FRANCINI REITZ SPANCESKI

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO – DESENVOLVIMENTO DE UM MODELO VOLTADO PARA INSTITUIÇÕES DE ENSINO

JOINVILLE
DEZEMBRO / 2004

FRANCINI REITZ SPANCESKI

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO – DESENVOLVIMENTO DE UM MODELO VOLTADO PARA INSTITUIÇÕES DE ENSINO

Trabalho de Conclusão de Curso submetido ao Instituto Superior Tupy, como parte dos requisitos para a obtenção do grau de Bacharel em Sistemas de Informação, sob orientação do professor Marcos Aurélio Pchek Laureano.

JOINVILLE
2004

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO – DESENVOLVIMENTO DE UM MODELO VOLTADO PARA INSTITUIÇÕES DE ENSINO

FRANCINI REITZ SPANCESKI

Este trabalho de diplomação foi julgado adequado para obtenção do Título de Bacharel em Sistemas de Informação, e aprovado em sua forma final pelo departamento de Informática do Instituto Superior Tupy.

Joinville, 16 de Dezembro de 2004.

_____

Marcos Aurélio Pchek Laureano, Mestre em Informática Aplicada.
Orientador

_____

Marco André Lopes Mendes, Mestre em Ciência da Computação.
Coordenador do Curso

Banca Examinadora:

_____

Amir Tauille, Mestre em Ciência da Computação.

_____

Fernando Cézar de Oliveira Lopes, Mestre em Ciência da Computação.

Dedico este trabalho à memória de José Henrique Reitz, meu pai, pessoa que admirei, amei e compreendi, pai que me deu a oportunidade de realizar os meus sonhos, e o amigo que me acompanhou nos momentos marcantes de minha vida.

AGRADECIMENTOS

Agradeço aos meus pais pelo apoio e incentivo no início do curso, ao meu marido pela paciência e compreensão em todos os momentos durante estes quatro anos, ao meu filho pelo amor e compreensão nos momentos de ausência.

Agradeço a SOCIESC pelo incentivo durante o curso, ao Professor Marcos Laureano pelo compartilhamento de sua experiência e orientação durante todo o trabalho, a Professora Glaci pela orientação quanto a metodologia, e a todos aqueles que direta ou indiretamente contribuíram nesta caminhada.

RESUMO

O presente trabalho aborda um estudo sobre política de segurança da informação que é uma das principais medidas de segurança adotadas pelas organizações com o objetivo de garantir a segurança da informação. Atualmente existem algumas metodologias e melhores práticas em segurança da informação, dentre elas está a NBR ISO 17799, que é a tradução da BS7799, esta norma foi usada durante este estudo e, por meio dela, será possível verificar o que devemos seguir para a elaboração de uma política de segurança da informação, as principais dificuldades para criação e implementação, os princípios de segurança da informação, a necessidade de envolvimento de toda a organização, sendo que pretende-se elaborar uma proposta modelo de política de segurança da informação voltada para instituições de ensino. O objetivo deste trabalho é apresentar algumas diretrizes básicas de uma Política de Segurança para uma empresa, utilizando como base os conceitos adquiridos pelo estudo na revisão bibliográfica.

Palavras Chave: Informação; Segurança da Informação; Medidas de Segurança; Política de Segurança.

ABSTRACT

The present work approaches a study on Security Policies of the information that is one of the main measures of security of the information. Currently there are some practical better methodologies and in security of the information , amongst them are NBR ISO 17799 that he is BS 7799 translation, this norm was used during this study and, for way of it, it will be possible to verify what we must follow for the elaboration of one politics of security of the information, the main difficulties for creation and implementation, the principles of security of the information, the necessity of envolvement of all the organization, being been that it is intended to elaborate a proposal model of Security Policies of the information come back toward Institutions of Education. The objective of this work is to present some basic lines of direction of one Security Policies for a company, being used as base the concepts acquired for the study in the bibliographical revision.

Words Key: Information; Security of the Information; Measures of Security; Security Policies.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

Nos tempos atuais a informação tornou-se o ativo mais valioso das grandes empresas, ao mesmo tempo, que passou a exigir uma proteção adequada. De forma assustadoramente crescente, as organizações, seus sistemas de informações e suas redes de computadores apresentam-se diante de uma série de ameaças, sendo que, algumas vezes, estas ameaças podem resultar em prejuízos para as empresas.

A segurança da informação visa protegê-la de um grande número de ameaças para assegurar a continuidade do negócio. Esta segurança é obtida a partir da implementação de uma série de controles, que podem ser políticas, práticas e procedimentos, os quais precisam ser estabelecidos para garantir que os objetivos de segurança específicos da organização sejam atendidos.

A dificuldade de entender a importância da segurança da informação ainda é muito grande. Muitas empresas começam a pensar na implantação de medidas de segurança após terem passado por algum tipo de incidente de segurança, que lhes tenha causado algum prejuízo.

A política de segurança de uma empresa é, provavelmente, o documento mais importante em um sistema de gerenciamento de segurança da informação. Seu objetivo é normatizar as práticas e procedimentos de segurança da empresa. Isso significa que dever ser simples, objetiva, de fácil compreensão e aplicação. Os controle de segurança, de um modo geral, e a política, em particular, devem ser definidos para garantir um nível de segurança coerente com o negócio da empresa.

O presente trabalho tem como objetivo fazer um estudo aprofundado sobre segurança da informação, detalhando este estudo sobre uma das medidas de segurança que é política de

segurança da informação, bem como o desenvolvimento de uma proposta modelo de política de segurança, desenvolvida para a realidade de instituições de ensino, apresentando a estrutura de informática da SOCIESC.

A política de segurança pode trazer ao ambiente de uma instituição de ensino regras e procedimentos que devem ser seguidos para a garantia da segurança da informação. É importante que as informações da política de segurança sejam divulgadas para todos os membros da instituição, sejam eles alunos, funcionários, alunos colaboradores ou estagiários, e que todos estejam conscientes da importância do seguimento desta política.

O presente trabalho está distribuído em 06 (seis) partes, sendo que a primeira é a introdução. A segunda parte inicia a revisão literária, apresentando os conceitos relacionados à segurança da informação, seus princípios, sua importância, as medidas de segurança que podem ser implantadas.

A terceira parte trata de política de segurança, de modo a abranger conceitos sobre política de segurança, seu planejamento, definição e implementação. Existem três tipos de políticas de segurança que foram abordados: Regulatória, Consultiva e informativa.

A quarta parte apresenta o histórico da SOCIESC, sua estrutura de recursos de informática, sua equipe de TI. Na quinta parte mostra o modelo de política de segurança desenvolvido, sendo dividida em política de segurança da estrutura de informática e política de segurança física. Finalmente a conclusão do trabalho, contribuições e sugestões para trabalhos futuros.

O modelo de política de segurança desenvolvido procura definir regras para que, independente do usuário, possa ser seguido um padrão de utilização dos diversos recursos que envolvem a segurança da informação em uma Instituição de Ensino, como a SOCIESC.

2 SEGURANÇA DA INFORMAÇÃO

A informação é um ativo que, como qualquer ativo importante para os negócios, tem um valor para a organização e conseqüentemente necessita ser adequadamente protegida. Para muitas empresas a informação é o maior patrimônio e protegê-la não é uma atividade simples, sendo que pode abranger várias situações, como: erro, displicência, ignorância do valor da informação, fraude, sabotagem, etc.

Define-se dados como um conjunto de bits armazenados como: nomes, endereços, datas de nascimentos, históricos acadêmico, etc. A informação é um dado que tenha sentido, como por exemplo, as notas ou informações acadêmicas de um aluno. O conhecimento é um conjunto de informações que agrega valor a organização.

> A informação pode existir de diversas formas, ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou através de meio eletrônico, mostrada em filmes ou falada em conversas. Seja qual for a forma apresentada ou meio através do qual a informação é compartilhada ou armazenada, é recomendado que seja sempre protegida adequadamente. (NBR ISO/IEC 17799, setembro 2001)

De acordo com a NBR ISO 17799[1], independente da forma que a informação se apresenta ela deve ser protegida de maneira adequada. A segurança deve ser considerada um dos assuntos mais importantes dentre as preocupações das organizações. Deve-se entender que segurança da informação não é uma tecnologia. Não é possível comprar um dispositivo que torne a rede segura ou um software capaz de tornar seu computador seguro. Segurança da informação não é um estado que se pode alcançar.

A segurança é a direção em que se pretende chegar, mas a empresa deve saber que

[1] Norma Brasileira homologada em setembro de 2001 pela ABNT para Gestão da Segurança da Informação

nunca chegará de fato ao destino. O que é possível fazer é administrar um nível aceitável de risco. Segurança é um processo, pode-se aplicar o processo à rede ou à empresa visando melhorar a segurança dos sistemas. (WADLOW, 2000, p.25]

O processo de segurança mostra que em muitos aspectos a segurança é semelhante à tríade grega:

- Analise o problema levando em consideração tudo que conhece: se o problema é a segurança da informação, este deve ser avaliado prestando atenção em tudo que poderá afetar o processo de segurança, visando a criação de uma solução para o problema.
- Sintetize uma solução para o problema a partir de sua análise: sabendo tudo o que pode prejudicar o processo de segurança, neste momento é importante a criação de uma solução que foi estabelecida a partir das informações analisadas anteriormente.
- Avalie a solução e aprenda em quais aspectos não correspondeu a sua expectativa: a solução adotada deve ser avaliado, visando a verificação de medidas ou decisões que não foram satisfatórias para a implantação do processo de segurança, podendo voltar a análise do problema e passando pelas etapas do processo de segurança novamente.

Depois de passar pelas etapas do processo de segurança, deve-se reiniciar este processo seguidamente, o procedimento da tríade grega, de analisar o problema, sintetizar uma solução e avaliar a solução, é um procedimento que pode ser aplicado para qualquer processo.

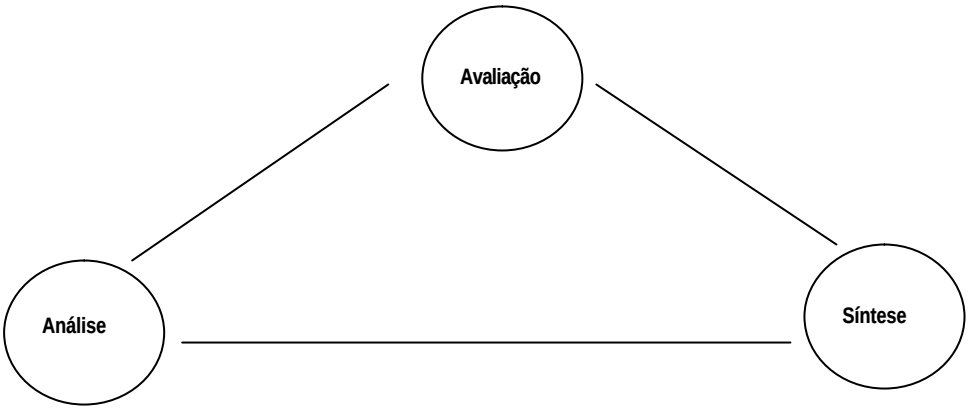


Figura 2.1 - Tríade Grega
Fonte: Livro Segurança da Informação

Os mecanismos de segurança adotados protegem a informação de um grande número de ameaças para assegurar a continuidade dos negócios, minimizar os danos empresariais e maximizar o retorno em investimentos e oportunidades.

> Nenhuma área da informática é tão apreciada como a segurança da informação, todo processo de segurança inicia e tem seu termino em um ser humano. Segurança não é uma questão técnica, mas uma questão gerencial e humana. Não adianta adquirir uma série de dispositivos de hardware e software sem treinar e conscientizar o nível gerencial da empresa e todos os seus funcionários. (OLIVEIRA, 2001, p.43)

De acordo com a afirmação acima, o ser humano tem um papel extremamente importante, na verdade, o processo de segurança começa e termina nas pessoas, os mecanismos de segurança somente serão eficientes se as pessoas se comprometerem com o uso e o façam conscientes dos benefícios para a organização, uma ferramenta ou política que não é usada, não poderá trazer resultados para a organização.

2.1 CLASSIFICAÇÃO DA INFORMAÇÃO

Segundo da descrição do item 5.2 da NBR ISO 17799, que trata da classificação da informação:

> O objetivo da Classificação da Informação é assegurar que os ativos da informação recebam um nível adequado de proteção. A informação deve ser classificada para indicar a importância, a prioridade e o nível de proteção. A informação possui vários níveis de sensibilidade e criticidade. Alguns itens podem necessitar um nível adicional de proteção ou tratamento especial. Um sistema de classificação da informação deve ser usado para definir um conjunto apropriado de níveis de proteção e determinar a necessidade de medidas especiais de tratamento.

A classificação da informação é importante para que as organizações possam determinar o nível de proteção que suas informações, de modo que a segurança de informações importantes para as organizações possa ser assegurada.

A classificação mais comum nos dia de hoje, é aquela que divide em quatro níveis: secreta, confidencial, interna e pública. (DIAS, 2000, p.53)

2.1.1 Secreta

Estas informações devem ser acessadas por um número restrito de pessoas e o controle sobre o uso destas informações deve ser total, são informações essenciais para a empresa, portanto, sua integridade deve ser preservada. O acesso interno ou externo por pessoas não autorizadas a esse tipo de informação é extremamente crítico para a instituição.

2.1.2 Confidencial

Estas informações devem ficar restritas ao ambiente da empresa, o acesso a esses sistemas e informações é feito de acordo com a sua estrita necessidade, ou seja, os usuários só podem acessá-las se estes forem fundamentais para o desempenho satisfatório de suas funções na instituição. O acesso não autorizado à estas informações podem causar danos financeiros ou perdas de fatia de mercado para o concorrente.

2.1.3 Interna

Essas informações não devem sair do âmbito da instituição. Porém, se isto ocorrer as conseqüências não serão críticas, no entanto, podem denegrir a imagem da instituição ou causar prejuízos indiretos não desejáveis.

2.1.4 Públicas

Informações que podem ser divulgadas para o público em geral, incluindo clientes, fornecedores, imprensa, não possuem restrições para divulgação.

2.2 PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

> Quando se pensa em segurança da informação, a primeira idéia que nos vem à mente é a proteção das informações, não importando onde estas informações estejam armazenadas. Um computador ou sistema computacional é considerado seguro se houver uma garantia de que é capaz de atuar exatamente como o esperado. Porém a segurança não é apenas isto. A expectativa de todo usuário é que as informações armazenadas hoje em seu computador, lá permaneçam, mesmo depois de algumas semanas, sem

> que pessoas não autorizadas tenham tido qualquer acesso a seu conteúdo. (DIAS, 2000, p.42)

O usuário espera que suas informações estejam disponíveis no momento e local que determinar, que sejam confiáveis, corretas e mantidas fora do alcance de pessoas não autorizadas. Essas expectativas do usuário podem ser traduzidas como objetivos ou princípios da segurança.

2.2.1 Autenticidade

O controle de autenticidade está associado com identificação de um usuário ou computador. O serviço de autenticação em um sistema deve assegurar ao receptor que a mensagem é realmente procedente da origem informada em seu conteúdo. Normalmente, isso é implementado a partir de um mecanismo de senhas ou de assinatura digital. A verificação de autenticidade é necessária após todo processo de identificação, seja de um usuário para um sistema ou de um sistema para outro sistema. A autenticidade é a medida de proteção de um serviço/informação contra a personificação por intrusos.

2.2.2 Confidencialidade

Proteger informações contra acesso por alguém não autorizado - interna ou externamente. Consiste em proteger a informação contra leitura e/ou cópia por alguém que não tenha sido explicitamente autorizado pelo proprietário daquela informação. A informação

deve ser protegida qualquer que seja a mídia que a contenha, como por exemplo, mídia impressa ou mídia digital. Deve-se cuidar não apenas da proteção da informação como um todo, mas também de partes da informação que podem ser utilizadas para interferir sobre o todo. No caso das redes de computadores, isto significa que os dados, enquanto em trânsito, não serão vistos, alterados, ou extraídos da rede por pessoas não autorizadas ou capturados por dispositivos ilícitos.

O objetivo da confidencialidade é proteger informação privada (cidadãos, indústrias, governo, militar).

2.2.3 Integridade

A integridade consiste em evitar que dados sejam apagados ou de alguma forma alterados, sem a permissão do proprietário da informação. O conceito de dados nesse objetivo é mais amplo, englobando dados, programas, documentação, registros, fitas magnéticas, etc. O conceito de integridade está relacionado com o fato de assegurar que os dados não foram modificados por pessoas não autorizadas.

A integridade de dados também é um pré-requisito para outros princípios da segurança. Por exemplo, se a integridade de um sistema de controle a um determinado sistema operacional pode ser violada, então a confidencialidade de seus arquivos pode ser igualmente violada. Enquanto o objetivo da confidencialidade está mais voltado à leitura de dados, a integridade preocupa-se mais com a gravação ou alteração de dados.

2.2.4 Disponibilidade

Ter as informações acessíveis e prontas para uso representa um objetivo crítico para muitas empresas.

Disponibilidade consiste na proteção dos serviços prestados pelo sistema de forma que eles não sejam degradados ou se tornem indisponíveis sem autorização, assegurando ao usuário o acesso aos dados sempre que deles precisar.

Um sistema indisponível, quando um usuário autorizado necessita dele, pode resultar em perdas tão graves quanto as causadas pela remoção das informações daquele sistema. Atacar a disponibilidade significa realizar ações que visem a negação do acesso a um serviço ou informação, como por exemplo: bloqueando no canal de comunicação ou do acesso a servidores de dados.

A segurança da informação visa a manutenção dos acessos às informações que estão sendo disponibilizadas. Isso significa que toda a informação deve chegar aos usuários de forma íntegra e confiável. Para que isto possa acontecer, todos os elementos da rede por onde a informação passa até chegar os destino devem estar disponíveis e devem também preservar a integridade das informações.

Por exemplo, se um funcionário gravou determinada informação a segurança da informação deve garantir que no momento em que a informação for acessada novamente ela esteja sem qualquer alteração, que não tenha sido feita pelo próprio dono da informação, que possa ser acessada sem qualquer problema.

2.3 VULNERABILIDADES

> A vulnerabilidade é o ponto onde qualquer sistema é suscetível a um ataque, ou seja, é uma condição encontrada em determinados recursos, processos, configurações, etc. Condição causada muitas vezes pela ausência ou ineficiência das medidas de proteção utilizadas de salvaguardar os bem da empresa. (Moreira, 2001, p.22)

Na definição acima Moreira afirma que a vulnerabilidade é o ponto onde poderá acontecer um ataque, ou seja, o ponto onde uma fraqueza ou deficiência de segurança poderá ser explorada, causando assim um incidente de segurança.

Uma vulnerabilidade pode partir das próprias medidas de segurança implantadas na empresa, se existir estas medidas, porém configuradas de maneira incorreta, então a empresa possuirá uma vulnerabilidade e não uma medida de segurança.

Quando pretende-se garantir a segurança da informação da empresa deve-se identificar os processos vulneráveis, se estes processos forem de grande importância para garantir a segurança da informação, as medidas e controles de segurança adequados são implementados.

O surgimento das vulnerabilidades pode ter diversas causas, podendo ser entendido como uma relação N para N, ou seja, cada empresa, cada ambiente pode possuir diversas vulnerabilidades e cada vulnerabilidade pode estar em diversos ambientes. (MOREIRA, 2001, p25)

As vulnerabilidades podem ser físicas, naturais, humanas, de software ou hardware, entre outras. Pode-se citar alguns exemplos de vulnerabilidades:

Físicas: falta de extintores, salas mal projetadas, instalações elétricas antigas e em conjunto com as instalações da rede de computadores.

Naturais: acumulo de poeira, umidade, possibilidade de desastre naturais, como

enchente, tempestade, terremotos, etc.

Humana: falta de treinamento, compartilhamento de informações confidenciais por parte dos funcionários da empresa, falta de comprometimento dos funcionários.

A figura 2.2 demonstra que as vulnerabilidades possibilitam os incidentes de segurança, sendo que estes afetam o negócio da empresa causando impactos negativos para seus clientes e demais envolvidos. Um incidente de segurança que possa afetar os princípios de segurança da informação estará afetando a imagem da empresa para seus clientes, se a informação não estiver disponível no momento em for necessário o acesso, sem qualquer alteração que possam vir a afetar os princípios de integridade e autenticidade das mesmas, então o incidente de segurança estará afetando o cliente que depende do acesso a esta informação e também a empresa. As vulnerabilidades são a principal causa dos incidentes de segurança.

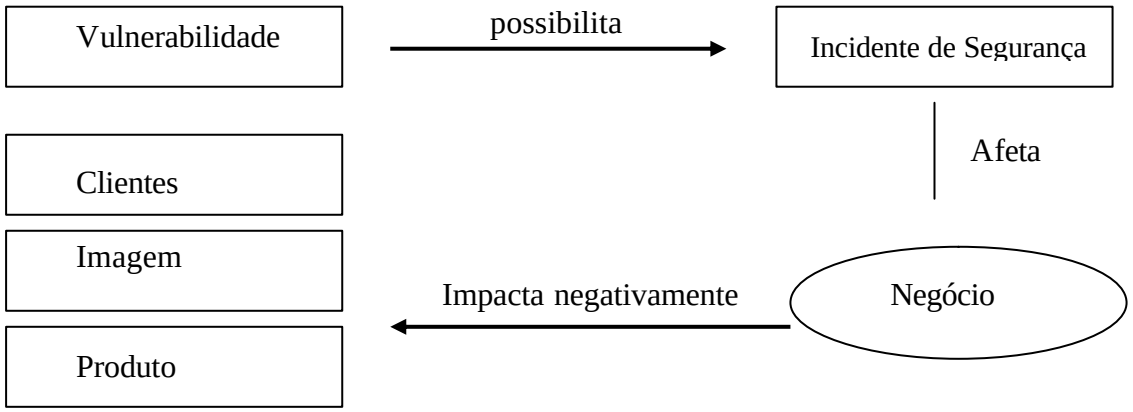


Figura 2.2 - Impacto dos incidentes de segurança nos negócios
Fonte: Livro Segurança Mínima p.27

A figura 2.3 ilustra a questão das vulnerabilidades em relação a incidentes de segurança, sendo que as ameaças, sejam elas internas ou externas, acontecem tentando

encontrar um ponto vulnerável, para que através dele possa passar pelas medidas de segurança e causar um incidente de segurança.

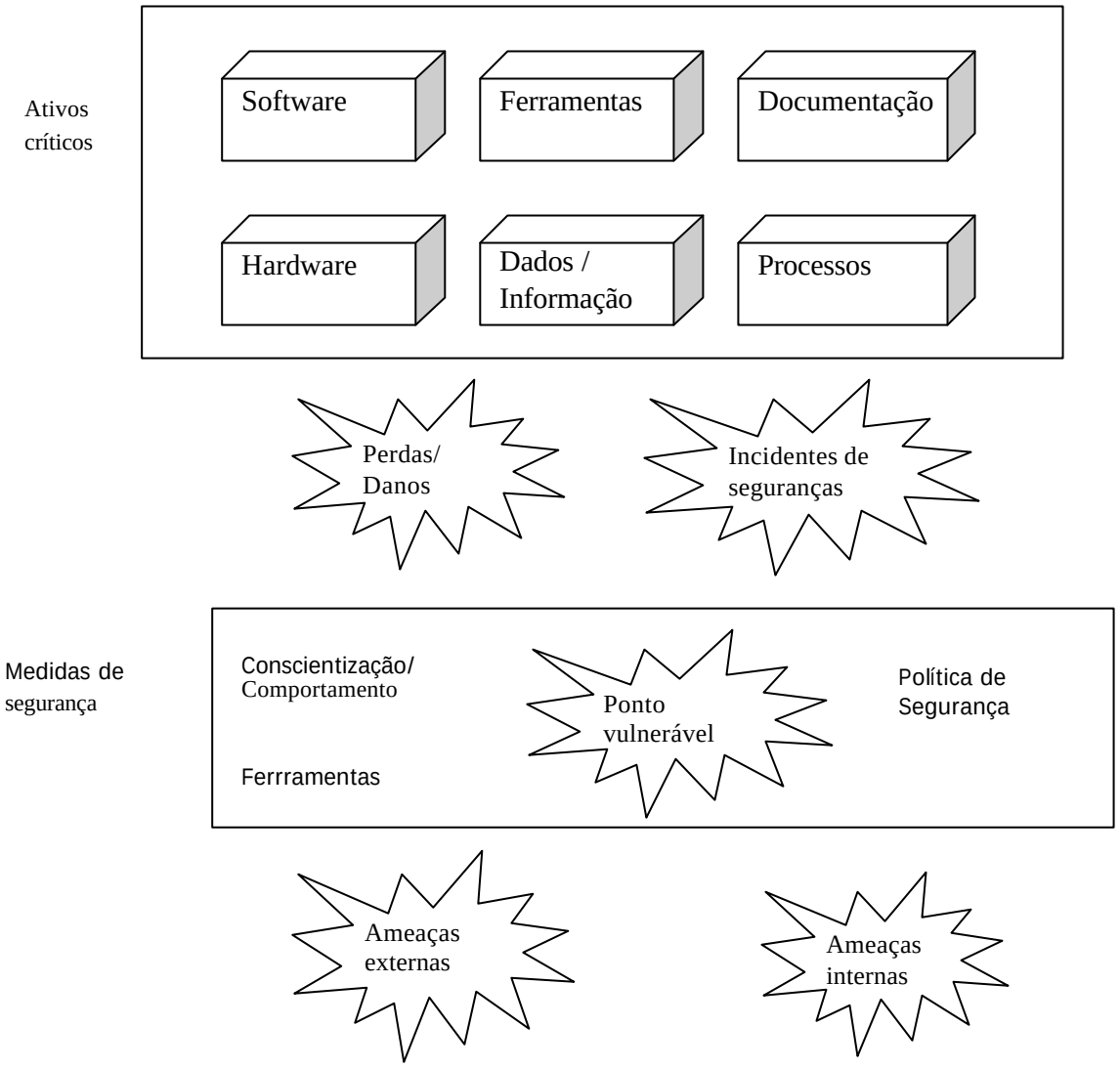


Figura 2.3 - Relação entre vulnerabilidade e incidente de segurança
Fonte: Livro Segurança mínima, p. 28

É importante perceber que se as medidas de segurança adotadas forem eficientes estas devem evitar um ponto vulnerável, pois assim as ameaças não se concretizariam em incidentes de segurança, já que não conseguiriam passar pelas medidas de segurança.

Os danos e perdas causados por um incidente de segurança acontecem em decorrência

de medidas mal implementadas ou mal utilizadas que possibilitam pontos vulneráveis. Algumas medidas de segurança podem ser adequadas para determinada situação e inadequada para outras. Deve-se buscar a melhor relação custo/benefício para garantia da segurança da informação. As vulnerabilidades irão diminuir a partir do momento que medidas adequadas de segurança sejam implantadas.

Moreira (2001, p.31) diz que medidas de segurança são esforços como procedimentos, software, configurações, hardware e técnicas empregadas para atenuar as vulnerabilidades com o intuito de reduzir a probabilidade de ocorrência da ação de ameaças e, por conseguinte, os incidentes de segurança.

Contudo, como comentado anteriormente, é importante pensar na relação custo/benefício, quando se pensa em medidas de segurança. À medida que o nível de segurança cresce o nível de vulnerabilidade decai. O ideal é que seja buscado o ponto de equilíbrio entre o nível de vulnerabilidades consideradas aceitáveis em relação ao nível de segurança ou as medidas de segurança implementadas.

Na verdade não existe um modelo ideal ou um pacote de segurança que pode ser usado para resolver os problemas de segurança nas redes.

Na maioria das vezes deve-se usar a combinação de várias estratégias de segurança de acordo com o nível de segurança que a empresa deseja atingir. Dentre elas destacam-se:

- Política de segurança;
- Cópias de Segurança;
- Controle de acesso;
- Segurança física;
- Firewall;
- Política de senha;
- Detecção de intrusão;

- Treinamento/conscientização dos usuários.

Dentre outras estratégias que podem complementar e garantir a segurança da informação da empresa. Será realizado um estudo detalhado sobre política de segurança, com o objetivo da criação de um modelo de política de segurança.

2.4 IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO

Nas décadas de 70 e 80 o enfoque principal da segurança era o sigilo dos dados. Entre 80 e 90, com o surgimento das redes de computadores, a proteção era feita não pensando nos dados, mas sim nas informações. A partir da década de 90, com o crescimento comercial das redes baseadas em *Internet Protocol*[2] (IP) o enfoque muda para a disponibilidade. A informática torna-se essencial para a organização, o conhecimento precisa ser protegido.

A segurança da informação e os negócios estão estritamente ligados. O profissional de segurança da informação precisa ouvir as pessoas, de modo a entender e saber como aplicar as tecnologias para a organização, sua estratégia de negócio, suas necessidades e sua estratégia de segurança.

A dificuldade de entender a importância de segurança ainda é muito grande. A segurança ainda é um campo relativamente novo, muitas empresas ainda não conseguem enxergar a sua importância, imaginando apenas que as soluções são caras e não trazem nenhum retorno financeiro, não imaginando as conseqüências que a falta da segurança poderá trazer para todo o negócio da empresa.

Este é o maior desafio da segurança, uma solução de segurança é imensurável e não resulta em melhorias nas quais todos podem notar que alguma coisa foi feita.

---

[2] Protocolo da Internet, IP é um conjunto de regras e formatos utilizado em redes em que a comunicação se dá através de pacotes de dados.

A empresa, ou os executivos e diretores, devem entender que a segurança tem justamente o papel de evitar que alguém perceba que alguma coisa esta errada.

O fato é que ninguém percebe a existência da segurança, apenas a inexistência dela, quando algum incidente acontece, resultando em grandes prejuízos para a empresa.

Esta visão reativa, com as decisões de segurança sendo tomadas após um incidente, traz uma série de conseqüências negativas para a organização. É preciso que as organizações passem a considerar a segurança da organização como um elemento essencial para o sucesso. Deve-se entender que as soluções de segurança não gerão gastos, mas é um investimento habilitador de seus negócios.

Segundo informações apresentadas na 9ª Pesquisa Nacional de Segurança da Informação (MÓDULO SECURITY, 2003), as organizações estão mudando sua opinião sobre a importância da segurança da informação. A Segurança da Informação tornou-se fator prioritário na tomada de decisões e nos investimentos das organizações no país. Essa informação é uma das principais conclusões apontadas pelos índices obtidos pela pesquisa.

Alguns resultados importantes que foram obtidos:

- Para 78% dos entrevistados, as ameaças, os riscos e os ataques deverão aumentar em 2004.
- Vírus (66%), funcionários insatisfeitos (53%), divulgação de senhas (51%), acessos indevidos (49%) e vazamento de informação (47%) foram apontados como as cinco principais ameaças à segurança das informações nas empresas.
- O percentual de empresas que afirmam ter sofrido ataques e invasões subiu de 43%, em 2002, para 77% em 2003.
- 60% indicam a Internet como principal ponto de invasão em seus sistemas.
- Política de segurança formalizada já é realidade em 68% das organizações.
- Pelo terceiro ano consecutivo, antivírus (90%), sistemas de backup (76,5%) e

firewall (75,5%) foram apontados como as três medidas de segurança mais implementadas nas empresas.

Os resultados obtidos reforçam a importância da informação para as empresas e principalmente a necessidade de segurança destas informações. A utilização de normas e padrões para que a segurança da informação esteja documentada e possa ser seguida é um fator importante que foi apontado.

A figura 2.4 mostra o ramo de atividade das empresas que foram entrevistadas durante 9ª Pesquisa Nacional de Segurança da Informação, a pesquisa teve uma amostra de 682 questionários, que foram coletados de março à agosto de 2003. Podemos perceber que os profissionais que participaram deste estudo estão distribuídos em diversos segmentos.

Figura 2.4 - Ramo de Atividade das Empresas entrevistadas
Fonte: 9º Pesquisa Nacional de Segurança da Informação, 2003, www.módulo.com.br

A preocupação das empresas em possuírem regras e procedimentos documentados se torna bastante clara na figura 2.5, onde mostra a empresa em relação a política de segurança, sendo que 50% das empresa possuem uma política de segurança atualizada. A pesquisa mostra um cenário positivo em relação ao aumento da política de segurança atualizada e a queda no item falta de consciência dos usuários, mostrada na figura 3.3, como principal obstáculo, podendo ser explicada pelo aumento da divulgação da política de segurança para todos os funcionários.

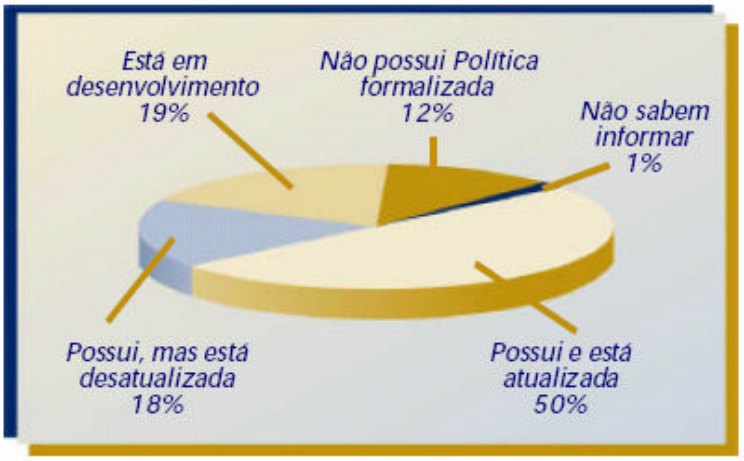


Figura 2.5 - Empresas que possuem Política de Segurança e a situação
Fonte: 9º Pesquisa Nacional de Segurança da Informação, 2003, www.módulo.com.br

A política de segurança aparece entre as principais medidas de segurança que, segundo as empresas, devem ser adotadas em 2004, figura 2.6. Em 2003, as empresas tiveram imensas dificuldades com a disseminação em massa de diversas pragas virtuais, isto pode explicar a primeira colocação de antivírus como a principal medida de segurança para 2004.

	%
Antivírus	76
Capacitação técnica	75
Sistemas de backup	72
Política de segurança	71
Procedimentos formalizados	71
Implementação de firewall	71
Análise de riscos	66
Criptografia	64
Sistemas de detecção de intrusos	63
Software de controle de acesso	58

Observação: o total de citações é superior a 100% devido à questão aceitar múltiplas respostas.

Figura 2.6 - Principais medidas de segurança para 2004
Fonte: 9º Pesquisa Nacional de Segurança da Informação, 2003, www.módulo.com.br

As figuras 2.7 e 2.8 mostram um comparativo entre os resultados da 8º e 9º Pesquisa

Nacional de Segurança da Informação, pode-se notar que as primeiras posições do ranking da medidas de segurança não se alteram de 2002 para 2003, no entanto, se notarmos o item política de segurança aumentou 12,5% em relação a 2002. Um fator importante é que as empresas estão percebendo a necessidade de mudar o cenário da segurança da informação, sendo que a política de segurança tem um papel importante para a segurança da informação nas empresas.

Ranking	2003	%	Ranking	2002	%
1	Antivírus	90	1	Antivírus	77
2	Sistemas de backup	76,5	2	Firewall	76
3	Firewall	75,5	3	Sistema de backup	69
4	Política de segurança	72,5	4	Capacitação técnica	63
5	Capacitação técnica	70	5	Intrusion detection	61
6	Software de controle de acesso	64	6	Política de segurança	60
7	Segurança física na sala de servidores	63	7	Proxy Server	58
8	Proxy Server	62	8	Monitoração de log	55
9	Criptografia	57	9	Análise de riscos	53
10	Análise de riscos	56	10	Software de controle de acesso	52

Figura 2.7 - Ranking das medidas de segurança adotadas
Fonte: 9º Pesquisa Nacional de Segurança da Informação, 2003, www.módulo.com.br

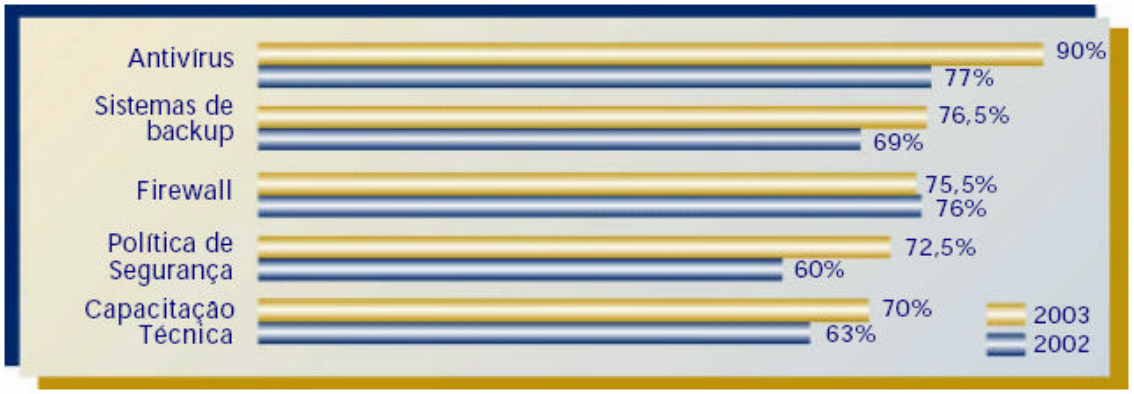


Figura 2.8 - Principais medidas de segurança adotadas
Fonte: 9º Pesquisa Nacional de Segurança da Informação, 2003, www.módulo.com.br

A Segurança da Informação tornou-se fator prioritário na tomada de decisões e nos investimentos das organizações no país. [9ª Pesquisa Nacional de Segurança da Informação. www.modulo.com.br]

Por exemplo, se um funcionário gravou determinada informação a segurança da informação deve garantir que no momento em que a informação for acessada novamente ela esteja sem qualquer alteração, que não tenha sido feita pelo próprio dono da informação, que possa ser acessada sem qualquer problema.

Os controles considerados como melhores práticas para a segurança da informação incluem: [NBR ISO 17799, p3].

- Documentação da política de segurança da informação;
- Definição das responsabilidades na segurança da informação;
- Educação e treinamento em segurança da informação;
- Relatório de incidentes de segurança;
- Gestão de continuidade do negócio.

2.5 CONCLUSÃO DO CAPÍTULO

Neste capitulo foi feito um estudo sobre a informação e a segurança da informação, pode-se perceber que a informação tem grande valor dentro das instituições em que estiver inserida e que a garantia da segurança da informação é extremamente importante para o sucesso do negócio das organizações.

A informação deve ser classificada de acordo com seu grau de importância, garantindo assim, a proteção adequada para cada informação, existem informações que podem ser divulgadas sem afetar o negócio da organização, porém, existem informações que são confidenciais e devem ser extremamente controlado o acesso a elas, evitando que possam ser acessadas por pessoas não autorizadas e prejudicar a organização.

A informação segura é aquela que obedece aos princípios de segurança da informação, garantindo a autenticidade, disponibilidade, integridade e confidencialidade da informação.

Todas as organizações sofrem ameaças, sejam elas internas ou externas, estas ameaças exploram algum ponto vulnerável, que pode ser, por exemplo, uma medida de segurança mal configurada. As medidas de segurança devem evitar a existência deste ponto vulnerável garantindo assim a segurança da informação.

Existe uma grande dificuldade de entender a importância da segurança da informação, as decisões de segurança, muitas vezes, são tomadas após um incidente de segurança. Porém, a preocupação das organizações com a segurança da informação vem crescendo, medidas para garantir a segurança da informação vem sendo implementadas com maior freqüência, sendo que a segurança da informação tornou-se um fator prioritário na tomada de decisões e nos investimentos das organizações.

Para garantir a segurança da informação várias medidas de segurança podem ser implementadas, dentre elas destaca-se a política de segurança da informação, sobre a qual será feito um estudo mais abrangente no próximo capítulo.

Será detalhado, a seguir, sobre política de segurança explicando sua importância, as fase o desenvolvimento da política, tipos de política e a criação de uma política.

3 POLÍTICA DE SEGURANÇA

A política de segurança é a base para todas as questões relacionadas à proteção da informação, desempenhando um papel importante em todas as organizações, sendo a elaboração de uma política de segurança da informação é essencial, pois definem normas, procedimentos, ferramentas e responsabilidades para garantir o controle e a segurança da informação na empresa.

Política de segurança é apenas a formalização dos anseios da empresa quanto à proteção das informações.

> Em um país, temos a legislação que deve ser seguida para que tenhamos um padrão de conduta considerado adequado às necessidades da nação para garantia de seu progresso e harmonia. Não havia como ser diferente em uma empresa. Nesta precisamos definir padrões de conduta para garantir o sucesso do negócio. (ABREU, 2002)

Na definição acima, política de segurança é comparada com a legislação que todos devemos seguir, de modo que o cumprimento da legislação nos garante que o padrão de contuda esta sendo seguido, a política de segurança também deve ser seguida por todos os funcionários de uma organização, garantindo assim a proteção das informações e o sucesso do negócio.

Segundo Wadlow (2000, p.40) uma política de segurança atende a vários propósitos:

- Descreve o que está sendo protegido e por quê;
- Define prioridades sobre o que precisa ser protegido em primeiro lugar e com qual custo;
- Permite estabelecer um acordo explícito com várias partes da empresa em relação ao valor da segurança;

- Fornece ao departamento de segurança um motivo válido para dizer “não” quando necessário;
- Proporciona ao departamento de segurança a autoridade necessária para sustentar o “não”;
- Impede que o departamento de segurança tenha um desempenho fútil.

A implementação pode ser considerada a parte mais difícil da política de segurança. Sua criação e sua definição envolvem conhecimentos abrangentes de segurança, ambiente de rede, organização, cultura, pessoas e tecnologias, sendo uma tarefa complexa e trabalhosa. Porém a dificuldade maior será na implementação desta política criada, quando todos os funcionários devem conhecer a política, compreender para que as normas e procedimentos estabelecidos realmente sejam seguidos por todos os funcionários.

3.1 PLANEJAMETO

O início do planejamento da política de segurança exige uma visão abrangente, de modo que os riscos sejam entendidos para que possam ser enfrentados. Para que a abordagem de segurança possa ser pró-ativa é essencial uma política de segurança bem definida, sendo que as definições das responsabilidades individuais devem estar bem claras facilitando o gerenciamento de segurança em toda a empresa.

Um ponto bastante importante para que a política de segurança seja seguida pela empresa é que seja aprovada pelos executivos, publicada e comunicada para todos os funcionários, de forma relevante e acessível.

O planejamento da política deve ser feito tendo como diretriz o caráter geral e abrangente de todos os pontos, incluindo as regras que devem ser obedecidas por todos.

A política de segurança pode ser dividida em vários níveis, podendo ser de um nível mais genérico, como o objetivo que os executivos possam entender o que está sendo definido, nível dos usuários de maneira que eles tenham consciência de seus papéis para a manutenção da segurança na organização, e podendo ser de nível técnico que se refere aos procedimentos específicos como, por exemplo, a implementação das regras de filtragem do firewall.

Segundo Dimitri (2002), podemos dividir a política de segurança em três tipos de textos: nível estratégico, nível tático e nível operacional, como mostra a figura 3.1.

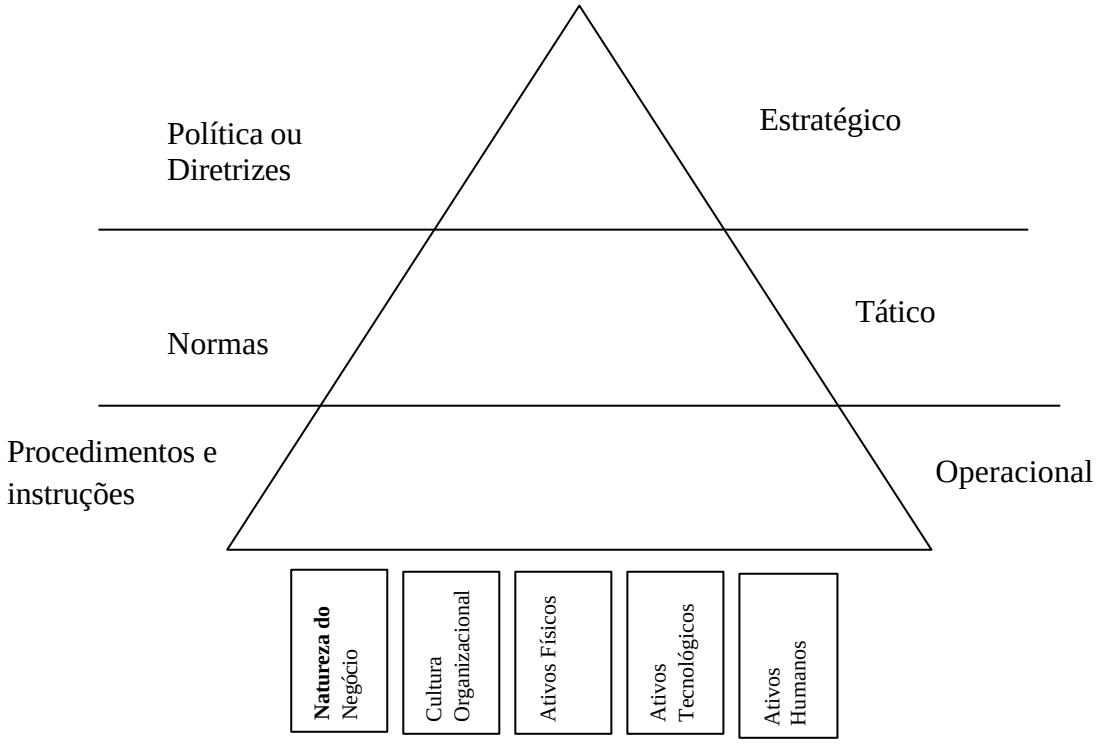


Figura 3.1 - Diagrama de conceito dos componentes da política
Fonte: Livro Segurança de redes p175

Nível estratégico: existem situações no dia-a-dia que precisamos tomar decisões. Algumas vezes o bom senso é ferramenta usada pelos profissionais para a tomada de decisão.

Isto ocorre porque se ninguém passou pela situação antes, e se não existe nenhuma orientação da empresa sobre o que fazer quando tal situação acontecer, o profissional decidirá qual a melhor solução para a resolução do problema.

Quando falamos em nível estratégico estamos falando em alinhamento nos valores da empresa, ou seja, no rumo a ser seguido. Quando necessário o profissional tomar uma decisão sobre uma situação nova, deve-se usar o bom senso na tomada da decisão seguindo os valores da empresa.

Nível tático: para o nível tático deve-se pensar em padronização de ambiente. Equipamentos, software, senhas, utilização de correio eletrônico, cópias de segurança, segurança física, etc. Tudo isso precisa e deve ser padronizado. Isso faz com que todos os pontos da empresa tenham o mesmo nível de segurança e não tenhamos um elo mais fraco na corrente.

Nível operacional: a palavra chave no nível operacional é detalhamento, para garantir a perfeição no atendimento e continuidade dos negócios, independentemente do fator humano. Se a configuração esta no papel, ou seja, se existe um padrão formalizado, então este padrão deve ser seguido e a configuração deve ser realizada de forma igual por todos.

A parte operacional da política de segurança vem exatamente para padronizar esses detalhes de configurações dos ambientes. Pode-se ter um padrão para toda a empresa, ou se existirem várias filiais pelo país, um padrão por estado. Isso irá depender da necessidade da empresa. O importante é saber que precisamos desse padrão.

A política é o elemento que orienta as ações e as implementações futuras, de uma maneira global, enquanto as normas abordam os detalhes, como os passos da implementação, os conceitos e os projetos de sistemas e controles. Os procedimentos são utilizados para que os usuários possam cumprir aquilo que foi definido na política e os administradores de sistemas possam configurar os sistemas de acordo com a necessidade da organização.

(SÊMOLA, 2003, p.105)

Os elementos de uma política de segurança devem manter a disponibilidade da infra-estrutura da organização, esses elementos são essenciais para a definição e implantação da política de segurança:

Vigilância: todos os funcionários da organização devem entender a importância da segurança para a mesma. No aspecto técnico a vigilância deve ser um processo regular e consistente incluindo o monitoramento dos sistemas e da rede.

Atitude: é a postura e a conduta em relação à segurança, é essencial que a política seja de fácil acesso e que seu conteúdo seja de conhecimento de todos os funcionários da organização. Atitude significa também o correto planejamento, pois a segurança deve fazer parte de um longo e gradual processo dentro da organização.

Estratégia: deve ser criativo quanto às definições da política e do plano de defesa contra intrusões, possuir a habilidade de se adaptar as mudanças. A estratégia deve ser definida de modo que as medidas de segurança a serem adotadas não influenciem negativamente no andamento dos negócios da organização.

Tecnologia: a solução tecnológica deverá suprir as necessidades estratégicas da organização, deve-se tomar cuidado com qualquer tecnologia um pouco inferior, pois poderá causar um falsa sensação de segurança, podendo colocar em risco toda a organização. O ideal é a implantação de uma política de segurança dinâmica em que múltiplas tecnologias e práticas de segurança são adotadas.

A figura3.2 mostra a importância dos elementos de uma política de segurança, sendo que estes levaram a uma Política de Segurança de Sucesso.

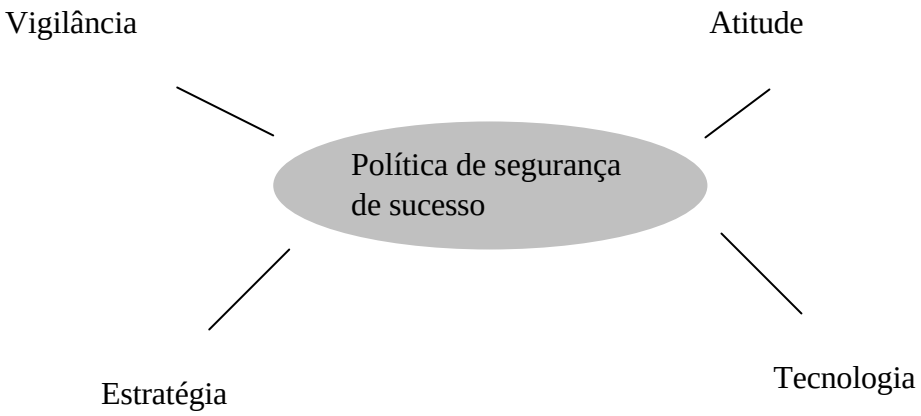


Figura 3.2 - Fatores de sucesso da política de segurança
Fonte: Livro segurança de redes, 2003, p178

Segundo a NBR ISO 17799 a política de segurança deve seguir as seguintes orientações:

- Definição de segurança da informação, resumo das metas e escopo e a importância da segurança como um mecanismo que habilita o compartilhamento da informação.
- Declaração do comprometimento da alta direção, apoiando as metas e princípios da segurança da informação.
- Breve explanação das políticas, princípios, padrões e requisitos de conformidade de importância específica para a organização, por exemplo:
    - Conformidade com a legislação e possíveis cláusulas contratuais;
    - Requisitos na educação de segurança;
    - Prevenção e detecção de vírus e *software* maliciosos;
    - Gestão de continuidade do negócio;
    - Conseqüências das violações na política de segurança da informação;

- Definição das responsabilidades gerais e especificas na gestão de segurança da informação, incluindo o registro dos incidentes de segurança.
- Referência à documentação que possam apoiar a política, por exemplo, políticas, normas e procedimentos de segurança mais detalhados de sistemas, áreas específicas, ou regras de segurança que os usuários devem seguir.

Sendo assim a política de segurança deve conter regras gerais e estruturais que se aplicam ao contexto de toda a organização, deve ser flexível o suficiente para que não sofra alterações freqüentes.

3.2 DEFINIÇÃO

A política de segurança deve ser definida de acordo com os objetivos de negócios da organização. Existem algumas diretrizes para se escrever a política de segurança (WADLOW, 2000, p.33):

- Mantenha-se compreensível: uma política de segurança deve ser de fácil entendimento para toda a organização, se ninguém ler ou se todos lerem, porém se não conseguirem entender, a política de segurança não será seguida. Para proporcionar algum beneficio, é necessário que a política esteja nas mãos das pessoas que deverão utilizá-la e, portanto, precisarão ler e lembrar seu conteúdo.
- Mantenha-se relevante: se existir necessidade a política de segurança poderá ser um documento extenso. Existe a tentação de escrever longas políticas elaboradas, apenas porque o volume impressiona a administração superior, porém se você disponibilizar esta política para que os funcionários leiam e comecem a usar, certamente haverá poucas chances de obter sucesso.

Uma solução para evitar este problema é criar várias políticas cada uma destinada a

um público específico dentro da empresa., assim cada política poderá ser pequena, direta e compreensível.

- Saiba o que não é relevante: algumas partes da política terão tópicos que não deverão ser conhecidos por todas as pessoas. É necessária uma seção descrevendo o tipo de informação considerada sensível, que não deverá ser comentada com estranhos.

Uma segunda seção deve ser mantida sobre o sigilo mais rígido e somente pode ser conhecida por pessoas do mais alto nível de confiança. Essa seção constitui a "consciência" de organização da segurança.

Há necessidade de uma lista explícita e atualizada dos assuntos sensíveis, permitindo que a equipe de segurança disponha de uma memória organizacional sobre o que não deve ser comentado.

- Leve-a sério: somente será eficaz se as pessoas a levarem a sério, para isto deve-se seguir dois itens:

Todos precisam saber que poderão ser punidos se executarem ou deixarem de executar determinadas ações.

Para agir de acordo com a política, é necessário realmente punir as pessoas que a violarem.

Não obedecer a um destes princípios poderá invalidar qualquer política.

As dificuldades surgem na definição e aplicação de penalidades. Estas questões de penalidades devem estar bem claras desde o inicio. É necessário realizar este processo de uma forma que estabeleça a culpa do transgressor no grau adequado, deixando claro a quem aplicar a punição que esta é justificada e correta, e preservando o apoio da administração superior.

- Mantenha-a atual: a política de segurança precisa ser um processo contínuo, assim como a segurança de rede que ela representa. Se não for mantido atual, o documento tornar-se-á obsoleto rapidamente.

Distribua-a as pessoas que precisam conhecê-la: possuir uma excelente política de segurança somente significará algo se for lida por quem não pertença à própria equipe de segurança. A política deverá estar disponível, de modo a ser acessada com facilidade, poderá ser disponibilizado um site web sobre a política de segurança.

Alguns detalhes relevantes em uma política de segurança podem ser inseridos em normas e procedimentos específicos. Alguns detalhes que podem ser definidos com base na análise do ambiente da rede e de seus riscos, são:

- A segurança é mais importante do que os serviços, caso não existir conciliação a segurança deve prevalecer.
- A política de segurança deve evoluir constantemente, de acordo com os riscos e as mudanças na estrutura da organização.
- Aquilo que não for expressamente permitido, será proibido.
- Nenhuma conexão direta com a rede interna, originária externamente, deverá ser permitida sem que um rígido controle de acesso seja definido e implementado.
- Os serviços devem ser implementados com a maior simplicidade possível.
- Devem ser realizados testes, a fim de garantir que todos os objetivos sejam alcançados.
- Nenhuma senha dever ser fornecida sem a utilização de criptografia.

3.3 IMPLEMENTAÇÃO

A implementação deve envolver toda a organização, todos os usuários devem conhecer e passar a utilizar a política. Um ponto importante para a aceitação e conformidade com a política definida é a educação, pois a falta de conscientização dos funcionários acerca

da importância e relevância da política irá torná-la inoperante ou reduzir sua eficácia.

Devem ser feitos programas de conscientização e divulgação da política, de modo que com a divulgação efetiva ela deverá tornar-se parte da cultura da organização.

Segundo a norma NBR ISO 17799, as seguintes análises críticas periódicas também devem ser agendadas:

- Verificação da efetividade da política, demonstrada pelo tipo, volume e impacto dos incidentes de segurança registrados.
- Análise do custo e impacto dos controles na eficiência do negócio.
- Verificação dos efeitos de mudanças na tecnologia utilizada.

Existem vários obstáculos que podem interferir durante a implantação da segurança da informação, na figura 3.3 existe um comparativo entre os principais obstáculos levantados nas duas últimas pesquisas Nacionais de Segurança da Informação realizadas em 2002 e 2003.

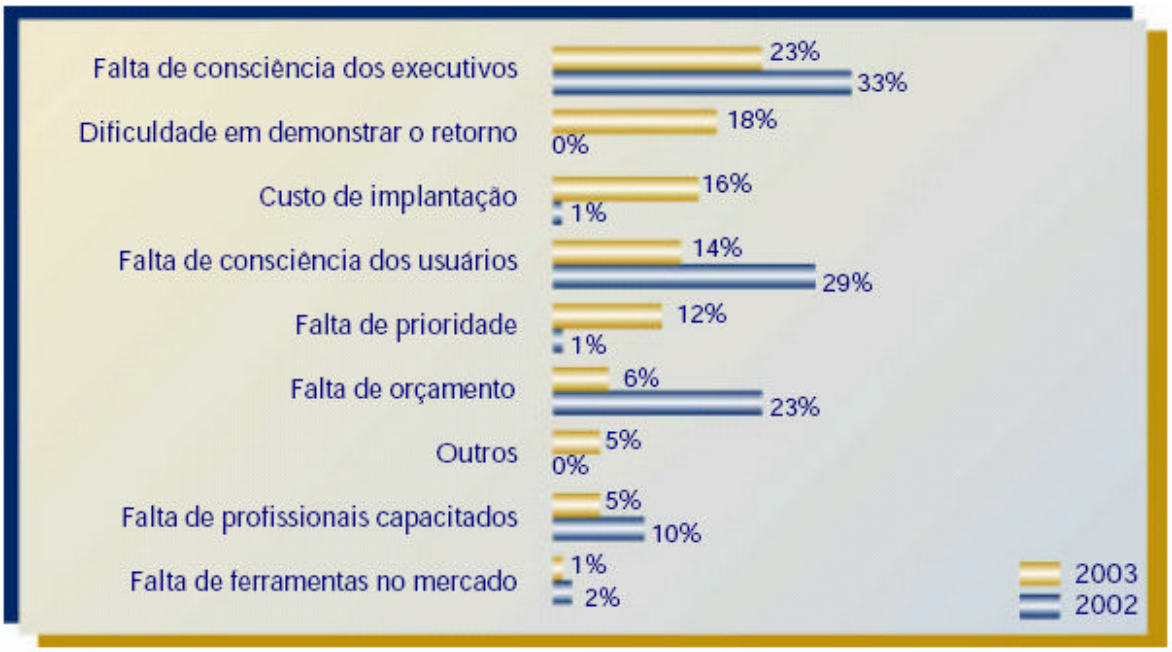


Figura 3.3 - Obstáculos para Implementação da Segurança da Informação
Fonte: 9º Pesquisa Nacional de Segurança da Informação, 2003, www.módulo.com.br

A falta de consciência dos executivos é um item que se destaca entre os obstáculos para implementação da segurança da informação como mostra na figura 3.3. Os executivos podem aprovar uma política de segurança apenas para satisfazer a equipe de segurança ou os auditores, comprometendo a própria organização. Os executivos devem ser convencidos de que o melhor a fazer é atuar de modo pró-ativo, em oposição ao comportamento reativo. O ideal é mostrar estudos que provam que é mais barato considerar a perspectiva de prevenir, deter e detectar do que a de corrigir e recuperar.

A falta de consciência dos usuários é outro item que demonstra um percentual elevado nos dois anos, isto deixa clara a necessidade de divulgação e treinamentos durante o processo de implementação da política, que possam esclarecer seus benefícios e importância do seguimento das normas e procedimentos adotados.

A dificuldade de demonstrar retorno, e o alto custo são itens importantes a serem comentados. O fato de não conseguir os recursos necessários reflete a falha em convencer os executivos da importância das informações e dos sistemas de informações da organização, que devem, portanto, ser protegidos. Deve-se esclarecer que a indisponibilidade de recursos significa prejuízos, pois os negócios podem ser interrompidos como decorrência de um ataque.

3.4 TIPOS DE POLÍTICAS

Existem três tipos de políticas: Regulatória, Consultiva e Informativa.

3.4.1 Regulatória

Ferreira (2003, p.34), afirma que políticas regulatórias são implementadas devido às necessidades legais que são impostas à organização. Normalmente são muito específicas para

um tipo de ramo de atividade.

Uma política regulatória é definida como se fosse uma série de especificações legais. Descreve, com grande riqueza de detalhes, o que deve ser feito, quem deve fazer e fornecer algum tipo de parecer, relatando qual ação é importante.

Deve assegurar que a organização esta seguindo os procedimentos e normas para seu ramo de atuação, provendo conforto para a organização na execução de suas atividades, pois estão seguindo os requisitos legais necessários para o seu ramo de atividade.

3.4.2 Consultiva.

Políticas consultivas não são obrigatórias, mas muito recomendadas. As organizações devem conscientizar seus funcionários a considerar este tipo de política como se fosse obrigatória.

A política consultiva apenas sugere quais ações ou métodos devem ser utilizados para a realização de uma tarefa. A idéia principal é esclarecer as atividades cotidianas do dia a dia da empresa de maneira bastante direta.

Deve-se considerar que é importante que os usuários conheçam essas ações para realização de suas tarefas para que possam ser evitados riscos do não cumprimento das mesmas, tais como:

- Possibilidade de omissão de informações importantes para tomada de decisões críticas aos negócios da organização;
- Falhas no processo de comunicação com a alta administração;
- Perda de prazos de compromissos importantes para os negócios da organização.

3.4.3 Informativa

Este tipo de política possui caráter apenas informativo, nenhuma ação é desejada e não existem riscos, caso não seja cumprida. Porém, também pode contemplar uma série de observações importantes, bem como advertências severas.

Por exemplo, a política pode ressaltar que o uso de um determinado sistema é restrito a pessoas autorizadas e qualquer funcionário que realizar algum tipo de violação será penalizado. Nesta sentença não são informados quais funcionários estão autorizados, mas este determinando severas conseqüências para quem desrespeitá-la.

3.5 CONCLUSÃO DO CAPÍTULO

Com o número crescente de incidentes de segurança, a informação precisa, cada vez mais estar protegida, de modo que medidas de segurança precisam ser implementadas para assegurar e garantir a segurança da informação.

Dentre as medidas de segurança implantadas pelas organizações está a política de segurança da informação que tem por objetivo definir procedimentos, normas, ferramentas e responsabilidades para garantir o controle e a segurança da informação na empresa.

Uma política de segurança deve ser definida de acordo com os objetivos do negócio da empresa, sendo que os executivos devem participar de seu planejamento, para que possa ser aceita por eles, lembrando que sua implementação e sucesso também dependerá de sua divulgação para todos os funcionários.

Existem vários obstáculos quando o assunto é a segurança da informação, porém a implementação de medidas de segurança como uma política de segurança da informação, faz com que todos percebam a necessidade de segurança da informação para a organização.

4 HISTÓRICO DA SOCIESC

A Sociedade Educacional de Santa Catarina, na época Escola Técnica Tupy foi fundada no ano de 1959 pelo então presidente da Fundição Tupy, Hans Dieter Schmidt, com o intuito de formar mão-de-obra especializada que estava em falta justamente da época da explosão industrial no Brasil.

Para o aperfeiçoamento profissional, foi aprovado um projeto de 1 milhão de DM (Marcos alemães) acordado entre o Brasil e a Alemanha em 1967. Nesse acordo juntamente com máquinas vieram especialistas para aplicar novas tecnologias, eles ficaram na Escola Técnica Tupy durante três anos implementando técnica, conhecimento, tradição e cultura de um modelo educacional europeu baseado em valores como: seriedade, competência, ética e cidadania. Além disso, engenheiros oriundos da Fundição Tupy e professores especializados fizeram parte do corpo docente. Era a Sociedade Educacional Tupy que nascia para o crescimento da comunidade.

Ultrapassando as fronteiras de Joinville, Santa Catarina e do Brasil a Escola Técnica Tupy cresceu, contribuindo na formação de profissionais para várias empresas, e em 1985 a Sociedade Educacional Tupy passou a ser a Sociedade Educacional de Santa Catarina - SOCIESC, desta vez dirigida por um conselho formado pelos presidentes das principais empresas de Joinville.

Atualmente a SOCIESC é mantenedora das seguintes entidades:

- Colégio Tupy - COT - ensino fundamental e médio;
- Escola Técnica Tupy - ETT - ensino técnico;
- Instituto Superior Tupy - IST - ensino superior e pós-graduação;

- Capacitação Empresarial - SCE - cursos de extensão e pós-graduação;
- Serviços de Engenharia - SSE - serviços de fundição, tratamento térmico; ferramentaria e laboratórios de materiais e metrologia.

Sendo que tem sua matriz em Joinville com filiais nas seguintes cidades: São Bento do Sul (SC), Curitiba (PR), Florianópolis (SC) e Apucarana (PR).

Abaixo, na tabela 4.1, a realidade atual da SOCIESC referente ao número de funcionários em cada uma das unidades.

Tabela 4.1 - Quadro de funcionários da Sociesc

Unidade	Funcionários
Joinville	567
São Bento do Sul	27
Florianópolis	37
Curitiba	30
Apucarana	12
Total	**673**

Fonte: RH da SOCIESC

A seguir, na tabela 4.2, o do número de alunos matriculados na SOCIESC até agosto de 2004, pode-se perceber que o número total de alunos é bastante elevado, sendo o maior número de alunos esta em Joinville, isto se deve ao fato de estar à 45 anos atuando na comunidade tendo o devido reconhecimento do seu trabalho nas empresas e famílias da região. As outras unidades estão crescendo nas comunidades em que estão inseridas e com grande reconhecimento das empresas de suas cidades.

Tabela 4.2 - Alunos matriculados até agosto de 2004

Número de Alunos					
Unidades	**Ensino Fundamental**	**Ensino Médio**	**Ensino Técnico**	**Ensino Superior**	**Pós Graduação**
Joinville	404	1679	1544	2045	680
São Bento do Sul	0	221	231	59	51
Florianópolis	0	16	16	554	0
Curitiba	0	0	215	0	0
Apucarana	0	0	131	0	0
Total	**404**	**1916**	**2137**	**2658**	**782**

Fonte: Secretaria da SOCIESC

4.1 VISÃO, MISSÃO E VALORES DA SOCIESC

Visão: Ser um centro de excelência e referência em educação e tecnologia.

Missão: Contribuir para o desenvolvimento humano e da comunidade através da educação e tecnologia.

Valores Compartilhados:

- Crescimento e reconhecimento: crescer de forma significativa e sustentada, tendo como base o reconhecimento da comunidade onde está inserida (ser reconhecida como bem social).
- Responsabilidade social: atuar na Educação, Cultura e Consciência Ecológica para a ética e sustentabilidade, sob uma visão sistêmica do homem e da sua relação com

a natureza.

- Valorização das pessoas: valorizar o crescimento do ser humano, despertando os talentos e criando um ambiente que favoreça a participação e o exercício da individualidade comprometido com a comunidade.

Em anexo o Organograma atual da SOCIESC (anexo I), mostrando a estrutura hierárquica da instituição.

4.2 HISTÓRIA DA EQUIPE DE TI NA SOCIESC

A história da área de TI na SOCIESC iniciou no ano de 1996, com a criação de um projeto de rede para ligar os departamentos e os laboratórios de informática, sendo que para isto foi contratada uma empresa externa. Os primeiros laboratórios em rede estavam localizados no bloco P e sala M7. Até aí ainda não havia uma equipe de TI, apenas uma equipe responsável pela criação e manutenção de sistemas internos. A primeira rede possuía “Windows NT 3.51 for WorkGroups” nas estações e um servidor de arquivos Novel.

Neste ano também foi feita a instalação do sistema Magnus para controle e administração da SOCIESC.

1997

Houve a contratação de funcionários para administrar a rede recém criada, atuando junto com os dois funcionários que já estavam na administração da rede. Neste mesmo ano foi contratado um profissional para manutenção de hardware e alguns estagiários para suporte aos usuários. Começou assim o que chamamos hoje de equipe de Apoio a TI.

- Expansão da rede para o bloco N, sala M6, bloco F e iniciou-se a instalação da rede nos departamentos.
- Instalação dos primeiros servidores “Windows NT 4.0 Server” e estações “Windows NT 4.0 Workstation”.
- A área de TI estava ligada diretamente à direção.
- Neste ano todos os departamentos foram interligados em rede.

1998

Por meio da contratação de um funcionário para dar suporte aos usuários, juntamente com um funcionário já contratado no ano anterior e alguns estagiários, iniciou-se a primeira equipe de suporte, no qual era responsável pelo suporte a rede, hardware e software. A manutenção aos sistemas internos continuava a cargo da equipe de sistemas.

1999

Iniciou-se uma migração dos servidores Windows para Linux. O primeiro a ser substituído foram os servidores de correio eletrônico e DNS e logo após o Firewall passou a ser Linux.

- Neste ano todos os departamentos foram interligados em rede.
- Aumento da equipe de suporte com a contratação de mais funcionários.
- Contratação de mais funcionários para a administração da rede.
- Á área de TI recebeu status de departamento e passou a ter um coordenador.

2000

Os funcionários da área de administração de rede foram transferidos para a área de ensino e os funcionários contratados no ano anterior passaram a administrar a rede.

- Iniciou-se um projeto de implantação de Linux para as estações em laboratórios.

- Todos os projetos de rede passam a ser desenvolvidos pelo próprio departamento.
- Mais dois servidores passaram a utilizar Linux como sistema operacional.
- Instalação de Linux em mais da metade dos laboratórios.
- Em 2000, havia três áreas distintas: suporte, administração da rede e sistemas, todas subordinadas ao coordenador da área e este subordinado ao setor administrativo/financeiro.
- Implantação de um novo sistema acadêmico em substituição aos sistemas desenvolvidos internamente.
- Aquisição de novos servidores
- Criada a Unidade da SOCIESC em São Bento do Sul com rede própria, sem comunicação com Joinville

2001

- Iniciada uma parceria com a FUNCITEC/UFSC, para disponibilização de um novo link de acesso à internet.

2002

- União das áreas de suporte, administração da rede e sistemas, tornando apenas uma equipe, chamada de equipe de informática. Administração da rede e sistemas passaram a trabalhar em uma mesma sala.
- Criada a Unidade da SOCIESC em Curitiba, com rede própria.
- Inicia-se um projeto de substituição do ERP.
- Inicia-se um projeto para substituição do sistema acadêmico.
- Inicia-se um projeto de interligação de rede das unidades de Joinville, São Bento do Sul e Curitiba.
- A equipe de informática passa a ser conhecida como Apoio a TI.

- Implantação do primeiro Help Desk.
- O departamento passa a ser subordinado a diretoria administrativa.

2003

- Instalação do primeiro Backbone Gigabit.
- Iniciado um projeto de reestruturação da rede.
- Iniciada a implantação do novo ERP.
- Iniciada a implantação do novo sistema acadêmico.
- Há uma diminuição da equipe de informática.

2004

- Implantação total do ERP – Logix
- Implantação total do Sistema Acadêmico – WAE
- Todas as unidades estão totalmente interligadas – voz e dados.

4.3 EQUIPE DE TI DA SOCIESC

A Equipe de TI da SOCIESC é dividida em 3 áreas principais:

- Administração de Rede: Criação e administração de contas de usuários (login, e-mail e etc.). Instalação e Manutenção dos servidores, controle de tráfego de rede e equipamentos ativos da Rede, controle dos dados dos usuários (backup, cotas e etc.)
- Sistemas: Administração dos Bancos de Dados e Sistemas (Acadêmico, específicos, ERP e etc.) suporte aos usuários, criação de contas de usuários, pequenas otimizações e etc.

- Suporte: Serviço de Help Desk, instalação e manutenção da rede, instalação e manutenção de laboratórios etc.

Atualmente a equipe de TI da SOCIESC obedece ao organograma mostrado na figura 4.1, sendo dividida em três áreas de responsabilidade de um coordenador. A equipe de TI atende toda a estrutura de informática da SOCIESC, tanto no que diz respeito à área de ensino, com os laboratórios de informática, quanto aos departamentos administrativos e de serviços.

Figura 4.1 - Organograma Funcionários da área de TI

Fonte : Departamento de TI da SOCIESC

4.4 DEFINIÇAO DA ESTRUTURA DE INFORMÁTICA

Após a apresentação do histórico da SOCIESC será realizado um modelo de Política de Segurança da Informação, porém, antes da criação deste modelo é importante a apresentação da estrutura de informática de forma mais detalhada, bem como, das dificuldades enfrentadas para garantia da segurança da informação e do bom funcionamento da estrutura de informática da SOCIESC.

A estrutura de informática da SOCIESC, em Joinville, é composta por 18 servidores na unidade de Joinville, conforme anexo II, sendo servidores de Internet, E-mail, Banco de Dados, Arquivos, Proxy, entre outros.

Existem contas de usuários da rede de computadores para o domínio Ensino, utilizada pelos alunos e professores nos laboratórios de informática, aproximadamente 6800 contas. As contas de usuários do domínio SOCIESC, são contas utilizadas por funcionários efetivos, estagiários e alunos colaboradores[3], aproximadamente 600 contas.

As estações de trabalho da rede de computadores na unidade de Joinville, que fazem parte do domínio ENSINO, estão localizadas em laboratórios de informática com, em média, 21 computadores, totalizando 550 computadores nos laboratórios, estes laboratórios são utilizados por alunos e professores dos cursos técnicos da Escola Técnica Tupy, do ensino fundamental e médio do Colégio Tupy, dos cursos superiores do Instituto Superior Tupy e dos cursos oferecidos pela Capacitação Empresarial.

As estações de trabalho do domínio SOCIESC estão localizadas em cada departamento, dependendo o número de funcionários de cada departamento, existem 280 computadores que fazem parte do domínio SOCIESC.

A SOCIESC possui sistema de administração acadêmica o WAE desenvolvido pela WISE Consultoria, utiliza banco de dados Oracle, nele são armazenadas todas as informações acadêmicas dos alunos, é acessado por professores para digitação de notas e emissão de relatórios através de seu módulo para Internet. É acessado também por funcionários da secretaria para cadastros gerais e emissão de documentos, como: diplomas, certificados, boletim escolar.

[3] Alunos colaboradores são alunos que ainda estão estudando na SOCIESC, porém recebem uma bolsa de estudos para trabalhar em áreas diversas como: secretaria, financeiro, biblioteca, auxiliando os colaboradores da SOCIESC em funções administrativas.

O ERP é o Logix desenvolvido pela Logocenter é utilizado pelos setores administrativos, para fazer solicitações de compra, controle de despesas, cadastramento dos funcionários, entre outros.

Conhecendo melhor a estrutura de informática da SOCIESC os itens tratados na Política de Segurança da Informação devem abranger situações dentro desta estrutura, considerando os usuários destes sistemas ou rede de computadores.

As informações que estão dentro da estrutura da SOCIESC podem ser apresentadas de diversas formas, sendo elas: arquivos eletrônicos armazenados nos servidores, informações no sistema de notas, registros de notas e freqüência em diários de classe, informações que podem ser acessadas no ERP, entre outras. Independente da forma que a informação será acessada pelo usuário ela deve obedecer aos princípios de segurança da informação garantindo a integridade, confidencialidade, autenticidade e disponibilidade das informações.

4.5 CONCLUSÃO DO CAPÍTULO

É de grande importância a criação de regras e padrões que possam esclarecer aos usuários da rede de computadores da SOCIESC procedimentos e ações que não devem acontecer ou que devem ser monitoradas para garantia da segurança da informação.

Como mostrado no decorrer deste capítulo a estrutura de informática da SOCIESC possui um número bastante elevado de computadores, usuários e recursos de informática para serem gerenciados, é importante a existência de uma política de segurança para que todos os usuários dos recursos de informática tenham conhecimento de suas responsabilidade, podendo assim auxiliar na segurança da informação de toda a instituição.

A SOCIESC é uma Instituição de Ensino com um grande número de alunos e um número bastante elevado de funcionários, será criado um modelo de política de segurança para Instituições de Ensino usando como referencia a SOCIESC.

5 POLÍTICA DE SEGURANÇA PARA INSTITUIÇÃO DE ENSINO

Quando falamos em uma Instituição de Ensino devemos lembrar que existem algumas particularidades em comparação a uma empresa, principalmente relacionada às pessoas que fazem parte de uma empresa ou em uma Instituição de Ensino.

Em Instituições de Ensino além do funcionário, temos também a pessoa do aluno que freqüenta as dependências das Instituições, assistindo suas aulas, sendo que durante estes momentos estará utilizando os recursos disponíveis e acessando informações das Instituições de Ensino a qual pertence. Em algumas Instituições pode existir ainda a pessoa do aluno bolsista, aquele aluno que estuda na Instituição, porém no período em que não esta em sala de aula ele trabalha em algum departamento da própria Instituição.

Uma Política de Segurança voltada para Instituições de Ensino deve ser criada de forma a estabelecer regras a serem seguidas por todos os usuários dos recursos de informática de maneira que todos sejam envolvidos e conscientizados da importância da segurança das informações da Instituição.

Para criação do modelo de política de segurança apresentado neste estudo foram utilizadas algumas informações como:

- A norma NBR ISO 17799 como referência, sendo que esta norma é o código de prática para a gestão da segurança da informação;
- Informações sobre a estrutura de informática da SOCIESC e necessidades de abrangência da política foram buscadas junto a equipe de TI da SOCIESC, conforme questionário em anexo (anexo III);
- Alguns modelos de política de segurança foram consultados como:

- Política de segurança e utilização dos recursos de rede da FURB (Fundação Universidade Regional de Blumenau);
- Política de Administração de Contas – UFRGS (Universidade Federal do Rio Grande do Sul);
- Modelo de Política de Segurança, NIC BR Security Office, entre outros.

Atualmente na SOCIESC não existe nenhuma política de segurança que esteja implantada e seguida por todos os funcionários, existe um procedimento para utilização de Notebooks e Palm-Tops particulares na rede SOCIESC e um termo de compromisso que a pessoa que estiver utilizando estes equipamentos deve preencher, estes documentos estão no anexo (anexo IV e anexo V), estes arquivos foram elaborados pela equipe de TI da SOCIESC e estão disponíveis ao acesso de todos os funcionários através do ISODOC (software para controle de documentos).

5.1 OBJETIVOS DA POLÍTICA DE SEGURANÇA

O objetivo é garantir que os recursos de informática e a informação estarão sendo usados de maneira adequada. O usuário deve conhecer regras para utilização da informação de maneira segura, evitando expor qualquer informação que possa prejudicar a Instituição de Ensino, os funcionários ou alunos.

Tem por objetivo, também, prestar aos funcionários serviços de rede de alta qualidade e ao mesmo tempo desenvolver um comportamento extremamente ético e profissional, de forma a evitar falhas de segurança que possam impossibilitar o acesso às informações, sendo que as ações da equipe de TI no que diz respeito a manutenção de recursos de informática possam ser justificadas com as regras estabelecidas na política. Ex.: a desativação e uma conta que tenha violado as regras da política de utilização de contas.

Deve fornecer ao funcionário informações suficientes para saber se os procedimentos descritos na política são aplicáveis a ele ou não, utilizando linguagem simples e de fácil entendimento por todos.

Assim, para assegurar os altos padrões de qualidade na prestação desses serviços, faz-se necessária a especificação de uma política de segurança da informação, visando esclarecer aos usuários a importância da proteção da informação e definindo normas e procedimentos para a utilização da rede, e conseqüentemente da informação que nela trafega.

A Política deve implementar controles para preservar os interesses dos funcionários, clientes e demais parceiros contra danos que possam acontecer devido a falha de segurança, deve-se descrever as normas de utilização e atividades que possa ser consideradas como violação ao uso dos serviços e recursos, os quais são considerados proibidos.

Pode-se definir como serviços e recursos os equipamentos utilizados pelos funcionários e alunos tais como: computadores, e-mails, acesso a Internet, informação em diretórios da rede e afins.

As normas descritas no decorrer devem sofrer alterações sempre que necessário, sendo que qualquer modificação deve ser registrada e divulgada, se existir necessidade de mudança no ambiente deve-se solicitar com tempo hábil para que as providencias necessárias sejam tomadas.

Tais normas são fornecidas, a título de orientação dos funcionários, alunos e demais envolvidos. Em caso de dúvida o usuário deverá procurar a equipe de segurança visando esclarecimentos.

Caso os procedimentos ou normas aqui estabelecidos sejam violados os usuários poderão sofrer punições que serão esclarecidas e detalhadas durante este documento.

Esta política aplica-se a todos os usuários dos sistemas ou computadores da rede SOCIESC, sendo eles: funcionários, estagiários, alunos colaboradores, terceiros ou visitantes,

alunos de toda a SOCIESC (Colégio Tupy, Escola Técnica Tupy, Instituto Superior Tupy e Capacitação Empresarial).

Todos os usuários dos sistemas ou computadores desempenham um papel essencial de apoio efetivo para que a política de segurança possa ser adotada por toda a organização. Deve-se assegurar que todos os usuários estejam conscientes da importância de cumprir as definições estabelecidas na política para garantir a segurança das informações acessadas por todos.

Todos devem estar cientes dos procedimentos de segurança, ter conhecimento da política, se necessário, devem receber treinamentos de como fazer uso correto das informações que nela estão definidas.

A política de segurança será dividida em políticas de segurança da estrutura de informática e política de segurança física. A primeira estará sendo dividida em outras políticas, como rede, e-mail, Internet, senhas, entre outras. A política de segurança física irá abordar o acesso a laboratórios, departamentos, segurança de equipamentos, documentos armazenados fisicamente, entre outros itens. Dentro de cada uma destas divisões serão criadas regras gerais, que podem ser aplicadas a todos, se existirem regras especificas para funcionários, alunos ou alunos colaboradores serão criadas divisões paras estas regras.

A seguir, será detalhada a política de segurança e informa-se que tudo o que não for permitido e/ou liberado é considerado violação à Política e passível de punição.

5.2 POLÍTICA DE SEGURANÇA DA ESTRUTURA DE INFORMÁTICA

A Política de Segurança da estrutura de informática abrange itens relacionados a segurança da informação relacionada a utilização desta estrutura, será contemplada: política

de utilização da rede, administração de contas, senhas, e-mail, acesso a Internet, uso das estações de trabalho, utilização de impressoras.

5.2.1 Política de Utilização da Rede

Esse tópico visa definir as normas de utilização da rede que abrange o login, manutenção de arquivos no servidor e tentativas não autorizadas de acesso. Estes itens estarão sendo abordados para todos os usuários dos sistemas e da rede de computadores da SOCIESC.

5.2.1.1 Regras Gerais

- Não são permitidas tentativas de obter acesso não autorizado, tais como tentativas de fraudar autenticação de usuário ou segurança de qualquer servidor, rede ou conta (também conhecido como *"cracking"*[4]). Isso inclui acesso aos dados não disponíveis para o usuário, conectar-se a servidor ou conta cujo acesso não seja expressamente autorizado ao usuário ou colocar à prova a segurança de outras redes;
- Não são permitidas tentativas de interferir nos serviços de qualquer outro usuário, servidor ou rede. Isso inclui ataques, tentativas de provocar congestionamento em redes, tentativas deliberadas de sobrecarregar um servidor e tentativas de "quebrar" (invadir) um servidor;

[4] Cracking é o nome dado a ações de modificações no funcionamento de um sistema, de maneira geralmente ilegal, para que determinados usuários ganhem algo com isso.

- Antes de ausentar-se do seu local de trabalho, o usuário deverá fechar todos os programas em uso, evitando, desta maneira, o acesso por pessoas não autorizadas, se possível efetuar o logout/logoff da rede ou bloqueio do computador através de senha;
- O usuário deve fazer manutenção no diretório pessoal, evitando acúmulo de arquivos desnecessários;
- Material de natureza pornográfica e racista não pode ser exposto, armazenado, distribuído, editado ou gravado através do uso dos recursos computacionais da rede;
- Jogos ou qualquer tipo de software/aplicativo não pode ser gravado ou instalado no diretório pessoal do usuário, no computador local e em qualquer outro diretório da rede, podem ser utilizados apenas os softwares previamente instalados no computador;
- Não é permitido criar e/ou remover arquivos fora da área alocada ao usuário e/ou que venham a comprometer o desempenho e funcionamento dos sistemas. As áreas de armazenamento de arquivos são designadas conforme mostra a tabela 5.1.

Tabela 5.1 - Compartilhamento das áreas de armazenamento de arquivos

Compartilhamento	Utilização
Diretório Pessoal (F:)	Arquivos Pessoais de responsabilidade do usuário dono deste diretório pessoal
Diretórios departamentais	Arquivos do departamento em que trabalha
Diretório público	Arquivos temporários ou de compartilhamento geral, para todos os alunos, por exemplo.

Fonte: Departamento de TI da SOCIESC.

Em alguns casos pode haver mais de um compartilhamento referente aos arquivos do departamento em qual faz parte.

- A pasta PÚBLICA ou similar, não deverá ser utilizada para armazenamento de arquivos que contenham assuntos sigilosos ou de natureza sensível, devem ser armazenadas apenas informações comuns a todos;
- Haverá limpeza semestral dos arquivos armazenados na pasta PÚBLICO ou similar, para que não haja acúmulo desnecessário de arquivos;
- É proibida a instalação ou remoção de softwares que não forem devidamente acompanhadas pelo departamento técnico, através de solicitação escrita que será disponibilizada, e deve conter autorização do coordenador da área do solicitante;
- Não são permitidas alterações das configurações de rede e inicialização das máquinas bem como modificações que possam trazer algum problema futuro;
- Quanto a utilização de equipamentos de informática particulares, computadores, impressoras, entre outros, a SOCIESC não fornecerá acessórios, software ou suporte técnico para computadores pessoais de particulares, incluindo assistência para recuperar perda de dados, decorrentes de falha humana, ou pelo mau funcionamento do equipamento ou do software;
- O acesso a sistemas, como sistema acadêmico (WAE), deve ser controlado pela identificação do usuário e pelas senhas designadas para usuários autorizados, as senhas compartilhadas devem ser excepcionais e autorizadas pela equipe técnica.

5.2.1.2 Regras para funcionários

- É obrigatório armazenar os arquivos inerentes à empresa no servidor de arquivos para garantir a cópia de segurança dos mesmos;

- É proibida a abertura de computadores para qualquer tipo de reparo, seja isto feito em departamentos ou laboratórios de informática, caso seja necessário o reparo deverá ocorrer pelo departamento técnico;
- Quanto à utilização de equipamentos de informática particulares o funcionário deverá comunicar a coordenação de seu departamento;
- Quando um funcionário é transferido entre departamentos, o coordenador que transferiu deve certificar-se de que todos os direitos de acesso aos sistemas e outros controles de segurança ainda serão necessários na sua nova função e informar a equipe de TI qualquer modificação necessária;
- Quando ocorrer a demissão do funcionário, o coordenador responsável deve informar a equipe técnica para providenciar a desativação dos acessos do usuário à qualquer recurso da rede. Deve-se verificar a necessidade de troca de senhas de contas de uso comum ao departamento, evitando o acesso às informações.

5.2.1.3 Regras para alunos

É apagado o conteúdo das contas de usuário do domínio ensino semestralmente, portanto o aluno ou professor que desejar manter suas informações deve providenciar a cópia dos arquivos sempre ao final do semestre.

Quanto a utilização de equipamentos de informática particulares o aluno deverá comunicar a coordenação de ensino responsável.

5.2.1.4 Regras para alunos colaboradores

O acesso as informações é feito através da conta criada pela equipe de segurança através de solicitação do coordenador responsável. Se não existir necessidade o aluno colaborador ou estagiário pode não ter conta de acesso a rede de computadores.

O acesso a diretórios ou compartilhamentos dos departamentos deve ser fornecido somente em caso de necessidade de acesso.

5.2.2 Política de Administração de contas

Este tópico visa definir as normas de administração das contas que abrange: criação, manutenção e desativação da conta. Esta política será dividida por usuários para facilitar o entendimento de todos.

5.2.2.1 Regras Gerais

Desativação da conta:

- É reservado o direito de desativar uma conta de usuário, por parte da equipe de segurança da SOCIESC, caso verifique-se a ocorrência de algum dos critérios abaixo especificados:
    - Incidentes suspeitos de quebra de segurança nas contas dos usuários;
    - Reincidência na quebra de senhas por programas utilizados pela equipe de segurança;

5.2.2.2 Regras para Funcionários

Todo funcionário da SOCIESC poderá ter uma conta para acesso aos recursos da rede de computadores da SOCIESC, os acessos a demais sistemas devem ser informados pelo coordenador da área no momento da solicitação da conta do usuário. Para solicitação da conta para novos funcionários os coordenadores devem proceder da maneira explicada abaixo.

Criação de contas:

- Todo funcionário pode obter uma conta de acesso a rede de computadores da SOCIESC, para isto:
    - O coordenador de departamento a que o funcionário pertence deverá fazer uma solicitação da criação da conta;
    - Esta solicitação deve ser feita através de e-mail para a equipe de segurança;
    - Deve-se informar o número da matrícula do funcionário, assim como os acessos que serão necessários para este usuário;
    - Os principais itens a serem informados referente aos acessos permitidos aos usuários são: será uma conta para acesso ao domínio SOCIESC, precisará de acesso ao domínio ensino, acesso ao sistema de ERP, acesso ao sistema acadêmico, criação da conta de email.
    - A equipe de segurança retornará para a coordenação de departamento as informações sobre a conta criada.

Manutenção da conta:

- Cada funcionário que tiver sua conta criada terá um espaço no servidor para gravar seus arquivos pessoais, é feita cópia de segurança dos arquivos do servidor do domínio SOCIESC diariamente;

- As contas que funcionários tenham no domínio ENSINO, utilizadas em laboratórios, não é feito cópia de segurança, portanto o próprio usuário deve fazer copia de segurança dos arquivos que julgar necessário;
- A manutenção dos arquivos na conta pessoal é de responsabilidade do usuário, sendo que o mesmo deve evitar acumulo de arquivos desnecessários e sempre que possível verificar o que pode ser eliminado;
- As contas podem ser monitoradas pela equipe de segurança com o objetivo de verificar possíveis irregularidades no armazenamento ou manutenção dos arquivos nos diretórios pessoais.

5.2.2.3 Regras para Alunos

Todo aluno da SOCIESC poderá ter uma conta para acesso aos recursos da rede de computadores, sendo que estará usando o domínio ENSINO, todos os usuários tem um limite de armazenamento de arquivos em seu diretório pessoal, qualquer necessidade de um espaço maior para armazenamento dos arquivos nos diretórios pessoais deve ser informado pelo professor a equipe de segurança da SOCIESC.

Criação de contas:

- A criação da conta do aluno é feita através do envio das informações de matrícula dos alunos pela secretaria. A cada semestre as informações das contas dos alunos são apagadas e uma nova senha é gerada. Alunos que não possuírem conta de acesso a rede de computadores devem solicitar a equipe de segurança a criação da mesma.

- A senha dos alunos é criada pela equipe de segurança no momento da criação da conta, esta senha pode ser alterada quando o usuário utilizar sua conta, sendo importante seguir regras para criação de senhas, que serão detalhadas neste documento.

Administração de contas:

- A SOCIESC não se responsabiliza por documentos, programas e relatórios dentro das contas pessoais dos usuários do domínio ENSINO, cabe aos usuários, a tarefa de salvar os arquivos periodicamente para, no caso de falhas rever seus dados;
- Não é feita cópia de segurança dos arquivos dos servidores do domínio ENSINO;
- É de responsabilidade do usuário as informações em seu diretório pessoal, sendo que o mesmo deve evitar o acumulo de arquivos desnecessários;
- As contas podem ser monitoradas pela equipe de segurança com o objetivo de verificar possíveis irregularidades no armazenamento ou manutenção dos arquivos nos diretórios pessoais.

5.2.2.4 Alunos Colaboradores ou Estagiários

A criação de conta para acesso a rede de computadores da SOCIESC para alunos trabalhadores ou estagiários dependerá da necessidade de utilização, se existir necessidade o procedimento será o mesmo utilizado para criação de contas para funcionários, o coordenador da área responsável deve informar ao departamento de segurança as informações para criação da conta.

5.2.3 Política de Senhas

As senhas são utilizadas pela grande maioria dos sistemas de autenticação e são consideradas necessárias como meio de autenticação. Porém, elas são consideradas perigosas, pois dependem do usuário, que podem, por exemplo escolher senhas óbvias e fáceis de serem descobertas, ou ainda compartilha-las com seus amigos.

5.2.3.1 Regras Gerais

Senhas são um meio comum de validação da identidade do usuário para obtenção de acesso a um sistema de informação ou serviço. Convém que a concessão de senhas seja controlada, considerando: as senhas temporárias devem ser alteradas imediatamente, não devem ser armazenadas de forma desprotegida, entre outros.

A senha deve ser redefinida pelo menos a cada dois meses, para usuários comuns e a cada mês para usuários de acesso mais restrito. As senhas devem ser bloqueadas após 3 à 5 tentativas sem sucesso, sendo que, o administrador da rede e o usuário devem ser notificados sobre estas tentativas.

As responsabilidades do administrador do sistema incluem o cuidado na criação e alteração das senhas dos usuários, além da necessidade de manter atualizados os dados dos mesmos.

As responsabilidades do usuário incluem, principalmente, os cuidados para a manutenção da segurança dos recursos, tais como sigilo da senha e o monitoramento de sua conta, evitando sua utilização indevida. As senhas são sigilosas, individuais e intransferíveis, não podendo ser divulgadas em nenhuma hipótese.

Tudo que for executado com a sua senha de usuário da rede ou de outro sistema será de inteira responsabilidade do usuário, por isso, tome todo o cuidado e mantenha sua senha secreta.

A *Request for Comments* (RFC) 2196, que é um guia para desenvolvimento de políticas de segurança de computador, comenta sobre como selecionar e manter senhas.

As senhas são efetivas apenas quando usadas corretamente, requer alguns cuidados na sua escolha e uso, como:

- Não utilize palavras que estão no dicionário (nacionais ou estrangeiros);
- Não utilize informações pessoais fáceis de serem obtidas, como o número de telefone, nome da rua, nome do bairro, cidade, data de nascimento, etc;
- Não utilize senhas somente com dígitos ou com letras;
- Utilize senha com, pelo menos, oito caracteres;
- Misture caracteres maiúsculos e minúsculos;
- Misture números, letras e caracteres especiais;
- Inclua, pelo menos, um caracter especial;
- Utilize um método próprio para lembrar da senha, de modo que ela não precise ser escrita em nenhum local, em hipótese alguma;
- Não anote sua senha em papel ou em outros meios de registro de fácil acesso;
- Não utilize o nome do usuário;
- Não utilize o primeiro nome, o nome do meio ou o sobrenome;
- Não utilize nomes de pessoas próximas, como da esposa(o), dos filhos, de amigos;
- Não utilize senhas com repetição do mesmo dígito ou da mesma letra;
- Não forneça sua senha para ninguém, por razão alguma;
- Utilize senhas que podem ser digitadas rapidamente, sem a necessidade de olhar para o teclado.

5.2.4 Política de Utilização de E-Mail

Esse tópico visa definir as normas de utilização de e-mail que engloba desde o envio, recebimento e gerenciamento das contas de e-mail.

Todos os usuários de e-mail devem tomar ciência que a Internet opera em domínio publico que foge do controle da equipe técnica da SOCIESC. As mensagens podem estar sujeitas a demora e serviços potencialmente não confiáveis.

Grande parte da comunicação do dia-a-dia passa através de e-mails. Mas é importante também lembrar que grande parte das pragas eletrônicas atuais chega por esse meio. Os vírus atuais são mandados automaticamente, isso significa que um e-mail de um cliente, parceiro ou amigo não foi mandado necessariamente pelo mesmo.

Nossos servidores de e-mail encontram-se protegidos contar vírus e códigos maliciosos, mas algumas atitudes do usuário final são importantes. Para isto é importante que algumas regras sejam obedecidas.

5.2.4.1 Regras Gerais

- O email deve ser utilizado de forma consciente, evitando qualquer tipo de perturbação a outras pessoas, seja através da linguagem utilizada, freqüência ou tamanho das mensagens;
- O envio de e-mail deve ser efetuado somente para pessoas que desejam recebê-los, se for solicitada a interrupção do envio a solicitação deve ser acatada e o envio não devera acontecer;

- É proibido o envio de grande quantidade de mensagens de e-mail (*spam)* que, de acordo com a capacidade técnica da Rede, seja prejudicial ou gere reclamações de outros usuários. Isso inclui qualquer tipo de mala direta, como, por exemplo, publicidade, comercial ou não, anúncios e informativos, ou propaganda política;

- É proibido reenviar ou de qualquer forma propagar mensagens em cadeia independentemente da vontade do destinatário de receber tais mensagens;

- Evite mandar e-mail para mais de 10 (dez) pessoas de uma única vez, é proibido o envio de e-mail mal-intencionado, tais como *mail bombing*[5] ou sobrecarregar um usuário, site ou servidor com e-mail muito extenso ou numerosas partes de e-mail;

- Caso a SOCIESC julgue necessário haverá bloqueios:

    1. De e-mail com arquivos anexos que comprometa o uso de banda ou perturbe o bom andamento dos trabalhos;

    2. De e-mail para destinatários ou domínios que comprometa o uso de banda ou perturbe o bom andamento dos trabalhos;

- É proibido o forjar qualquer das informações do cabeçalho do remetente;

- Não é permitido má utilização da linguagem em respostas aos e-mails comerciais, como abreviações de palavras, uso de gírias;

- É obrigatória a manutenção da caixa de e-mail, evitando acúmulo de e-mails e arquivos inúteis;

- Obrigatoriedade da utilização do protocolo IMAP para recebimento dos e-mails provenientes do domínio sociesc.com.br;

- A cota máxima de e-mails armazenados não deve ultrapassar os 250 MegaBytes;

[5] Excesso de mensagens enviadas a uma caixa postal, a ponto de congestionar o tráfego do provedor. Mensagem enviada a uma caixa postal que, em conseqüência, de sua grande extensão acaba por travar o computador.

- Obrigatoriedade da utilização do Web Mail ou do programa Mozilla, Outlook Express, Outlook 2000 ou outro software homologado pelo departamento técnico, para ser o cliente de email;
- Para certificar-se que a mensagem foi recebida pelo destinatário, deve-se, se necessário, utilizar procedimentos de controles extras para verificar a chegada da mensagem, devem ser solicitadas notificações de “recebimento” e “leitura”;
- Não execute ou abra arquivos anexados enviados por emitentes desconhecidos ou suspeitos;
- Não abra arquivos anexados com as extensões .bat, .exe, .src, .lnk e .com se não tiver certeza absoluta que solicitou este email;
- Desconfie de todos email com assuntos estranhos e/ou em inglês. Alguns dos vírus mais terríveis dos últimos anos tinham assuntos como: ILOVEYOU, Branca de neve pornô, etc;
- Evite anexos muito grandes;

5.2.4.2 Regras para funcionários

- Não devem ser enviadas mensagens de correio eletrônico cujo conteúdo seja confidencial ou restrito a SOCIESC, não podendo tornar-se público;
- Não utilize o email da SOCIESC para fins pessoais;
- É obrigatória a utilização de assinatura nos e-mails, seguindo padrão a ser estabelecido pela SOCIESC.

5.2.5 Política de acesso a Internet

Esse tópico visa definir as normas de utilização da Internet que engloba desde a navegação a sites, downloads e uploads de arquivos.

A Internet é uma ferramenta de trabalho e deve ser usada para este fim pelos funcionários e alunos da SOCIESC, não é permitido o seu uso para fins recreativos durante o horário de trabalho ou de aula.

5.2.5.1 Regras Gerais

- Somente navegação de sites é permitida. Casos específicos que exijam outros tipos de serviços, como download de arquivos, deverão ser solicitados diretamente à equipe de segurança com autorização do supervisor do usuário que deseja este acesso;
- É proibida a divulgação de informações confidenciais da SOCIESC em grupos de discussão, listas ou bate-papo, não importando se a divulgação foi deliberada ou inadvertida, sendo possível sofrer as penalidades previstas nas políticas e procedimentos internos e/ou na forma da lei;
- Caso a SOCIESC julgue necessário haverá bloqueios de acesso à:

    1. arquivos que comprometa o uso de banda ou perturbe o bom andamento dos trabalhos;

    2. domínios que comprometa o uso de banda ou perturbe o bom andamento dos trabalhos;

- Obrigatoriedade da utilização do programa *Mozilla*, *Internet Explorer*, ou outro software homologado pelo departamento técnico, para ser o cliente de navegação;

- Não será permitido software de comunicação instantânea, não homologados/autorizados pela equipe técnica;
- Não será permitida a utilização de softwares de *peer-to-peer* (P2P), tais como *Kazaa, Morpheus* e afins;
- O acesso a sites com conteúdo pornográfico, jogos, bate-papo, apostas, é bloqueado e as tentativas de acesso serão monitorados;
- Não será permitida a utilização de serviços de streaming, tais como Rádios On-Line, Usina do Som e afins.

5.2.5.2 Regras para funcionários

- Poderá ser utilizada a Internet para atividades não relacionadas com os negócios durante o horário de almoço, ou fora do expediente, desde que dentro das regras de uso definidas nesta política;
- Os funcionários com acesso à Internet podem baixar somente programas ligados diretamente às atividades da empresa e devem providenciar o que for necessário para regularizar a licença e o registro desses programas;
- Funcionários com acesso à Internet não podem efetuar upload[6] de qualquer software licenciado para à SOCIESC ou de dados de propriedade da SOCIESC ou de seus clientes, sem expressa autorização do responsável pelo software ou pelos dados;
- Haverá geração de relatórios dos sites acessados por usuário, se necessário a publicação desse relatório e prestação de contas do usuário dos acessos;

[6] upload significa transferir um arquivo do seu computador para outro computador na Internet

5.2.6 Política de uso das Estações de trabalho

Cada estação de trabalho possui códigos internos os quais permitem que ela seja identificada na rede. Sendo assim, tudo que for executado na estação de trabalho será de responsabilidade do usuário. Por isso, sempre que sair de frente da estação de trabalho tenha certeza que efetuou o logoff ou bloqueou a estação de trabalho.

5.2.6.1 Regras Gerais

- Não utilize nenhum tipo de software/hardware sem autorização da equipe técnica;
- Não é permitido gravar nas estações de trabalho MP3, filmes, fotos e software com direitos autorais ou qualquer outro tipo que possa ser considerado pirataria;
- Mantenha nas estações de trabalho somente o que for supérfluo ou pessoal. Todos os dados relativos à SOCIESC devem ser mantidos no servidor, onde existe sistema de backup diário e confiável;
- Os arquivos gravados em diretórios temporários das estações de trabalho podem ser acessados por todos os usuários que utilizarem a mesma, portanto não pode-se garantir sua integridade e disponibilidade. Poderão ser alterados ou excluído sem prévio aviso e por qualquer usuário que acessar a estação.

5.2.7 Política de uso de impressoras

Esse tópico visa definir as normas de utilização de impressoras disponíveis nos departamentos da SOCIESC, esta política é aplicada somente a funcionários e alunos

trabalhadores que utilização impressoras em seus departamentos, sendo que, nos laboratórios de ensino, que são utilizados pelos alunos, não existem impressoras instaladas.

5.2.7.1 Regras Gerais

- Ao mandar imprimir, verifique na impressora se o que foi solicitado já está impresso;
- Se a impressão deu errado e o papel pode ser reaproveitado na sua próxima tentativa, recoloque-o na bandeja de impressão. Se o papel servir para rascunho, leve para sua mesa. Se o papel não servir para mais nada, jogue no lixo.
- Não é permitido deixar impressões erradas na mesa das impressoras, na mesa das pessoas próximas a ela e tampouco sobre o gaveteiro;
- Se a impressora emitir alguma folha em branco, recoloque-a na bandeja;
- Se você notar que o papel de alguma das impressoras está no final, faça a gentileza de reabastecê-la. Isso evita que você e outras pessoas tenham seus pedidos de impressão prejudicados e evita acúmulo de trabalhos na fila de impressão;
- Utilize a impressora colorida somente para versão final de trabalhos e não para testes ou rascunhos.

5.3 POLÍTICA DE SEGURANÇA FÍSICA

O objetivo desta política é prevenir o acesso não autorizado, dano e interferência às informações e instalações físicas da organização. A segurança física dos equipamentos de informática e das informações da empresa deve ser protegidas de possíveis danos, será

abordada a segurança físicas dos laboratórios de informática, das instalações de TI, dos equipamentos no geral e procedimentos para garantir a segurança física.

5.3.1 Política de controle de acesso

Existem áreas que merecem maior atenção quanto ao controle da entrada de pessoas, estas áreas são departamentos que contém informações ou equipamentos que devem ser protegidos, como por exemplo: sala de servidores, departamentos como financeiro, setor de documentação, departamento de recursos humanos, sala de coordenadores e diretores, entre outras.

Convém que estas áreas sejam protegidas por controles de entrada apropriados para assegurar que apenas pessoas autorizadas tenham acesso liberado. Instalações desenvolvidas para fins especiais que abrigam equipamentos importantes exigem maior proteção que o nível normalmente oferecido. As instalações da equipe de TI devem ser localizadas e construídas buscando minimizar: acesso público direto, riscos ao fornecimento de energia e serviços de telecomunicações.

5.3.1.1 Regras Gerais

Apenas pessoas autorizadas podem acessar as instalações da equipe de TI, sendo que os funcionários devem usar crachás de identificação.

Departamentos que tratem com informações confidenciais de alunos, como por exemplo, documentação, informações financeiras, acadêmicas o acesso deve ser permitido somente para pessoas autorizadas.

A temperatura umidade e ventilação das instalações que abrigam equipamentos de informática e de comunicações, devem estar de acordo com os padrões técnicos especificados pelos fabricantes dos equipamentos.

Se acontecer a perda de chaves de departamentos ou laboratórios a coordenação responsável deve ser informada imediatamente para que possa providenciar a troca da fechadura e de outras cópias da chave perdida.

5.3.2 Política de mesa limpa e tela limpa

A política de mesa limpa deve ser considerada para os departamentos e utilizada pelos funcionários da SOCIESC, de modo que papéis e mídias removíveis não fiquem expostas à acessos não autorizado.

A política de tela limpa deve considerar que se o usuário não estiver utilizando a informação ela não deve ficar exposta, reduzindo o risco de acesso não autorizado, perda e danos à informação.

5.3.2.1 Regras Gerais.

Os papéis ou mídias de computador não devem ser deixados sobre as mesas, quando não estiverem sendo usados devem ser guardados de maneira adequada, em preferência em gavetas ou armários trancados.

O ambiente dos departamentos devem ser mantidos limpo, sem caixa ou qualquer outro material sobre o chão de modo que possa facilitar o acesso de pessoas que estiverem no departamento.

Sempre que não estiver utilizando o computador não deixar nenhum arquivo aberto, de modo que as informações possam ser visualizadas por outras pessoas que estiverem no departamento.

Agendas, livros ou qualquer material que possam ter informações sobre a empresa ou informações particulares devem sempre ser guardadas em locais fechados, evitando o acesso.

Chaves de gavetas, armários, de portas de acesso à departamento, de laboratórios de informática devem ser guardadas em lugar adequado, não devem ser deixadas sobre a mesa ou guardadas com o professor/funcionário.

5.3.3 Política de utilização de laboratórios de informática e salas de projeção

Para utilização de laboratórios e equipamentos de informática algumas regras devem ser cumpridas para que possa ser feito uso correto das instalações evitando qualquer tipo de dano a equipamentos em laboratórios que possam prejudicar a utilização dos mesmos.

5.3.3.1 Regras Gerais

O acesso a laboratórios de informática deve ser controlado, somente sendo permito o uso dos mesmos com um funcionário responsável.

É de responsabilidade do professor/funcionário que utilizou o laboratório zelar pela ordem das instalações, sendo necessária qualquer tipo de manutenção a equipe técnica deve ser informada.

No momento em que entrar no laboratório o funcionário responsável deve verificar se todos os computadores estão funcionando corretamente, após a utilização esta verificação deve ser repetida, qualquer problema a equipe técnica deve ser informada , para que a solução possa ser providenciada o mais rápido possível.

Os equipamentos devem ser trancados e em segurança quando deixados sem supervisão, não sendo permitida a utilização de laboratórios sem supervisão.

Nenhum equipamento pode ser conectado aos sistemas ou rede sem aprovação prévia e, se necessário, sob supervisão.

Alimentos, bebidas, fumo e o uso de telefones móveis e celulares são proibidos nos laboratórios.

As chaves de acesso aos laboratórios devem ficas guardadas em locais que o acesso seja controlado, que não seja permitida a entrada de pessoas não autorizadas, evitando que possam ter acesso as chaves.

Se a utilização do laboratório não estiver prevista no horário do laboratório esta utilização devera ser feita somente mediante a reserva do laboratório, garantindo assim que exista um registro de utilização dos laboratórios.

5.4 TERMO DE COMPROMISSO

O termo de compromisso é utilizado para que os funcionários, alunos, alunos colaboradores e estagiários se comprometam formalmente em seguir a política de segurança, tomando ciência das punições impostas ao seu não cumprimento.

No termo de compromisso podem ser reforçados os principais pontos da política de segurança, deve ser assinado por todos os funcionários e estagiários, e deve ser renovado sempre que necessário. O anexo VI é um modelo de termo de compromisso.

5.5 VERIFICAÇÃO DA UTILIZAÇÃO DA POLÍTICA

Para garantir as regras mencionadas acima a SOCIESC se reserva no direito de:

- Implantar softwares e sistemas que podem monitorar e gravar todos os usos de Internet através da rede e das estações de trabalho da empresa;
- Inspecionar qualquer arquivo armazenado na rede, estejam no disco local da estação ou nas áreas privadas da rede, visando assegurar o rígido cumprimento desta política;
- Foram instalados uma série de softwares e hardwares para proteger a rede interna e garantir a integridade dos dados e programas, incluindo um firewall, que é a primeira, mas não a única barreira entre a rede interna e a Internet;

5.6 VIOLAÇÃO DA POLÍTICA, ADVERTÊNCIA E PUNIÇÕES

Ao detectar uma violação da política, a primeira coisa a fazer é determinar a sua razão, ou seja, a violação pode ter ocorrido por negligência, acidente ou erro; por desconhecimento da política ou por ação previamente determinada, ignorando a política estabelecida. Um processo de investigação deve determinar as circunstâncias da violação, como e porque ela ocorreu.

Nos termos da Política, a SOCIESC procederá ao bloqueio do acesso ou o cancelamento do usuário caso seja detectado uso em desconformidade com que foi estabelecido ou de forma prejudicial à Rede.

É recomendado o treinamento dos usuários em segurança da informação, como forma de conscientização e divulgação da política de segurança a ser seguida por todos. O programa de treinamento em segurança deve fazer parte do programa de integração de novos funcionários e do programa de integração de novos alunos (ao início de cada ano letivo), devendo ser feitos treinamentos de reciclagem para os funcionários mais antigos.

5.6.1.1 Regras para funcionários

Caso seja necessário advertir o funcionário, será informado o departamento de Recursos Humanos para interagir e manter-se informado da situação.

O não cumprimento, pelo funcionário, das normas estabelecidas neste documento seja isolada ou acumulativamente, poderá causar, de acordo com a infração cometida, as seguintes punições: Comunicação de descumprimento, Advertência ou suspensão, Demissão por justa causa.

Comunicação de descumprimento: Será encaminhado ao funcionário, por e-mail, comunicado informando o descumprimento da norma, com a indicação precisa da violação praticada. Cópia desse comunicado permanecerá arquivada junto ao Departamento de Recursos Humanos na respectiva pasta do funcionário.

Advertência ou suspensão: A pena de advertência ou suspensão será aplicada, por escrito, somente nos casos de natureza grave ou na hipótese de reincidência na prática de infrações de menor gravidade.

Demissão por justa causa: Nas hipóteses previstas no artigo 482 da Consolidação das Leis do Trabalho, conforme anexo VII.

Fica desde já estabelecido que não há progressividade como requisito para a configuração da dispensa por justa causa, podendo a Diretoria, no uso do poder diretivo e

disciplinar que lhe é atribuído, aplicar a pena que entender devida quando tipificada a falta grave.

5.6.1.2 Regras para alunos

Caso seja necessário advertir o aluno, será informado o departamento de Assessoria de Ensino para interagir e manter-se informado da situação.

O não cumprimento pelo aluno das normas estabelecidas neste documento seja isolada ou acumulativamente, poderá causar, de acordo com a infração cometida, as seguintes punições:

Comunicação de descumprimento: Será encaminhado ao aluno, através da Assessoria de Ensino, comunicado informando o descumprimento da norma, com a indicação precisa da violação praticada. Cópia desse comunicado permanecerá arquivada junto ao Departamento de Assessoria de Ensino na respectiva pasta do aluno.

Advertência ou suspensão: A pena de advertência ou suspensão será aplicada, por escrito, somente nos casos de natureza grave ou na hipótese de reincidência na prática de infrações de menor gravidade. Antes da aplicação desta punição será realizado o conselho de disciplina, conforme regimento escolar que detalha os direitos e deveres dos alunos e as definições dos conselhos de disciplina.

Expulsão: A decisão de expulsar um aluno é tomada durante conselho de disciplina.

No Guia Acadêmico (anexo VIII), existe um capítulo que trata sobre o Regime Disciplinar ou Conselho de Disciplina, no qual existem regras definidas sobre os participantes do conselho, sua finalidade e as ações corretivas que podem ser tomadas.

5.7 CONCLUSÃO DO CAPÍTULO

Durante este capítulo foi desenvolvido um modelo de política de segurança voltada para instituições de ensino, utilizando a estrutura de informática da SOCIESC para criação da mesma, visando sempre a criação de regras gerais dentro de cada política, sendo que quando existir regras especificas para alunos, funcionários ou alunos colaboradores estas foram detalhadas dentro da respectiva política.

O modelo apresentado procurou ser abrangente o suficiente para que todos os usuários da rede de computadores tenham regras a serem seguidas, de modo que estas regras possam ser do entendimento de todos.

6 CONCLUSÃO

Este estudo abordou a segurança da informação, seus objetivos, as dificuldades de compreender sua importância, os princípios de segurança, as medidas de segurança, dentre elas a política de segurança que é objetivo deste estudo. Desta forma, foi realizada a criação de um modelo de política de segurança.

A dependência progressiva das organizações com relação aos sistemas de informações computadorizados as torna cada vez mais vulneráveis a ameaças. Na sociedade da informação, ao mesmo tempo que as informações são consideradas um dos principais ativos de uma organização, elas estão, também sobre constante riscos. Com isso a segurança da informação tornou-se um ponto extremamente importante para a sobrevivência das organizações.

Dentre as medidas de segurança implantadas pelas organizações, para garantir a segurança da informação, está a política de segurança que tem por objetivo definir normas, procedimentos, ferramentas e responsabilidades que devem ser seguidas pelos usuários das organizações, de modo a garantir a segurança da informação.

A política de segurança é a base para todas as questões relacionadas à proteção da informação, desempenhando um papel importante nas organizações.

Para o desenvolvimento do modelo de política de segurança foi utilizada a norma NRB ISO 17799, que é a tradução da norma BS 7799 homologada em setembro de 2001 pela ABNT. Esta norma trata da Gestão de segurança da informação cobre os mais diversos tópicos da área de segurança, possuindo um grande número de controles e requerimentos que devem ser atendidos para garantir a segurança das informações de uma empresa.

É importante a definição, para usuários da rede de computadores da SOCIESC, de regras que devem ser seguidas para a utilização de maneira adequada dos recursos de

informática, assim como para a garantia da segurança física. O modelo de política de segurança desenvolvido visa a descrição destas regras de modo acessível ao entendimento dos usuários.

A política de segurança pode ser definida em três níveis: estratégico, tático e operacional, sendo que no nível estratégico define-se diretrizes mais genéricas de modo que os executivos possam entender o que esta sendo definido, no nível tático deve-se falar em normas, padronizações fazendo que todos os pontos da empresa tenham o mesmo nível de segurança, no nível operacional são definidos procedimentos e intrusões, de modo que se a configuração esta no papel não há como ser realizada de forma diferente, independente de quem estiver realizando. O modelo desenvolvido se aplica ao nível tático, pois foram definidas regras, com o objetivo que todos sigam um padrão de utilização dos recursos, garantindo a segurança das informações.

Este estudo procurou abranger a segurança da informação, tendo seu objetivo voltado para política de segurança da informação, sendo desenvolvido um modelo de política de segurança, fica a certeza que este trabalho trouxe contribuições importantes, como:

- Identificação cenário atual da segurança da informação e das medidas de segurança utilizadas pelas empresas;

- Estudo da utilização e da importância da política da segurança como uma importante medida de segurança utilizada pelas empresas;

- Desenvolver um estudo sobre os modelos de políticas de segurança utilizadas em Instituições de Ensino;

- Desenvolvimento de um modelo de política de segurança.

Para trabalhos futuros a política de segurança fica como sugestão a abrangência de alguns itens como:

- A segurança na troca de informações entre as filiais, atualmente esta comunicação entre as filiais é feita através de um link frame relay com a Brasil Telecom, porém não existe nenhum controle quando as prioridades de acesso as informações ou regras quanto as esses acessos;

- A segurança física dos laboratórios de informática sendo monitorada através da implantação de ações importantes como: criação de um local único para armazenamentos das chaves de acesso aos laboratórios, com um funcionário responsável pela entrega e recebimento destas chaves e por reservas de laboratórios que forem necessárias, de modo a evitar várias cópias destas chaves em departamentos de ensino e ter um controle da utilização do laboratório.

Para a implementação da política a sugestão é que sejam criados vários documentos referentes a cada política, e estes documentos sejam disponibilizados ao acesso de todos os funcionários, além disto sejam divulgados para os alunos e demais envolvidos.

Durante a implementação da política de segurança toda a organização deve ser envolvida. Se necessário devem ser feitos treinamentos conscientizando a importância da segurança da informação e do envolvimento de cada um na utilização e divulgação da política de segurança.

7 REFERÊNCIAS

CHOLEWA, Rômulo Moacyr. Segurança em Redes – Conceitos Básicos. Disponível em: http://www.rmc.eti.br/documentos/tutoriais/tutorial_seguranca.pdf . Acesso em: 20 ago 2004.

MARTINI, Renato. Curso de Segurança em Redes Linux. Disponível em: http://www.lemon.com.br/canais/tutoriais/ . Acesso em: 20 ago 2004.

SCUA. Conceitos de Segurança da Informação. Disponível em: http://www.scua.com.br Acesso em: 21 ago 2004.

SCUA. Política de Segurança - Principais Etapas de Elaboração. Disponível em: http://www.scua.com.br/seguranca/conceitos/politica_etapas.htm . Acesso em: 21 ago 2004.

RIBEIRO, Mário Sérgio. A Norma Brasileira para a Gestão da Segurança da Informação (ISO/IEC 17799). Disponível em: http://www.scua.com.br . Acesso em 21 ago 2004.

Criando Senhas Seguras. Disponível em: http://www.infowester.com/tutsenhas.php . Acesso em 30 ago 2004.

Gestão de Segurança da Informação. Disponível em: http://www.dnv.com.br/certificacao/sistemasdegestao/segurancadainformacao/index.asp. Acessado em 31 ago 2004.

NERY, Fernando. Por que proteger as informações ? Disponível em: www.modulo.com.br. Acesso em 31 ago 2004. Módulo Security, 2004.

Principais aspectos na Segurança de Redes de Computadores. Disponível em http://webserver.reder.unb.br/security/introducao/aspectos.htm . Acessado em 08 set 2004

OLIVEIRA, Salomão de. Segurança da Informação – Quando decidir investir ? Disponível em: www.modulo.com.br. Acesso em 10 set 2004.

ABREU, Dimitri. **Melhores práticas para classificar as informações.** Disponível em: www.modulo.com.br. Acessado em 10 set 2004.

Política de Administração de contas. Disponível em: www.cesup.ufrgs.br/cesup/politicas. Acessado em: 12 set 2004

RFC 2196 : Site Security Handbook. Disponível em: http://www.rfc-editor.org/. Acessado em: 20 set 2004.

Política de segurança e utilização dos recursos de rede e computacionais dos laboratórios LCI e LEA. Disponível em http://www.inf.furb.br/info/Politica_Seguranca.pdf. Acessado em 10 out 2004

NBR ISO/IEC 17799 : Tecnologia da informação – Código de prática para a gestão de segurança da informação. ABNT, 2001

OLIVEIRA, Wilson José de. **Segurança da Informação**. Florianópolis : Visual Books, Maio, 2001.

WADLOW, Tomas A. **Segurança de Redes : Projeto e gerenciamento de redes seguras.** Rio de Janeiro : Campus, 2000. Tradução: Fábio Freitas da Silva

NAKAMURA, Emilio Tissato. GEUS, Paulo Lício de. **Segurança de Redes em ambientes coorporativos.** São Paulo : Editora Futura, 2003

FERREIRA, Fernando Nicolau Freitas. **Segurança da Informação.** Rio de Janeiro : Ciência Moderna, 2003

MOREIRA, Nilton Stringasci. **Segurança Mínima.** Rio de Janeiro : Axcel Books, 2001

8 ANEXOS

ANEXO I – ORGANOGRAMA SOCIESC

ANEXO II – SERVIDORES DA SOCIESC – UNIDADE JOINVILLE

ANEXO III – QUESTIONARIO SOBRE ESTRUTURA DE INFORMATICA DA SOCIESC

ANEXO IV – DIRETRIZES PARA USO DE NOTEBOOK PARTICULAR

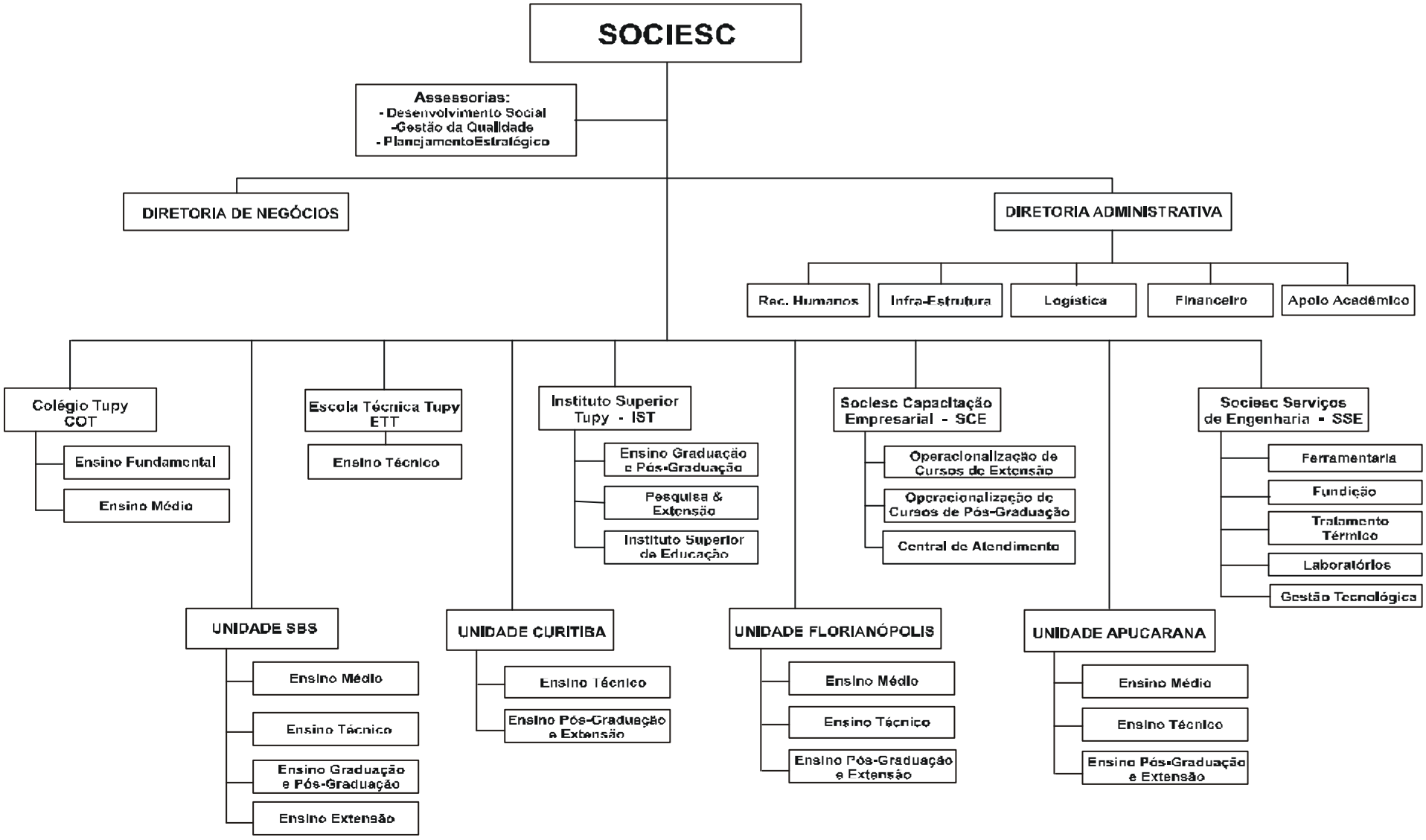
ANEXO V – TERMO DE RESPONSABILIDADE PARA UTILIZAÇÃO DE NOTEBOOK PARTICULAR

ANEXO VI – MODELO TERMO DE COMPROMISSO

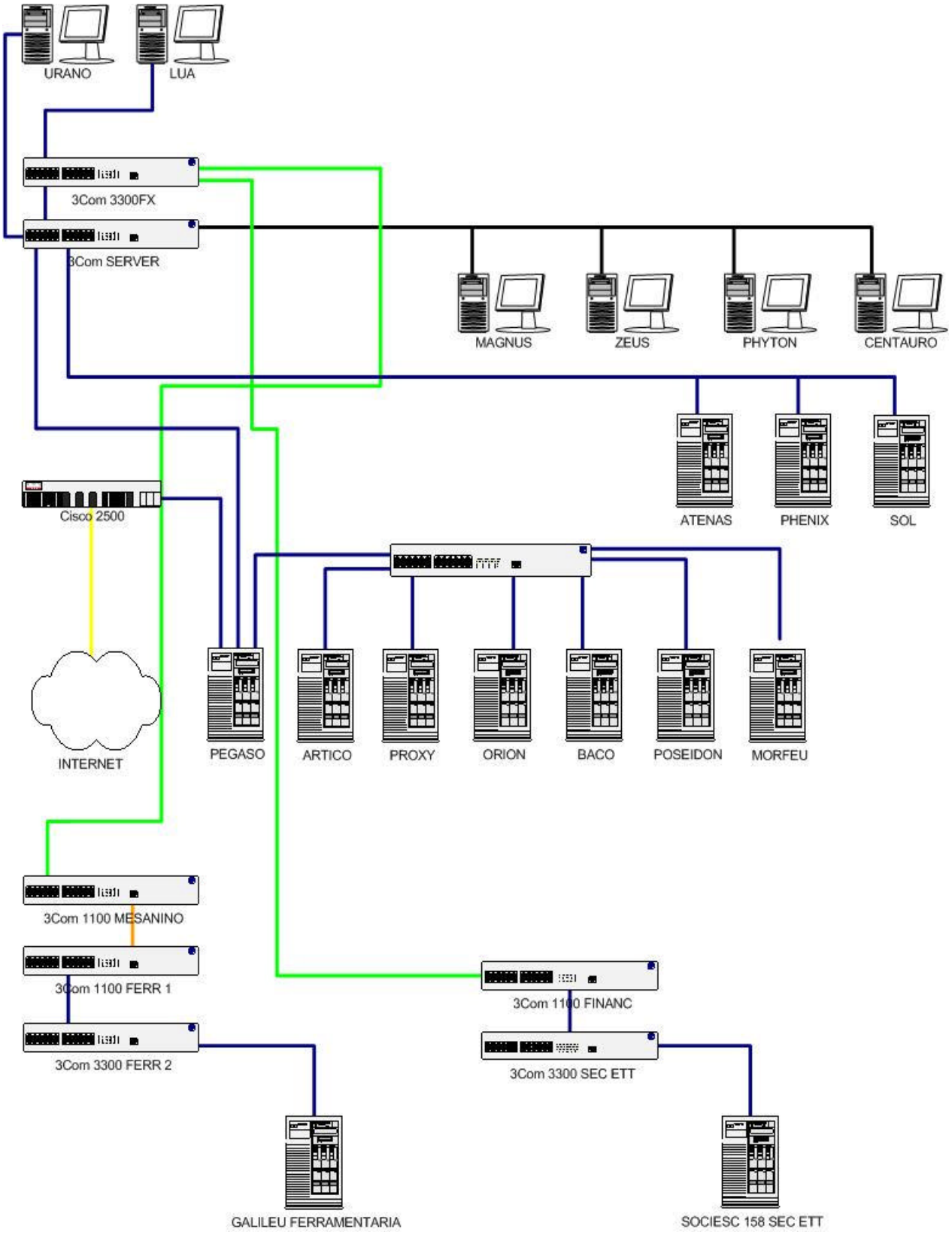
ANEXO VII – ARTIGO 482 DA CLT

ANEXO VIII – REGIMENTO ESCOLAR ALUNOS COT, ETT E IST.

Anexo I – ORGANOGRAMA SOCIESC



Anexo II – Servidores da SOCIEC – Unidade Joinville



Anexo III – Questionário sobre estrutura de informática da SOCIESC
- Questões sobre a SOCIESC unidade de Joinville

1) Qual a estrutura organizacional da equipe de informática da SOCIESC?

   1 coordenador de informatica
   1 administrador de rede (líder de equipe)
   2 analistas de suporte
   2 analistas de sistemas (sendo um líder de equipe)
   4 auxiliares de informática
   2 estagiarios

2) Qual o número de servidores da SOCIESC?

   18 em Joinville

3) Quem são os usuários dos recursos de informática? (acadêmicos, departamentos administrativos/professores)

   Alunos, professores e funcionários a fim.

4) Como é dividida a estrutura de informática (número de computadores, domínios) entre laboratórios de ensino e departamentos?
   São dois domínios, ensino e sociesc. O primeiro atendendo a rede ensino e o segundo a rede corporativa.
   Rede administrativa – aproximadamente 280 computadores
   Rede ensino – aproximadamente 550 computadores

5) Qual o número de computadores (estações de trabalho) da rede?

Dividida entre laboratórios de ensino e departamentos.
Rede administrativa – aproximadamente 280 computadores
Rede ensino – aproximadamente 550 computadores

6) É utilizado algum ERP? Qual?

   Sim. Logix

7) É utilizado algum sistema acadêmico? Qual?

   Sim. WAE

8) Qual o Banco de dados utilizado?

   Oracle

9) Como é feita a troca de informações entre as unidades?

Através de um link Frame-relay da Brasil telecom

10) Existe alguma política de segurança sendo utilizada?

Não existe nenhuma política definida

11) O que seria necessário abranger uma política de segurança para a realidade da SOCIESC ?

Seria interessante que uma Política de Segurança pudesse abranger uma política para senhas, política para uso dos laboratórios, de backup, de acesso. Como existem usuário diferenciados (alunos, funcionários e alunos colaboradores) é importante que as políticas possam abranger a todos os usuários.

- Outras unidades

11) Existe uma equipe de informática para cada unidade? Como é feita a manutenção dos computadores, servidores?

Em São bento do Sul e Ctba existe uma pessoa em cada para dar suporte a duvidas de usuários e realizar pequenas manutenções nos computadores.
A manutenção nos servidores é realizada remotamente via link de interligação e nos casos mais graves uma equipe é deslocada para solucionar o problema.

12) Qual a estrutura de informática das outras unidades (servidores, estações de trabalho, laboratórios de ensino)?

servidores
3 em São bento do Sul
2 em CTBA
6 em Florianopolis
2 em Apucarana

estações

120 computadores aproximadamente em SBS
50 computadores aproximadamente em CTBA
220 computadores aproximadamente em Floripa
20 computadores aproximadamente em Apucarana

Anexo IV – Diretrizes para uso de Notebook particular

SOCIESC	DIRETRIZES PARA USO DE NOTEBOOKS E PALM-TOPS PESSOAIS NA SOCIESC	DC 9008 **Rev. 01** **15/06/04**

Notebooks e palm-tops	- Fica autorizado o uso de notebooks e palm-tops pessoais, na rede computadores da SOCIESC. - A Sociesc tem o direito de periodicamente auditorar os notebooks utilizados na instituição, visando proteger suas informações bem como garantir que aplicativos ilegais não estejam sendo executados na instituição. - Casos de desrespeito às diretrizes deste DC serão encaminhadas à diretoria da SOCIESC para deliberação.
É de responsabilidade do proprietário	- A instalação do Sistema Operacional a ser utlizado no mesmo, bem como dos aplicativos a serem utilizados no notebook, salvo exceções de aplicativos específicos autorizados pela direção da unidade através da RQ 9029. - Manter sempre o aplicativo de antivírus atualizado em seu notebook. Caso não tenha nenhum aplicativo de antivírus instalado em seu notebook, o uso do mesmo fica proibido na instituição. - Usar somente aplicativos legalizados em seu notebook, de preferência que tenha sempre em mãos a nota fiscal e/ou licença de uso do aplicativo ou uma cópia autenticada do mesmo.
Acesso a rede	- A SOCIESC atualmente não considera o uso de notebooks e palm tops pessoais, como uma ameaça de risco à segurança da informação adotada na instituição. Portanto, deixa livre a possibilidade do uso de notebooks e palm tops pessoais no ambiente de rede da instituição. - Caso seja necessário conectar o notebook na rede da instituição, é necessário que o proprietário faça uma solicitação de serviços de infraestrutura, conforme PQ 9005 para que seja realizada uma verificação das configurações de rede e do aplicativo de anti-vírus instalado. - É responsabilidade do setor de Informática as configurações relativas aos dispositivos de rede e configurações de domínio no ambiente de rede da SOCIESC, que precisam ser realizadas para o funcionamento em rede dos notebooks.
Restrições	- Não podem ser executados nos notebooks, aplicativos de característica maliciosa, que visam comprometer ao funcionamento da rede, bem como a captura de informações confidenciais, como por exemplo: senhas de usuários. - Fica proibida a apropriação de arquivos que não seja de uso pessoal do proprietário do notebook. Todos os arquivos que sejam da instituição, não podem ser carregados nos notebooks, sem autorização da diretoria responsável pelos dados.

Anexo V – Termo de Responsabilidade para utilização de Notebook particular

TERMO DE RESPONSABILIDADES PARA NOTEBOOKS DE PARTICULAR

1. Do Objeto: O presente termo objetiva a cessão à _____ de utilização de notebooks na rede SOCIESC, em todos as suas unidades (campi).

2. Do Prazo: O presente instrumento vigorará imediatamente a partir da assinatura deste.

3. USUÁRIO ficará responsável por:

- Toda e qualquer manutenção/despesa que for necessária para o funcionamento do equipamento.
- Possuir um aplicativo Antivírus devidamente registrado e atualizado.
- Instalar apenas aplicativos com licença de livre distribuição, ou que o mesmo tenha adquirido a sua licença.
- Não copiar, reproduzir ou distribuir documentos, arquivos ou programas que forem de direito da Sociedade Educacional de Santa Catarina.
- Todo e qualquer prejuízos que, por sua culpa, na utilização do equipamento, vier causar à terceiros, durante o tempo de vigência deste TERMO.
- Respeitar as diretrizes descritas no DC 9008.

E assim, por estarem justos e contratados assinam o presente instrumento em 02 (duas) vias de igual forma e teor, na presença das testemunhas abaixo, para que surta seus jurídicos e legais efeitos.

Joinville(SC), ___ de _____ de 20___.

_____ Informática

_____ Nome do Usuário

Anexo VI – Modelo Termo de Compromisso

TERMO DE COMPROMISSO

Identificação do Empregado/Aluno

NOME:	
MATRÍCULA:	

Comprometo-me a:

1. Executar minhas tarefas de forma a cumprir com as orientações da Política de Segurança e com as Normas e Padrões vigentes.
2. Utilizar adequadamente os equipamentos da Instituição, evitando acessos indevidos aos ambientes computacionais aos quais estarei habilitado, que possam comprometer a segurança das informações.
3. Não revelar fora do âmbito profissional, fato ou informações de qualquer natureza que tenha conhecimento devido a minhas atribuições, salvo em decorrência de decisão competente do superior hierárquico.
4. Acessar as informações somente por necessidade de serviço e por determinação expressa do superior hierárquico.
5. Manter cautela quando a exibição de informações sigilosas e confidenciais, em tela, impressoras ou outros meios eletrônicos.
6. Não me ausentar do local de trabalho sem encerrar a sessão de uso do computador ou sistema, evitando assim o acesso por pessoas não autorizadas.
7. Observar rigorosamente os procedimentos de segurança estabelecidos quanto à confidencialidade de minha senha, através dos quais posso efetuar operações a mim designadas nos recursos computacionais que acesso, procedendo a:

a. Substituir a senha inicial gerada pelo sistema, por outra secreta, pessoal e intransferível;
b. Não divulgar a minha senha a outras pessoas;
c. Nunca escrever a minha senha, sempre memorizá-la;
d. De maneira alguma ou sobre qualquer pretexto, procurar descobrir as senhas de outras pessoas;
e. Somente utilizar o meu acesso para os fins designados e para os quais estiver devidamente autorizado, em razão de minhas funções;
f. Responder em todas as instâncias, pelas conseqüências das ações ou omissões de minha parte que possam por em risco ou comprometer a exclusividade de conhecimento da minha senha ou das transações a que tenho acesso;
g. Reportar imediatamente ao superior imediato ou ao Administrador de Segurança em caso de violação, acidental ou não, da minha senha, e providenciar a sua substituição.
h. Solicitar o cancelamento de minha senha quando não for mais de minha utilização.

Declaro estar ciente das determinações acima, compreendendo que quaisquer descumprimentos dessas regras podem implicar na aplicação das sansões disciplinares cabíveis.

Joinville, _____ de _____ de _____.

_____

Assinatura do Empregado/Aluno

Anexo VII – Artigo 482 da CLT

Art. 482. Constituem justa causa para rescisão do contrato de trabalho pelo empregador:

a) ato de improbidade;

b) incontinência de conduta ou mau procedimento;

c) negociação habitual por conta própria ou alheia sem permissão do empregador, e quando constituir ato de concorrência à empresa para a qual trabalha o empregado, ou for prejudicial ao serviço;

d) condenação criminal do empregado, passada em julgado, caso não tenha havido suspensão da execução da pena;

e) desídia no desempenho das respectivas funções;

f) embriaguez habitual ou em serviço;

g) violação de segredo da empresa;

h) ato de indisciplina ou de insubordinação;

i) abandono de emprego;

j) ato lesivo da honra ou da boa fama praticado no serviço contra qualquer pessoa, ou ofensas físicas, nas mesmas condições, salvo em caso de legítima-defesa, própria ou de outrem;

k) ato lesivo da honra ou da boa fama ou ofensas físicas praticadas contra o empregador e superiores hierárquicos, salvo em caso de legítima-defesa, própria ou de outrem;

l) prática constante de jogos de azar.

Parágrafo único. Constitui igualmente justa causa para dispensa de empregado, a prática, devidamente comprovada em inquérito administrativo, de atos atentatórios à segurança nacional.

Anexo VIII – Regimento Escolar

No guia acadêmico todos os itens referente a conduta do aluno, seus direitos, deveres, entre outros. Define-se, também, sobre o conselho de disciplina ou regime disciplinar, segue o modelo apresentado para os alunos do IST. Para alunos da ETT e COT, também existe o guia acadêmico.

TÍTULO IX - DO REGIME DISCIPLINAR

Art. 120 O Conselho de Disciplina será formado por:

I- Coordenação de Ensino;

II- Coordenador do Curso;

III- dois representantes do Corpo Docente; e

IV- um representante do Corpo Discente.

Art. 121 O Conselho de Disciplina tem por finalidade:

I- analisar casos de alunos, cujas transgressões infrinjam as normas regimentais; e

II- avaliar e aplicar corretivos disciplinares a alunos.

Art. 122 Caberá recurso das decisões do Conselho de Disciplina ao Conselho Deliberativo. As deliberações dessas primeira e segunda instância serão comunicadas à Secretaria e aos envolvidos.

Art. 123 *Entende-se por Corretivo:*

I- advertência oral ou escrita;

II- privação de atividades acadêmicas por tempo determinado;

III- realização de tarefas específicas isoladamente, ou em combinação com itens I ou II; e

IV- trancamento de matrícula, com entrega da transferência.

Art. 124 O infrator terá direito à defesa mediante exposição oral ou escrita, quando terá a oportunidade de esclarecer e justificar o seu envolvimento.

Art. 125 Outros casos disciplinares discentes não previstos neste título serão também analisados e avaliados pelo Conselho de Disciplina.

Parágrafo único. Detalhamentos do funcionamento do Conselho de Disciplina serão determinados pelo Conselho Deliberativo.

Art. 126 Aos funcionários e ao Corpo Docente serão aplicadas as seguintes penalidades, respeitadas as disposições legais:

I- advertência;

II- suspensão; e

III- demissão.

Art. 127 É de competência da Diretoria a aplicação das sanções previstas no artigo anterior.

Art. 128 São vedadas as sanções e penalidades que atentarem contra a dignidade da pessoa ou contra a saúde física e mental.

Art. 129 O regime disciplinar será decorrente das disposições legais aplicáveis a cada caso.