UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
DEPARTAMENTO ACADÊMICO DE MECÂNICA
CURSO SUPERIOR EM TECNOLOGIA EM MECATRÔNICA INDUSTRIAL

MARLON ARIEL EIZO NAGANO
RONALDO KENJI YOKOO

GESTÃO DE SEGURANÇA: PROTEÇÃO DA INFORMAÇÃO E DO PATRIMÔNIO EMPRESARIAL.

TRABALHO DE CONCLUSÃO DE CURSO

CURITIBA
2011

MARLON ARIEL EIZO NAGANO
RONALDO KENJI YOKOO

GESTÃO DE SEGURANÇA: PROTEÇÃO DA INFORMAÇÃO E DO PATRIMÔNIO EMPRESARIAL.

Trabalho de Conclusão de Curso de graduação apresentado à disciplina de Trabalho de Diplomação do curso Superior de Tecnologia em Mecatrônica Industrial dos Departamentos Acadêmicos de Eletrônica (DAELN) e Mecânica (DAMEC) da Universidade Tecnológica Federal do Paraná – UTFPR, como requisito parcial a obtenção do Título de Tecnólogo.

Orientador: Prof. Luiz Carlos de Oliveira.

CURITIBA
2011

MARLON ARIEL EIZO NAGANO
RONALDO KENJI YOKOO

GESTÃO DE SEGURANÇA: PROTEÇÃO DA INFORMAÇÃO E DO PATRIMÔNIO EMPRESARIAL.

Este trabalho de conclusão de curso foi apresentado no dia 20 de junho de 2011, como requisito parcial para obtenção do título de Tecnólogo em Mecatrônica Industrial outorgado Universidade Tecnológica Federal do Paraná. Os alunos foram arguidos pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado.

_____

Prof. Milton Luiz Poli
Coordenador de Curso
Departamento Acadêmico de Mecânica (DAMEC)

_____

Prof. Dr. Décio Estevão do Nascimento
Responsável pela Atividade de Trabalho de Conclusão de Curso
Departamento Acadêmico de Eletrônica (DAELN)

BANCA EXAMINADORA

_____

Prof.: Luiz Carlos de Oliveira
Orientador

_____

Prof. M. Sc. Edson Sganzerla

_____

Prof. Marcio Augusto Lombardi

RESUMO

NAGANO, Marlon Ariel Eizo; YOKOO, Ronaldo Kenji. **Gestão de Segurança**: Proteção da informação e do Patrimônio Empresarial. 2011. 71f. Trabalho de Conclusão de Curso (Curso Superior de Tecnologia Mecatrônica Industrial), Departamentos Acadêmicos de Eletrônica e de Mecânica, Universidade Tecnológica Federal do Paraná. Curitiba, 2011.

No atual cenário em que as empresas estão inseridas, num mercado competitivo e altamente dinâmico, no qual a tecnologia influencia os resultados econômicos e o desenvolvimento sociocultural, faz-se necessário zelar pelo patrimônio, tendo em vista a permanência de suas atividades no mercado, é importante a preservação de seus ativos. Nas instituições financeiras, o risco está presente e é mais sensível a falhas operacionais e tecnológicas pois a segurança está intimamente ligada a sua imagem. Nesse contexto, vamos analisar a abordagem de segurança de uma instituição financeira quanto à proteção da informação, pessoas e patrimônio, ao comparar as políticas de segurança adotadas por essa instituição com os fundamentos da obra de Mandarini (2005): Segurança Corporativa Estratégica, e o impacto que o sistema praticado de gestão de segurança empresarial possui no cotidiano dos funcionários. As metodologias adotadas envolvem o levantamento de dados relacionados à segurança empresarial e a análise das políticas de segurança praticadas pela empresa que é objeto de estudo desse trabalho. O resultado da pesquisa revela que a área de segurança empresarial é relativamente recente, embora o acervo bibliográfico acerca da matéria seja escasso, o conteúdo vem ganhando forma e tornou-se parte essencial da rotina dos funcionários e que demanda planejamento e a colaboração de todos para o sucesso e sobrevivência da empresa.

Palavras-chave: Proteção da informação. Gestão de segurança corporativa. Mercado financeiro.

ABSTRACT

NAGANO, Marlon Ariel Eizo; YOKOO, Ronaldo Kenji. Security Management: Company Information and Assets Protection. 2011. 71 P. Monograph (Mechatronic Industry Technology), Academy Departments of Electronic and Mechanical. Universidade Tecnológica Federal do Paraná. Curitiba, 2011.

The present scenery that companies are inserted on, in a competitive and highly dynamic market, where all kind of technology influences on the results of economics matters and social culture development demands the patrimony watch over, keeping in sight that it's an essential asset, making the business feasible, consequently, the permanence of its activity in the market. At financial institutions, the risk is present and it`s highly exposed to operational and technological failures, because security is closely connected to its image. In this context, we will analyze de security management policy of a financial corporation by its information, people and assets protection criteria, and compare the security management with the title of Mandarini (2005): Strategic Corporate Security Management, broach the impact of the corporate security policy has upon employee routine. The research mythology was based to gather data from titles connected to corporate security and analyze the security policy of the company studied in this work. The result reveals the subject of corporate security is new, although there is not much information about the matter, the subject gained shape and became closely related to the employees routine and demands planning and cooperation of everybody for the company success and survival

Key-words: information protection, security management; financial market.

LISTA DE GRÁFICOS

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE FIGURAS

LISTA DE ABREVIATURAS

DC	– Diretoria de Controles Internos
DR	– Diretoria de Riscos
DS	– Diretoria de Segurança
RH	– Recursos Humanos
SCorp	– Segurança Corporativa
SGC	– Segurança da Gestão dos Conhecimentos
SGai	– Segurança da Gestão de Áreas e Instalações
SInfo	– Segurança das Informações
SInsu	– Segurança dos Insumos
SOp	– Segurança das Operações
SPlj	– Segurança dos Planejamentos
SSup	– Segurança dos Suportes
STcom	– Segurança das Telecomunicações
STI	– Segurança da Tecnologia da Informação

LISTA DE SIGLAS

ABNT	– Associação Brasileira de Normas Técnicas
ANTT	– Agência Nacional de Transportes Terrestres
BACEN	– Banco Central do Brasil
DAELN	– Departamento Acadêmico de Eletrônica
DPF	– Departamento da Polícia Federal
CEFET-PR	– Centro Federal de Educação Tecnológica do Paraná
CIESP	– Centro das Indústrias do Estado de São Paulo
CIPA	– Comissão Interna de Prevenção de Acidentes no trabalho
CLT	– Consolidação das Leis de Trabalho
CPD	– Central de Processamento de Dados
CPI	– Código de Prevenção de Incêndios
CREA	– Conselho Regional de Engenharia e Arquitetura
DRT	– Delegacia Regional do Trabalho
EJA	– Educação para Jovens e Adultos
EPI	– Equipamentos de Proteção Individual
FEBRABAN	– Federação Brasileira dos Bancos
FIESP	– Federação das Indústrias do Estado de São Paulo
LER	– Lesão por Esforço Repetitivo
MEC	– Ministério da Educação e Cultura
MTE	– Ministério do Trabalho e Emprego
MPAS	– Ministério da Previdência Social
NATELN	– Normas de Apresentação de Trabalhos Acadêmicos do DAELN
NR	– Norma Regulamentadora
ONUDC	– Organização das Nações Unidas sobre Drogas e Crime
SECAD	– Secretaria de Educação Continuada, Alfabetização e Diversidade
SESMT	– Serviço especializado em Engenharia de Segurança e Saúde no Trabalho
SFN	– Sistema Financeiro Nacional
SIPAT	– Secretaria Interna de Prevenção de Acidentes de Trabalho
SST	– Segurança e Saúde no Trabalho
PCMSO	– Plano de Controle Médico de Saúde Ocupacional
PCN	– Plano de Continuidade dos Negócios
PUC-SP	– Pontifícia Universidade Católica de São Paulo
QVT	– Qualidade de Vida no Trabalho

SUMÁRIO

1.0 INTRODUÇÃO

A presente proposta, a ser abordada nesse trabalho de conclusão de curso, analisa o atual cenário da política de gestão de segurança praticada em uma instituição financeira de grande porte, de atuação nacional e internacional, baseado nos conceitos de segurança empresarial da obra de Mandarini (2005): Segurança Corporativa Estratégica e da importância quanto à proteção da informação e do patrimônio empresarial.

As instituições financeiras possuem forte vínculo com a segurança, pois sua imagem remete a esse aspecto: guarda de numerário. A confiança gera valor agregado à empresa, tornando um diferencial frente ao mercado.

Um dano causado por falha na segurança de controle interno[1] poderia arruinar a reputação da empresa, causar-lhe sansões de órgão reguladores ou até mesmo sua falência, como foi o caso do banco francês: Société Générale, que em 2007 sofreu perda de aproximadamente € 4,9 bilhões (cerca de R$ 7,0 bilhões) e uma multa de € 4,0 milhões pelo Banco Central francês em virtude de falha nos procedimentos de controle e verificação interna.

Para regulamentar riscos inerentes às funções bancárias e elevar a solidez financeira do sistema bancário internacional, em 1974 foi estabelecido o Comitê de Supervisão Bancária, constituído pelas autoridades financeiras dos países integrantes do G-10, organização internacional que reúne representantes dos bancos centrais das onze maiores economias do mundo: Bélgica, Canadá, Estados Unidos, França, Itália, Japão, Holanda, Reino Unido, Alemanha, Suécia e a Suíça, esta última incorporada em 1964, mantendo o nome do grupo.

Por esse Comitê, foi instituído o Acordo de Basiléia II (2004), em complemento ao Acordo de Basiléia I (1988), que regulamenta o risco de capital no sistema financeiro. No Brasil, em consonância com esse Acordo, foi publicada a resolução do Banco Central do

[1] De acordo com a FASB (Financial Standards Board), **controle interno** consiste num conjunto de políticas e procedimentos que são desenvolvidos e operacionalizados Accounting para garantir razoável certeza acerca da confiança que pode ser depositada nas demonstrações financeiras e nos seus processos correlatos. (WIKIPÉDIA, 2007)

Brasil - Bacen 3.380 referindo-se a gestão de risco e a estrutura de gerenciamento de risco operacional. (CONTROLES INTERNOS, 2008).

A arquitetura organizacional de controle e gerenciamento de riscos e segurança da instituição analisada neste trabalho está disposto conforme a Figura 01:

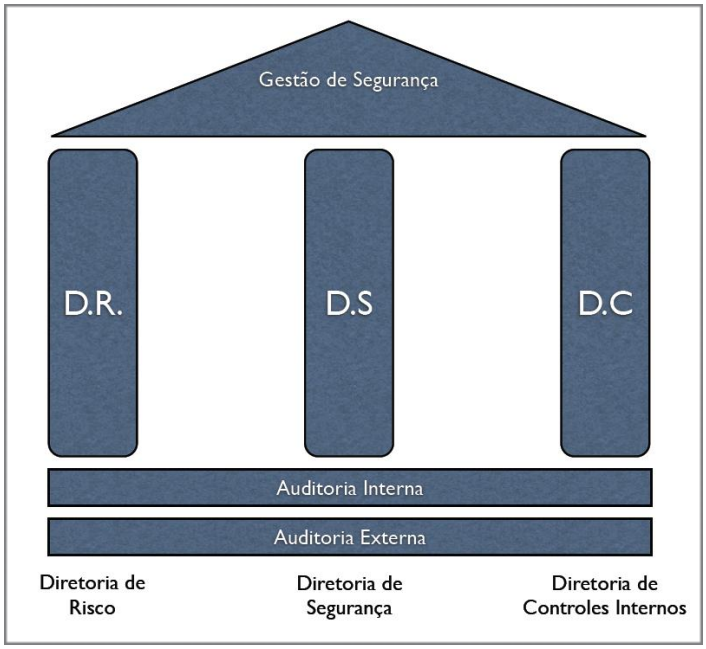

Figura 01: Segurança Corporativa - Gestão de Segurança.
Fonte: Adaptado de Gestão de Segurança (2009, p. 26).

Conforme arquitetura organizacional da empresa analisada, disposto em normativo interno, está vinculada diretamente à Presidência: diretoria de controles internos, diretoria de estratégia e organização, diretoria de gestão de segurança, diretoria jurídica e diretoria de marketing e comunicação. Subordinadas a Vice-Presidência de crédito, controladoria e risco global: a diretoria de gestão de riscos, diretoria de controladoria, diretoria de crédito, diretoria de reestruturação de ativos operacionais e contadoria. Assim, ficam estabelecidos os pilares que compõem a gestão de segurança.

No aspecto de supervisão, em 2002, foi instituída a lei SARBANNES-OXLEY, nos Estados Unidos. O que, de acordo com Gomes e Junior (2007), confere à governança corporativa a responsabilidade de transparência na gestão empresarial a fim de evitar fraudes, além de estabelecer rotinas de auditoria e segurança.

Todas as organizações que operam na bolsa de valores de Nova York, NYSE deverão cumprir a referida lei:

> "A lei SOX teve grande influência em empresas de capital aberto nos Estados Unidos, pois são obrigadas a cumpri regras com mais rigorosidade, proporcionando transparência e credibilidade para com os investidores." (SILVA et al. 2011, p13).

Os planos de segurança armada, no Brasil, estão condicionados a aprovação do Departamento da Polícia Federal, conforme disposto na Lei 7.102/83, portaria 387/2006 – DPF, a qual também regula os serviços de vigilância armada e bancária.

Em relação à proteção de pessoas e ambientes cumprem-se os dispositivos das Normas Regulamentadoras (NR) - Ministério do Trabalho e Emprego (MTE), sugestões de verificação da Secretaria de Segurança e Saúde no Trabalho (SSST).

Dado o exposto, conforme Mandarini (2005), "o financiamento da atividade de segurança não é um mero desembolso; trata-se, na verdade, de inequívoco e compensador investimento no próprio negócio".

1.1 Objetivos

1.1.2 Objetivo Geral

Analisar a abordagem da gestão de segurança de uma instituição financeira quanto à proteção da informação, pessoas e patrimônio.

1.1.3 Objetivos Específicos

Analisar as práticas adotadas para proteção da informação, pessoas e patrimônio;

Apresentar a importância Disseminação da cultura de gestão de controles internos e de segurança, no processo de conscientização dos funcionários quanto aos fatores que eventualmente gerem riscos operacionais e à saúde;

Relatar impactos no mercado, risco de imagem e aspectos legais pertinentes a política de gestão na Segurança e Qualidade de Vida no Trabalho.

1.2 Metodologia

A concepção do trabalho obedecerá algumas etapas, apresentadas com maiores detalhes na sequência.

1.2.1 Pesquisa bibliográfica

Levantamento de referenciais bibliográficos pertinentes ao tema: Gestão de segurança no trabalho, abrangendo literaturas específicas (livros), trabalhos acadêmicos (mestrados, artigos) e manuais (cartilhas).

1.2.2 Desenvolvimento

Relato histórico dos avanços e desenvolvimento da gestão de segurança e técnicas adotadas no segmento bancário, forças trabalhistas (sindicatos), regulamentações oficiais (leis), acidentes causados por negligência/falha no ambiente de trabalho, garantias, medidas preventivas, exigências (serviços/licitações).

1.2.3 Análise

Relevando-se a imagem e a importância social da empresa no mercado, analisando o atual sistema de gestão de segurança desempenhado no ambiente de trabalho, baseado no modelo de gestão de segurança corporativa estratégica, sugerida por Mandarini (2005), distribuindo em quatro segmentos da gestão de Segurança Corporativa (SCorp), os quais são processos essenciais desenvolvidos pela empresa: áreas e instalações, conhecimentos, recursos humanos e processos.

1.2.4 Documentação

Será elaborada a documentação detalhada da pesquisa efetuada, bem como eventuais tabelas, dados técnicos obtidos que venham a beneficiar o conteúdo desse trabalho. As formatações seguirão conforme as normas exigidas pelo Departamento Acadêmico de Eletrônica (DAELN) e as Normas de Elaboração de Trabalhos Acadêmicos da Universidade Tecnológica Federal do Paraná.

1.3 Justificativa

A atual dinâmica no qual as empresas estão submetidas exige de seus dirigentes ações que reafirmem o seu compromisso social, econômico e ambiental, pois influenciam na imagem da companhia, evitam desgastes do nome da organização com ações trabalhistas/sindicais e órgão fiscalizadores, e estabelecem um diferencial frente à concorrência.

Com o desenvolvimento da tecnologia, houve também a expansão e a modernização do crime organizado, não sendo uma preocupação somente da sociedade, mas também das empresas e do governo.

Viu-se a necessidade de estabelecer parâmetros mensuráveis para o cálculo de risco, no intuito de proteger os ativos e prevenir possíveis perdas devido às falhas/fraudes operacionais, oriundas de agentes internos à organização, ou a ações criminosas de agentes externos, que poderiam causar potenciais danos financeiros.

Neste contexto, o modelo de gestão praticada pela empresa afetará significativamente o seu desempenho e resultados econômicos, somando-se a dinâmica do mercado, serão demandadas constantes reavaliações desses modelos, tendo em vista o plano de continuidade nos negócios[2] e sua permanência de atuação no mercado.

[2] "O Plano de Continuidade de Negócios (PCN), o qual é a tradução de Business Continuity Plan (BCP), é o desenvolvimento preventivo de um conjunto de estratégias e planos de ação de maneira a garantir que os serviços essenciais sejam devidamente identificados e preservados após a ocorrência de um desastre*, e até o retorno à situação normal de funcionamento da empresa dentro do contexto do negócio do qual ela faz parte." (WIKIPÉDIA, 2011).

2.0 GESTÃO DE SEGURANÇA CORPORATIVA

2.1 Abordagem

Como contextualizado anteriormente, as instituições financeiras possuem forte vínculo com segurança, pois são guardiões do sigilo bancário e responsáveis pela aplicação de recursos captados de seus clientes, tendo a obrigação de, quando for solicitado, devolver os valores depositados.

A fim de garantir transparência nas atividades envolvidas e controle de recursos, as empresas estão sobre forte supervisão de órgãos reguladores e fiscais nacionais e internacionais, seguindo elevados padrões de governança corporativa.

Porém, não é apenas com a gestão da guarda de numerário que um banco deve se preocupar. Como toda empresa, faz-se necessária a adoção de uma política de gestão de segurança que englobe os recursos humanos, áreas e instalações, operações e informações, com o intuito de proteger seus ativos, sejam eles tangíveis ou intangíveis, como pode ser observado na Figura 02.

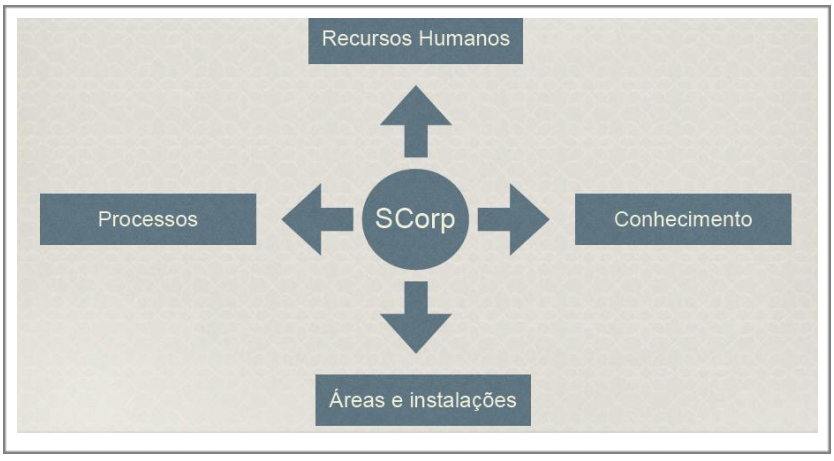

Figura 02: Estratégia da Segurança Corporativa
Fonte: Mandarini (2005, p.84)

A conscientização e modernização da sociedade e da tecnologia contribuíram para que as companhias também desenvolvessem a corresponsabilidade pela saúde e bem estar de seus funcionários. Devendo atender exigências normativas por órgãos reguladores, como o Ministério do Trabalho e Emprego (MTE) por meio das Normas Regulamentadoras (NR) e ações/acordos sindicais.

2.2 Segurança da Gestão de Áreas e Instalações (SGai)

2.2.1 Aspectos Legais

A gestão de segurança não pública começou a ser discutida e ganhar forma, no Brasil, no fim da década de 60, e que de acordo com Lima (2010), pela incapacidade de o Estado gerir de modo adequado à segurança pública e, principalmente, a bancária. Por esse motivo, foi delegado aos bancos implementarem a sua própria gestão de segurança.

Por não possuírem recursos necessários, essas instituições extinguiram de seu quadro orgânico os setores de segurança armada e optaram pela terceirização desse serviço. Nesse momento, verificou-se que era preciso regulamentar as atividades da segurança privada.

O Departamento da Polícia Federal ficou responsável pela fiscalização da segurança armada, de acordo com a Lei n˚ 9.017/95, nas empresas que adotarem esse tipo de vigilância. Para Moretti (2006), o Ministério da Justiça promoveu melhoras implacáveis quanto às normas de capacitação e atuação da segurança privada no Brasil, pela publicação da Portaria 387/2006 DPF, em 28 de agosto de 2006.

Conforme a divisão do autor, Mandarini (2005), os principais tópicos que são de interesse da Segurança da Gestão das Áreas e Instalações (SGai) são:

- Localização;
- Acesso;
- Iluminação;
- Prevenção e combate a incêndio.

2.2.1.1 Localização

Deverá ser dispensado tratamento diferenciado às instalações que estejam localizadas em áreas de risco, pois os índices de criminalidade são diferentes em toda a extensão geográfica do país. Seja pela especificidade nos procedimentos de segurança, dotação de funcionários, guarda de numerário, trabalho em conjunto com a polícia local.

> (...) atualizado o perfil social, econômico e até político da vizinhança e dos arredores, via controle de indicadores - por exemplo, principais ilícitos, lideranças e facções criminosas atuantes na área, principais lideranças comerciais, comunitárias e políticas - é imprescindível o estabelecimento de relações cordiais com os departamentos de segurança de outras empresas (...) (MANDARINI, 2005, p.98).

Conforme disseminado pela empresa via Universidade Corporativa, pela Diretoria de Segurança (DIGES), releva-se as condições naturais do local onde a empresa está instalada, como ocorrência de enchentes, terremotos, furacões, atividades que possam impedir a continuidade das atividades da empresa, bem como elaborar planos de contingência para que a administração possa rapidamente avaliar os danos/prejuízos causados e agilizar os processos de recuperação para a retomada das atividades.

2.2.1.2 Acesso

O controle de acesso tem por base permitir o trânsito de pessoas e veículos a um determinado ambiente da instituição. Os critérios adotados para que esse controle seja efetivo dependerá de como a administração planejar e implementar as soluções de segurança por ela escolhidos.

A SGai preocupa-se com a proteção do ambiente físico da empresa para, principalmente, evitar danos aos ativos que devem ser preservados.

> (...) atos de sabotagem, depredações, acidentes, mau uso deliberado ou imperícia, imprudência, negligência, roubo, furto, desvio - enfim, qualquer ação deliberada ou não com potencial para causar dano patrimonial. (MANDARINI, 2005, p.93).

Assim, a prioridade de monitoramento e controle encontra-se nas áreas consideradas sensíveis, ou seja, aquelas onde estão localizados os projetos classificados como segredos da empresa, locais onde estão instalados componentes críticos para o normal funcionamento da corporação como: banco de dados, servidores, Central de Processamento de Dados (CPDs),

ou onde estejam estocados/armazenados itens altamente periculosos: ogivas nucleares, artifícios inflamáveis, radioativos, tóxicos ou de altíssimo valor patrimonial: obras de arte, joias, lingotes de ouro.

Os itens sugeridos para monitorar, controlar ou impedir o acesso a áreas e instalações, conforme alguns itens previstos nas normas da Polícia Federal relativas à segurança bancária e Mandarini (2005), são:

- Portarias;
- Cancelas;
- Portões;
- Guaritas;
- Catracas;
- Leitores biométricos.

2.2.1.3 Iluminação

É de interesse da SGai, como prega o autor Mandarini (2005), o planejamento da iluminação dos setores da empresa, todo o seu circuito desde a disposição das lâmpadas de emergência, da operacionalização dos geradores de energia até os responsáveis por sua manutenção.

Ao dificultar ações que possam prejudicar a segurança do RH e a proteção patrimonial contra agentes criminosos, tais como:

- Prejudicar a captura de imagem das câmeras de segurança;
- Desativar dispositivos de segurança (alarmes, sensores, portas);
- Facilitar atos de fraude e furtos;
- Ligações clandestinas em fiações.

A correta iluminação em locais de trabalho é de responsabilidade da SGai para que haja o desempenho das atividades de trabalho sem interrupções, a visibilidade sem prejuízo à saúde dos funcionários e a melhor utilização da luz natural nos ambientes.

2.2.1.4 Prevenção e Combate a Incêndios

É de interesse da SGai o planejamento quanto à prevenção e combate a incêndios, uma vez que há riscos contra o patrimônio e os ativos da empresa.

O processo de evacuação e condução de pessoal deve ser executado por funcionários capacitados, de acordo com as recomendações do Serviço Especializado em Engenharia de Segurança e Medicina no Trabalho (SESMT), e, conforme Mandarini (2005), é quando a SGai deve participar com mais intensidade, bem como a instalação e localização dos dispositivos contra incêndios (alarmes, extintores, mangueiras, sensores) e esses devem passar por manutenção, checagem e troca para que estejam em perfeito funcionamento quando acionados.

De acordo com normativo interno da instituição financeira analisada nesse trabalho, todos os projetos e arquitetura e urbanismo devem estar em conformidade com as exigências das normas de segurança previstas pelo Conselho Regional de Engenharia e Arquitetura (CREA), Associação de Brasileira de Normas Técnicas (ABNT) e Código de Prevenção de Incêndios (CPI), procedimentos regulamentados em instruções corporativas internas.

2.2.2 Monitoria de acesso em instituições financeiras

Os níveis de classificação de acesso aos ambientes internos são baseados na Teoria dos Círculos Concêntricos, sugerido por Mandarini (2005), em que a criticidade do acesso ao ambiente vai do mais baixo ao mais elevado, do circulo periférico ao central, respectivamente, como pode ser observado na Figura 03:

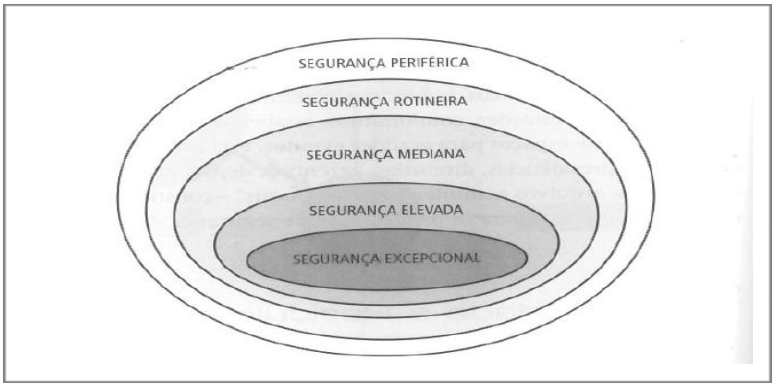

Figura 03: Teoria dos Círculos Concêntricos
Fonte: Mandarini (2005, p.92)

As estações de trabalho, dados, arquivos, salas de diretorias, unidades administrativas, táticas e estratégicas, ou qualquer outro ambiente interno de uma organização em que, caso ocorra o vazamento de informação sigilosa, haverá graves danos econômicos para a empresa, são consideradas sensíveis.

Em virtude da especificidade do assunto, os gerentes responsáveis pelo departamento devem determinar o nível de acesso, salvo os casos já padronizados por normativo da empresa que devam ser observados por todo o conglomerado.

> A determinação do tipo e do grau de criticidade do risco ou ameaça a que se submete cada área ou instalação, a aplicação da metodologia de avaliação e a formalização de um diagnóstico constituem a essência da SGai. (MANDARINI, 2005 p.93).

Deve-se também evitar estabelecer níveis de acesso não compatíveis com o que deveria ser determinado. Por exemplo: o controle de acesso a uma biblioteca não pode ser o mesmo praticado em um CPD, pois possuem finalidades diferentes.

a) Excepcional: áreas de excepcional sensibilidade/ periculosidade, de acesso restrito ao pessoal estritamente envolvido com as atividades afim;

b) Elevada: áreas de elevada sensibilidade/ periculosidade, de acesso ao pessoal intimamente envolvida com as atividades afim;

c) Mediana: áreas de mediana sensibilidade/ periculosidade, de acesso ao pessoal relacionado as atividades afim;

d) Rotineira: áreas de baixa sensibilidade/ periculosidade, de acesso as pessoas que precisam de trato funcional as atividades ali desenvolvidas;

e) Periférica: áreas isentas de sensibilidade/ periculosidade, que estão dentro dos limites do perímetro da instituição.

Quadro 01: Gradação de Segurança para as áreas.
Fonte: Mandarini (2005, p.93)

Conforme normativo interno da empresa analisada, todos os funcionários/colaboradores devem estar devidamente identificados nas dependências do conglomerado quando estiverem desempenhando suas funções, dentro da jornada de trabalho. A identificação não autoriza o acesso irrestrito a todos os ambientes internos da empresa. Há instalações em que apenas os funcionários que desempenham as atividades-fim podem acessar.

Nesse caso, são utilizados dispositivos de identificação, como: teclado para coleta de senhas, leitores biométricos e cartões de acesso.

Figura 04: Leitor Biométrico com coleta de senha
Fonte: Trade Informática (2010)

Assim, a política de Segurança da Gestão das Áreas e Instalações (SGAI) assume um caráter preventivo contra o patrimônio físico causado pelo uso indevido de informações, espionagem, sabotagem, depredação, furtos, que possam acarretar danos patrimoniais.

Reforça Mandarini (2005) que outros recursos além do controle de acesso devem ser empregados a fim de inibir ou desencorajar tentativas que vão contra os bens tangíveis. Por exemplo, o uso dos instrumentos abaixo descriminados:

Figura 05: Porta Giratória Banco do Brasil - Porto Alegre
Fonte: G1 Globo (2007)

A porta giratória faz parte da exigência legal para instituições financeiras, com fulcro portaria 387/2006, Capítulo V, Art. 62 inciso IV e Art. 67 (Departamento da Polícia Federal). Ratificado pela Febraban, é um instrumento de proteção física visa evitar a entrada de materiais metálicos lesivos a segurança pessoal, além de retardar a ação dos criminosos.

Os portais, ao contrário das portas giratórias, possuem caráter informativo, não impedindo o acesso de pessoal munido de acessórios metálicos.

Figura 06: Portal Detector de Metais
Fonte: Dectamax (2010)

Esses são alguns exemplos de equipamentos que uma organização pode utilizar para proteger-se de acessos de usuários ou funcionários munidos de instrumentos metálicos lesivos a segurança de pessoas.

Dispositivos de identificação e monitoria utilizados são os Circuitos Fechados de Televisão (CFTV), de presença obrigatória nas instituições financeiras, conforme exigência do departamento da polícia federal, 387/2006, Capítulo V, Art. 62, inciso III. Tais dispositivos são empregados em diferentes setores da economia como: supermercados, shopping centers, aeroportos, lojas em geral, centros universitários, fábricas, museus, entre outros. Conforme disseminado pela Universidade Corporativa da instituição financeira analisada, identificam os agentes causadores de ocorrências irregulares: furtos, depredações, invasões, fraudes. Para Uvo (2011), em matéria publicada pela Administradores: Empresas reforçam segurança para inibir assaltos:

> Ter um sistema de segurança reforçado resolve porque minimiza riscos, reprime a ação de determinado criminoso e mesmo quando o crime é inevitável, existe a possibilidade de identificação dos criminosos.

De acordo com o disposto no normativo interno do banco analisado, a redação do Plano de Segurança é de responsabilidade da empresa de Segurança contratada que atende a dependência, e a sua aprovação está condicionada a fiscalização e o parecer favorável da Polícia Federal.

Com essas implementações, verificou-se que houve redução nos índices de assaltos em instituições financeiras, como pode ser observada na tabela abaixo, divulgado a imprensa pela Federação Brasileira de Bancos (FEBRABAN[3]).

[3] A **FEBRABAN** - Federação Brasileira de Bancos é a principal entidade representativa do setor bancário brasileiro. Foi fundada em 1967 para fortalecer o sistema financeiro e suas relações com a sociedade e contribuir para o desenvolvimento econômico e social do País.
O objetivo da Federação é representar seus associados em todas as esferas – Poderes Executivo, Legislativo e Judiciário e entidades representativas da sociedade – para o aperfeiçoamento do sistema normativo, a continuada melhoria da produção e a redução dos níveis de risco. Também busca concentrar esforços que favoreçam o crescente acesso da população em relação a produtos e serviços financeiros. (Federação Brasileira dos Bancos)

Tabela 01: Número de ocorrências de assaltos em bancos

Ano	Ocorrências
2000	1.903 assaltos
2001	1.302 assaltos
2002	1.009 assaltos
2003	886 assaltos
2004	743 assaltos
2005	585 assaltos
2006	674 assaltos
2007	529 assaltos
2008	509 assaltos
2009	430 assaltos

Fonte: Sindicato dos Bancários de Florianópolis (2010)

Medidas preventivas de segurança colaboram para desmotivar ações de assaltos e ajudam a manter níveis aceitáveis de risco contra o patrimônio empresarial. Aliado à capacitação dos funcionários, sendo eles orgânicos a empresa ou terceirizados, em relação à mobilização para preservar os ativos corporativos.

> A prevenção de incidente de segurança relativo a pessoas, ativo físicos e financeiros, imagem e informação, melhora a avaliação da eficiência operacional dos processos vinculados a esses fatores, quando comparam-se itens como custo do processo, possibilidades de perda e o resultado esperado. Evitar ilícitos, em ambientes físicos ou virtuais, e garantir a disponibilidade de negócios e serviços impactam diretamente o resultado, objetivo maior da empresa. (GESTÃO DE SEGURANÇA, 2008. P. 17).

Na empresa, objeto desse trabalho, a disseminação dos conceitos de preservação do patrimônio e de segurança ocorre por meio de cursos auto-instrucionais, provas de certificação interna. Estas são um incentivo para ampliar a participação dos funcionários na gestão corporativa, nos aspectos negociais e administrativos, e por normas internas, o que padroniza procedimentos para controle e verificação dos recursos de cada unidade do conglomerado.

2.3 Recursos Humanos/ Segurança e Saúde no Trabalho

2.3.1 Contexto

No cenário tecnológico atual onde os setores da economia submetem-se a acirrada competição nos negócios, resultado do capitalismo e modernização da sociedade e da informatização, reflete a vivência de uma nova era intitulada como do conhecimento, sucessora a era industrial.

A diferença é, conforme Mandarini (2005), que na era do conhecimento o foco principal está no cliente. A busca pela satisfação desses clientes agrega valor aos produtos e serviços, em necessidade as constantes melhorias relacionadas à qualidade e a imagem da empresa, e que de acordo com Lastres e Albagli (1999), modificou os processos organizacionais em busca da satisfação de necessidades de cada cliente e a constante cadência dos preços para fazer frente à concorrência.

A dinâmica sofreu sensíveis alterações, as mudanças são rápidas, a criatividade substituiu estruturas inflexíveis de gestão, abrindo espaço para a valorização do trabalho em equipe, do ponto de vista de Terra (2009, p.3), em seu artigo Gestão da Criatividade, “as empresas estão sendo obrigadas a reinventarem-se para poder crescer”, e que “a criatividade agrega valor ao conhecimento”.

Junto com o desenvolvimento e a maleabilidade que essa nova era trouxe, houve a modernização do crime. O crime organizado movimenta cerca U$ 500 bilhões por ano, segundo estimativa publicada no site oficial da Organização das Nações Unidas sobre Drogas e Crime (ONUDC[4]).

[4] O Escritório das Nações Unidas sobre Drogas e Crime (UNODC) implementa medidas que refletem as três convenções internacionais de controle de drogas e as convenções contra o crime organizado transnacional e

Sem políticas de segurança adequadas, o crime poderia neutralizar o desenvolvimento econômico de um país. Reafirmado na obra didática de capacitação interna da empresa analisada, desenvolvido pela Diretoria de Gestão de Segurança (DIGES), Universidade Corporativa (2009), a gestão estratégica de segurança também precisou sofrer alterações, deixando de ser uma atividade segregada a um único departamento da empresa, estendendo a responsabilidade a todos os seus funcionários.

A preocupação com a segurança é inerente ao desenvolvimento humano e sempre esteve presente ao longo da história da sociedade. Tratando-se de saúde e qualidade de vida no trabalho, denotou-se que a intervenção de órgãos reguladores e do próprio estado nas empresas é recente.

Segundo relatos históricos, a insalubridade e periculosidade no ambiente de trabalho acentuaram-se com o êxodo rural, na transição do feudalismo para a primeira revolução industrial, onde ocorreu o crescimento exponencial da população dos grandes centros urbanos, causando o excesso de mão de obra não especializada. Para Junior (2004), os operários camponeses não tiveram capacitação de como manusear os equipamentos fabris e nem estavam preparados para exercerem atividades repetitivas.

No cenário industrial da época, início século XVIII, o trabalho infantil era comum, segundo Kassouf (2005), agravada pela capacidade econômica dos trabalhadores da época para custear as despesas de suas famílias, impedia que o próprio trabalhador pudesse investir nas melhorias de condições de trabalho, tanto que os índices de acidentes entre as crianças eram elevados.

---

contra a corrupção. O trabalho do UNODC está baseado em três grandes áreas: saúde, justiça e segurança pública. Dessa base tripla, desdobram-se temas como drogas, crime organizado, tráfico de seres humanos, corrupção, lavagem de dinheiro e terrorismo, além de desenvolvimento alternativo e de prevenção ao HIV entre usuários de drogas e pessoas em privação de liberdade. (Escritório das Nações Unidas Sobre Drogas e Crime).

Figura 07: Trabalho infantil sem as mínimas condições de segurança
Fonte: Planeta Educação (2008)

No Brasil, a implantação de políticas voltadas para a prevenção e combate aos acidentes de trabalho veio tardiamente, com o objetivo de reverter à imagem do país perante o mundo ao assumir a liderança nos índices de acidentes de trabalho, em 1972, de acordo com o Instituto Brasileiro de Geografia e Estatísticas (IBGE).

Descrito no: Manual Prático de Legislação de Segurança e Medicina no Trabalho (2003), desenvolvido pela Federação das Indústrias de São Paulo (FIESP) e o Centro das Indústrias do Estado de São Paulo (CIESP), a partir da década de 70, ao iniciar os estudos e discussões a respeito do tema de segurança do trabalho, originou-se o Serviço Especializado em Engenharia de Segurança e Medicina no Trabalho (SESMT), genuinamente brasileira e de referência mundial, contribuiu para o desenvolvimento da Comissão Interna de Prevenção a Acidentes (CIPA), a qual já era prevista no decreto Lei 7.036, 10 de novembro de 1944.

2.3.2 Gestão de Segurança no R.H

Conforme Mandarini (2005), a Gestão de Recursos Humanos e Áreas e instalações estão presentes em todas as empresas. Portanto, faz-se necessário conhecer o perfil dos funcionários que reúnam características não lesivas ao quadro e ao patrimônio empresarial, utilizando os recursos e critérios de seleção da gestão de pessoas.

> [...] gestão de pessoas é a função que permite a colaboração eficaz das pessoas e empregados, funcionários, recursos humanos, talentos ou qualquer outra denominação utilizada para alcançar os objetivos organizacionais e individuais. (CHIAVENATO, 2004, p.10).

Alguns casos não são filtrados pela segurança de R.H, o que não implica na incompetência das políticas adotadas pela empresa, sendo consideradas ocorrências isoladas, como algumas ocorrências apresentadas no quadro abaixo:

a) Jérôme Kerviel - operador do Banco francês *Société Generale,* que causou prejuízos milionários a empresa em decorrência de fraude e descumprimento de normativos e controles internos;

b) Carlos Estevan de Brito - funcionário da Petrobrás, causa prejuízo de R$ 1 milhão a empresa por roubo e desvio de materiais em 2009;

c) Nicholas Leeson - operador do banco inglês *Barings*, levou a empresa a falência em 1995 em virtude de prejuízos acumulados no mercado de ações.

Quadro 02: Fraudes e falhas na segurança
Fonte: Adaptado de Universidade Corporativa BB (2008, p. 12).

No intuito de reduzir a admissão de pessoal com características indesejáveis, a gestão de segurança de R.H deve estabelecer critérios no exame e seleção dos candidatos. Relacionamos algumas características citadas por Mandarini (2005), no quadro abaixo:

a) pessoas que sofrem de dependências químicas (drogas, entorpecentes, álcool);

b) pessoas com comportamentos compulsivos (organização, pontualidade, etc);

c) pessoas com comportamento desleixado, reacionário, com excesso de destemor);

d) jogadores inveterados, apostadores compulsivos, perdulários, etc;

e) pessoas violentas, maus hábitos, errantes;

Quadro 03: Contratação quando identificados os perfis apresentados
Fonte: Mandarini (2005, p.132)

Esses foram alguns exemplos que a estratégia de segurança de RH deve desenvolver na fase de recrutamento. Existem cuidados específicos durante todo o histórico do funcionário

na empresa: na admissão, efetivação, demissão/desligamento e na aposentadoria que podem ser encontrados em bibliografias especializadas na condução de políticas de segurança de recursos humanos, dada a extensão do assunto.

2.3.3 Especificidades do banco analisado

Por tratar-se de empresa em que a União detém controle de acima de 50% do capital acionário, a contratação de pessoal se dá através de concurso público. BRASIL, Constituição Federal (1988). **Capítulo V - Da Administração Pública, Art. 37. Inc. II.**

> **II** - a investidura em cargo ou emprego público depende de aprovação prévia em concurso público de provas ou de provas e títulos, de acordo com a natureza e a complexidade do cargo ou emprego, na forma prevista em lei, ressalvada as nomeações para cargo em comissão declarado em lei de livre nomeação e exoneração.

Observa-se, pelos editais de abertura do concurso, que há o estudo da vida regressa dos candidatos como: a análise de certidões negativas nos cartórios de polícia municipais e estaduais, folha de antecedentes junto à polícia federal, a atual situação do candidato perante a legislação eleitoral, além da compatibilidade cadastral junto às instituições de proteção de crédito, a fim de desempenhar atividades bancárias.

> Um dos fatores que mais influenciam a eficiência das instituições é o recurso humano (RH) empregado. Por isso mesmo, é inequívoca a importância do processo de recrutamento, seleção e contratação utilizado, bem como as ações de acompanhamento do comportamento e do desempenho profissional. (MANDARINI, 2005, p.130).

Após a fase de ingresso, inicia-se o período de experiência, na atual legislação do regime trabalhista Consolidação das Leis de Trabalho (CLT), prevê o prazo de 90 dias, o qual é dado uma oportunidade de a empresa e o funcionário avaliarem perfis e interesses.

Enfatiza Mandarini (2005) que a partir da admissão, o R.H continua a acompanhar o desenvolvimento do funcionário quanto à orientação/capacitação profissional, medidas disciplinares, até a fase de desligamento/aposentadoria.

Cabe ao R.H à condução dos exames de seleção internos para o preenchimento dos cargos comissionados, divulgar as normas e pré-requisitos para investidura dos cargos. Todo o processo seletivo interno segue as disposições normativas internas da empresa, desta forma, a coordenação de recursos humanos busca transparência e imparcialidade, validando os

interesses da empresa em conjunto com as práticas de segurança ao avaliar o comportamento corporativo dos candidatos, níveis de conhecimentos técnicos e interação profissional.

> ... tal atividade não pode ser executada apenas como uma forma de preencher os cargos existentes. Antes de iniciar o processo, é preciso que seja feito um planejamento criterioso em relação da identificação das competências essências à organização, análise do perfil do cargo e escolha das técnicas de seleção mais adequadas. (GROSS; LIMA, 2008, p.8)

Dado o exposto, os procedimentos adotados para proteção de R.H estão em sintonia com os conceitos de Mandarini (2005), quando a empresa estabelece critérios para inclusão de trabalhadores, observando as características desejáveis, que se adéquem às atividades desenvolvidas pela instituição e as competências requisitadas pelo cargo.

2.3.4 Segurança e Saúde no Trabalho

A CIPA foi instituída pela lei 7.036, 10 de novembro de 1944, no Brasil. Nasceu da convenção firmada entre os países membros em 1921 da Organização Internacional de Trabalho (OIT[5]). Diferentemente do SESMT a CIPA tem origem estrangeira e, de acordo com Mores (1997) em sua dissertação de mestrado pela Universidade Federal de Santa Catarina, intitulada: A CIPA analisada sob a ótica da ergonomia e da organização do trabalho-proposta de criação da Comissão de Estudos do Trabalho, que mesmo após as reestruturações legais que CIPA sofreu desde sua constituição, ainda é necessário que ocorra a revisão da NR-5 visando maior mobilização participativa dos trabalhadores quanto à prevenção de acidentes no trabalho.

Conforme mencionado anteriormente, de acordo com os dados do IBGE, o Brasil obteve o maior índice de acidentes de trabalho no mundo em 1972. De acordo com o próprio instituto: “Em um período de fragilidade no tocante a segurança dos trabalhadores no Brasil”, o governo interferiu nas relações trabalhistas entre funcionários e empresários, em busca de maior qualidade de vida e segurança no ambiente de trabalho, editando normas e instituindo órgãos fiscalizadores.

[5] Fundada em 1919 com o objetivo de promover a justiça social, a Organização Internacional do Trabalho (OIT) é a única das Agências do Sistema das Nações Unidas que tem estrutura tripartite, na qual os representantes dos empregadores e dos trabalhadores têm os mesmos direitos que os do governo. (Organização Internacional do Trabalho).

De acordo com o relato histórico da CIPA, Rocha (2011), em 1977 foi promulgada a CLT onde está previsto regulamentos em relação à Segurança e Medicina no Trabalho. No ano seguinte foram incorporadas vinte e oito normas regulamentadoras através da Portaria n° 3.214/78 pela Secretaria de Segurança e Saúde no Trabalho

Desde então, a segurança e saúde no trabalho passam a ter presença obrigatória nas empresas e ganham importância em todos os setores da economia.

O Ministério do Trabalho e Emprego acompanha e divulga os dados estatísticos de ocorrências de acidentes de trabalho.

Tabela 02: Resultado da fiscalização da Segurança e Saúde no Trabalho, acumulado de janeiro a novembro de 2010.

Setor Econômico		Ações Fiscais	Trabalhadores alcançados	Notificações *	Autuações **	Embargos / Interdições	Acidentes analisados	
Agricultura		9.223	958.289	15.218	7.391	149	66	
Comércio		30.481	1.967.486	16.743	6.526	345	177	
Construção		28.023	2.302.717	14.057	18.131	2.644	462	
Educação		1.983	245.803	253	202	4	7	
Hotéis/Restaurantes		5.666	237.313	801	576	33	23	
Ind. Alimentos	Indústria	4.222	1.241.344	3.818	2.399	178	159	
Ind. Madeira e Papel		1.720	154.504	2.800	694	66	39	
Ind. Metal		6.326	1.483.789	7.288	3.133	216	192	
Ind. Mineral		3.006	249.310	4.602	2.911	128	89	
Ind. Químicos		2.613	620.013	2.502	1.479	78	118	
Ind. Tecido e Couro		4.404	776.997	4.055	1.309	23	55	
Indústrias - Outras		1.747	150.920	1.749	554	37	39	
Instituições Financeiras		1.123	177.674	337	233	2	2	
Saúde		4.126	842.170	5.268	1.654	46	74	
Serviços		7.729	2.210.370	2.433	2.403	90	106	
Transporte		6.932	1.168.632	2.459	1.637	58	65	
Outros		3.095	697.878	1.034	883	49	32	
TOTAL		122.421	15.485.209	85.417	52.115	4.146	1.701	

2010

Fonte: Ministério do Trabalho e Emprego (2010)

Como pode ser observado na tabela acima, lidera o setor de construção em índices de acidentes de trabalho, já o setor financeiro possui a menor quantidade de ocorrências.

Existem estudiosos que abordam de modo intenso a problemática do setor de construção quanto ao elevado índice de acidentes de trabalho. Benite, 2004, em sua dissertação de mestrado pela Universidade de São Paulo (USP): Sistema de Gestão da Segurança e Saúde no Trabalho para empresas construtoras, reafirma a importância da presença do engenheiro de segurança nesse setor da economia.

Conforme os dados complementares, publicados pelo Ministério da Previdência Social, em relação às doenças e acidentes de trabalho, o setor de “atividades financeiras” lidera com percentual de 11,6 % dos 723,5 mil casos analisados pelo órgão, no ano de 2010.

Em matéria publicada pela Folha de São Paulo, São Paulo, 29 abr. 2007, o setor bancário assume a liderança em doenças causadas pelo trabalho, uma delas - Lesão por Esforço Repetitivo (LER/DORT), como pode ser observado na Figura 08:

Figura 08: Índices de doenças trabalhistas por setor econômico.
Fonte: Mundo Ergonomia (2007)

A S.S.T., empresa especializada em segurança e medicina no trabalho, classifica os riscos dos quais os funcionários estão expostos, como pode ser observado na tabela 4, de forma didática, em cinco grupos: físico, químico, biológico, ergonômico e acidentes de trabalho.

Nas instituições financeiras se aplica os riscos ergonômicos, tendo em vista o caráter da função administrativo dessas atividades, o que engloba também os danos à saúde psíquica causada por stress ou assédio moral. Para Marofuse e Marziale (2001, p. 24):

A ampliação do conteúdo das atividades, para o bancário, resultou na intensificação e aceleração do ritmo de trabalho, das operações executadas da utilização dos dados e pela exigência do aumento da produtividade. Assim, ao contrário de liberar o trabalhador, das tarefas repetitivas, a automação bancaria e o seu processo de informatização, desqualificam-no, substituindo a intervenção inteligente do operador por regulamentos e controle automáticos, que exigem dele somente atenção e precisão de gestos.

GRUPO I:	GRUPO II:	GRUPO III:	GRUPO IV:	GRUPO V:
Riscos Físicos	Riscos Químicos	Riscos Biológicos	Riscos Ergonômicos	Risco de Acidentes
Ruído	Poeiras	Vírus	Esforço Físico Intenso	Arranjo físico inadequado
Vibrações	Fumos	Bactérias	Levantamento e transporte manual de peso	Máquinas e equipamentos sem proteção
Radiações ionizastes	Névoas	Protozoários	Exigência de postura inadequada	Ferramentas inadequadas ou defeituosas
Radiações não ionizastes	Neblinas	Fungos	Controle rígido de produtividade	Iluminação inadequada
Frio	Gases	Parasitas	Imposição de ritmos excessivos	Eletricidade
Calor	Vapores	Bacilos	Trabalho em turno e noturno	Probabilidade de incêndio ou explosão
Pressões anormais	Substâncias, compostos ou produtos químicos em geral		Jornada de Trabalho prolongada	Armazenamento inadequado
Umidade			Monotonia e repetitividade	Animais peçonhentos

			Outras situações causadoras de stress físico e/ou psíquico	Outras situações de risco que poderão contribuir para a ocorrência de acidentes

Quadro 04: Classificação de Riscos no trabalho
Fonte: Segurança e Saúde no Trabalho (2011)

Para minimizar os efeitos negativos inerentes as atividades administrativas, pode-se fazer uso de Equipamentos de Proteção Individual (EPIs) nos escritórios aliadas a atividades físicas durante o expediente de trabalho, sob a ótica de Santos (2001, p.2) em seu estudo dirigido: Ergonomia e Segurança Industrial, "... abordagem preventiva, que procura evitar a ocorrência de situações patogênicas,...".

Segundo aponta estudos levantados pelo Ministério da Educação e Cultura (MEC), no material publicado para o projeto Educação para Jovens e Adultos (EJA), um dos problemas do Brasil é a elitização do ensino, por muito tempo, uma pequena parcela da população brasileira teve acesso pleno a educação e cultura, o que ocasionou o problema de exclusão social.

O tema de "Segurança no Trabalho" ganhou destaque especial em um dos cadernos desenvolvidos pela Secretaria de Educação Continuada, Alfabetização e Diversidade (SECAD) para o projeto EJA, abordando aspectos das leis trabalhistas e normas regulamentadoras (NRs) de maneira integrada com o cotidiano do trabalhador, de acordo com Neves (2011) em seu artigo: Trabalho em Educação com Jovens e Adultos, "Os jovens e adultos trabalhadores buscam na escola uma significação social para suas práticas, suas vivencias e seus saberes".

Para Rocha (2011), a principal proteção de qualquer trabalhador é um ambiente livre de riscos.

De acordo com a Lei 6.514 de dezembro de 1977, Capítulo V da CLT, caso ocorra acidente, intoxicação, lesão em decorrência de execução de atividades de trabalho, considera-se o fato como acidente.

A Federação das Indústrias do Estado de São Paulo (FIESP) em parceria com o Centro das Indústrias do Estado de São Paulo (CIESP) desenvolveu um manual intitulado: Legislação de Segurança e Medicina no Trabalho (2003), o qual descreve as implicações e características de acidentes de trabalho, abordando as Normas Regulamentadoras que devem ser observadas pelas empresas e seus funcionários.

2.3.4 Soluções adotadas

Todos os procedimentos abaixo descritos são benefícios, direitos, procedimentos ou normas estipuladas pelo banco que é objeto de estudo desse trabalho, formalizados por meio de acordo coletivo de trabalho, renovável anualmente, e regulamentados pela publicação de normas e procedimentos internos, restrito para consulta ao público interno, que devem ser observados por todos os funcionários da ativa e estão autorizados para consulta exclusivamente no ambiente de trabalho, em meio eletrônico via intranet, mediante identificação funcional e senha eletrônica.

O setor financeiro possui o maior índice de doenças causadas pelo trabalho, como observado nos dados anteriores, conforme divulgado pelos órgãos oficiais MTE e MPAS, a instituição financeira analisada assumiu a postura de reverter esse quadro. Para tanto, foram programadas ginásticas laborais, massagens durante o expediente de trabalho e instruções quanto à prática regular de exercícios físicos ao fornecer auxílio financeiro para tais atividades.

> A ginástica laboral é a combinação de atividades físicas que tem como características comuns, melhorar a condição física do indivíduo para o seu trabalho, promovendo a saúde e a socialização dos trabalhadores, além de atuar na prevenção terapêutica das possíveis doenças osteomusculares e ligamentares. (COOPERCAMPOS, 2011, p. 1).

Essas instruções são publicadas por meio de cartazes em locais de ampla visualização e fácil acesso. Faz parte desse processo equipes responsáveis pela: difusão de notícias aos funcionários, mobilização em tarefas de desenvolvimento regional sustentável, capacitação e comunicação de sugestões à gerência.

Atrelada à disseminação da informação está a CIPA que regularmente promove palestras em relação à saúde e segurança no trabalho. Faz parte da agenda da CIPA: a Semana Interna de Prevenção de Acidentes de Trabalho (SIPAT), prevista na Portaria n° 3.214, NR 5,

item 5.16, onde ocorrem eventos, durante o expediente, direcionados ao tema escolhido em relação à saúde e segurança no trabalho.

> O principal objetivo da SIPAT é promover e divulgar a importância da prevenção de acidentes no trabalho. Para alcançar esses resultados, são oferecidas ao trabalhador, atividades que possam orientar e conscientizar quanto à importância de se eliminar os acidentes do trabalho, criando-se atitudes positivas para reconhecer e corrigir as práticas nocivas ao ambiente de trabalho. (LOBO, 2011).

Em 2010 foi implantado o SESMT na empresa, que é objeto de estudo desse trabalho, com quadro orgânico de profissionais capacitados, os mesmos estão vinculados aos Recursos Humanos e as Gerências Regionais de Gestão de pessoas, presentes em todos os estados do país.

Alguns produtos utilizados nos escritórios para auxílio ergonômico:

Figura 09: Apoio para mouse.
Fonte: Loja Maxipas (2011)

Aliados aos apoios para o teclado e para os pés, os produtos colaboram para a manutenção correta da postura dos funcionários que trabalham em frente ao computador por longo período de tempo.

Figura 10: Apoio para teclado.
Fonte: Comercial EPI (2011)

Tendo em vista que o mercado financeiro possui os maiores índices de doenças de trabalho e o prejuízo assumido pelo total de dias não trabalhados, deve-se difundir a importância do tema ergonomia aos funcionários, de acordo com Peres (2007), em matéria publicada na Folha de São Paulo, o país gasta cerca de R$ 981 milhões com ler em bancários.

Segundo a política de segurança do banco, publicado no material de capacitação voltado para segurança corporativa e pessoal, autoria da Diretoria de Segurança/Universidade Corporativa BB, é atribuído o principal desafio: "a mudança de comportamento[6]".

Figura 11: Apoio para os pés
Fonte: Loja Maxipas (2011)

Tendo em vista o desafio do banco citado anteriormente, o plano QVT assume um papel importante na SCorp, pois os funcionários devem estar dispostos a cumprir os regulamentos internos da empresa:

> Para que se evitem resistências, a cooperação, participação e envolvimento do público interno (PI) podem ser estimulados por ações de *endomarketing*, indispensável aliado para promover a "venda" interna da SCorp, considerando todos os fatores que possam dificultar a integração das medidas e procedimentos de segurança previstos na vida das pessoas e na rotina da corporação. (MANDARINI, 2005, p. 19).

Ainda podem ser considerados alguns fatores motivadores, diretamente vinculados à Qualidade de Vida no Trabalho, que colaboram para a melhor participação do público interno, conforme Vasconcelos (2001, p.24): realização, reconhecimento, o próprio trabalho, responsabilidade e progresso ou desenvolvimento.

> Qualidade de vida no trabalho pode ser utilizada para que as organizações renovem suas formas de organização no trabalho, de modo que, ao mesmo tempo em que se eleve o nível de satisfação do pessoal, se eleve também a produtividade das empresas, como resultados de maior participação dos empregados nos processos relacionados ao seu trabalho. (FERNANDES, 1996, p. 35).

[6] Da disposição por parte dos funcionários em cooperar na proteção dos ativos da empresa.

2.4 Gestão de Segurança dos Processos

A Segurança dos Processos abrange as atividades e serviços de uma instituição. Foi dividida por Mandarini (2005), para um melhor entendimento, em três segmentos:

Segurança das Operações (SOp);

Segurança dos Planejamentos (SPlj);

Segurança dos Insumos (SInsu)

2.4.1 Segurança das Operações (SOp)

De acordo com os conceitos de Mandarini (2005), a segurança das operações preocupa-se em determinar, dentre as atividades ou serviços da empresa, o grau de periculosidade[7] e sensibilidade[8] ou os riscos que esses processos representam à empresa, à sociedade, ao ser humano e à preservação do meio ambiente.

De acordo com Portella (2005, p. 55), cabe à empresa desempenhar as políticas de segurança física: "... visando a incolumidade das instalações, dos seus processos e produtos, bem como o de seus empregados, clientes, usuários ou visitantes.".

Para o auxílio na determinação da criticidade das operações que representem determinado grau de periculosidade ou que afetem a normalidade das atividades da empresa, recomenda-se o uso de atribuição numérica a cada fator analisado, como pode ser observado no Quadro 05:

[7] São considerados periculosos todos os processos que incluam operações cujos procedimentos ou atividades impliquem ameaças ou riscos para as instalações, pessoas, RH, e meio ambiente. (MANDARINI, 2005, p. 157).

[8] São considerados sensíveis todos os processos que incluam operações que demandem procedimentos ou atividades cujo perfil exerça, direta ou indiretamente, influência sobre a regularidade, a normalidade e a continuidade da atividade institucional. (MANDARINI, 2005, p.157).

Periculosidade	Sensibilidade	Criticidade
Não causam dano às pessoas e/ou ao meio ambiente	Não dificultam o processo operacional da instituição	1
Causam leve dano às pessoas e/ou ao meio ambiente	Causam baixa dificuldade ao processo operacional da instituição	2
Causam médio dano às pessoas e/ou ao meio ambiente	Causam média dificuldade ao processo operacional da instituição	3
Causam grave dano às pessoas e/ou ao meio ambiente	Causam alta dificuldade ao processo operacional da instituição	4
Causam gravíssimo dano às pessoas e/ou ao meio ambiente	Causam altíssima dificuldade ao processo operacional da instituição	5

Quadro 05: Níveis de Criticidade
Fonte: Mandarini (2005, p.159)

Tal procedimento permite que sejam estipulados níveis de prioridade em ações de contingência caso ocorra anormalidade no desempenho das atividades que, para a empresa, são essenciais na continuidade dos negócios.

Para Mandarini (2005), a Segurança das Operações preocupa-se, prioritariamente, em proteger o *core business,* atividade principal, mantendo foco secundário nas instalações, pessoas e meio ambiente.

Para melhor gerenciar os riscos inerentes às atividades da instituição, são objetos de análise apenas os processos considerados periculosos ou sensíveis. Isso remete aos ativos intangíveis da empresa, como a imagem.

Para a instituição analisada, a segurança sob a percepção de um cliente a respeito de um banco "está intimamente ligada ao nível de confiança que é depositado em uma instituição financeira". (GESTÃO DE SEGURANÇA, 2008, p. 16).

A inobservância dos procedimentos para a execução de processos considerados sensíveis ou periculosos, mesmo que representem perdas inexpressivas, podem levar a impactos negativos por publicidade depreciativa o que prejudica a imagem/marca da

instituição. De acordo com Matos e Veiga (2003, p. 71), a repercussão negativa pode estar atrelada ao comportamento da empresa (social ou ética) e não ao evento produto, definindo que: “um evento relacionado à empresa é aquele que não envolve atributos específicos do produto ou afeta seu uso funcional”.

2.4.2 Segurança dos Planejamentos (SPlj)

Muito utilizado pelos executivos e administradores, o planejamento permite direcionar as ações estratégicas da empresa frente ao mercado e alinhar as políticas da empresa com o desenvolvimento/capacitação dos funcionários e colaboradores e gerenciamento dos produtos e serviços dos fornecedores para melhor atender as expectativas dos clientes. Objetiva antecipar um resultado esperado.

> ... o planejamento é um aspecto particular do processo decisório, tendo características especiais. Sua tarefa principal, uma vez determinados os objetivos da organização e estudadas as condições ambientais que a envolvem, é de estabelecer as ações racionais para o alcance satisfatório de tais objetivos. (PORTELLA, 2003, p. 169).

Para Kotler (1975), ao definir a relação da empresa com o ambiente interno e externo, visando à oportunidade de planejar a abordagem e definir limites de atuação da organização frente ao mercado, tem-se o planejamento estratégico.

De acordo com Mandarini (2005), interessa a SPlj todos os planejamentos, não somente aqueles considerados sensíveis. O autor divide os planejamentos em sensíveis e não sensíveis. Dependendo da sensibilidade apresentada, cabe a SPlj estabelecer parâmetros para determinar os níveis de confidencialidade e as pessoas ou setores que deverão ter conhecimento do planejamento analisado.

Em relação aos considerados não sensíveis, Mandarini (2005) sugere que a SPlj restringe-se a manter as normas impostas pela alta administração ou por cada setor da empresa. Quando os planejamentos são considerados sensíveis, estes têm de exercer o planejamento para assegurar que a operação se concretize, com o grau de confidencialidade exigido.

No entanto somente esta divisão entre planejamentos sensíveis e não sensíveis não é suficiente para garantir a sua segurança, pois cada caso possui sua peculiaridade. Há

necessidade de fazer um levantamento de todos os aspectos inerentes aos planejamentos tais como amplitude e a profundidade das medidas e procedimentos de segurança mais adequados.

> ... para atender o planejamento estratégico é necessário examinar a estrutura organizacional da organização, normalmente dividida em três níveis: alta administração, unidades de negócio da empresa e produto. Desta maneira, é de incumbência da alta administração elaborar e desenvolver o planejamento estratégico corporativo para levar a empresa a um futuro promissor e rentável. (BARBOSA; BRONDANI, 2005 p. 16).

Um dos métodos utilizados para definir a sensibilidade/criticidade do planejamento estratégico, é estabelecer níveis de sensibilidade, como mostrado na Tabela 03:

Tabela 03: Grau de Sensibilidade do Planejamento

Influência	Valor
Nenhuma	1
Baixíssima	2
Baixa	3
Média	4
Alta	5
Altíssima	6

Fonte: Mandarini (2006, p. 170)

Determinado os níveis de sensibilidade, relacionam-se os planejamentos analisados: P1, P2 e P3 com os níveis de planejamento por ele almejados: N1, N2 e N3.

Para os planejamentos e os níveis de planejamento, citamos os seguintes exemplos:

P1: Um banco selecionar uma empresa seguradora veículos para fechar parceria estratégica na comercialização de seus seguros;

P2: Criação de modalidade de pacote de serviços exclusivo no mercado bancário;

P3: Instalação remota de itens de segurança nos computadores do conglomerado da empresa.

N1: Nível de influência de conclusão do projeto sob o aspecto de sigilo;

N2: Nível de influência dos resultados do planejamento sobre o negócio;

N3: Nível de influência sobre as condições de segurança do planejamento do projeto sobre a empresa.

Tabela 04: Sensibilidade do Planejamento

Planejamento/ Sensibilidade	**N1**	**N2**	**N3**	**Peso**	**Sensibilidade (Soma x Peso)**
P1	6	6	1	2	26
P2	6	6	1	2	26
P3	1	3	6	1	13

Fonte: Adaptado de MANDARINI (2005, p.170).

Logo, os planejamentos P1 e P2 terão prioridade sob o aspecto de segurança no planejamento/execução, pois os impactos negativos são maiores para a empresa na ocorrência de sinistro.

2.4.3 Segurança dos Insumos (SInsu)

Consideram-se insumos, todo material e equipamento utilizado em um processo de produção e interessa a Segurança dos Insumos (SInsu) os classificados como periculosos ou sensíveis.

É de atribuição da Segurança Corporativa os planejamentos de como os insumos deverão ser: estocados, da sua utilização, do transporte (saída, trajeto e recebimento) e do seu descarte.

Para Mandarini (2005), em cada situação apresentada acima, deverão ser adotados procedimentos de controle e checagem diferenciados.

2.4.3.1 Estoque

A SInsu atuará em conjunto com a SGai para certificar-se de que os itens guardados em prateleira, almoxarifados ou estocados preservem suas características, inviolabilidade e integridade. Podem ser adotados o controle de acesso a esses ambientes fazendo uso de uma

ou mais soluções de segurança apresentadas pela SGai, dependendo do caso, e a execução de procedimentos de conferência ou verificação definidos pela SInsu.

> Buscam em conjunto com os controles administrativos, assegurar quantidade, qualidade, especificações, componentes, validade, e, especialmente, a inviolabilidade, incolumidade e integridade dos materiais. (MANDARINI, 2005 p. 181).

- Vistorias sistemáticas e sigilosas;
- Instalação de sensores de temperatura;
- Controle de quantidade de itens estocados;
- Controle de validade

São algumas rotinas adotadas para monitorar os insumos que não estão em uso, acrescenta Mandarini (2005), deve-se evitar a guarda de materiais considerados sensíveis e periculosos, sua adoção deve ocorrer em situações de exceção, e a proteção desses itens assume caráter meramente procedimental.

2.4.3.2 Utilização

As medidas de segurança corporativa iniciam-se a partir do recebimento do insumo pelos funcionários. Recomenda-se que a utilização do item objeto de controle seja manuseada por um RH específico. Por exemplo, os funcionários responsáveis por operar aparelhos de radioterapia também serão encarregados de reabastecer a fonte de energia desses equipamentos, sejam por cápsulas de césio, cobalto ou irídio. O rastreamento desses itens quando centralizado a um público restrito, ou a um único RH facilita o controle e procedimentos de segurança ou apuração de responsabilidades.

> ... um dos procedimentos que se destacam no uso do ICSP refere-se à conveniência de sua utilização por um único RH, ou do seu emprego por segmento institucional determinado. (MANDARINI, 2005 p. 186).

2.4.3.3 Transporte

Duas variáveis são consideradas nos transportes dos insumos: ostensividade (evidente) e discrição. Na ostensividade deseja-se evidenciar ao público o que está sendo protegido, enquanto a discrição o objetivo é manter em sigilo a identidade do que está sob proteção.

A escolha dependerá do que está sendo transportado, dos níveis de segurança demandados e da importância dispensada aos objetos.

No intuito de desencorajar ações criminosas, no transporte de grandes valores deve-se evitar a discrição e optar pela ostensividade, o mesmo se aplica ao deslocamento de explosivos, inflamáveis, e tóxicos. Em contrapartida, é desejável a discrição no transporte de pequenos valores.

De acordo com a Agência Nacional de Transportes Terrestres (ANTT), "o transporte rodoviário de produtos perigosos por vias públicas, é disciplinado pelo Decreto 96.044, de 18 de maio de 1988." O referido decreto prevê a capacitação profissional das pessoas envolvidas no transporte de cargas perigosas além da ostencividade adequada para identificação do material transportado.

De acordo com Mandarini (2005), a ostensividade por si, é inconveniente quando se aplica a segurança, pois se perde o caráter sigiloso, porém, como nos exemplos acima citados, normas e exigências legais recomendam ações ostensivas para garantir a própria segurança.

Também interessa a SInsu os tipos de transporte utilizados, pois para cada solução de deslocamento, procedimentos diferentes serão adotados para o estudo: da agilidade, capacidade física, rastreabilidade, restrições/impedimentos, aspectos técnicos.

O autor cita alguns tipos de transporte:

- Hidroviário;
- Rodoviário;
- Aéreo;

Os riscos inerentes ao transporte de cargas são objeto de estudo da SInsu, como a probabilidade de furto, extravio e acidentes. O autor reforça que maiores cuidados devem ser empreendidos quando se trata se itens periculosos ou sensíveis. Portanto, a operação de transporte terá como pilar ações procedimentais que visem a sua concretização, tendo em vista:

- Proteção da vida;

- Proteção do patrimônio
- Minimização de impactos ambientais;
- Otimização de recursos;

2.5 Segurança da Gestão do Conhecimento (SGC)

Como foi citado no início desse capítulo, as corporações estão inseridas na era do conhecimento, um ativo importante para a manutenção dos negócios e hoje, alvo de espionagem por parte de concorrentes ou pessoas mal intencionadas.

Existem inúmeros significados para conhecimentos e interessa a SGC proteger os dados e informações que são sigilosos e que fazem parte de ações estratégicas da empresa. De acordo com Mandarini (2005, p. 203), “confere maior segurança no processo decisório e permite decidir com mais oportunidade e menos oportunismo, e todo dado ou informação de interesse disponível a que a instituição teve acesso e todo resultado hábil, obtido oportunamente a partir de um processo de produção”.

Independente do setor econômico em que a empresa atue todos os seus funcionários manuseiam diariamente algum tipo de informação, e pelo menos uma possui um grau de sensibilidade, ou seja, de compartimentação interna.

Por esse motivo, a administração deve estabelecer critérios de acesso a esses dados /informação, para salvaguardar o que é de interesse da empresa, bem como o manuseio dos materiais que os abrigam, o transporte, reprodução, arquivamento e destruição/expurgo.

De acordo com os conceitos de Gestão de Segurança (2008, p.47), “Os aspectos de segurança atingiram tamanha complexidade que há necessidade de desenvolvimento de equipamentos mais especializados para a sua implementação e gerenciamento.”.

No manuseio das informações, sejam elas abrigadas em chips, documentos, vídeos, disquetes, CDs, pen-drives, é recomendado, segundo Mandarini (2005), adotar procedimentos criteriosos quando da expedição de suportes que contenham informações sigilosas, a possibilidade de rastreamento durante o transporte, e por fim quando da recepção do conteúdo.

Por exemplo, noticiado por JUNIOR (2008), na Folha OnLine. Petrobras confirma furto de dados sigilosos. Pelo roubo dos computadores da Petrobrás, transportados em um container, sob custódia da empresa terceirizada Halliburton, em que haviam dados estratégicos e sigilosos armazenados no disco rígido desses computadores, trouxe a tona suspeitas de espionagem industrial.

> O avanço na tecnologia dos computadores que permite o acesso dos dados da empresa sejam realizados a partir do próprio local de trabalho, ou mesmo de casa, tem tornado fácil o acesso aos planos estratégicos da empresa às informações sobre pesquisa e desenvolvimento, e dados sobre o processo produtivo, permitindo a cópia ou transferência sub-reptícia de preciosos segredos industriais. (BESSA, 2001 p. 4).

Por se tratar de um assunto bastante abrangente, a matéria sobre Segurança da Gestão dos Conhecimentos, Mandarini (2005) subdividiu em quatro tópicos, sendo eles:

- Segurança da Informação (SInfo);
- Segurança dos Suportes (SSup);
- Segurança das Telecomunicações (STcom)
- Segurança da TI.

2.5.1 Segurança da Informação (SInfo)

Nem todas as informações são consideradas sensíveis, algumas podem ser amplamente divulgadas ao público interno e externo, como fatos relevantes ao mercado, parcerias estratégicas entre empresas, por exemplo. Outros por sinal devem ser resguardados do público, inclusive dos funcionários que não estão diretamente envolvidos no processo, por exemplo, no desenvolvimento de um produto exclusivo.

> Um grande desafio que as organizações enfrentam é estabelecer quais informações devem ser classificadas, efetivamente, como altamente sigilosas, de acesso limitado. Isto porque, existe uma tendência a considerar que todas as informações que trabalhamos na organização são muito sigilosas. (GESTÃO DE SEGURANÇA, 2008, p. 60).

Salienta Mandarini (2005) que cabe a Segurança da Informação proteger os dados e informações contidos em documentos, disquetes, pen-drives, mídias de armazenamento (CDs, DVDs, VHS), maquetes, ferramentas de *back-up*, inclusive odores característicos que definam

a imagem do ambiente da empresa (amplamente utilizados em lojas de roupas, perfumarias e confeitarias).

2.5.2 Segurança dos Suportes (SSup)

Terá relações estreitas com a SInfo, pois, de acordo com Mandarini (2005), os limites da segurança dos dados e informações com os suportes que os contêm não possuem fronteiras definidas e os procedimentos de segurança adotados para um são aplicados em outro.

Os suportes são definidos como todo o material que abrigam dados e informações. A segurança dos suportes interessa especificamente os suportes físicos (documentos, fotos, projetos, esquemas, plantas), pois os dados lógicos, armazenados em meios eletrônicos é objeto de estudo da Segurança da Tecnologia da Informação.

Os procedimentos adotados na SSup partem da classificação dos suportes, levando em consideração quais dados/informações vão abrigar e o seu grau de sigilosidade, como, por exemplo, a classificação da informação adotada pelo governo brasileiro prevista no Decreto n° 4.553, de 27 de Dezembro de 2002:

- Ultrassecretos;
- Secretos;
- Confidenciais;
- Reservados;
- Públicos.

A definição do grau de confidencialidade do documento é determinada por quem o expediu. A compartimentação seguirá o padrão de confidencialidade, pois um documento classificado como ultrassecreto será destinado a um público restrito, ou a uma única pessoa, sendo o seu conteúdo indivulgável.

> ... independentemente da relevância ou tipo da informação, a gestão dos dados organizacionais é estratégica, pois possibilita o apoio para a tomada de decisões em qualquer âmbito institucional. Algumas informações são centrais para a organização e a divulgação parcial ou total destas pode alavancar um número de repercussões cuja complexidade pode ser pouco ou nada administrável pela organização com consequências possivelmente nefastas. (LAUREANO, 2005 p. 8).

A redação desses documentos seguirá padrões que possam facilmente identificá-lo. Mandarini (2005) recomenda o uso de linguagem objetiva, evitando estrangeirismos e erudismo, seguindo o padrão de redação corporativa determinada pela empresa, que deixem claros a interpretação de seu conteúdo para o destinatário.

O autor enfatiza ainda que alguns procedimentos de segurança do transporte, adotados pela Segurança dos Insumos, no controle da expedição, trajetória e recebimento desses documentos, podem ser empregados para:

- Geração de protocolos de controle ao expedir o conteúdo;
- Escolha do meio de transporte;
- Recebimento do item por RH próprio;
- Gerar confirmação do recebimento.

Outros tópicos importantes abordados pela segurança dos suportes são: controle de reprodução/cópia dos conteúdos, monitoria da informação (ver se está sendo difundida na empresa para evitar a fuga ou vazamento de informações); decisão do que deve ser arquivado e como fazê-lo; e destruição de documentos.

A segurança do arquivamento preocupa-se com: ações procedimentais de acesso aos dados/informações, áreas e instalações, e a conservação dos meios utilizados para a sua armazenagem.

A digitalização proporcionou a otimização de espaço físico além de agilizar a busca de arquivos quando consultados. Por esse motivo, também se recomenda restringir o acesso a esse banco de dados ao RH específico, seja por meio de senhas de acesso, uso de protocolos de pedido de arquivo e termos de confidencialidade, acordo de sigilo entre funcionário e a empresa.

> Há menos de uma década, bastavam um cadeado, correntes reforçadas num portão e um cachorro feroz para manter a empresa e seus dados protegidos dos gatunos. Hoje, com a maior parte das informações digitalizadas, é preciso ir além. Não dá para deixar de investir em softwares de segurança e no treinamento de funcionários para preservar os segredos da empresa. (LAUREANO, 2005 p. 64).

Quando os arquivos guardados não forem mais necessários, o processo de destruição/expurgo também exige ações procedimentais de controle. Ao observar o prazo de validade do arquivo ou o cumprimento de determinação ordem superior para o expurgo. Mandarini (2005) aconselha que sejam registrados: local, data e hora, bem como testemunhas que afirmem quando os dados forem destruídos.

> A partir da especificação, configuração e implantação de controles físicos, tecnológicos e humanos preocupados com o manuseio, armazenamento, transporte e descarte das informações, consegue-se reduzir e administrar os riscos. (SÊMOLA, 2001 p. 5)

O Lixo Classificado é destinado a tudo que contenha alguma informação sobre a empresa e a destruição desses arquivos é diferenciado, afirma Mandarini (2005). As soluções mais comum é o emprego de trituradores de papéis, cartões magnéticos, CDs e DVDs.

2.5.3 Segurança das Telecomunicações (STcom)

Neste tópico da Gestão da Segurança dos Conhecimentos é dispensada especial atenção a todos os meios capazes de transmitir dados, sejam elas por pessoas, satélites, rádio, telefone, e-mails. A preocupação central dessa área da segurança corporativa está na interceptação de dados.

> ... a STcom compreende, não só os meios de transmissão de registros escritos, como mensageiros, telegramas e faxes; transmissão da voz, como telefones e rádios; transmissão da imagem, como satélites e circuitos de TV; mas também todas as modalidades de transmissão digital, como e-mail, por exemplo. (MANDARINI, 2005, p. 250).

Embora não seja possível extinguir o risco, as chances de ocorrer interceptação de informação podem ser minimizadas adotando práticas que salvaguardem o que é de interesse estratégico.

A correta manutenção dos equipamentos escolhidos para transmitir dados colabora para a segurança dos próprios meios de transmissão. Para tanto, deve-se observar o local onde estão armazenados, fisicamente, os dados, checando a acessibilidade para vistorias, auditorias, troca de componentes, desinstalação quando obsoletos, aspectos naturais – exposição a adversidades climáticas, por exemplo – e também controle de acesso.

> Redes de telecomunicação são altamente vulneráveis a falhas naturais de hardware e software e ao uso indevido dos programadores, operadores de computador, pessoal de manutenção e usuários finais. É possível, por exemplo,

> grampear linhas de telecomunicação e interceptar dados ilegalmente. (LAUREANO, 2001, p. 19).

Na segurança das telecomunicações, a restrição de acesso aos equipamentos não é o suficiente para a proteção de dados, do ponto de vista de Mandarini (2005), pelo motivo das informações serem transmitidas por meios eletromagnéticos, radiofrequência. Assim, cabe à segurança instalar componentes que dificultem a interceptação. O equipamento comumente adotado é o *scrambler*, durante a transmissão de dados, tornam as informações inteligíveis, e as restauram na recepção.

2.5.4 Segurança da Tecnologia da Informação (STI)

A Segurança da T.I.[9] aborda a compartimentação e confidencialidade sob a ótica tecnológica dos equipamentos que abrigam as informações, bem como a disponibilização desses dados aos funcionários.

Trata também de ações procedimentais de segurança, pois os aspectos técnicos da disciplina extrapolam os limites de atribuição da SCorp, ficando ao seu cargo a proteção dos componentes que integram o sistema do processamento de dados.

> É exatamente da previsão das medidas e procedimentos necessários e mais adequados à salvaguarda desse "todo" que a Segurança Corporativa deve participar intensamente. (MANDARINI, 2005 p. 270).

Juntamente com a TI, a SCorp deve definir políticas de procedimentos de verificação e acessos para prevenir violações que prejudiquem: a confidencialidade, fidedignidade e integridade dos dados e informações.

É de responsabilidade dessa disciplina assegurar que os sistemas que compõem o processamento de informações sejam constantemente monitorados de modo a salvaguardá-los

---

[9] A **Tecnologia da Informação** (TI) pode ser definida como um conjunto de todas as atividades e soluções providas por recursos de computação. Na verdade, as aplicações para TI são tantas - estão ligadas às mais diversas áreas - que existem várias definições e nenhuma consegue determiná-la por completo.
A TI é uma grande força em áreas como finanças, planejamento de transportes, *design*, produção de bens, assim como na imprensa, nas atividades editoriais, no rádio e na televisão. O desenvolvimento cada vez mais rápido de novas tecnologias de informação modificou as bibliotecas e os centros de documentação (principais locais de armazenamento de informação), introduzindo novas formas de organização e acesso aos dados e obras armazenadas; reduziu custos e acelerou a produção dos jornais e possibilitou a formação instantânea de redes televisivas de âmbito mundial. (WIKIPÉDIA, 2011)

de violações e acessos indiscriminados. São os componentes desse sistema: aplicações, softwares básicos e hardwares, como podem ser observados na figura 12.

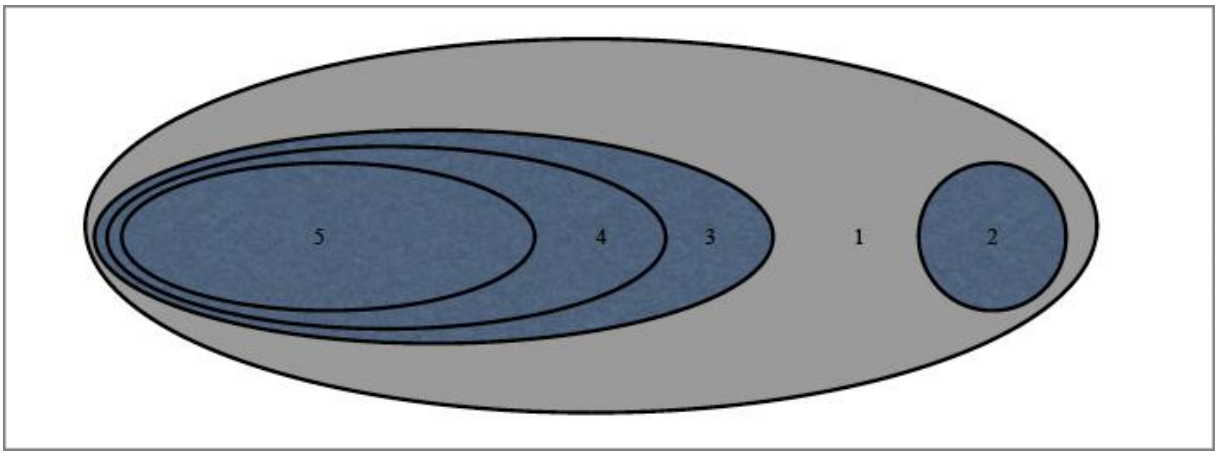

Figura 12: Sistemas da TI
Fonte: Mandarini (2005, p.269)

Em que:

1: Sistemas dos Conhecimentos;

2: Sistemas de Procedimentos Manuais;

3: Subsistemas de Aplicações;

4: Softwares Basicos;

5: Hardwares.

A ação conjunta da SGai com STcom, para Mandarini (2005), garante os requisitos mínimos para a manutenção da segurança do sistema de processamento de informações ao gerir o controle de acesso aos locais onde estão instaladas as máquinas e o cumprimento dos procedimentos inerentes as: atualização, manutenção, verificações periódicas, substituição, auditorias.

Além das variáveis acima citadas, os planos que configuram a própria proteção da TI devem ser observados, como o controle de acesso a internet, verificação e filtragem do conteúdo permitido para visualização, os *firewalls*, barreiras lógicas contra invasão de especialistas (*hackers*) em uma rede de computadores, ação de vírus e execução de agentes nocivos aos programas, bem como o gerenciamento do e-mail corporativo: "... agregam custo

(conexão) e perigo (vírus) absolutamente desnecessários a atividade laborativa", (MANDARINI, 2005, p. 278).

Segundo o autor, o papel do controle é limitar e fiscalizar os acessos no intuito de: prevenir, dificultar, impedir e neutralizar tentativas de violação. A abordagem de controle releva os parâmetros definidos de compartimentação e confidencialidade a que cada RH está submetido, visto que os níveis de acesso são diferenciados. Isso facilita o controle/monitoria dos demais segmentos da empresa, seja pelos acessos, isolamento de acesso à internet, análise do fluxo de e-mails.

Assim, devem-se estabelecer critérios para concessão de acesso as informações, baseado na política da necessidade de conhecer - compartimentação, a prerrogativa de um setor ou departamento da empresa de consultar o banco de dados é justificada pela atividade fim. "Pois o processo de autorização decide se uma pessoa, programa ou dispositivo tem permissão para acessar determinado dado, programa de computador ou serviço." (GESTÃO CORPORATIVA, 2008, p. 64).

O mesmo se aplica a confidencialidade dessas informações. Deve haver o comprometimento dos funcionários quanto à política de sigilo adotada pela companhia tendo em vista salvaguardar informações relativas aos negócios, contribuindo até mesmo a própria segurança pessoal.

> As pessoas são o elemento central de um sistema de segurança. Partindo do princípio que uma organização pode ser definida, também, como um conjunto de pessoas que nela trabalham e que os incidente de segurança sempre envolvam pessoas, fica fácil perceber o porquê das pessoas serem o elemento mais importante para a segurança. (GESTÃO DE SEGURANÇA, 2008, p. 143).

2.5.5 Práticas adotadas no banco

Segundo os normativos e procedimentos internos da empresa, as informações bem como seus acessos são classificadas em quatro níveis de sensibilidade:

1) Voltado para público interno e externo, pois o seu conteúdo é interesse coletivo;

2) Voltado para o público interno, apresenta sensibilidade baixa e seu conteúdo é de interesse dos funcionários;

3) Voltado para o público interno, apresenta média sensibilidade e requer determinados cuidados quanto ao manuseio, reprodução e compartimentação de conteúdo. Voltado para pessoas que trabalham com o assunto-fim;

4) Voltado para o público interno, apresenta elevada sensibilidade, sendo que seu conteúdo é destinado somente às pessoas estritamente envolvidas com o assunto-fim.

Os funcionários utilizam um aplicativo, de extensão nacional, exclusivo para uso e instalação no local de trabalho, onde pode ser acessado: o banco de dados da empresa, operações financeiras, cadastro de clientes, extrato de contas bancárias, controle de despesas, gerenciamento de RH entre outros. E para a segurança de acesso, utilizam-se dois parâmetros: uma chave de identificação funcional, composta de sete dígitos, exclusiva para cada funcionário e uma senha composta de oito dígitos, que deve ser alterada a cada seis meses, não sendo possível, no momento da alteração, utilizar as últimas duas senhas.

Para isso, todos os colaboradores assinaram, via meio eletrônico, um acordo de compromisso em relação ao sigilo das informações disponíveis para consulta bem como a ciência da responsabilidade pelo correto uso dos aplicativos de sistema da empresa. Alguns deles são interligados com outras instituições como a SERASA, Receita Federal do Brasil e Banco Central.

O uso indevido desses sistemas pode comprometer a veracidade das informações prestadas a esses órgãos, comprometendo a imagem da empresa e o que pode acarretar sansões legais além de abertura de processo sob medida disciplinar.

Em relação à segurança de TI, os acessos a esses conteúdos são restritos a determinado perfil de atuação do funcionário lotado em setor específico. Por exemplo, o departamento de engenharia não precisa ter acesso nas operações de câmbio ou no extrato de contas de investimento de clientes.

A administração de acesso é de responsabilidade de funcionário comissionado do segmento gerencial. Mesmo assim, caso o departamento não precise do acesso para desenvolver suas atividades, o item fica indisponível para sua concessão.

Se, em caráter de exceção, for preciso conceder acesso em um aplicativo e se esse estiver indisponível para concessão, a administração do departamento deverá formalizar o

pedido para a sua diretoria (superiora hierárquica), que o analisará, se for deferido, será solicitado o desbloqueio do acesso para diretoria de gestão de segurança.

Os acessos à internet são restritos aos departamentos que precisam desse meio de consulta para desempenhar suas funções, evitando assim a sobrecarga dos servidores e prevenindo a contaminação dos computadores por softwares maliciosos. Aliada a barreiras lógicas de acesso a determinados conteúdos e endereços eletrônicos, favorecem um ambiente de segurança, diminuindo a exposição da rede de computadores a própria segurança de informação e dados a riscos.

Essas práticas estão em conformidade com a política da SCorp ao estabelecer níveis de compartimentação do conhecimento: até que ponto há a necessidade de conhecer.

Foi definida a política do uso de componentes portáteis para armazenagem de dados como hardware externo e pen drives. Pela empresa ter contratado serviços de uma companhia de segurança antivírus, todos componentes periféricos devem ser diagnosticados em relação à presença de softwares maliciosos antes de serem executados.

Outro tópico importante na gestão de segurança do conhecimento é a confidencialidade. Uma vez que a transmissão de dados e informações possui estreita ligação com sistemas informatizados, dado a demanda e agilidade na execução de operações e a magnitude da empresa, devem ser estipulados procedimentos que salvaguardem os sistemas de processamento de dados.

No tocante a segurança de telecomunicações, todo o cabeamento telefônico em que o setor do banco atua é de exclusiva responsabilidade da empresa, não podendo ser delegado ou registrado licitação para fazê-lo. Isso visa à proteção contra interceptação de dados.

3.0 Análise

Ao descrever o maior desafio da empresa - mudar o comportamento das pessoas para que as mesmas tenham disposição para aplicar os procedimentos de segurança corporativa no ambiente de trabalho por meio de ferramentas educacionais, gerenciais e conscientização - foi efetuada uma pesquisa interna, por meio de um questionário.

3.1 Pesquisa de conceitos

O questionário foi aplicado ao público restrito de funcionários, de um determinado departamento da empresa. Os resultados demonstram o que é refletido nas atividades diárias dessas pessoas no ambiente de trabalho, em relação à segurança corporativa, baseada nos segmentos propostos por Mandarini (2005).

A cada item foi atribuído um conceito numérico na escala de 1 a 5, sendo que o conceito 1 é caracterizado como totalmente inadequado e o conceito 5 como totalmente adequado. Os itens avaliados para cada segmento da segurança corporativa foram:

A) **Segurança das Áreas e Instalações**

Procuramos abordar qual a opinião do público interno:

- De acesso de pessoas no ambiente interno da organização;
- O planejamento de evacuação em caso de incêndios;
- Iluminação do ambiente;
- Adequação e conservação das instalações;
- Sinalização.

B) Segurança de RH

Procuramos abordar qual a opinião do público interno em relação aos procedimentos de segurança:

- Da admissão de pessoas;

• Dos critérios de avaliação em estágio probatório;

• Da avaliação comportamental dos funcionários.

C) Segurança de processos

Procuramos abordar qual a opinião do público interno em relação aos procedimentos na segurança:

• Em relação aos planejamentos de procedimentos operacionais;

• Controle das atividades que causam impactos negativos a imagem da empresa por falhas operacionais;

• O grau de segurança repassada pelas orientações normativas e procedimentos operacionais.

D) **Segurança de conhecimentos**

Procuramos abordar qual a opinião do público interno em relação aos procedimentos na segurança:

• De controle que salvaguarde informações de caráter confidencial ou estratégico;

• Do controle para consulta, armazenagem, e destruição de arquivos;

• Da política de concessão de acesso a informações pelo critério da “necessidade de conhecer”;

• Apresentada pelos sistemas tecnológicos da empresa.

Ainda foram apurados dois itens que indicam a disposição dos funcionários em conhecer as práticas das atividades da segurança corporativa no trabalho.

3.2 Resultados

A nota corresponde à média aritmética dos conceitos atribuídos para cada item do segmento da segurança corporativa, resultando nos seguintes gráficos:

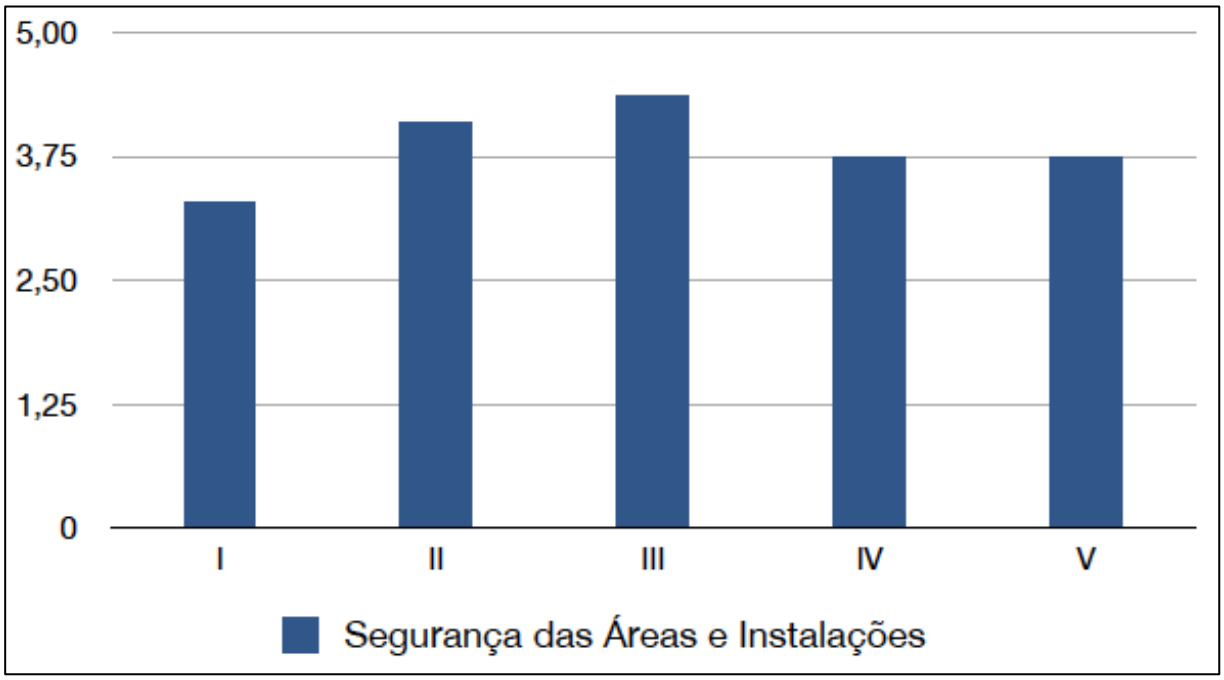

Gráfico 1: Segurança das Áreas e Instalações
Fonte: Autoria Própria

Em que:

I - acesso de pessoas ao ambiente interno da empresa;

II - o planejamento de evacuação em caso de incêndio;

III - iluminação do ambiente;

IV - adequação e conservação das instalações físicas;

V - sinalização.

O controle de acesso de pessoas nos escritórios da empresa recebeu o conceito menor entre os avaliados, com média aritmética de 3,83, em contrapartida, a segurança de iluminação dos ambientes recebeu o maior conceito, com média aritmética de 4,36.

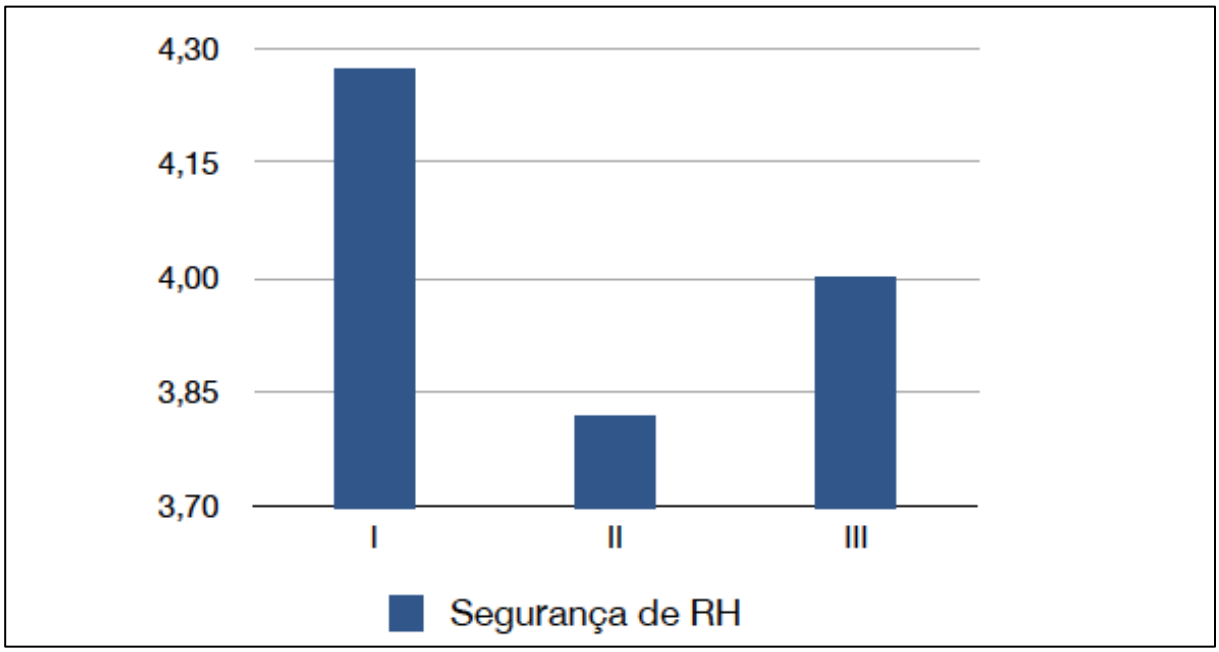

Gráfico 2: Segurança de RH
Fonte: Autoria Própria

Em que:

I - admissão de pessoas;

II - critérios de avaliação em estágio probatório;

III - avaliação comportamental dos funcionários;

O menor conceito foi atribuído ao critério adotado pela administração para avaliar o RH durante o estágio probatório, com média aritmética de 3,81 enquanto os procedimentos adotados para resguardar a empresa de riscos na admissão de RH receberam o maior conceito, com média aritmética de 4,27.

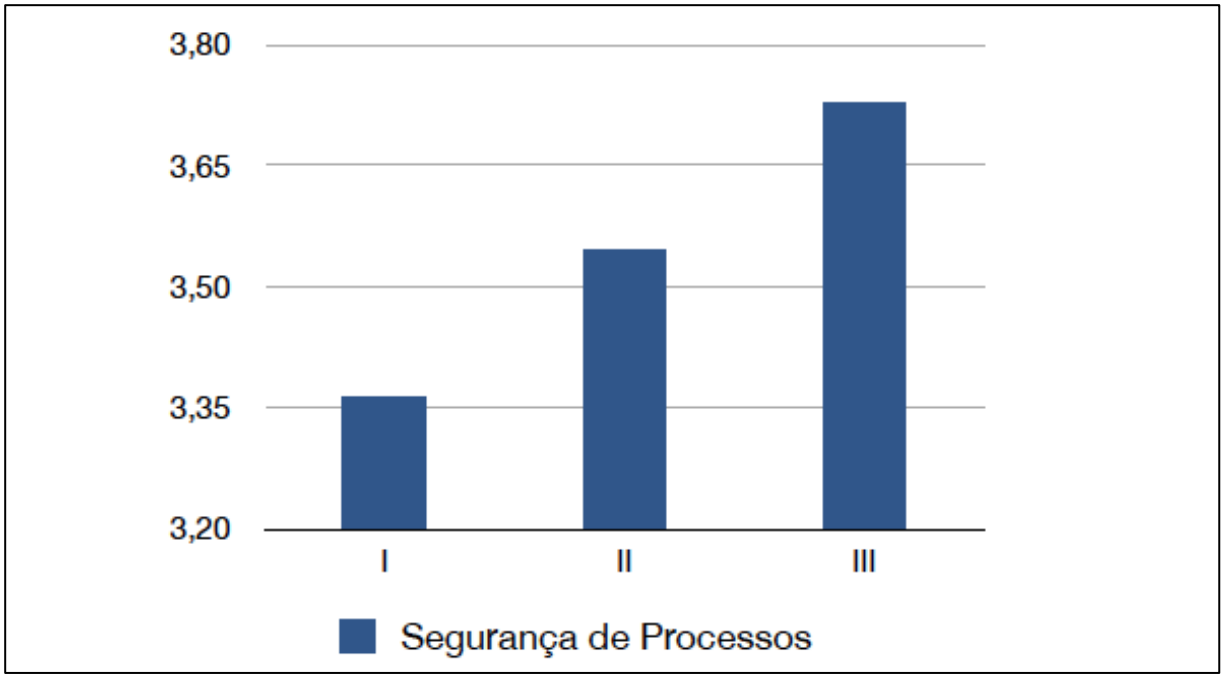

Gráfico 3: Segurança de Processos
Fonte: Autoria Própria

Em que:

I - controle das atividades que causam impactos negativos a imagem da empresa por falha operacional;

II - grau de segurança repassada pela interpretação de orientações normativas;

III - planejamento de procedimentos operacionais;

O menor conceito foi atribuído ao controle das atividades consideradas sensíveis, com média aritmética de 3,36 e o planejamento gerencial para executar as atividades operacionais recebeu o maior conceito nesse segmento, com média aritmética de 3,72.

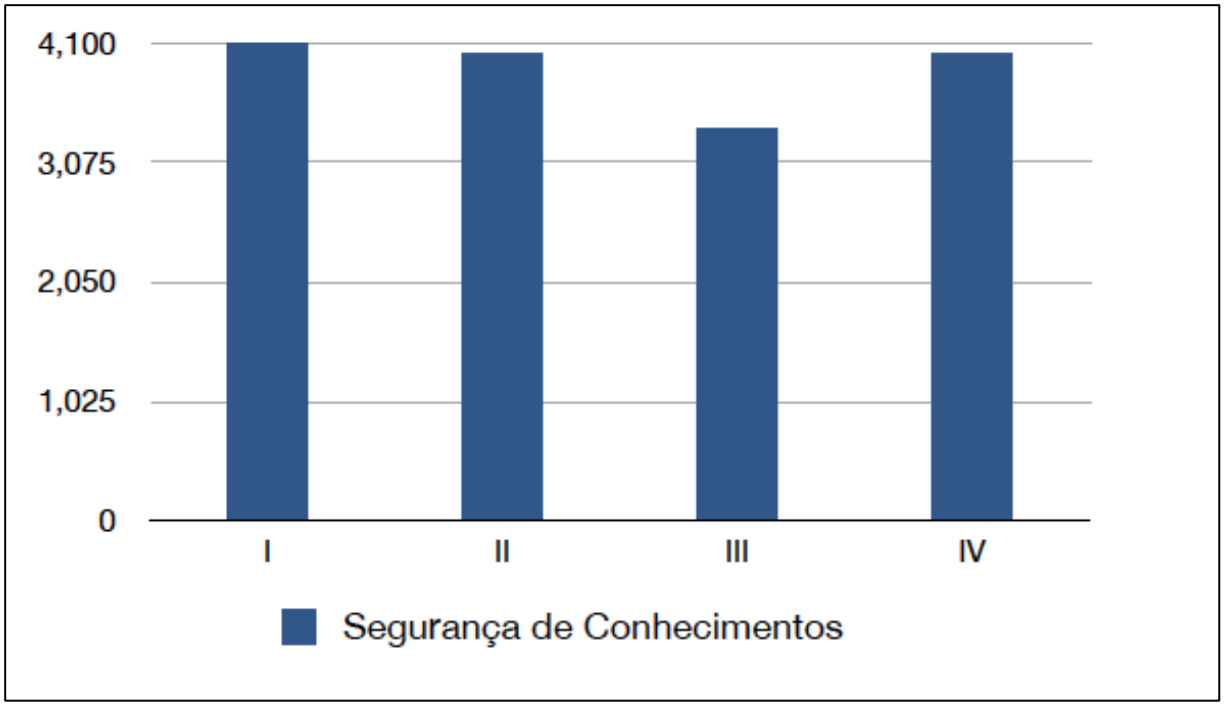

Gráfico 4: Segurança de Conhecimentos
Fonte: Autoria Própria

Em que:

I - controle que salvaguarde informações de caráter confidencial ou estratégico;

II - controle para consulta, armazenagem e destruição de arquivos;

III - política para concessão de acesso a informações pelo critério da "necessidade de conhecer";

IV - sistemas tecnológicos e ferramentas de trabalho fornecidas pela empresa.

O menor conceito foi atribuído à política de concessão de acesso a informações, com média aritmética de 3,63 e houve empate de conceitos entre o gerenciamento de arquivos e a segurança apresentada pelas ferramentas de trabalho e soluções tecnológicas fornecidas pela empresa, com média aritmética 4,0.

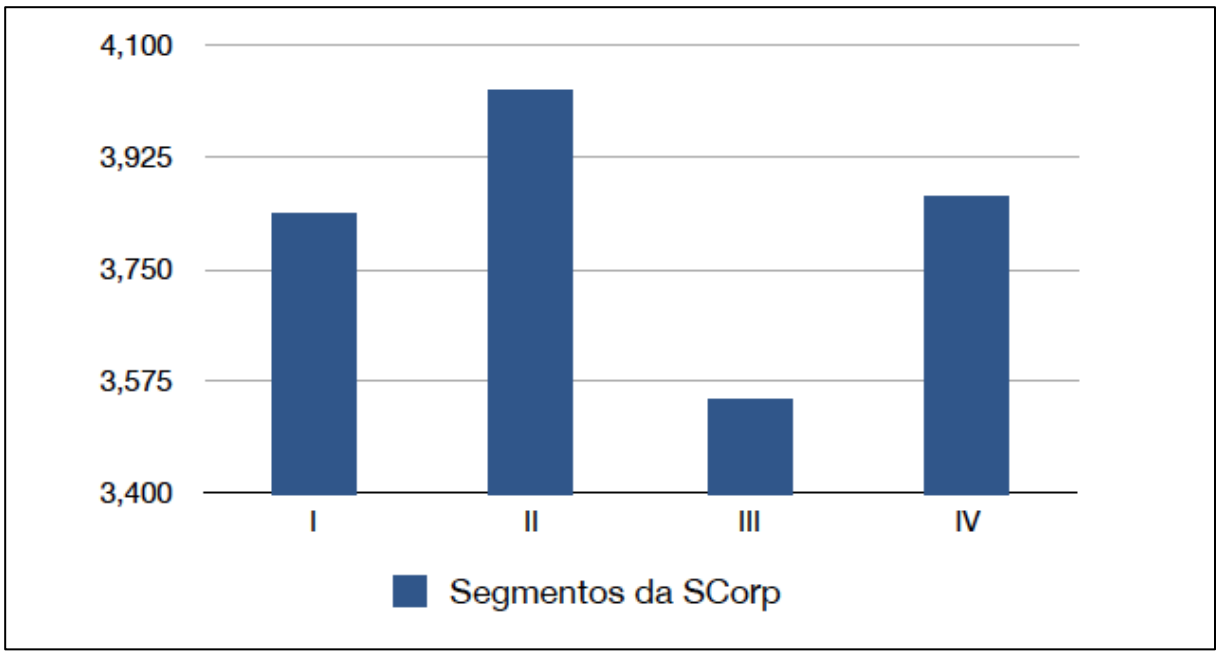

Gráfico 5: Segurança da SCorp
Fonte: Autoria Própria

Em que:

I - Segurança de Áreas e Instalações;

II - Segurança de RH;

III - Segurança de Processos;

IV - Segurança de Conhecimentos.

Entre os segmentos da Gestão Estratégica de Segurança Corporativa, observa-se que a Segurança de RH obteve o maior conceito pelo público avaliador, com média geral de 4,03 e o menor conceito foi atribuído às políticas de gestão de segurança dos processos, com média geral de 3,54.

A pesquisa revela que os funcionários estão mais dispostos em aplicar e implementar medidas de segurança no trabalho, com média aritmética de 4,63, a conhecer as políticas de segurança, com média aritmética de 4,36, conforme pode ser observado no gráfico abaixo.

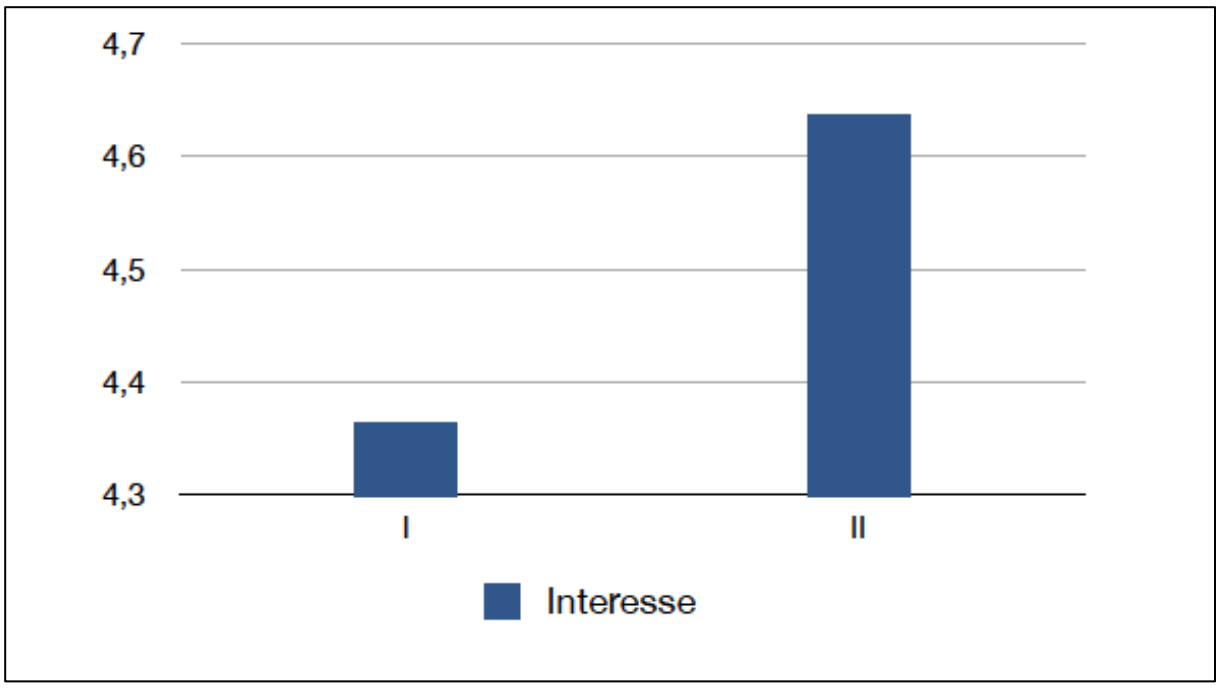

Gráfico 6: Interesse
Fonte: Autoria Própria

Em que:

I - Conhecer as políticas de segurança Corporativa;

II - Aplicar e implementar que visem à segurança dos ativos da empresa;

3.3 Interpretação

A partir dos resultados acima obtidos, podem-se quantificar os procedimentos que merecem maior atenção sob o ponto de vista da segurança.

Foi observado que o controle para execução de atividades que potencialmente prejudiquem a imagem da empresa por falha operacional poderia ser implementada.

Dentre as diversas soluções possíveis para incrementar a segurança operacional, para esse caso seria apropriado confeccionar o fluxograma, tipo de diagrama o qual pode ser entendido como uma representação esquemática de um processo, ou *flowchart* de atividades inerentes ao serviço.

Aliado ao respaldo das normas operacionais internas, ao definir os passos de execução operacional vê-se a oportunidade de estudar eventos imprevistos que possam interromper o fluxo normal do processo. Simular situações críticas e ao definir os procedimentos de contingência constitui caráter preventivo, que é justamente o objetivo da segurança estratégica.

> (...) quando seus resultados agregam grande diferencial de segurança ao processo institucional como um todo, evitam que agregue insegurança ao referido processo e desenvolvem uma profícua mentalidade de segurança no ambiente corporativo. (MANDARINI, 2005, p. 83).

Constitui política do banco, que todas as suas dependências analisem os impactos causados por situações imprevistas que afetem o desenvolvimento de suas atividades, testá-las e formalizá-las em documento para consulta, implementos e revisões periódicas.

O resultado demonstra que o quadro funcional está disposto a aplicar procedimentos de segurança, conforme Mandarini:

> A segurança corporativa deve ser implementada de maneira que incentive o envolvimento do público interno com os objetivos que busca alcançar. As medidas e procedimentos que prevê devem interferir minimamente e ser de forma natural absorvidos e adotados pelo processo institucional. (MANDARINI, 2005, p. 292).

4.0 Considerações finais

A Segurança Corporativa á altamente dinâmica, multidisciplinar e que os setores responsáveis pelo assessoramento, gestão, normatização, fiscalização, treinamento e capacitação da gestão de segurança possuem forte influência em todos os departamentos da empresa.

Sendo multidisciplinar e de grande extensão, seu conteúdo é complexo e exige estudo minucioso do projeto de implante da gestão de segurança, ainda que alguns tópicos da própria segurança corporativa demandem conhecimentos técnicos, sua política estará em integrada aos negócios e com as atividades e operações cotidianas da empresa, assegurando a continuidade dos seus negócios e longevidade de atuação no mercado.

Tão importante quanto salvaguardar o que é estratégico é a qualidade de vida no ambiente de trabalho. E que as pessoas fazem parte da proteção dos ativos da empresa, todavia também seja exigida de órgãos governamentais e atenção ao cumprimento das normas regulamentadoras que visam à manutenção da saúde e bem estar do RH, no desempenho de suas atividades.

Ao incentivar os funcionários a adotar e exercer práticas que visem à proteção patrimonial, ativos tangíveis e intangíveis, contribui-se para implementos de processos e controles internos. Como observado, o maior desafio da empresa que é objeto de análise desse trabalho é: “mudar o comportamento das pessoas”.

Portanto, por mais eficiente que o controle seja em uma organização, a falha operacional sempre estará presente, e o objetivo não é erradicá-la, embora fosse o ideal, mas sim minimizar os impactos negativos decorrente dela, para que não prejudique o andamento dos negócios da empresa a ponto de paralisar suas atividades.

5.0 REFERÊNCIAS

ACORDO DE BASILÉIA. **Bank for International Settlements.** Disponível em: <http://www.bis.org/ >. Acesso em: 01 ago. 2010.

ACORDO DE BASILÉIA 2. **Legislação e Normas. Basiléia II**. Disponível em: <http://www.bacen.gov.br/?BASILEIA2 >. Acesso em: 01 ago. 2010.

AGÊNCIA NACIONAL DE TRANPORTES TERRESTRES. **Faq – Transportes Terrestres de Produtos Perigosos.** Disponível em: <http://www.antt.gov.br/faq/produtos_perigosos.asp>. Acesso em: 07 mar. 2011

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Informação e documentação-Trabalhos Acadêmicos – Apresentação**: NBR 14724. Rio de Janeiro, 2002. 6 p.

BANCO CENTRAL DO BRASIL (BACEN). **O que é e o que faz do Banco Central do Brasil**. Disponível em: <http://www.bcb.gov.br/pre/portalCidadao/bcb/bcFaz.asp?idpai=PORTALBCB>. Acesso em: 06 jan. 2011.

BARBOSA, Emerson R; BRONDANI, Gilberto. Planejamento Estratégico Organizacional. **Revista Eletrônica de Contabilidade**. Universidade Federal de Santa Maria, RS. Dezembro 2004 – Fevereiro 2005. Volume: 1. N.2 Disponível em: < http://w3.ufsm.br/revistacontabeis/anterior/artigos/vIn02/a08vIn02.pdf> Acesso em: 05 abr. 2011.

BENITE, Anderson. **Sistema de Gestão Segurança e Saúde no Trabalho para Empresas Construtoras**. 2004. Dissertação (Mestrado em Engenharia). Universidade de São Paulo. Disponível em: < http://www.pcc.usp.br/fcardoso/Dissertação%20Anderson%20-%20Completa%20-%20Final.pdf>. Acesso em: 18 jan. 2011

BESSA, Jorge da Silva. **A espionagem econômica.** Artigo (2001). Associação Brasileira dos Analistas de Inteligência Competitiva (ABRAIC). Disponível em:< http://www.fiescnet.com.br/senai/conhecimento/arquivos/anais/DraKira/EspionagemEconomica-JorgeBessa.pdf>. Acesso em: 27 mar. 2011.

BRASIL, Constituição Federal (1988). **Capítulo V - Da Administração Pública, Art. 37. Inc. II.** Disponível em: <http://www.stf.jus.br/portal/constituicao/constituicao.asp>. Acesso em 07 fev. 2010

BRASIL, Decreto n° 4553 de 27 de Dezembro de 2002 Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências. **Diário Oficial da União República Federativa do Brasil**, Brasília, DF, 30 dez. 2002. Disponível em: < http://www010.dataprev.gov.br/sislex/paginas/23/2002/4553.htm>. Acesso em: 20 abr. 2011.

BRASIL, Lei n° 7.102 de 20 de Junho de 1983. Dispõe sobre segurança para estabelecimentos financeiros, estabelece normas para constituição e funcionamento das empresas particulares que exploram serviços de vigilância e de transporte de valores, e dá outras providências**. Diário Oficial da União República Federativa do Brasil**, Brasília, DF, 21 jun. 1983. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L7102.htm>. Acesso em: 20 abr. 2011

BRASIL, Portaria 387/2006. Departamento da Polícia Federal. DG.DPF. **Diário Oficial da União República Federativa do Brasil**, Brasília, DF, 01 set. 2006. Disponível em: <http://www.dpf.gov.br/>. Acesso em 20 abr. 2011.

COOPERCAMPOS, informativo interno. Santa Catarina, 10. Fev. 2011, ed. 85, p. 1. Disponível em: <http://www.copercampos.com.br/editar/arquivos/editar_informativo/09022011coperacao85.pdf>. Acesso em: 15 mar. 2011

CHIAVENATO, Idalberto. **Gestão de Pessoas: e o novo papel dos recursos humanos Organizacionais**. Rio de Janeiro. Elsevier, 2004.

Empresas reforçam segurança para inibir assaltos. **Administradores**. Maio, 08 2010. Disponível em: <http://www.administradores.com.br/informe-se/administracao-e-negocios/empresas-reforcam-seguranca-para-inibir-assaltos/33087/>. Acesso em: 08 mar. 2011.

ENDOMARKETING. **O que é endomarketing.** Disponível em: <http://www.endomarketing.com/endomarketing.html>. Acesso em: 15 jan. 2011.

ESCRITÓRIO DAS NAÇÕES UNIDAS SOBRE DROGAS E CRIME (UNODC). Brasil e Cone Sul. **Sobre o ONUDC**. Disponível em: <http://www.unodc.org/southerncone/pt/sobre-unodc/index.html>. Acesso em: 06 jan. 2011.

FEDERAÇÃO BRASILEIRA DOS BANCOS (FEBRABAN). **Sobre a Febraban**. Disponível em: <http://www.febraban.org.br/Febraban.asp>. Acesso em 05: jan. 2011.

FEDERAÇÃO BRASILEIRA DOS BANCOS (FEBRABAN). **Portas Giratórias**. Disponível em: < http://www.febraban.org.br/Arquivo/Destaques/destaque-giratoria.asp>. Acesso em 05: jan. 2011.

GOMES, Adriano da Silva; JUNIOR, Antonio Robles. **Os Impactos na Atividade de Auditoria Independente com a Introdução da Lei de Sarbannes-Oxlei.** Disponível em: <http://www.eac.fea.usp.br/cadernos/completos/48/adriano-antonio-pg103a111.pdf>. Acesso em: 15/02/2011.

GOVERNANÇA CORPORATIVA. **O que é Governança Corporativa**. Disponível em: < http://www.bmfbovespa.com.br/cias-listadas/consultas/governanca-corporativa/governanca-corporativa.aspx?Idioma=pt-br >. Acesso em: 05 jan. 2011.

GROSS, Lima; LIMA, Julio Sérgio. A seleção de pessoal. O desafio de agregar talentos à organização. **Instituto Catarinense de Pós Graduação**, SC. 23 out. 2008. Disponível em: < http://www.icpg.com.br/artigos/rev04-05.pdf>. Acesso em 20 mar. 2011.

HOSS, O.; ROJO, C.A.; GRAPEGGIA, M. **Gestão de ativos intangíveis: da mensuração à competitividade por cenários**. São Paulo: Atlas, 2010.

INSALUBRIDADE. **Conceito de Insalubridade**. Rui Juliano Perícias. Disponível em: < http://www.manualdepericias.com.br/conceitoinsalubridade.asp>. Acessado em: 05 jan. 2011.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATISTICAS. **Dia nacional de prevenção de acidentes no trabalho.** Disponível em: < http://www.ibge.gov.br/ibgeteen/datas/acidentes/home.html> Acesso em: 03 mar. 2011.

JUNIOR, Cirilo. Folha OnLine, RJ, 14 fev. 2008, Petrobrás confirma roubo de informações sigilosas. Disponível em: <http://www1.folha.uol.com.br/folha/dinheiro/ult91u372319.shtml>. Acesso em: 10 abr. 2011.

JÚNIOR, José Cairo. O acidente de trabalho e a responsabilidade civil do empregador. 2. ed. São Paulo: LTr, 2004.

KASSOUF, Ana Lúcia. **Trabalho Infantil: Causas e Consequências.** Universidade de São Paulo (USP). Disponível em: < http://www.cepea.esalq.usp.br/pdf/texto.pdf>. Acesso em: 20 fev. 2010.

LASTRES, Helena; ALBAGLI, Sarita. **Informação e Globalização na Era do Conhecimento.** Editora Campus Ltda, 1999. Disponível em: < http://www.uff.br/ppgci/editais/saritalivro>. Acesso em: 20 fev. 2011.

LAUREANO, Marcos Aurelio Pchek. GESTÃO DE SEGURANÇA DA INFORMAÇÃO. PUC-PR (2005). Disponível em: <www.m**laureano**.org/aulas_material/gst/apostila_versao_20.pdf> Acesso em: 15 mar. 2011.

LER NO MERCADO. **10 perguntas e respostas sobre as LER/Dort**. Bras Golden mundo ergonomia. Disponível em: < http://www.mundoergonomia.com.br/website/artigo.asp?id=3166&cod=1847&idi=1&xmoe=74&moe=74 > . Acesso em: 07. ago. 2010.

LEI PROÍBE PORTA GIRATÓRIA EM BANCOS EM SP. G1-São Paulo, São Paulo, 12 fev. 2007. Disponível em: < http://g1.globo.com/Noticias/SaoPaulo/0,,MUL215745-5605,00-LEI+PROIBE+PORTA+GIRATORIA+EM+BANCOS+DE+SP.html>. Acesso em: 09 fev. 2010.

LIMA, Sabrina Ferreira. **O sigilo Bancário e a violação ilegal dos direitos à intimidade e privacidade**. Direito Net. 08 jun. 2004. Disponível em: < http://www.direitonet.com.br/artigos/exibir/1593/O-sigilo-bancario-e-a-violacao-ilegal-dos-direitos-a-intimidade-e-privacidade>. Acesso em: 20 jan. 2011.

LIMA, Siderley A. de, Segurança Empresarial. WEBArtigos. Administração e Negócios. 02 fev.2010. Disponível em: < http://www.webartigos.com/articles/46287/1/SEGURANCA-EMPRESARIAL/pagina1.html>. Acesso em: 07 mar. 2011.

LOBO, Rafael. **SIPAT.** WEBartigos. 22 fev. 2011. Disponível em: <http://www.webartigos.com/articles/59810/1/SIPAT/pagina1.html.> Acesso em: 07 mar. 2011.

MACHADO, João Luiz de Almeida. **Condições de Trabalho na Revolução Industrial**. De olho na história. Disponível em:< http://www.planetaeducacao.com.br/portal/artigo.asp?artigo=1055>. Acesso em: 19/01/2010.

MANDARINI, Marcos. **Segurança Corporativa Estratégica**. São Paulo: Manole, 2005.

MAROFUSE, N; MARZIALE, M. Mudanças no trabalho e na vida dos bancários portadores de L.E.R. Rev. Latino Americana de Enfermagem, São Paulo, SP. Julho, 2001, 9 (4): p. 19-24. Disponível em: <http://www.scielo.br/pdf/rlae/v9n4/11478.pdf>. Acesso em: 15 abr. 2011.

MORE, Lucila Fernandes. **A CIPA analisada sob a ótica da ergonomia e da organização do trabalho-proposta de criação da Comissão de Estudos do Trabalho.** Dissertação (1997). Universidade Federal de Santa Catarina. Disponível em:< http://aspro02.npd.ufsc.br/pergamum/biblioteca/index.php?resolution2=1024_1&tipo_pesquisa=#posicao_dados_acervo>. Acesso em: 09 fev. 2011.

MATOS, Celso A.; VEIGA, Ricardo T. Os efeitos da publicidade negativa nas atitudes dos consumidores. **Caderno de Pesquisas em Administração**, São Paulo, abril/junho 2003, p. 69-86. Disponível em: <http://www.ead.fea.usp.br/cad-pesq/arquivos/v10n2art5.pdf>. Acesso em: 07 abr. 2011.

MORETTI, Cláudio dos Santos. As mudanças na Segurança privada no Brasil. Revista Eletrônica Brasiliano & Associados. n. 25, p. 6-18, out. 2006.

NEVES, Maria de Fátima Gama. **Trabalho em Educação com Jovens e Adultos**. Artigo (2011). Disponível em:< http://www.webartigos.com/articles/57574/1/TITULO-TRABALHO-EM-EDUCACAO-COM-JOVENS-E-ADULTOS/pagina1.html>. Acesso em: 20 abr. 2011.

NORMAS REGULAMENTADORAS. Legislação e Normas. Ministério de Trabalho e Emprego. Disponível em: < http://portal.mte.gov.br/legislacao/normas-regulamentadoras-1.htm >. Acesso em: 05 set. 2010.

OCORRÊNCIAS E ACIDENTES NO TRABALHO. **Segurança e Saúde no Trabalho.** Inspeção do Trabalho. Ministério de Trabalho e Emprego. Disponível em: < http://portal.mte.gov.br/seg_sau/resultados-da-fiscalizacao-em-seguranca-e-saude-no-trabalho-brasil-2010.htm >. Acesso em: 07 ago. 2010.

OCORRÊNCIAS DE ASSALTOS EM AGÊNCIAS BANCÁRIAS. **Febraban Divulga número de assaltos a bancos**. Contraf/CUT. Disponível em: < http://www.seebfloripa.com.br/index.php?option=com_content&view=article&id=1063:febraban-divulga-numero-de-assaltos-a-bancos&catid=57:saude-seguranca&Itemid=248> Acesso em: 10 jan. 2010.

ORGANIZAÇÃO INTERNACIONAL DO TRABALHO (OIT). Apresentação. Disponível em: < http://www.oit.org.br/content/apresentação> . Acesso em: 05 jan. 2011.

PERES, Leandra. Folha de São Paulo, SP, 29 abr. 2007, O país gasta cerca de R$ 981 milhões com ler em bancários. Disponível em: < http://www.cmqv.org/website/artigo.asp?cod=1461&idi=1&moe=212&id=9550>. Acesso em: 10 abr. 2011.

PERICULOSIDADE. **Conceito de Periculosidade.** Rui Juliano Perícias. Disponível em: <http://www.manualdepericias.com.br/conceitopericulosidade.asp >. Acesso em: 05 jan. 2011.

PREVIDÊNCIA SOCIAL. **Sobre a previdência Social**. Ministério da Previdência Social. Disponível em: <http://www.previdenciasocial.gov.br/conteudoDinamico.php?id=33>. Acesso em: 05 jan. 2011.

POLÍCIA FEDERAL. **Plano de Segurança Bancária.** Disponível em: <http://www.dpf.gov.br/servicos/seguranca-privada/servicos/plano-de-seguranca-bancaria> Acesso em: 07 jan. 2011.

PORTELLA, Paulo Roberto Aguiar. **Segurança física. Sistemas de Proteção**. História, Metodologia e Doutrina. Ed. 3˚, Rio de Janeiro, 2010.

RAMOS, Anderson (org.). ***Security Officer* - 1**: Guia oficial para formação de gestores em segurança da informação. Porto Alegre, RS: Zouk, 2006.

ROCHA, Osvaldo F. N. **EPI, Por que?** Artigo (2011). PUC-SP. Disponível em: < http://www.pucsp.br/cipa/artigos/epi.htm> Acesso em: 18 fev. 2011.

ROCHA, Luiz Fernando. **História da CIPA.** Disponível em: < http://acordocoletivo.org/2011/03/01/historia-da-cipa-2/>. Acesso em: 10 mar. 2011.

SANTOS, Neri dos. **Ergonomia e Segurança Industrial.** Estudo Dirigido, n˚,1. Universidade Federal de Santa Catarina. Disponível em:< http://www.ergonomianotrabalho.com.br/artigos/Os_objetivos_da_Ergonomia.pdf>. Acesso em: 25 mar. 2011.

SEGURANÇA DA INFORMAÇÃO. Conceitos e definição. Origem: Wikipédia, a enciclopédia livre. Disponível em: <http://pt.wikipedia.org/wiki/Segurança_da_informação> . Acesso em: 01 ago. 2010.

SÊMOLA, Marcos. **Gestão da segurança da informação**: visão executiva da segurança da informação aplicada ao *Security Officer*. Rio de Janeiro: Elsevier, 2003.

SÊMOLA, Marcos. Segurança da Informação: Lendas e Verdades. **Coluna Firewall**. 30 jun. 2001. Disponível em: < http://www.semola.com.br/disco/Coluna_IDGNow_33.pdf>. Acesso em: 16 abr. 2011.

SEGURANÇA E SAÚDE NO TRABALHO. Riscos. **Tabelas de Riscos**. Segurança e Medicina no trabalho. Disponível em: < http://www.sstvda.com/riscos.html> . Acesso em: 05 jan. 2011.

SILVA, et al. A lei de Sarbanex Oxley e seus efeitos nas transparências para os investidores brasileiros em empresas S/A. São Paulo, SP, des. 2007. Disponível para consulta em: < http://www.praticacontabil.com/contadorperito/Lei_Sarbanes_Oxley_e_seus_efeitos.pdf>. Acesso em: 08 mar. 2011.

SERVIÇO ESPECIALIZADO EM ENGENHARIA DE SEGURANÇA E SAÚDE NO TRABALHO. **Breve história sobre o SESMT.** Disponível em: <http://segurancaesaudedotrabalho.blogspot.com/2009/07/breve-historia-sobre-o-sesmt.html> Acesso em: 19 dez. 2010.

STRESS E ASSÉDIO MORAL. LIPP, M. N. **Pesquisas Sobre o Stress no Brasil**. São Paulo: Papirus,1996**.** Disponível em: < http://www.assediomoral.org>. Acesso em: 15 jan. 2011.

TERRA, José Cláudio. **Gestão da Criatividade.** Artigo (2009). Biblioteca Terra Fórum Consultores. Disponível em: < http://www.slideshare.net/jcterra/gesto-da-criatividade>. Acesso em: 05 abr. 2011.

UNIVERSIDADE CORPORATIVA BB, **Controles Internos**. Brasília, 2008.

UNIVERSIDADE CORPORATIVA BB, **Gestão de Segurança**. Brasília, 2008.

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ. **Normas para elaboração de trabalhos acadêmicos.** Curitiba, 2008.

VASCONCELOS, Anselmo Ferreira. **Qualidade de Vida no Trabalho: Origem, Evolução e Perspectivas.** Artigo 2001. Disponível em: < http://www.ead.fea.usp.br/cad-pesq/arquivos/v08-1art03.pdf>. Acesso em: 07 mar. 2011.

APÊNDICE A – RISCOS

A tabela abaixo relaciona os riscos que poderão prejudicar o desenvolvimento desse trabalho:

Risco	**(G)**	**(O)**	**IR = GxO**	**M.C. se IR ≥ 30 ou G, O ≥ 5**
Aluno ou equipe sem acesso a informações importantes para realizar o trabalho	5	2	10	I
Conflito entre componentes da equipe	5	4	20	II
Problema formulado não pode ser resolvido	5	6	30	III
Orientador abandona o projeto	10	1	10	IV
Orientador não orienta	7	1	7	V
Conflito entre orientador e co-orientador	6	6	36	VI
Membro da equipe abandona projeto	4	1	4	Não se aplica
Financiamento é cancelado	1	1	1	Não se aplica

Glossário:

(G): Gravidade, sendo $1 \leq G \leq 10$

(O): Probabilidade de ocorrência, sendo $1 \leq O \leq 10$

IR : Índice de Risco

M.C.: Medida de Contingência

Medidas de Contingência:

I - Busca por outros referenciais que se enquadrem no tema abordado neste trabalho;

II - Não chegando a entendimento, recorrer à intermediação do orientador do projeto

III - Reformular/alterar o tópico abordado que não seja passível de solução;

IV - Procurar avaliar os motivos do abandono e se a decisão é irreversível, caso não seja obtido sucesso, buscar auxílio do orientador do curso;

V - Recorrer ao co-orientador e convocar reunião entre membros da equipe e os orientadores para chegar a um consenso e explicitar os problemas identificados;

VI - Verificar o motivo que provocou o desentendimento e avaliar se a solução poderá ser resolvida com a alteração de um dos tópicos apresentados nessa proposta. Não sendo possível, deve-se recorrer à instância superior de coordenação e expor os motivos de desacordo, em busca de solução.

APÊNDICE B - PESQUISA DE CAMPO

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO DE ELETRÔNICA E DEPARTAMENTO DE MECÂNICA
CURSO SUPERIOR DE TECNOLOGIA EM MECATRÔNICA INDUSTRIAL
MÓDULO: 6° PERÍODO
UNIDADE CURRICULAR: TRABALHO CONCLUSÃO DE CURSO

Segurança Corporativa
Pesquisa de Campo

O objetivo dessa pesquisa é saber como está conceito dos funcionários participantes em relação às políticas de segurança corporativa da empresa e da sua execução nas atividades operacionais diárias.

Para cada item, atribua um conceito numérico dentro da escala de 1 - 5 sendo que o conceito 1 representa totalmente inadequado e conceito 5 totalmente adequado.

Segurança das Áreas e Instalações

Item	Conceito
Acesso de pessoas ao ambiente interno da empresa	
O planejamento de evacuação em caso de incêndios	
Iluminação do ambiente	
Adequação e conservação das instalações físicas	
Sinalização	

Segurança de RH

Item	Conceito
Da admissão de pessoas	
Dos critérios de avaliação em estágio probatório	
Da avaliação comportamental dos funcionários	

Segurança de processos

Item	Conceito
Em relação às atividades que causem impactos negativos a imagem da empresa por falha operacional	
O grau de segurança repassada pela interpretação de orientações normativas	
Do planejamento de procedimentos operacionais	

Segurança de conhecimentos

Item	Conceito
De controle que salvaguarde informações de caráter confidencial ou estratégico	
Do controle para consulta, armazenagem, e destruição de arquivos	

Item	Conceito
Da política de concessão de acesso a informações pelo critério da "necessidade de conhecer"	
Sistemas tecnológicos da empresa	

Agora atribua um conceito na escala numérica de 1 a 5 para os dois itens a seguir, sendo que o conceito 1 caracteriza total indisposição e o conceito 5 caracteriza total disposição:

Item	Conceito
Em Conhecer as políticas de Segurança Corporativa da Empresa	
Em aplicar, implementar procedimentos que visem à segurança dos ativos da empresa	