Instituir formas de identificação capazes de distinguir um funcionário de um visitante e categorias diferentes de funcionário, se for o caso.		
B) Exigir a devolução de bens de propriedade da instituição quando o funcionário é desligado ou demitido.		
C) Controlar a entrada e a saída de equipamentos, registrando data, horários e local da visita e, dependendo do grau de segurança necessário, acompanha- lo até o local de destino.		
D) Instituir vigilância no prédio, 24 horas por dia, 7 dias na semana.		
E) Supervisionar a atuação da equipe de limpeza, manutenção e vigilância.		
F) Não instalar, em áreas de acesso publico, equipamentos que possam acessar a rede interna.		
G) Orientar os funcionários a não deixarem os computadores sem qualquer supervisão de pessoa autorizada, por exemplo, durante o horário de almoço ou quando se ausentarem de sua sala por tempo prolongado.		
H) Encorajar o bloqueio de teclado, a guarda de documentos confidenciais, disquetes, backups e laptops em armários com chave, etc.		
I) Utilizar mecanismos de controle de acesso físico, tais como fechaduras, câmeras de vídeo e alarmes.		
J) Proteger as linhas telefônicas e outros dispositivos de comunicação contra ‘grampo’.		
K) Proteger fisicamente os backups.		
L) Restringir o acesso a computadores e impressoras que manipulem dados confidenciais .		
M) Instituir política de descarte de equipamentos, dispositivos e documentos em papel que possam conter informações confidenciais.		

Quadro 2: Lista de Verificação para Controle de Acesso Físico

Lista de Verificação para Auditoria da Tecnologia da Informação

ÁREA:	
TIPO DE AUDITORIA:	
DATA DA AUDITORIA:	
EQUIPE DA AUDITORIA (NOME / FUNÇÃO NA EQUIPE)	

Controles de Acesso Lógico	**C**	**NC**
A)Conceder acesso aos usuários, apenas aos recursos realmente necessários para a execução de suas tarefas.		
B) Restringir e monitorar o acesso a recursos críticos.		
C) Utilizar softwares de controle de acesso lógico.		
D) Revisar periodicamente as listas de controle de acesso.		
E) Evitar dar orientações ao usuário durante o processo de logon		
F) Bloquear a conta do usuário após certo numero de tentativas frustradas de logon.		
G) Restringir acesso a determinados periféricos.		
h) Fornecer contas apenas a pessoas autorizadas.		
I) Não fornecer a mesma conta para mais de um usuário.		
J) Ao conceder a conta ao usuário, informa-lo sobre as políticas de senha daorganização.		
K) Bloquear se possível, a escolha de senhas consideradas frágeis e orientar o usuário na escolha de senhas mais seguras.		
L) Orientar os usuários para não armazenarem senhas em arquivos ou envia-las por e-mail.		
M) Armazenar as senhas no sistema sob a forma criptografada.		
N) Prevenir o uso freqüente de senhas já utilizadas pelo mesmo usuário anteriormente.		
O) Estabelecer um prazo máximo utilização de uma mesma senha.		
P) Informar os usuários quanto aos perigos de divulgação de senhas.		
Q) Impedir que os usuários sejam capazes de ler os arquivos de senha, identificar e trocar senhas de outros usuários.		
R) Desabilitar contas inativas, sem senhas ou com senhas padronizadas.		
S) Desabilitar as senhas de ex-funcionários.		

Quadro 3: Lista de verificação para Controle de Acesso Lógico

7.2 Execução

No transcurso da auditoria, a equipe deve reunir evidências confiáveis, relevantes e úteis para a consecução dos objetivos da auditoria. Os resultados da auditoria (achados e conclusões) devem ser suportados pela correta interpretação e análise dessas evidências.

- Evidência física – observações de atividades desenvolvidas pelos funcionários e gerentes, sistemas em funcionamento, local equipamentos, etc.
- Evidência documentária – resultado da extração de dados, registro de transações, listagens, etc.
- Evidência fornecida pelo auditado - transcrições de entrevistas, cópias de documentos cedidos, fluxogramas, políticas internas, e-mails trocados com a gerência, justificativas, relatórios, etc.
- Evidência analítica - comparações, cálculos e interpretações de documentos.

Toda essa documentação, geralmente organizada em papéis de trabalho, deve estar disponível para auxiliar a equipe na elaboração do relatório. Nem todas as evidências podem ser investigadas detalhadamente e descritas no relatório final, o auditor deve analisar cada caso segundo a sua importância para a consecução dos objetivos, tempo e esforço necessários para esclarecer todos seus pontos nebulosos.

Uma evidência considerada incompatível com a auditoria em execução, pode servir como indicativo para outra auditoria. A manutenção dos papéis de trabalho é essencial tanto para a elaboração do relatório da auditoria em questão, como para o planejamento de futuras auditorias.

Para efetuar a execução dos trabalhos de auditoria, são construídos *Checklist(s),* conforme mostra o Quadro 4 (ANEXO C) abaixo:

AUDITORIA da TECNOLOGIA DA INFORMAÇÃO em INDUSTRIA MOVELEIRA EVIDENCIA: Segurança da Informação AUDITOR: Kenion

Checklist Empresa_____Data___/___/__Hora____:__
Ambiente: [ ] Interno [ ] Externo [ ] Windows [ ] Linux [ ] Internet _____ Categoria: [ ]Física [ ]Lógica [ ]Documentação [ ]Infraestrutura [ ]Comunicação de dados [ ]Informações [ ]Sistemas [ ]Notebook [ ] Senhas [ ] _____ Processo: _____ _____ Medida de segurança: _____ _____ Verificação: _____ Incidente provável: _____ _____ Ação requerida: _____ Resultado esperado: _____ Situação encontrada: _____ Eficiente [ ] Deficiente [ ] Ineficiente [ ] Não se aplica [ ] Impacto no negocio Alto[ ] Médio[ ] Baixo[ ]

Quadro 4: *CheckList*.

7.3 Relatórios

Nos relatórios da auditoria, a equipe, apresenta seus achados e conclusões, bem como os fatos sobre a entidade auditada, comprovações recomendações e determinações. A linguagem utilizada nos relatórios deve ser compatível com quem irá recebê-los.

7.3.1 A Quem se Dirige o Relatório?

Dependendo do motivo que levou à realização da auditoria, o relatório pode ser encaminhado à diretoria da organização, ao organismo que financia a entidade auditada ou ao organismo responsável pelo controle de auditoria geral da entidade. Faz-se necessário identificar os pontos mais relevantes e adaptar o relatórios de acordo com o público alvo.

7.3.2 Relatórios Preliminares

Antes mesmo de iniciar os trabalhos de campo, na fase do planejamento da auditoria, são coletadas informações preliminares sobre a entidade, seus sistemas, os recursos necessários, a composição da equipe, metodologias, objetivos de controle e procedimentos a serem adotados. Uma estrutura de relatório deve ser definida e todas essas informações devem ser transcritas para o relatório.

Durante os trabalhos de campo, é importante documentar tudo que foi feito, observado e dito pelos entrevistados. Os textos referentes a cada entrevista podem ser utilizados no relatório. A equipe deve confirmar os fatos relatados e apresentar ao entrevistado, antes da revisão final do relatório os assuntos tratados durante a entrevista, evitando mal-entendidos ou desvios de interpretação.

Ao término das investigações de cada área, um relatório parcial deve ser apresentado contendo as deficiências encontradas (entrevista para discussão de deficiências encontradas). As justificativas apresentadas podem ser anexadas ao parecer.

7.3.3 Relatório final

O relatório final deve se revisado por toda a equipe de auditores, a fim de evitar inconsistências, erros ou lacunas em relação aos padrões e práticas da organização auditada. Uma crítica externa, também e conveniente nesse ponto. Segue abaixo a seguinte estrutura:

- **Dados da entidade auditada** - nome, endereço, natureza jurídica, relação de responsáveis, etc.

- **Síntese** - um breve resumo do conteúdo. É útil para a alta direção obter uma visão geral e rápida dos principais pontos da auditoria.

- **Dados da auditoria** - objetivos, período de fiscalização, composição da equipe, metodologia adotada, natureza da auditoria, e objeto (controles gerais, desenvolvimento de sistemas, aplicativo específico, etc.).

- **Introdução** - histórico da entidade, conclusões de auditorias anteriores, estrutura hierárquica do departamento de informática, sua relação com outros departamentos, descrição do ambiente computacional, evolução tecnológica, principais sistemas e projetos.

- **Falhas detectadas** - apresenta em detalhes, as falhas e irregularidades detectadas durante a auditoria. Além das descrições, são apresentados comentários iniciais, justificativa do auditado e o parecer final da equipe para cada falha (preferências e recomendações). É aconselhável dividi-la por sub-áreas fiscalizadas, para haver um encadeamento lógico de idéias.

- **Conclusão** - síntese dos pontos principais do relatório e as recomendações ou determinações finais da equipe para a correção das falhas ou irregularidades encontradas.

- **Pareceres da gerência superior** - as gerências superiores podem dar seu parecer a respeito dos achados e recomendações da equipe de auditores, concordando integralmente ou em partes com os pontos de vista da auditoria, ou ainda discordando inteiramente.

Os Relatórios finais podem ser demonstrados de maneira eficaz de acordo com o Quadro 5 (ANEXO D) abaixo citado:

AUDITORIA EM SEGURANÇA DA INFORMAÇÃO	**RELATÓRIO DE AUDITORIA INTERNA**	***CODIGO: RQ-*** ***Página 1/1***

Auditoria Nº: **Data:** **SETOR AUDITADO DVIN** **Responsável:** **Auditor:** **Luiz Fernando**
OBJETIVOS DA AUDITORIA
ITEM AUDITADO
PONTOS POSITIVOS E NEGATIVOS DA AUDITORIA
RELAÇÃO DE REGISTROS DE NÃO CONFORMIDADES
SUGESTÕES E COMENTÁRIOS DOS AUDITORES
EQUIPE DE AUDITORES
Kenion César Michelato Colaço **Auditor lider** **Nome/Visto:**_____ _____ _____ _____

Quadro 5: Relatório de Auditoria Interna.

7.4 Auditoria por Entrevistas

A auditoria por entrevistas permite ao longo da auditoria serem feitas entrevistas com dirigentes e funcionários da entidade auditada, com intuito de apresentar o plano da auditoria a ser realizada, coletar dados, identificar falhas e indícios de irregularidades e, por fim, apresentar os resultados dos trabalhos. As entrevistas em uma auditoria podem ser divididas por etapas, conforme abaixo relacionadas:

- Entrevistas de apresentação: Apresentação da equipe, cronograma das atividades, objetivos, áreas, período, metodologias. Estrutura do relaorio (resultado da auditoria);
- Entrevistas de coleta de dados: Coleta de dados sobre os sistemas ou ambiente de informática. Nessa entrevista podem ser identificados os pontos fortes e fracos de controle, falhas e possíveis irregularidades. O entrevistado deve saber de antemão como serão usados esses dados e conhecer o relatórios a cerca da entrevista.
- Entrevistas de discussão de deficiências encontradas: Ao término das investigações são apresentadas as deficiências encontradas. Ao discuti-las podem ser apresentadas justificativas para essas deficiências, podendo ser desconsiderada as falhas ou relatadas as justificativas.
- Entrevista de encerramento: É apresentado o resumo dos resultados (pontos fortes, falhas mais relevantes, comentários, recomendações).

Segundo Dias (2000), várias metodologias podem ser utilizadas eu uma auditoria da tecnologia da informação, desde uma simples observação, em visitas à entidade, até entrevistas com seus funcionários e dirigentes e uso de técnicas ou ferramentas de apoio.

8. ANÁLISES DOS RESULTADOS

Para a realização da auditoria da TI em ambiente computacional, foi utilizada a técnica de entrevista. Como já foi dito, a entrevista é composta de três etapas primordiais para o processo de auditoria: Planejamento, Execução e Relatório final da auditoria.

A entrevista é uma das técnicas eficientes para a efetivação da auditoria em TI. Durante sua aplicação ao ambiente computacional verificou-se que muitos itens da lista de verificação (controle de segurança física e lógica) não foram aplicáveis, pelo fato da entidade não dispor dos recursos e procedimentos que uma política da segurança da informação (ISO/IEC 17799/27002) exige. Todavia estas questões não interferiram no resultado final, sendo possível detectar não conformidades na auditoria.

8.1 Metodologia da Análise

- Fotos (APÊNDICES): foram tiradas fotos de pontos relevantes como vulnerabilidades, áreas críticas, ambientes e acessos a informações conformes, abrangendo a área computacional, naquilo que poderia ser de interesse para os resultados da auditoria.
- Levantamentos no ambiente computacional: foram feitos levantamentos no ambiente para informações relevantes.
- Entrevista: Foram feitas entrevistas com o administrador de TI. Utilizou-se uma lista de verificação para controle de acesso físico e lógico (baseado em Dias, 2000).

8.2 Análise de Controle de Acesso Físico

O objetivo do controle de acesso físico é prevenir acesso não autorizado, dano e interferência às informações e instalações físicas das entidades.

Devem ser adotados controles para minimizar o risco de ameaças potenciais, incluindo furto, incêndio, explosões, fumaça, água (falha no abastecimento e ou danificar aparelhos computacionais), poeira, vibração, efeitos químicos, interferência no suprimento de força, segurança em cabeamento, radiação eletromagnética e acesso indevido físico.

8.2.1 Plano de Ação

- Implementar alterações em processos não conformes e adotar melhorias em processos conformes no controle de acesso físico, sugeridos por uma possível implantação de uma política da segurança da informação.

- **Instituir formas de identificação capazes de distinguir um funcionário de um visitante e categorias diferentes de funcionário, se for o caso** (correspondente ao item (A – quadro 2– APÊNDICE A)): **Conforme.**

- A entidade possui portaria de entrada e saída para funcionários e visitantes;

- Distinguir funcionário de visitante e ou serviço terceirizado por intermédio de crachá de identificação.;

- Os colaboradores possuem uniforme para uso obrigatório distinguindo de visitantes.

- **Exigir a devolução de bens de propriedade da instituição quando o funcionário é desligado ou demitido.** (correspondente ao item B – quadro 2) **Conforme.**

- É determinado pela entidade a devolução imediata de qualquer equipamento e ou material computacional de posse do colaborador para uso interno ou externo.

- Evidenciar registro de devolução constando data e especificação do material devolvido.

- **Controlar a entrada e a saída de equipamentos, registrando data, horários e local da visita e, dependendo do grau de segurança necessário, acompanhá-lo até o local de destino** (correspondente ao item C – quadro 2: **Conforme.**

- Foi evidenciado o controle de entrada e saída de equipamentos pelo administrador de TI por um registro constando: data,equipamento e responsável pela retirada do equipamento e ou material.

- **Instituir vigilância no prédio, 24 horas por dia, 7 dias na semana** (correspondente ao item (D – quadro 2– APÊNDICE A)): **Conforme.**

- É evidenciado a vigilância 24 horas por dia nos 7 dias da semana, pela equipe terceirizada de vigilância e câmeras de segurança por toda a entidade;

- Monitoração de câmeras por sistema integrado, rastreados por *software* interno.

- **Supervisionar a atuação da equipe de limpeza, manutenção e vigilância** (correspondente ao item (E – quadro 2) **Não Conforme.**

- Foi evidenciado a falta de supervisão e acompanhamento referente a equipe de limpeza no ambiente computacional.

- Deverá existir registro de entrada e saída da equipe de limpeza, constando data, hora e responsável

- **Não instalar em áreas de acesso público, equipamentos que possam acessar a rede** correspondente ao item (F – quadro 2– APÊNDICE A)): **Não Conforme.**

- Foi evidenciado em áreas de acesso público instalações de equipamentos que possam acessar a rede.

- Deverá existir salas computacionais que não comprometam a integridade da informação, devidamente fechadas.

- **Orientar os funcionários a não deixarem os computadores sem qualquer supervisão de pessoa autorizada, por exemplo, durante o horário de almoço ou quando se ausentarem de sua sala por tempo prolongado** (correspondente ao item (G– quadro 2– APÊNDICE A)). **Não Conforme.**

- Deverá existir em alguns ambientes computacionais, salas apropriadas para acomodação dos equipamentos e materiais.

- Deverá constar registro de entrada e saída somente de colaboradores autorizados pelo determinado setor, devidamente trancados e climatizados.

- **Encorajar o bloqueio de teclado, a guarda de documentos confidenciais, disquetes, backups e laptops em armários com chave,** (correspondente ao item (H – quadro 2 – APÊNCIDE A)) **Não Conforme.**

- Foi evidenciado o não bloqueio de teclado em nenhum ambiente computacional;

- Deverá existir treinamento e conscientização dos usuários de equipamentos computacionais, implantado e monitorado pelo administrador de TI.

- Registrar a entrada e saída dos usuários da sala de guarda de documentos confidenciais, constando: data, horário e usuário.

- **Utilizar mecanismos de controle de acesso físico, tais como fechaduras, câmeras de vídeo e alarmes** (correspondente ao item (I – quadro 2– APÊNDICE A). **Não Conforme.**

- Foi evidenciado vários ambientes computacionais no departamento de produção em ambiente aberto sem nenhum controle de acesso físico, tais como: sala fechada, climatizada, fechaduras e ou alarmes contra invasão;

- Deverá existir salas, fechaduras e alarmes em 100% do ambiente computacional.

- **Proteger as linhas telefônicas e outros dispositivos de comunicação contra 'grampo'** (correspondente ao item (J – quadro 2: **Não Conforme.**

- Foi evidenciado nenhuma proteção de linha telefônica ou dispositivos de comunicação contra grampos;

- Deverá exister um comprometimento da alta gerência em implantar um política contra possíveis grampos nos sistemas computacionais;

- Monitoramento e rastreabilidade de possíveis detecções de grampos, sob responsabilidade do administrador de TI.

- **Proteger fisicamente os *backups*** (correspondente ao item (K – quadro 2– APÊNDICE A)). **Conforme.**

- Foi evidenciado a guarda e proteção física dos processos de *backups,* sala fechada e climatizada.

- **Restringir o acesso a computadores e impressoras que manipulem dados confidenciais** (correspondente ao item (L – quadro 3 – APÊNDICE A). **Não Conforme.**

- Foi evidenciado a falta de segurança a dados confidenciais: sala do administrador de TI em ambiente aberto;

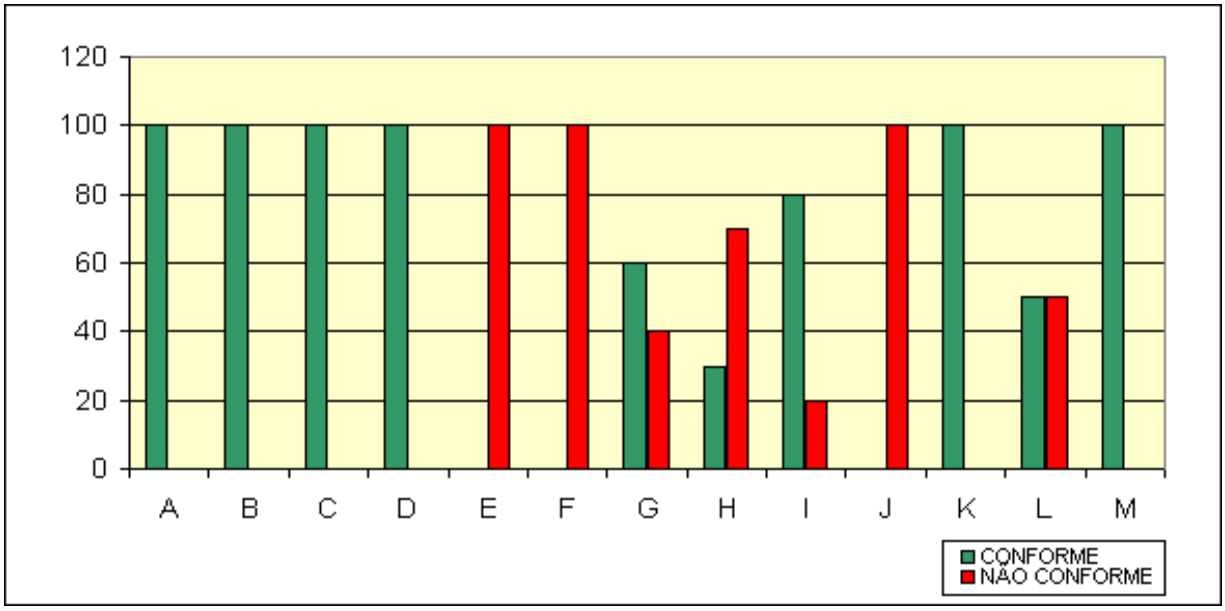
- Providenciar sala devidamente fechada, climatizada e com alarme contra invasão interna ou externa.

- **Instituir política de descarte de equipamentos, dispositivos e documentos em papel que possam conter informações confidenciais** (correspondente ao item (M – quadro 2). **Conforme.**

- Foi evidenciado a política de descarte de equipamentos e dispositivos, para um galpão apropriado para acomodar componentes descartados;

- Documentos em papel contendo informações confidenciais são incinerados.

Para a realização da auditoria em controle de acesso físico foi utilizado a técnica de entrevista como demonstrado no quadro2, o critério utilizado para cada item foi: conforme e não conforme, a figura 6 mostra o resultado da auditoria de cada item.



	A	B	C	D	E	F	G	H	I	J	K	L	M
CONFORME	100	100	100	100	0	0	60	30	80	0	100	50	100
NÃO CONFORME	0	0	0	0	100	100	40	70	20	100	0	50	0

MÉDIA CONFORME	**64%**
MÉDIA NÃO CONFORME	**36%**
TOTAL	**100%**

Figura 6: Gráfico demonstrativo da auditoria em controle de acesso físico e itens relacionados abaixo:

A) Instituir formas de identificação capazes de distinguir um funcionário de um visitante e categorias diferentes de funcionário, se for o caso.

B) Exigir a devolução de bens de propriedade da instituição quando o funcionário é desligado ou demitido.

C) Controlar a entrada e a saída de equipamentos, registrando data, horários e local da visita e, dependendo do grau de segurança necessário, acompanhá-lo até o local de destino.

D) Instituir vigilância no prédio, 24 horas por dia, 7 dias na semana.

e) Supervisionar a atuação da equipe de limpeza, manutenção e vigilância.

F) Não instalar, em áreas de acesso público, equipamentos que possam acessar a rede interna.

G) Orientar os funcionários a não deixarem os computadores sem qualquer supervisão de pessoa autorizada, por exemplo, durante o horário de almoço ou quando se ausentarem de sua sala por tempo prolongado.

H) Encorajar o bloqueio de teclado, a guarda de documentos confidenciais, disquetes, *backups* e laptops em armários com chave, etc.

I) Utilizar mecanismos de controle de acesso físico, tais como fechaduras, câmeras de vídeo e alarmes.

J) Proteger as linhas telefônicas e outros dispositivos de comunicação contra ‘grampo’.

K) Proteger fisicamente os *backups.*

L) Restringir o acesso a computadores e impressoras que manipulem dados confidenciais .

M) Instituir política de descarte de equipamentos, dispositivos e documentos em papel que possam conter informações confidenciais.

8.3 Análise de Controle em Acesso Lógico

Os objetivos do controle de acesso lógico é seguir os princípios para o exercício da segurança lógica, organizacional e confidencialidade, nos momentos do ciclo administrativo (planejamento, execução, controle, auditoria), e nível empresarial (operacional, tático, estratégico) são:

- Estabelecer autoridade aos recursos humanos engajados com as plataformas de informática;
- Assegurar lealdade e proporcionar confiabilidade aos profissionais e usuários de informática da organização;
- Viabilizar meios para o reconhecimento de ações empresariais autorizadas;
- Avaliar o grau de segurança que cada informação requer.

8.3.1 Plano de Ação

- Implementar alterações em processos não conformes e adotar melhorias em processos conformes no controle de acesso lógico, sugeridos por uma possível implantação de uma política da segurança da informação.

- **Conceder acesso aos usuários, apenas aos recursos realmente necessários para a execução de suas tarefas.** (correspondente ao item (A – quadro 3 – APÊNDICE B)). **Conforme.**

- A entidade possui um tipo de serviço de concessão aos usuários, via servidor, utilizando o modelo ERP que modulariza os setores e restringe cada setor para a execução de suas tarefas.

- **Restringir e monitorar o acesso a recursos críticos. .** (correspondente ao item (B – Quadro 3 – APÊNDICE B)). **Conforme.**

- Foi evidenciado que a entidade possui uma política interna para restrição de acesso a recursos críticos.

- A entidade deverá providenciar para que o acesso a recursos críticos seja rastreado pelo administrador de Ti de forma a não propiciar danos a informações criticas da entidade.

- **Utilizar softwares de controle de acesso lógico.** (correspondente ao item (C– quadro 3). **Conforme.**

- Assim como no item acima a entidade utiliza softwares controlando o acesso lógico de usuários em redes internas e externas.

- **Revisar periodicamente as listas de controle de acesso.** (correspondente ao item (D– quadro 3). **Não Conforme.**

- Foi evidenciado que o Administrado de TI não periodicamente as listas de controle de acesso.

- Deverá existir um controle priorizando as listas de controle por ser um processo que pode colocar em risco a segurança da informação.

- **Evitar dar orientações ao usuário durante o processo de *logon.*** (correspondente ao item (E– quadro 3). **Não Conforme.**

- Foi evidenciado junto aos usuários do sistema computacional que nem sempre o administrador de TI evita dar orientações aos seus usuários durante o algum processo de *logon.*

- Deverá existir uma política onde haja concientização do administrado de Ti junto aos usuários para que não incite o usuário a praticar atos ilícitos durante o processo de *logon.*

- **Bloquear a conta do usuário após certo número de tentativas frustradas de *logon.*** (correspondente ao item (F– quadro 3). **Conforme.**

- Foi evidenciado que durante o processo de acesso a rede e ou de *logon*, se o usuário ao tentar acessar o *logon/senha* e errar por 5 (cinco) vezes a mesma operação o sistema bloqueia a conta do usuário.

- **Restringir acesso a determinados periféricos.** (correspondente ao item (G– quadro 3). **Não Conforme.**

- Foi evidenciado durante a entrevista que o administrador de Ti restringi o acesso a determinados periféricos de maneira que venha a atrapalhar e ou atrasar o processo de alguns usuários por necessitarem de um periférico simples como: entrada *usb*

- A maioria dos equipamentos 60% são muito antigos não oferecendo determinados periféricos.

- A entidade deverá providenciar a troca destes equipamentos para que o processo do usuário melhore com esses periféricos.

- Foi evidenciado que existe política interna para restrição de periféricos por usuários usarem de maneira indevida esses periféricos.

- **Fornecer contas apenas a pessoas autorizadas.** (correspondente ao item (H-quadro 3 - APÊNDICE B)). **Conforme.**

- A entidade fornece uma conta por usuário e que estão envolvidas em processos computacionais.

- **Não fornecer a mesma conta para mais de um usuário.** (correspondente ao item (I– quadro 3 - APÊNDICE B)). **Conforme.**

- A entidade possui uma política interna que uma conta não pode possuir dois

usuários, por existir processos internos que podem ser prejudiciais a informação se for usada de forma indevida ou por outro usuário mal intencionado.

- **Ao conceder a conta ao usuário, informa-lo sobre as políticas de senha da organização.** (correspondente ao item (J– quadro 3). **Não Conforme.**

- A entidade não possui uma política de senhas.

- Deverá existir uma política que possa ao conceder uma determinada senha ao usuário informa-lo sobre o risco que pode acontecer a informação se uma senha cair em posse de usuários mal intencionados.

- houve relato de alguns usuários que o administrador de TI as vezes informa o usuário de como usar sua senha de forma devida.

- **Bloquear se possível, a escolha de senhas consideradas frágeis e orientar o usuário na escolha de senhas mais seguras.** (correspondente ao item (K– quadro 3). **Conforme.**

- Foi evidenciado que o administrador de TI orienta os usuários a não escolher senhas frágeis e ou que sejam fáceis de serem rastreadas.

- **Orientar os usuários para não armazenarem senhas em arquivos ou envia-las por e-mail.** (correspondente ao item (L– quadro 3). **Não Conforme.**

- A maioria em quase sua totalidade afirmou que nunca houve uma orientação que suas senhas e ou arquivos não fossem armazenadas.

- O administrador de TI deveria criar uma política interna para orientar seus usuários a não armazenarem esse tipo de informação, por propiciar em uma possível invasão de *ip* e ou arquivos, possam servir de porta de entrada para *hackers* da informação.

- **Armazenar as senhas no sistema sob a forma criptografada.** (correspondente ao item (M -quadro 3). **Conforme.**

- Foi evidenciado que o administrador de TI que todas as senhas são armazenadas e protegidas por criptografia e ou *firewall* contra invasores externos.

- **Prevenir o uso freqüente de senhas já utilizadas pelo mesmo usuário anteriormente.** (correspondente ao item (N – quadro 3). **Conforme.**

- Foi evidenciado que o administrador de TI previne e não autoriza o uso de senhas anteriores pelo mesmo usuário.

- A entidade correria o risco de ser invadida por um antigo usuário que possuíra senha do sistema, tornando a informação vulnerável do usuário atual.

- **Estabelecer um prazo máximo utilização de uma mesma senha.** (correspondente ao item (O – quadro 3). **Não Conforme.**

- Foi evidenciado que a maioria dos usuários de senha 70% utilizam uma mesma senha por um longo período e ou desde seu ingresso na entidade.

- Não existe orientação do administrador de Ti para que atualizem senhas e ou *logon*.

- Deverá existir um treinamento e ou orientação do administrador de TI para que os usuários troquem suas senhas periodicamente para que as senhas não sejam rastreadas por usuário indevido ou não autorizado.

- **Informar os usuários quanto aos perigos de divulgação de senhas.** (correspondente ao item (P – quadro 3). **Conforme.**

- Foi evidenciado que os usuários foram unânimes ao dizer que o administrador de TI informa quanto aos perigos que possam surgir quanto a divulgação de senhas.

- **Impedir que os usuários sejam capazes de ler os arquivos de senha, identificar e trocar senhas de outros usuários.** (correspondente ao item (Q – quadro 3). **Conforme.**

- O administrador de Ti tem por obrigação e objetivo de impedir que usuários de um mesmo sistema ou rede venha a rastrear senhas de outros usuários.

- Como política interna se esta questão vier a acontecer o usuário sofrerá pena de demissão por justa causa.

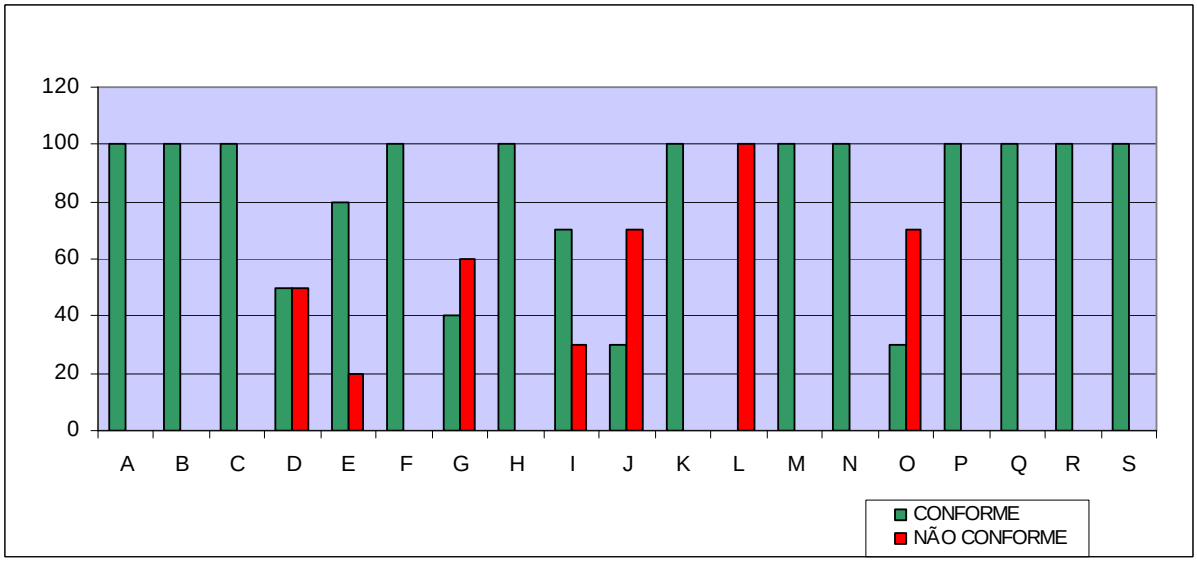
- **Desabilitar contas inativas, sem senhas ou com senhas padronizadas.** (correspondente ao item (R – quadro 3). **Conforme.**

- Foi evidenciado que o administrador de TI desabilita por imediato contas inativas, pelo fato de existir o perigo de usuários mal intencionados venham a utilizar contas habilitadas para fins que contrariem as regras da entidade.

- **Desabilitar as senhas de ex-funcionários.** (correspondente ao item (S – quadro 3). **Conforme.**

- Foi evidenciado que o administrador de TI desabilita por imediato contas inativas de antigos usuários que se desligam da entidade.

Para a realização da auditoria em controle de acesso lógico foi utilizado a técnica de entrevista como demonstrado no quadro 3, o critério utilizado para cada item foi: conforme e não conforme, a figura 7 mostra o resultado da auditoria de cada item.



A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
100	100	100	50	80	100	40	100	70	30	100	0	100	100	30	100	100	100	100
0	0	0	50	20	0	60	0	30	70	0	100	0	0	70	0	0	0	0

MÉDIA CONFORME	**79%**
MÉDIA NÃO CONFORME	**21%**
TOTAL	**100%**

Figura 7: Gráfico demonstrativo da auditoria em controle de acesso lógico e itens relacionados abaixo:

A) Conceder acesso aos usuários, apenas aos recursos realmente necessários para a execução de suas tarefas.

B) Restringir e monitorar o acesso a recursos críticos.

C) Utilizar softwares de controle de acesso lógico.

D) Revisar periodicamente as listas de controle de acesso.

E) Evitar dar orientações ao usuário durante o processo de *logon.*

F) Bloquear a conta do usuário após certo numero de tentativas frustradas de *logon.*

G) Restringir acesso a determinados periféricos.

H) Fornecer contas apenas a pessoas autorizadas.

I) Não fornecer a mesma conta para mais de um usuário.

J) Ao conceder a conta ao usuário, informa-lo sobre as políticas de senha da organização.

K) Bloquear se possível, a escolha de senhas consideradas frágeis e orientar o usuário na escolha de senhas mais seguras.

L) Orientar os usuários para não armazenarem senhas em arquivos ou envia-las por e-mail.

M) Armazenar as senhas no sistema sob a forma criptografada.

N) Prevenir o uso freqüente de senhas já utilizadas pelo mesmo usuário anteriormente.

O) Estabelecer um prazo máximo utilização de uma mesma senha.

P) Informar os usuários quanto aos perigos de divulgação de senhas.

Q) Impedir que os usuários sejam capazes de ler os arquivos de senha, identificar e trocar senhas de outros usuários.

R) Desabilitar contas inativas, sem senhas ou com senhas padronizadas.

S) Desabilitar as senhas de ex-funcionários.

9 RELATÓRIO FINAL

- **Dados da entidade auditada:** A Santos Andirá nasceu da iniciativa dos irmãos Ângelo e Domingos dos Santos. Em Janeiro de 1.961 começava uma jornada vitoriosa, contando com poucas ferramentas, máquinas reformadas e a produção de móveis com operações essencialmente manuais, mas já prevalecia um respeito pelo julgamento maior juiz de qualquer produto: O CLIENTE. A fábrica funcionava na rua Alagoas no município de Andirá, com a razão social de Irmãos Santos e já projetava no comércio moveleiro da região. Em setembro de 1978, a fábrica passou a ter denominação de Indústria e Comércio de Móveis Santos Ltda, ocupando uma área de 4.000 m às margens da BR 369, na entrada de Andirá-PR. Em 1.987 surgiu a atual razão social: SANTOS ANDIRÁ INDÚSTRIA DE MÓVEIS LTDA. É uma das maiores indústrias moveleiras da América Latina e conta hoje com aproximadamente 600 funcionários. Esses colaboradores, altamente treinados e a tecnologia de ponta, proporcionam capacidade produtiva de 420.000 dormitórios/ano.

- **Síntese:** Os principais pontos da auditoria de TI evidenciando segurança física e lógica do ambiente computacional foi verificar a autenticidade dos processos de informática existentes na entidade auditada, para a relevância da auditoria foram identificados pontos positivos e negativos de acordo com a entrevista feita junto ao administrador de TI, o ambiente demonstrou a falta de uma política de segurança da informação consistente que traria obrigatoriedade em se cumprir normas que atualmente são inexistentes na entidade.

- **Dados da Auditoria:** O objetivo da auditoria foi levantar dados existentes no ambiente computacional da entidade, auditoria foi efetuado por um auditor líder Kenion César Michelato Colaço, a metodologia adotada foi a de Entrevista, dividida em três etapas: Planejamento, Execução e Relatório Final, sua natureza foi adotar a auditoria de TI por se tratar de um ambiente computacional.

- **Introdução:** A estrutura hierárquica do departamento de informática da entidade é definida por: 1 Administrador de TI que gerencia e monitora todo o ambiente computacional, 1 Técnico de Informática que auxilia nos processos computacional diários. A entidade possui aproximadamente 100 microcomputadores em rede, todos *logan* do servidor de domínio, 7 servidores, onde estão instalados além do servidor de Domínio (WINDOWS), o de Aplicativo (WINDOWS), os de Banco de Dados (UNIX), e de *Internet* (LINUX). Todas as estações rodam windows, desde 98 ao vista. Os Pc's acessam o sistema ERP, os servidores possuem anti –virus para segurança da informação e monitoramento da rede por software de rastreabilidade. O sistema computacional interagem os setores para que a informação seja processada rapidamente sendo essencial para o processo de produção da entidade.

- **Falhas Detectadas:** As falhas foram identificadas de acordo com a entrevista efetuada sobre cada item do ambiente computacional evidenciando segurança física e lógica, como comentário inicial a falta de uma política para a segurança da informação, justificada pelo administrador de TI. Abaixo serão citadas falhas detectadas durante a auditoria.

Segurança Física: Ambientes computacionais em lugares abertos no departamento de produção com acesso a rede, falta de treinamento aos usuários com relação ao equipamento: ausência do usuário no horário de almoço e ou troca de turno, bloqueio de teclado, guarda de documentos confidenciais, alguns pc's com acesso a rede sem bloqueio de *logon,*as linhas telefônicas e ou outros dispositivos de comunicação não são protegidos contra grampo,

Segurança Lógica: As listas de controles de acesso não são revisadas periodicamente, durante o processo de manutenção de *logon* o administrador de TI não evita orientações ao usuário podendo ter vazamento de informação, restrição a determinados periféricos somente para 60% dos usuários, foi evidenciado o fornecimento de senha para mais de um usuário, falta de orientação aos usuários pela gerencia de Ti para não armazenarem senhas em

arquivos e ou envia-las por *email,* foi evidenciado o não estabelecimento de prazo máximo para utilização de uma mesma senha.

- **Conclusão:** A recomendação final da equipe para a correção de falhas foi sugerir a implantação de uma política da segurança da informação nos parâmetros e exigências da política para que se cumpra de maneira conforme os processos desenvolvimentos pela gerencia de Ti da entidade.

- **Pareceres da Gerência Superior:** A gerencia superior demonstrou satisfação e clareza com relação as condições conformes e não conformes que se encontra a atual situação da entidade, respeitando os achados e recomendando possíveis melhorias junto ao auditor.

10 CONCLUSÃO E TRABALHOS FUTUROS

A segurança está relacionada à necessidade de proteção contra o acesso ou manipulação, intencional ou não, de informações confidenciais por elementos não autorizados, e a utilização não autorizada do computador ou seus dispositivos periféricos. A necessidade de proteção deve ser definida em termos das possíveis ameaças e riscos e dos objetivos de uma organização, formalizada nos termos de uma política de segurança.

Com o presente trabalho foi possível estudar diferentes técnicas de auditoria de tecnologia da informação, e afirmar que quanto mais cedo for implantada uma política de segurança da informação e por conseqüência o ambiente computacional for auditado oficialmente baseando-se em normas específicas para a segurança da informação, melhor será o resultado em melhorias. Pôde-se observar que o compromisso com a segurança da informação é desconsiderada em muitos itens que compõem o ambiente computacional. Dentre os motivos, estão a necessidade de uma política de segurança da informação, para que a entidade siga as normas exigidas por esta política de segurança. Porém, empresas que desconsiderarem a empregabilidade de políticas de segurança certificadas, acabam por sofrer ameaças, ataques e danos irreversíveis para seu ambiente computacional.

Este estudo revela, através dos resultados da auditoria interna, a existência de problemas relacionados com a segurança da informação, que dificultam a rastreabilidade de possíveis danos a informação.

A técnica por entrevistas é um método de auditoria rápida que permite auditar o ambiente computacional utilizado pela entidade. Porém seu resultado não é uma técnica definitiva para auditorias de tecnologia da informação.

Como sugestão para trabalhos futuros, recomenda-se, que após concluir-se a auditoria no ambiente computacional, seja implantada a Política de Segurança da Informação na empresa, uma vez que a informação é um bem de valor intangível, e que não basta apenas estas possuírem meios tecnológicos e informatizados para protegê-las contra danos e ataque internos e externos, desta forma, a Entidade necessita de uma Política de Segurança bem estruturada, com o

objetivo de alcançar a solução que deixe as informações integras e seguras tomando como base a norma de segurança NBR ISSO/IEC 17799/27002.

> “Na implantação de uma política de segurança a primeira tarefa a ser realizada é a definição do que se deseja, fixando-se os objetivos a serem atendidos, definindo-se os meios e recursos necessários, estabelecendo-se as etapas a cumprir e os prazos das mesmas. Só após haver uma avaliação do que é necessário fazer é que se começa a executar o planejado. Ainda assim, o planejado raramente atende todas as situações que aparece, de modo que, frequentemente, a necessidade de acertar desvios de rota ou até mesmo mudar radicalmente o planejado originalmente.”
>
> (CARUSO, 1999).

11 REFERÊNCIAS BIBLIOGRÁFICAS

----------(1994b). *Government auditing standards***:** 1994 revision.

_____ (1990). *Case study evaluations*. Washington.

_____ (1991). *Designing evaluations*. Washington.

_____ (1994a). *Approach and methodology selection workshop***:**

_____. *Qualidade Total em Informática*. 3.ed. São Paulo: Atlas, 1999.

17799:2005: Tecnologia da informação - *código de prática para a gestão da segurança da informação*, 2005.

ALTER, S. *Information Systems: a Management Perspective.* Menlo Park, Califórnia: Benjamin Cummings, 1996.

ALVES, A. Gustavo. *Segurança da Informação* – Uma visão inovadora da gestão. Rio de Janeiro: Ciência Moderna, 2006.

AMOR, D. *A (r)evolução do E-business.* São Paulo: Makron Books, 2000.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT**.** *NBR ISO/IEC.* Atlas, 2002.

BEUREN, I. M. Gerenciamento da Informação: um recurso estratégico no processo de gestão empresarial. São Paulo: Atlas, 1998.

BOYTON, William C.; Johnson, Raymond N; Kell Walter G. *Auditoria.* São Paulo:

BRITO, M. J. *Tecnologia da Informação e Mercado Futuro* – O caso da BM&F.

CARUSO, Carlos Alberto Antônio; STEFFEN, Flavio Deny. *Segurança em informática e de informações*. 2. ed. rev. e ampl. São Paulo: SENAC, 1999. 366 p.

CHORAFAS, D. N. *Implementing and Auditing the Internal Control System*. Great Britain: Palgrave, 2001.

CRUZ, Flávio da. *Auditoria Governamental.* São Paulo: Atlas, 1997.

DIAS, Cláudia. *Segurança e Auditoria da Tecnologia da Informação* –Axel Books do Brasil Editora Ltda, 2000.

FERREIRA, Fernando Nicolau Freitas e ARAÚJO, Márcio Tadeu. *política de segurança da informação*: Guia Prático para Embalagem e Implementação, Rio de Janeiro: Editora Ciência Moderna Ltda., 2006.

GABBAY, M. S**.** *Fatores influenciadores na implementação de ações de gestão de segurança da informação: um estudo com executivos e gerentes de tecnologia da informação em empresas do Rio Grande do Norte.* Tese (mestrado) – Universidade Federal do Rio Grande do Norte, 2003.

GAO (1989). *Content analysis:* a methodology for structuring and analyzing written material. Washington.

GIL, A. L. *Auditoria de Computadores.* 5.ed. São Paulo: Atlas, 2000.

GIL, A. L. *Auditoria de Computadores***.** 5.ed. São Paulo: Atlas, 2000.

< http://www.udesc.br/esag/professores >, Acesso em 28 de Agosto de 2008.

MAGALHÃES, Antônio de Deus F. *Auditoria das Organizações:* Metodologias Alternativas ao Planejamento e à Operacionalização dos Métodos e das Técnicas. São Paulo: Atlas, 2001.

MAÑAS, A. V. Administração de Sistemas de Informação. São Paulo: Érica, 1999.

MENEZES, C. Josué. *Gestão da Segurança da Informação*. São Paulo: Mizuno, 2006.

NETO, Ubiratan. *Dominando Linux Firewall Iptables***.** Rio de Janeiro: Ciência Moderna,

NBR ISO/IEC 17799 – *Tecnologia da Informação:* Código de Prática para a Gestão da Segurança da Informação. Associação Brasileira de Normas Técnicas – ABNT, 2001/2005. Disponível para aquisição no site: <http://www.abnt.gov.br>.

POLLONI, E. G. F. *Administrando Sistemas de Informação*. São Paulo: Futura, 2000.

PRAS, A.; HAZENWINKEL, H.; HENGSTUM, E. *Management of the World-Wide*

SÊMOLA, M. 2003: *Gestão da Segurança da Informação.* 1.Ed. Rio de Janeiro: Campus, 2003.

STAIR, Ralph M. *Princípios de Sistemas de Informação:* uma abordagem gerencial. Rio de Janeiro: Livros Técnicos e Científicos, 1998.

Tecnologia da Informação e Estratégia Empresarial. São Paulo: FEA/USP, 1996.

Thinking in ERP Systems Implementations. 24º Encontro da Associação Nacional dos Programas de Pós-Graduação em Administração. Florianópolis: ENANPAD, 2000.

TRIBUNAL DE CONTAS DA UNIÃO – *Manual de Auditoria de Sistemas* – 1998.

Web. Anais 15ª SBRC, p. 340-345, Maio 1997.

WOOD, T. J.; CALDAS, M. P. *The Part and the Whole: Reductionism an Complex.*

APÊNDICES

APÊNDICE A

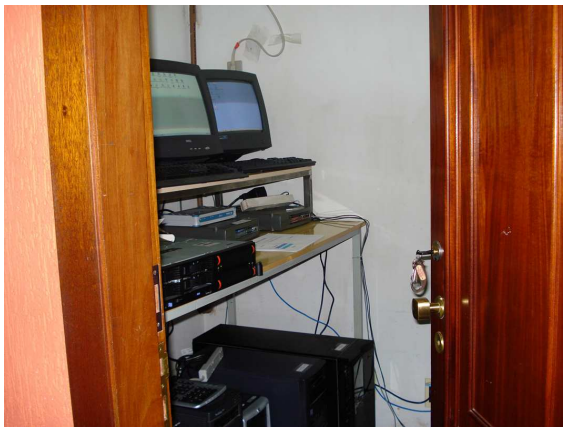
Portaria da Entrada para Identificação: Identificação de entrada e saída de funcionário/visitante.

Portaria da Entrada da Entidade: Vigilância 24 horas (câmeras e guardas armados)

Entrada do setor Administrativo: Vigilância 24 horas câmeras monitoradas por *software*/circuito integrado.

Ambiente Computacional do Setor Industrial: Computadores e Impressoras em ambiente aberto, vulnerabilidade ao equipamento.

Mecanismo de controle de acesso físico:
Câmeras monitoram todo ambiente computacional.

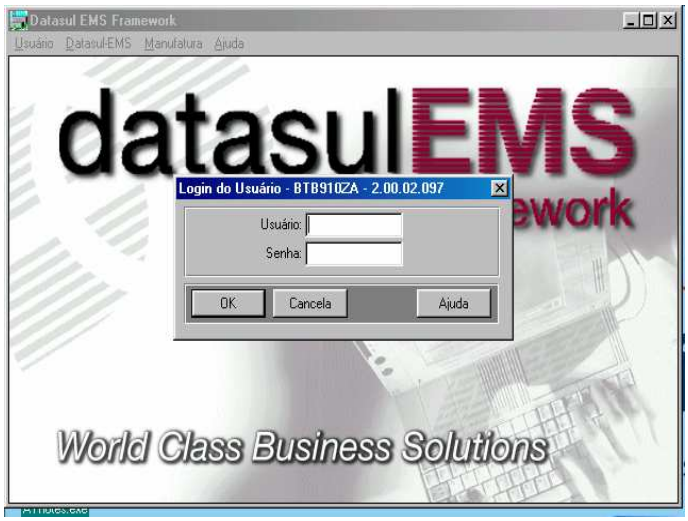


Sala de Backups:
Controle de Acesso a sala de Backup.

Ambiente computacional do setor de produção:
Ambiente aberto sem alarmes ou fechaduras.

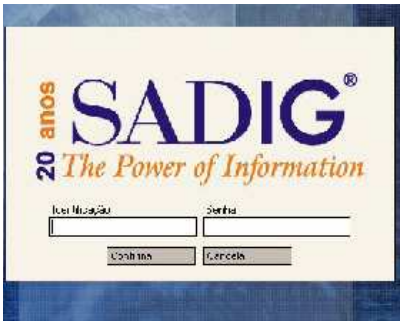
Sala de Monitoração do Administrador de TI:
Ambiente aberto desprotegido de invasão física, perigo a integridade da informação.

APÊNDICE B



Concessão de acesso aos usuários

Controle de *Login* e Senha por usuário.



Restrição e Monitoramento a Recursos Críticos

Acesso restrito a área de Vendas da entidade.

ANEXOS

ANEXO A

Lista de Verificação para Auditoria da Tecnologia da Informação.

ÁREA:	**DIV IN – DIVISÃO DE INFORMÁTICA**
TIPO DE AUDITORIA:	**AUDITORIA DE TI**
DATA DA AUDITORIA:	**23 DE SETEMBRO DE 2008**

EQUIPE DA AUDITORIA (NOME / FUNÇÃO NA EQUIPE)		
KENION CÉSAR MICHELATO COLAÇO		**AUDITOR LÍDER**

Controles de Acesso Físico	**C**	**NC**
A) Instituir formas de identificação capazes de distinguir um funcionário de um visitante e categorias diferentes de funcionário, se for o caso.	**X**	
B) Exigir a devolução de bens de propriedade da instituição quando o funcionário é desligado ou demitido.	**X**	
C) Controlar a entrada e a saída de equipamentos, registrando data, horários e local da visita e, dependendo do grau de segurança necessário, acompanha- lo até o local de destino.	**X**	
D) Instituir vigilância no prédio, 24 horas por dia, 7 dias na semana.	**X**	
E) Supervisionar a atuação da equipe de limpeza, manutenção e vigilância.		**X**
F) Não instalar, em áreas de acesso publico, equipamentos que possam acessar a rede interna.		**X**
G) Orientar os funcionários a não deixarem os computadores sem qualquer supervisão de pessoa autorizada, por exemplo, durante o horário de almoço ou quando se ausentarem de sua sala por tempo prolongado.		**X**
H) Encorajar o bloqueio de teclado, a guarda de documentos confidenciais, disquetes, backups e laptops em armários com chave, etc.		**X**
I) Utilizar mecanismos de controle de acesso físico, tais como fechaduras, câmeras de vídeo e alarmes.		**X**
J) Proteger as linhas telefônicas e outros dispositivos de comunicação contra 'grampo'.		**X**
K) Proteger fisicamente os backups.	**X**	
L) Restringir o acesso a computadores e impressoras que manipulem dados confidenciais .		**X**
M) Instituir política de descarte de equipamentos, dispositivos e documentos em papel que possam conter informações confidenciais.	**X**	

Quadro 2: Lista de Verificação para Controle de Acesso Físico

ANEXO B

Lista de Verificação para Auditoria da Tecnologia da Informação

ÁREA:	**DIV IN – DIVISÃO DE INFORMÁTICA**
TIPO DE AUDITORIA:	**AUDITORIA DE TI**
DATA DA AUDITORIA:	**24 DE SETEMBRO DE 2008**

EQUIPE DA AUDITORIA (NOME / FUNÇÃO NA EQUIPE)		
KENION CÉSAR MICHELATO COLAÇO		**AUDITOR LÍDER**

Controles de Acesso Lógico	**C**	**NC**
A) Conceder acesso aos usuários, apenas aos recursos realmente necessários para a execução de suas tarefas.	**X**	
B) Restringir e monitorar o acesso a recursos críticos.	**X**	
C) Utilizar softwares de controle de acesso lógico.	**X**	
D) Revisar periodicamente as listas de controle de acesso.		**X**
E) Evitar dar orientações ao usuário durante o processo de logon		**X**
F) Bloquear a conta do usuário após certo numero de tentativas frustradas de logon.	**X**	
G) Restringir acesso a determinados periféricos.		**X**
h) Fornecer contas apenas a pessoas autorizadas.	**X**	
I) Não fornecer a mesma conta para mais de um usuário.		**X**
J) Ao conceder a conta ao usuário, informa-lo sobre as políticas de senha da organização.		**X**
K) Bloquear se possível, a escolha de senhas consideradas frágeis e orientar o usuário na escolha de senhas mais seguras.	**X**	
L) Orientar os usuários para não armazenarem senhas em arquivos ou envia-las por e-mail.		**X**
M) Armazenar as senhas no sistema sob a forma criptografada.	**X**	
N) Prevenir o uso freqüente de senhas já utilizadas pelo mesmo usuário anteriormente.	**X**	
O) Estabelecer um prazo máximo utilização de uma mesma senha.		**X**
P) Informar os usuários quanto aos perigos de divulgação de senhas.	**X**	
Q) Impedir que os usuários sejam capazes de ler os arquivos de senha, identificar e trocar senhas de outros usuários.	**X**	
R) Desabilitar contas inativas, sem senhas ou com senhas padronizadas.	**X**	
S) Desabilitar as senhas de ex-funcionários.	**X**	

Quadro 3: Lista de verificação para Controle de Acesso Lógico

ANEXO C

AUDITORIA da TECNOLOGIA DA INFORMAÇÃO em INDUSTRIA MOVELEIRA EVIDENCIA: Segurança da Informação AUDITOR: Kenion

Checklist 001

Empresa: **Indústria de Móveis Santos Ltda** Data **24/09/08** / Hora:**13:00**

Ambiente: [ ] Interno [ ] Externo [**x**] Windows [ ] Linux [ ] Internet

Categoria: [ ]Física [**x**]Lógica [ ]Documentação [ ]Infraestrutura [ ]Comunicação de dados [ ]Informações [ ]Sistemas [ ]Notebook [ ] Senhas [ ]

Processo: **Controle de senhas**

Medida de segurança: **Restringir o uso de *logins* e senhas, por usuário individualmente, permitindo ao usuário *logar* sua senha setorialmente, por ex: Crédito/Cobrança , não sendo possível acessar outro setor.**

Verificação: **A verificação por usuário, é executada por intermédio de um programa de rastreabilidade por usuário/ *login*/ senha.**

Incidente provável: **Invasão indevida de usuário, em setor não autorizado pela gerência de TI.**

Ação requerida: **Investigação do *login*/senha do usuário invasor, conforme normas da entidade, sujeito a demissão por justa causa.**

Resultado esperado:**Conformidade e confiabilidade no uso de *login*/senha por usuário.**

Situação encontrada: **Item em conformidade.**

Eficiente	Deficiente	Ineficiente	Não se aplica
[**X**]	[ ]	[ ]	[ ]

Impacto no negocio

Alto[**X**] Médio[ ] Baixo[ ]

1 Quadro 4: *CheckList*.

ANEXO C

AUDITORIA da TECNOLOGIA DA INFORMAÇÃO em INDUSTRIA MOVELEIRA EVIDENCIA: Segurança da Informação AUDITOR: Kenion

Checklist 001

Empresa: **Indústria de Móveis Santos Ltda** Data **23/09/08** / Hora:**13:00**

Ambiente: [ ] Interno [ ] Externo [**x**] Windows [ ] Linux [ ] Internet

Categoria: [**x** Física [ ]Lógica [ ]Documentação [ ]Infraestrutura [ ]Comunicação de dados [ ]Informações [ ]Sistemas [ ]Notebook [ ] Senhas [ ]

Processo: **Instituir vigilância no prédio, 24 horas por dia, 7 dias na semana.**

Medida de segurança: **A vigilância é feita 24 horas por dia nos 7 dias da semana, pela equipe terceirizada de vigilância fortemente armados e câmeras de segurança por toda entidade.**

Verificação: **Vigilância rotativa por relógio de ponto (hora/hora)**

Incidente provável: **Invasão indevida de usuário, em setor não autorizado pela Vigilância de plantão.**

Ação requerida: **Investigação do *login*/senha do usuário invasor, conforme normas da entidade, sujeito a demissão por justa causa.**

Resultado esperado:**Conformidade e confiabilidade no uso de *login*/senha por usuário.**

Situação encontrada: **Item em conformidade.**

Eficiente	Deficiente	Ineficiente	Não se aplica
[**X**]	[ ]	[ ]	[ ]

Impacto no negocio

Alto[**X**] Médio[ ] Baixo[ ]

Quadro 4: *CheckList*.

ANEXO D

AUDITORIA EM SEGURANÇA DA INFORMAÇÃO	RELATÓRIO DE AUDITORIA INTERNA	CODIGO: RQ- Página 1/1

Auditoria Nº: 002/08 Data: **26/09/2008** SETOR AUDITADO DVIN Responsável: Luiz Fernando Auditor: Kenion
OBJETIVOS DA AUDITORIA
Levantar possíveis não conformidades no Sistema de Gestão Integrado ISO 9001/2000 e 14001/96 , evidenciando Segurança Lógica e Física da Informação.
ITEM AUDITADO
Controle de Senhas.
PONTOS POSITIVOS E NEGATIVOS DA AUDITORIA
Pontos Positivos: As atualizações de controle de senhas estão sendo realizadas de acordo com as mudanças nos procedimentos.
RELAÇÃO DE REGISTROS DE NÃO CONFORMIDADES
O item controle de senhas se encontra conforme os procedimentos exigidos pela entidade.
SUGESTÕES E COMENTÁRIOS DOS AUDITORES
Convém atualizar o treinamento especifico em controle de senhas para usuários do sistema computacional da entidade.
EQUIPE DE AUDITORES
Kenion César Michelato Colaço Auditor lider Nome/Visto:_____ _____ _____ _____

Quadro 5: Relatório de Auditoria Interna.