

**LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO DO RN
BACHARELADO EM SISTEMAS DE INFORMAÇÃO**

Andreza da Câmara Raposo

AUDITORIA DE SEGURANÇA NO AMBIENTE DE INFORMÁTICA
UM ESTUDO DE CASO NA FACULDADE NATALENSE PARA O
DESENVOLVIMENTO DO RIO GRANDE DO NORTE

**AUDITORIA DE SEGURANÇA NO AMBIENTE DE INFORMÁTICA
UM ESTUDO DE CASO NA FACULDADE NATALENSE PARA O
DESENVOLVIMENTO DO RIO GRANDE DO NORTE**

Monografia apresentada ao curso de
Bacharelado em Sistemas de
Informação da Faculdade Natalense
para o Desenvolvimento do RN como
requisito parcial para a obtenção do
título de

Andreza da Câmara Raposo

Orientador: Prof. Vísio Romão de Azevedo

**Natal
2002**

Natal
2002

LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO DO
RIO GRANDE DO NORTE

Andreza da Câmara Raposo

AUDITORIA DE SEGURANÇA NO AMBIENTE DE INFORMÁTICA
CASO NA FACULDADE NATALENSE PARA O DESENVOLVIMENTO DO RIO GRANDE DO NORTE



**AUDITORIA DE SEGURANÇA NO AMBIENTE DE INFORMÁTICA
UM ESTUDO DE CASO NA FACULDADE NATALENSE PARA O
DESENVOLVIMENTO DO RIO GRANDE DO NORTE**

Andreza da Câmara Raposo

Monografia apresentada e aprovada em 14 de março de 2002, para a obtenção do título de Bacharel em Sistemas de Informação da Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte.

Monografia apresentada ao curso de
Bacharelado em Sistemas de
Informação da Faculdade Natalense
para o Desenvolvimento do RN como
requisito parcial para a obtenção do
título em Bacharel em Sistemas de
Informação

Orientador: Prof. Ytalo Rosendo do Amaral

Natal
2002

RB-13.743 M



004.6.004.4

R167a

2002

Raposo, Andreza da Câmara

Auditoria de Segurança no Ambiente de Informática: Um Estudo de Caso na Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte/ Andreza da Câmara Raposo ____ Natal . FARN, 2002

xpx.

Monografia (BSI) – Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte.

1. Segurança de Dados-Monografia.

2. Auditoria de Segurança em Informática – monografia

I. Título

RN/FARN/BC

CDU-0046.004-4

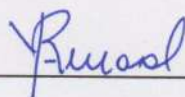
LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO DO
RIO GRANDE DO NORTE

DEDICATORIA

AUDITORIA DE SEGURANÇA NO AMBIENTE DE INFORMÁTICA UM ESTUDO DE
CASO NA FACULDADE NATALENSE PARA O DESENVOLVIMENTO DO RIO
GRANDE DO NORTE

Andreza da Câmara Raposo

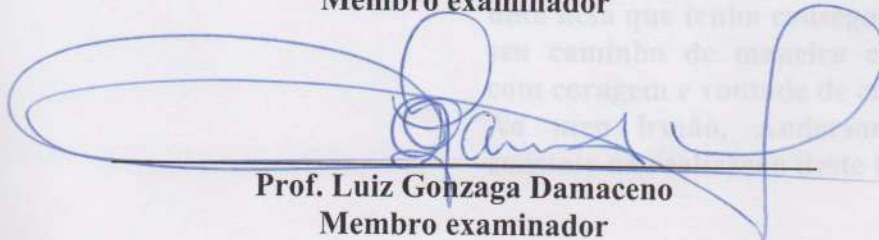
Monografia apresentada e aprovada em 14 de DEZEMBRO de 2002, pela banca
examinadora composta pelos seguintes membros



Ytalo Rosendo de Amaral
Orientador



Prof. Livia Maria Martins da Silva
Membro examinador



Prof. Luiz Gonzaga Damaceno
Membro examinador

Natal, 14 de 12 de 2002.

AGRADECIMENTOS

DEDICATORIA

Este trabalho foi concluído com o apoio de Patrícia Falcão Pessoa pelo seu carinho e atenção por ter proporcionado a mim a oportunidade especial de ter conseguido conteúdo suficiente para este trabalho a Sônia Gomes da Silveira de ter me deixado com uma pontinha de esperança que ia conseguir e também de ter falado palavras de conforto quando mais precisei da sua confiança. A dedicação e o carinho, amizade e a segurança que me passou por me estar acompanhando cada passo do meu trabalho de longe mas assim com a maior força e esta Prof. Luiz Genzaga Damasceno o obrigado e pouco por sua atenção especial pela sua ajuda que não vai lhe esquecer como pessoa e professor. Por isso, venho agradecer a todos com as mais sinceras palavras, esperando ter atingido os fins pretendidos neste empreendimento e atendido as expectativas de todos que contribuíram para sua construção.

Assim, agradeço a todos os meus professores, pelos ensinamentos ministrados e pela atenta confiança que me deram para este trabalho ser realizado.

Aos meus professores revisores e orientadores, em especial o Prof. Yvelo Fernando do Amaral, que incondicionalmente me distinguiu com sua atenção e soube perceber os erros e acertos deste trabalho, fazendo-o sempre melhor para melhorar cada vez mais.

A Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte, principalmente aos gestores de seus recursos, professores e funcionários é importante que me ofereçam para a realização e conclusão desta oportunidade de ter me dada atenção suficiente para este trabalho a ser realizado.

E a todos que, de alguma forma, contribuíram na elaboração deste trabalho.

Aos meus pais dedico este trabalho, como resultado do esforço e também do apoio que deles recebi em todos os projetos de minha vida.

Aos meus avós que sempre sonho de ter uma neta que tenha conseguido alcançar o seu caminho de maneira certa e dignar com coragem e vontade de crescer.

Ao meu irmão, Anderson pelo apoio constate na realização deste trabalho.

AGRADECIMENTOS

Este trabalho foi construído com o apoio de Patrícia Folcone Pessoa pelo seu carinho e atenção por ter proporcionar a minha pessoa uma atenção especial de ter conseguido conteúdo suficiente para este trabalho a Stenio Gomes da Silveira de ter me deixado com uma pontinha de esperança que ia conseguir e também de ter falado palavras de consolo quando mais precisei da alta confiança. A dedicação e o carinho, amizade e a segurança que me passou por ter estado acompanhando cada passo do meu trabalho de longe mais assim com a maior força o meu Prof. Luiz Gonzaga Damaceno o obrigado e pouco por sua atenção especial pela sua aluna que não vai lhe esquecer como pessoa e professor. Por isso, venho agradecer a todos com as mais sinceras palavras, esperando ter atingido os fins pretendidos neste empenho conjunto e atendido as expectativas de todos que contribuíram para sua construção.

Assim, agradeço a todos os meus professores, pelos ensinamentos ministrados e pelo estímulo confiança que me deram para este trabalho ser realizado.

Aos meus professores revisores e orientadores, em especial o Prof. Ytalo Rosendo do Amaral, que incondicionalmente me distinguiu com sua atenção e soube perceber os erros e acertos deste trabalho, fazendo-o sempre melhor para melhorar cada vez mais.

A Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte, particularmente nas pessoas de seus diretores, professores e funcionários é suporte que me ofereceram para a realização e conclusão desta oportunidade de ter me dada atenção suficiente para este trabalho a ser realizado.

E a todos que, de alguma forma, contribuíram na elaboração deste trabalho.

ABSTRACT

The evolution of the security has facilitated extraordinary to the security ambient and people in the entire world. In this context, the greatest concern started to resurge in this

RESUMO

A evolução da segurança tem facilitado extraordinariamente a segurança das empresas e pessoas no mundo inteiro, entretanto uma grande preocupação começou a ressurgir nesse ambiente: a segurança da informação. Esse é um dos mais comentados nos meios de tecnologia da informação atualmente, e consciência da sua importância, foi proposta com a pesquisa a ser desenvolvida na instituição que será supervisionado na medida para melhoria da segurança no ambiente computacional da empresa. Ao longo da pesquisa serão apresentadas as principais técnicas de ataques e ameaças existentes com base na ISO17799.

ABSTRATC

The evolution of the security has facilitated extraordinary to the security ambient and people in the entired world, however a great concern started to resurge in this ambient: the most commented security of information. The one of in the ways of technology of the information currently, and conscience of its importance, was considered with the research to be develop in the institution that supervise measure for improvement of the security in the coputacional environment of winipress. The soon of search will be presented the main technic of attacks and threat existing with the base in the ISO1 7799.

SUMÁRIO

1- INTRODUÇÃO.....	8
2- PROBLEMA DE PESQUISA	9
2.1- Referencial Teórico.....	10
2.1.1- Histórico da Segurança.....	11
2.2- Princípios da Segurança da Informação	11
2.3- Criptografia.....	12
2.4- Considerações sobre criptografia	12
2.5 –Técnica de Ataques e Ameaças.....	13
2.5.1-Plano de Incidentes.....	13
2.5.2- Incidentes de Segurança da Informação	13
2.6- Vírus	16
2.7- Auditoria de Segurança.....	16
2.8 – Definições de Segurança.....	17
2.8.1-Informação.....	17
2.9 – ISO 1779.....	18
2.9.1 – Quais as principais acessões da ISO17799.....	18
2.9.2-Certificações.....	22
3-ANÁLISE.....	23
4 – CONCLUSÃO	26
ANEXO.....	27
BIBLIOGRAFIA.....	28

1. INTRODUÇÃO

Este trabalho fará um estudo na Liga de Ensino do Rio Grande do Norte mais precisamente, Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte, através de uma auditoria de segurança no processo informatizado do vestibular para saber como ocorre a segurança dos dados do vestibular, ou seja, a inscrição, as correções das provas, bem como os resultados finais e as listagens dos candidatos aprovados no concurso.

Para ter boa reputação e ser bem aceito, um sistema de seleção para vagas no ensino superior precisa de alta imparcialidade. Isto é, a seleção de qualidade precisa ter transparência em suas regras e promover a máxima equidade no julgamento.

Antes da era da segurança a informática tinha pouca importância nas empresas. A tecnologia da informação atuava na retaguarda ou na melhoria de processos, mas muito dificilmente era um elemento de segurança. Hoje as empresas dependem cada vez mais da segurança da informação para o seu funcionamento, ela automatiza e ao mesmo tempo agrega seguro aos processos organizacionais. A segurança é grande e está cada vez mais sendo utilizada de forma constante.

O ataque e invasões acontecem a todo instante, as suas conseqüências cobrem uma enorme gama de possibilidade de perda de tempo, quem está seguro?

O termo hacker, que há cinco anos atrás era praticamente desconhecido, atualmente é assunto em qualquer conversa.

O objetivo deste trabalho é levantar informações sobre a segurança do sistema do vestibular da FARN. Com isso será realizado um levantamento bibliográfico do procedimento de segurança.

As etapas a serem realizado neste projeto são as seguintes:

- Elaboração de um checklist de normas de segurança .
- Aplicação do checklist nos procedimentos do sistema de correção das provas do vestibular da FARN.

A metodologia de uma pesquisa qualitativa e descritiva. Qualitativa simplesmente por não usar dados numéricos. Descritiva por analisar, classificar, explicar e interpretar os casos pesquisados sem interferir ou questionar os resultados obtidos.

A pesquisa será realizada em três etapas (pesquisa bibliográfica, estudo de caso, analisar e por fim os resultados).

Estudo de caso tem servido para estudar o funcionamento de uma instituição e determinar focos de mudança ou de intervenção.

Na pesquisa bibliográfica será realizada uma revisão teórica sobre livros, periódicos e artigos, de todos os termos e conceitos importantes referente à monografia.

2. PROBLEMA DE PESQUISA

Na sociedade da informação, ao mesmo tempo em que as informações são consideradas o principal patrimônio de uma organização, as informações estão sob constante risco, como nunca estiveram antes. Com isso, a sua segurança de informações tornou-se um ponto crucial para a sobrevivência das instituições.

Um erro nos sistemas informatizados pode comprometer instituições do mercado financeiro, indústrias, sistema de telecomunicações, de assistência médica, entre outros. Enfim, pode afetar a sociedade de inúmeras maneiras, tamanha a dependência dos equipamentos e sistemas computadorizados. O que aconteceria se as informações institucionais caíssem nas mãos da concorrência, fossem apagadas ou adulteradas? Quais seriam as conseqüências para a continuidade dos negócios da instituição? O vazamento de informações sobre seus clientes comprometeria sua credibilidade e daria maiores oportunidades aos concorrentes.

Nunca foi tão fácil atacar os sistemas informatizados, já que os sistemas de informações institucionais conectados em redes externas aumentam significativamente os riscos de segurança e muitas das ferramentas de ataque, utilizadas antigamente apenas por agências de inteligência, hoje estão disponíveis a qualquer pessoa.

Os departamentos de informática, por sua vez, esperam que seus sistemas sejam eficientes, atendam as necessidades dos usuários e estejam protegidos contra qualquer ameaça que possa comprometer seu funcionamento. A segurança também está relacionada com teste de hardware, software e prevenção de erros cometidos pelos usuários.

Outro aspecto a ser considerado pela gerência é que os sistemas de informática, para operarem de forma adequada e garantirem a segurança das informações da organização, necessitam de ambientes controlados, protegidos contra desastres naturais (incêndio, terremoto, enchente), falhas estruturais (interrupção do fornecimento de energia elétrica, sobrecargas elétricas), sabotagem, fraudes, acessos não autorizados (hackers, espionagem industrial, venda de informações confidenciais).

2.1- Referencial Teórico

De acordo com Dias (1999, p.42), o conceito de Sistema de Segurança Auditoria é:

“A segurança de informações, a primeira idéia que nos vem a mente a proteção das informações, não importando onde estejam (no papel , na memória do computador) conceitualmente , um computador ou sistema computacional é considerado seguro se houver uma garantia de que capaz de atuar exatamente como é esperado”.

O sistema de segurança de auditoria faz parte de novas técnicas de informações que esta surgindo no mercado da grande empresa.

Gil (1999, p 150) explica que:

“A segurança diz respeito à modificação inadequada dos recursos tecnologia, informação e software a confiabilidade diz respeito à captação endivida desce mesmo recursos tecnológicos. Para a manutenção da segurança confidencialidade necessitamos validar e avaliar controles lógicos inseridos, bem como para proteger informações e programas”.

Segundo estudos realizado por Garther, Wirelles e Robil Simpson com o uso corporativo de Personal Digital Assistente (PDAS) pode apresentar uma ameaça a segurança de dados armazenados na redes de computadores. (MODULO,2002)

“De acordo com o diretor de consultoria Wirelles do Garther , Robil Simpson, as ferramentas para prover segurança nesses casos estão demorando muito para serem adotado. Simpson também acredita os departamento TI precisam encorajar os demais funcionários a adotar medidas de segurança quando estão usando aparelho moves “ senha e números de identificação pessoal precisam ser usados”.

Segundo Alberto Bastos os novos rumos da gestão de segurança com as normas ISO 17799 e BS7799 e uma estratégia de segurança baseada na ISO 17799 tem a segurança da informação que esta se tornando um diferencial competitivo nas grandes empresas.

Novos rumos da gestão

“O objetivo da norma é fornecer recomendações para gestão da segurança da informação para o uso por aqueles que são responsáveis pela introdução, implementação ou manutenção da segurança em suas empresas. A ISO 17799 estabelece uma base comum para o desenvolvimento de normas de segurança organizacional e das praticas efetivas da gestão da segurança organizacional e das praticas efetivas da gestão da segurança , facilitando o benchmark dos processos e provendo confiança nos relacionamentos entre as organizações.”

2.1.1- Histórico da Segurança

Ao longo da história, desde a mais remota antiguidade, o ser humano vem buscando controlar as informações que julga importante. Conforme [Scheneier (2001)], na antiga China a própria linguagem escrita era usada como uma forma de criptografia na medida em que somente as classes superiores podiam aprender a ler e a escrever. Outros povos, como os egípcios e os romanos deixaram registrados na história sua preocupação com o trato de certas informações, especialmente as de valor estratégico e comercial. Com a Segunda Guerra Mundial, a questão da segurança ganhou uma nova dimensão, na medida em que sistemas automáticos e eletromecânicos foram criados tanto para criptografar como para efetuar a criptoanálise e quebrar a codificação (SCHNEIER,2001)

Quando falamos em segurança da informação, a primeira idéia que nos vem a mente é a proteção das informações, não importando onde estejam (no papel ou na memória do computador) conceitualmente, um computador ou sistema computacional e considerando seguro se houver uma garantia de que ele é capaz de atuar exatamente como o esperado (DIAS 1999).

2.2 Princípios da Segurança da Informação

A segurança da informação busca reduzir os riscos de vazamentos, fraudes, erros, uso indevido, sabotagens, paralisações, roubo de informações ou qualquer outra ameaça que possa prejudicar os sistemas de informação ou equipamentos de um indivíduo ou organização.

Segundo PUTTINI (2001: web), uma solução de segurança adequada deve satisfazer os seguintes princípios:

- **Confiabilidade:** significa proteger informações contra sua revelação para alguém que não-autorizado. Consiste em proteger a informação contra leitura ou cópia por alguém que não tenha sido explicitamente autorizado pelo proprietário daquela informação.
- **Autenticidade:** o controle de autenticidade está associada com identificação correta 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.
- **Integridade:** a integridade consiste em proteger a informação contra modificação sem a permissão explícita do proprietário daquela informação. A modificação inclui ações como escrita, alteração de conteúdo, alteração de status, remoção e criação de informação.

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

2.3 Criptografia

A criptografia vem, na sua origem, da fusão de duas palavras gregas:

- CRIPTO= ocultar, esconder
- GRAFIA= escrever

Criptografia é arte ou ciência de escrever em cifra ou código. É então um conjunto de técnicas que tornam uma mensagem incompreensível permitindo apenas que o destinatário que conheça a chave de encriptação possa a descrever e ler a mensagem com clareza.

2.4 Consideração sobre Criptografia

Muitas vezes a criptografia é considerada como sinônimo de segurança. A criptografia é necessária, mas não suficiente, para uma segurança forte. Na Internet, as maiorias das criptografias são utilizadas em aplicações como e-mail e software de navegação. Contudo, ataques comuns ao sistema operacional podem superar as aplicações de criptografia e mesmo a autenticação do sistema operacional.

2.5 Técnicas de Ataques e Ameaças

Para se garantir a proteção de uma rede ou sistema é importante conhecer as ameaças e técnicas de ataques utilizadas pelos invasores, para então aplicar as medidas e ferramentas necessárias para proteção desses recursos.

Sem o conhecimento desses fatores, toda a aplicação de mecanismos de proteção pode ser anulada, pois se existir algum ponto vulnerável ou protegido de maneira incorreta todo sistema estará comprometido.

Dessa maneira, esta seção busca identificar as principais ameaças e técnicas de ataques contra a segurança da informação.

2.5.1 – Plano de Resposta a Incidentes

Mesmo a melhor infraestrutura de segurança da informação não pode garantir que intrusos ou outras ações maliciosas ocorram. Quando um incidente de segurança ocorre, e um

fator crítico para organização ter maior para responder a esse evento. A velocidade a qual uma organização pode reconhecer, analisar, e responder a um incidente de segurança limita os estragos e diminui os custos de restauração. A habilidade de usar essa informação para preparar ou prevenir ocorrências similares aprimora a segurança geral de uma organização.

O Plano de resposta a incidentes é um documento que descreve as diretrizes gerais e procedimentos para tratamento dos principais incidentes de segurança que podem ocorrer na organização, promovendo ao pessoal de suporte instruções sobre as medidas a serem tomadas para a identificação e correção dos mesmos.

O tipo de tratamento dado aos incidentes de segurança varia de acordo com a sua intensidade e risco. Porém, o encaminhamento deve ser decidido em acordo com a alta direção da empresa e com o respaldo do departamento jurídico.

2.5.2 Incidentes de Segurança da Informação

Justiça indícia hacker de DVD. (IDG NOW)

Um adolescente norueguês que se transformou em herói por ter quebrado o código de segurança de filmes em DVD, foi indiciado pela justiça de seus país segundo. Jon Lech Johansen tinha 15 anos quando escreveu e distribuiu o programa DeCSS, no final de 1999, que permitia violar a segurança dessas mídias.

Agora, com 18 anos, o rapaz, apelidado de DVD-Jon, se transformou em um ídolo no underground. Após dois anos de investigação a justiça decidiu levá-lo a corte em um caso que colocara em xeque as novas leis de crimes de computação implementadas na Noruega.

No processo, a Motion Picture Association of América, que representa os maiores estúdios de Hollywood, acusa o jovem de ter invadido sua propriedade e deixado vulnerável para um futuro roubo. Se condenado Johansen poderá vir a pegar dois anos de prisão.

O programa criado por ele permitiu que se copiasse filmes em DVD em um computador e até mesmo transmiti-los baixados da web. Tal infração poderia custar milhões de dólares em prejuízos anuais a indústria cinematográfica.

Uma guerra contra o crime digital (JT Web)

Há uma guerra sendo travada no ciberespaço contra o crime digital. Desde 1995, agências federais do governo americano estão tentando deter o exército de hackers, espiões e terroristas que podem tornar a internet insegura para a democracia.

Esse medo tem fundamento, já que nenhuma parte do mundo industrializada está a salvo do desastre digital. Estão sendo realizados freqüentemente ataques bem-sucedidos as usinas de energia elétricas, bancos e fabricas entre outros.

O negócio não é brincadeira. Exemplos de ameaças não faltam.

Em fevereiro, um hacker israelense de 19 anos, conhecido como Amalyzer, e dois adolescentes da Califórnia penetraram nos computadores do Departamento de Defesa dos Estados Unidos, levando o terror de que essa invasão estava relacionada com o aeroporto pela interpol.

Em 1994, o hacker russo Vladimir Levir entrou nos sistemas do Citibank e roubou US\$ 12 milhões. Ele ficou foragido durante um ano. Até ir a Londres e ser preso no aeroporto pela interpol.

Britânico acusado de invadir rede do Pentágono (TERRA)

WASHINGTON -As autoridades federais americanas acusaram formalmente na noite da última terça-feira um administrador de computadores britânicos de ter invadido 92 redes de computadores operadas pelas Forças Armadas Americanas e pela Nasa. Um ataque que teria tirado do ar os computadores de uma instalação naval de Nova Jersey, imediatamente depois dos ataques de 11 de setembro. Segundo as autoridades, dois dos sistemas atacados pelo hacker ficavam no Pentágono. As invasões também teriam desativado temporariamente a rede que serve ao Distrito Militar de Washington. As autoridades apresentaram indiciamentos nos sistemas judiciais de Virginia e Nova Jersey contra o hacker, chamado Gary Ckinnon. Ele tem 36 anos, vive na região londrina de Horsey e foi indiciado por oito acusações de crime eletrônico, incluindo a invasão de seis redes pertencentes a empresas privadas. De acordo com os documentos entregues a justiça em Virginia, McKinnon teria causado US\$ 900 mil em danos a computadores localizados em 14 estados americanos. Em a Nova Jersey, o hacker foi acusado de entrar em uma rede de 300 computadores da estação naval de armas Earle, em

Colts Neck, tendo roubado 950 senhas de acesso. Divido invasão, ocorrida imediatamente depois dos ataques de 11 de setembro, a rede ficou fora do ar por cerca de uma semana, disseram os oficiais. O local fornece munição e suprimentos para reabastecer a frota do atlântico da marinha americana.

"Esta foi uma invasão grave a uma rede vital das forças armadas em um momento no qual nossa nação precisava convocar todas as suas defesas para um possível novo ataque", disse o promotor americano Christopher J. Christie.

Se McKinnon for considerado culpado, deve passar no máximo cinco anos na prisão. Ele poderá ser obrigado a pagar uma multa de US\$250 mil, acrescentou Christie. Segundo confirmou Christie, em um pronunciamento terça-feira, o governo americano avalia a possibilidade de pedir a extradição do hacker, uma medida rara em casos de crime digital.

Cibercrimes (UOL)

A polícia de Mato Grosso do Sul descobriu que o hacker Guilherme Amorim de Oliveiras tem R\$ 3 milhões em uma conta bancária. Além desviar dinheiro de vários bancos brasileiros, o estudante de 18 anos tinha milhares de senhas de cartões de crédito de clientes dos Estados Unidos. E maior golpe financeiro pela Internet já descoberto no Brasil. Guilherme foi preso em flagrante num hotel de Campo Grande quando desviava R\$25 mil de uma conta bancária, mas foi libertado, na semana passada, por ordem judicial. A polícia comprovou o desvio de R\$120 mil pela internet de 50 contas de um grande banco brasileiro, em vários estados. Outros três bancos teriam sido vítimas da quadrilha. O laudo pericial tem 219 páginas. No computador apreendido com o adolescente está lacrado, mas a polícia, computador do estudante os peritos encontraram dados cadastrais e senhas de 3.500 clientes de crédito, também encontrou conversas virtuais envolvendo lavagem de dinheiro e compras de armas. O perito da polícia técnica Maurílio Rodrigues Ferreira diz estar assustado com o caso. Cópias da perícia vão ser encaminhadas para a Polícia Federal, o serviço de inteligência do governo e também para a Polícia Norte-Americana (FBI). Há suspeita de que Guilherme tenha invadido pela Internet sistemas de acesso restrito nos Estados Unidos. "Segundo a Polícia Norte-Americana, já estavam rastreando um hacker aqui no Brasil com o mesmo operante, porém não conseguiam detectar essa pessoa", conta o delegado Reinaldo Amaral Filho. A federação dos Bancos diz que a pessoa que teve sua conta "invadida" tem como única solução procurar a agência bancária, e pedir providências.

As informações são do site do Jornal Hoje. Rede globo de televisão (10/07/2002).

2.6 Vírus

“Provavelmente o tipo de quebra de segurança mais conhecida popularmente é o vírus”ED. CONSULTORIA(2001:web)

Os vírus são programas espúrios inseridos em computadores contra vontade do usuário e desempenham funções indesejadas. Alguns vírus têm a capacidade de se reproduzir e infectar outros dispositivos por toda a rede, já outros não se reproduzem, mas são distribuídos em falsos programas na rede ou em CDs vendidos em publicações.

A cada dia surgem centenas de vírus e o combater a esse tipo de invasão é uma tarefa constante. As principais contra-medidas são a instalação de programas antivírus atualizados em todos as estações de trabalho e servidores. É recomendável deixar programas antivírus residentes na memória para proteção em tempo real

2.7 Auditoria de Segurança

A auditoria é uma atividade relativamente nova no Brasil, ainda no estágio embrionário em termos técnicas, haja visto que legislação específica brasileira vêm abordando superficialmente o assunto, sem definir de forma clara e precisa os procedimentos que os profissionais da área deveriam adotar por ocasião das auditorias das demonstrações financeiras.

Auditoria da tecnologia da informação abrange ainda controles que podem influenciar a segurança de informação e o bom funcionamento dos sistemas de toda a organização.

Auditoria da segurança de informação determina a postura da organização com relação à segurança. Avalia a política de segurança e os controles relacionados com aspectos de segurança institucional mais globais. Na verdade, a auditoria de segurança de informações faz parte da auditoria da tecnologia da informação.

A auditoria da segurança está atenta em verificar se o dia a dia de operação do ambiente de segurança está em alinhamento com a informação da política de segurança. A política de segurança deve ser a base da auditoria. Este é o padrão ao qual as configurações estão ponderadas. Sem uma política de segurança compreensiva não se consegue medir se estar se conseguindo alcançar a meta de manter um ambiente seguro. Informações sobre políticas de segurança variam de site para site, mas a alguns que não tem uma política escrita

por inteiro. Se já tem uma política de segurança então a auditoria irá verificar se as ações feitas vão de acordo com a política de segurança.

2.8 – Definições de Segurança:

2.8.1 Informação:

Segundo o AURELIO(1995), informação é dado acerca de alguém ou algo do conhecimento e segundo a teoria da informação, a medida da redução da incerteza.

Segurança da Informação conforme definido pela ISO/IEC 17799:2000, é a proteção contra um grande número de ameaças às informações, de forma a assegurar a continuidade do negócio, minimizando danos comerciais e maximizando o retorno de investimentos e oportunidades. A segurança da informação é caracterizada pela preservação dos seguintes atributos básicos:

a) **Confidencialidade:** São riscos produzidos por pessoas que tem acesso a documentos, sistemas de informações ou ambientes de processamento. Tais riscos diminuem com o emprego de funcionários de confiança evitando que pessoas não autorizadas possam ter acesso aos equipamentos.

b) **Integridade:** Precisão e validade. Acontece quando o empregado ou contratado não processa toda a informação, isto é o faz de um modo incompleto. Para minimizar esse risco, deve-se cuidar para que as informações críticas não possam ser apagadas ou falsificadas.

c) **Disponibilidade:** garantia de que os usuários autorizados tenham acesso à informação e aos recursos associados, quando necessário.

2.9 - ISO 17799(www.modulo.com.br)

A ISO 17799 é bem abrangente, pretendendo contemplar todos os aspectos da segurança da informação. Nesse sentido, divide-se em 9 capítulos ou partes, cada qual abordando um aspecto da segurança da informação. A Norma Brasileira segue a mesma estrutura de capítulos, itens e controles. Os capítulos que compõem a norma são os seguintes:

- 1- Política de Segurança
- 2- Segurança Organizacional
- 3- Classificação e Controle dos Ativos de Informação
- 4- Segurança em Pessoas
- 5- Segurança Ambiental e Física
- 6- Gerenciamento das Operações e Comunicações

7- Controle de Acesso

8- Desenvolvimento de Sistemas e Manutenção

9- Conformidade

2.9.1 - Quais as principais sessões da ISO17799(www.modulo.com.br)

A ISO17799 é baseada na manutenção da integridade, disponibilidade e confidencialidade das informações (consideradas como bens). Para garantir essas premissas, a ISO17799 é subdividida em 10 sessões principais que identificam o sucesso da implementação de um programa de segurança da informação. Essas 10 sessões são ainda expandidas em controles mais detalhados, totalizando 127 controles. Abaixo um resumo das 10 sessões da ISO17799 para avaliação e conhecimento:

1) Política de Segurança

Os objetivos dessa sessão são:

Prover diretrizes, gerência e suporte a política de segurança da empresa;

- 1.1) Política de segurança da informação;
- 1.2) Revisões e avaliações periódicas do processo como um todo;
- 1.3) Modernização constante das políticas adotadas;

2) Segurança da Organização

Os objetivos dessa sessão são:

- 2.1) Ter total segurança nas instalações físicas da empresa;
- 2.2) Manter a segurança organizacional mesmo quando o acesso aos recursos de processamento de informações for realizado por outras empresas;
- 2.3) Fiscalizar o acesso do corpo funcional em horário inadequados, entre outros;

3) Classificação e Controle de Bens

Os objetivos dessa sessão são:

- 3.1) Manter proteção apropriada ao patrimônio físico da empresa;
- 3.2) Garantir que os patrimônios em forma de informação recebam níveis adequados de proteção.

4) Segurança de Pessoal

Os objetivos dessa sessão são:

- 4.1) Reduzir as chances de erros humanos, roubos, fraudes ou mau uso das facilidades disponibilizadas pela empresa;
- 4.2) Assegurar que os usuários conheçam as ameaças de segurança e estejam preparados para contribuir com a política de segurança da informação durante o curso normal de trabalho;
- 4.3) Minimizar o risco de incidentes e criar mecanismos de aprendizado com os incidentes já registrados;
- 4.2) Definição de segurança no trabalho e resourcing;
- 4.3) Segurança e responsabilidade de trabalho;
- 4.4) Política de pessoal;
- 4.5) Acordos de confidencialidade;
- 4.6) Condições de emprego;
- 4.7) Treinamento de usuários;
- 4.8) Educação para segurança da informação;
- 4.9) Resposta a incidentes de segurança e maus funcionamentos;
- 4.10) Informação quanto aos incidentes de segurança;

5) Segurança Física e Ambiental

Os objetivos dessa sessão são:

- 5.1) Combater acesso não autorizado às dependências da empresa;
- 5.2) Prevenir perdas, danos ou quaisquer comprometimentos ao patrimônio da empresa que possa causar interrupção em sua atividade;
- 5.3) Prevenir quanto a retirada de informação não autorizadas e remoção de dispositivos que armazenam esses dados;
- 5.4) Prevenção de falhas de alimentação elétrica (uso de no-breaks ou geradores de energia);
- 5.5) Prevenção de catástrofes naturais de diversos tipos;
- 5.6) Prevenção eventos premeditados;
- 5.7) Ambientes seguros onde estão localizados as máquinas;
- 5.8) Segurança quanto ao armazenamento dos dados;
- 5.9) Instalações adequadas para os ambientes de trabalhos;
- 5.10) Deslocamento dos equipamentos entre setores de forma segura;

6) Gerenciamento da Operação dos Computadores e Comunicações

Os objetivos dessa sessão são:

- 6.1) Assegurar a correta utilização e operação dos recursos de processamento da informação disponibilizados pela empresa;
- 6.2) Minimizar os riscos de falhas no sistema;
- 6.3) Proteger a integridade da informação e do software que está sendo operado;
- 6.4) Manter a integridade e a disponibilidade do ambiente de processamento e de comunicações;
- 6.5) Garantir a guarda correta de informações nas redes e dispositivos de armazenamento;
- 6.6) Prevenir danos que possam causar a paralisação de serviços da empresa;
- 6.7) Prevenir qualquer tipo de dano, modificação ou mau uso de informações trocadas entre organizações.

7) Controle de Acesso ao Sistema

Os objetivos dessa sessão são:

- 7.1) Controlar o acesso à informação;
- 7.2) Prevenir os funcionários dos usuários quanto ao acesso não autorizado aos sistemas de informação;
- 7.3) Prover segurança e proteção dos disponibilizados pela rede de computadores;
- 7.4) Detectar atividades não autorizadas através de auditorias periódicas;
- 7.5) Infra-estrutura administração e coordenação da segurança de informação;
- 7.6) Atribuição de responsabilidade aos usuários quanto a segurança da informação;
- 7.7) Controle das atribuições e permissões dos técnicos;
- 7.8) Consultoria de especialista em segurança da informação;
- 7.9) Cooperação entre organizações;
- 7.10) Avaliações constantes dos dados, levando em consideração a confiabilidade das informações e, conseqüentemente, a sua segurança;
- 7.11) Segurança de acesso aos dados por terceiros deverá haver uma política bastante definida para esse pessoal;

8) Desenvolvimento e Manutenção de Sistemas

Os objetivos dessa sessão são:

- 8.1) Garantir que a segurança é parte essencial para os sistemas de informação;
- 8.2) Prevenir perdas, alterações não autorizadas ou mau uso de dados do sistema de informação através dos usuários não-autorizados;

- 8.3) Proteger a autenticidade, confidencialidade e integridade da informação;
- 8.4) Garantir que atividades de suporte projetos de TI (Tecnologia da Informação) sejam conduzidos de forma segura;
- 8.5) Sempre manter a segurança das aplicações e dos dados.
- 8.6) Exigências de segurança dos sistemas;
- 8.7) Analise dos exigências de segurança e especificação dos dados;
- 8.8) Segurança dos aplicativos;
- 8.9) Validação dos dados;
- 8.10) Controle de processo interno;
- 8.11) Mensagem autenticada;
- 8.12) Criptografia;
- 8.13) Política de utilização de controles de criptografia;
- 8.14) Segurança dos arquivos que compõem o sistema;
- 8.15) Gerenciamento e controle do Sistema Operacional;
- 8.16) Proteção das informações quando estiver na fase de teste;
- 8.17) Desenvolvimento de software dentro da própria empresa;
- 8.18) Avaliação da necessidade de alteração de sistema a melhoria do funcionamento dos sistemas;

9) Conformidade

Os objetivos dessa sessão são:

- 9.1) Evitar que sejam desconsiderados quesitos legais que possam vir prejudicar civil ou criminalmente a empresa sob o foco estatutário, regulatório ou contratual;
- 9.2) Certificar-se de que existe coerência entre os sistemas com a política de segurança adotada;
- 9.3) Maximizar os processos de auditoria, reduzindo suas interferências.
- 9.4) Conformidade com exigências legais;
- 9.5) Identificação de legislação aplicável;
- 9.6) Registro de propriedade intelectual;
- 9.7) Proteção de registros organizacionais;
- 9.8) Proteção dos dados e isolamento das informações pessoais;
- 9.9) Prevenção contra abuso no uso da informação nas instalações da empresa, ou seja, executar tarefas pessoas no ambiente de trabalho;
- 9.10) Regulamento de controles criptográficos;

2.9.2 Certificações

A Modelo Security Solutions (24/09/2002), empresa brasileira líder em segurança da informação acaba de conquistar a certificação internacional de segurança BS7799, considerada o padrão mais completo do mundo para o gerenciamento de segurança da informação. O processo foi conduzido por auditores internacionais independentes da DNV Det Norske Veritas. Quando uma empresa certifica seu sistema de Gestão de segurança da informação, está reforçando ao mercado seu compromisso com a implementação de controle e sua preocupação com a produção das informações de seu cliente, afirmou Alberto Bastos, sócio-fundador e diretor de tecnologia da Modulo. Em todo o mundo, só existem 141 empresas certificadas até o momento, demonstrando nosso pioneirismo em conquistar esta certificação.

São realizadas cópias diárias e semanais, sendo que as cópias semanais são geradas com duplicidade.

Uma cópia fica disponível na própria instituição e a outra cópia é guardada no cofre. Dessa maneira essa cópia reserva fica protegida contra desastres naturais, roubo ou qualquer outro incidente físico que possa ocorrer na empresa.

As cópias são a forma de controle de acesso aos recursos de um sistema ou uma rede. Entre tanto, se elas forem utilizadas constantemente, podem deixar um sistema ou uma rede ainda mais vulnerável.

Sendo assim, foi necessário que alguns procedimentos referentes à escolha e utilização das cópias fossem reformulados na empresa.

Na segurança física os servidores estavam agrupados em uma sala onde ainda não havia controle, onde só pode entrar pessoas autorizadas como administrador de sistema e gerente do CPD. Além disso, para garantir a segurança física dos equipamentos contra fogo, foi instalado mais um ponto de alarme nesse local.

Com base na segurança da ISO17799 foi realizado comparação de segurança nas instituições.

Nas instituições serão somente registrados os 09 itens que abrangem a ISO.

Política de Segurança

o Revisões de avaliação periódicas do processo de segurança;

3. ANALISE

Neste trabalho foi analisado os pontos mais importantes de segurança das instalações da FARN.

Uma vez abordada a fundamentação teórica necessária, cabe agora descrever as atividades desenvolvidas no campo de segurança e a sua relação com toda teoria obtida através da universidade e pesquisa.

Os estudos das ameaças e técnicas de ataques, essa foi uma das fases mais intrigantes do desenvolvimento da segurança. Nela foram estudadas as ameaças a segurança da tecnologia da informação e as principais tecnologias de ataques utilizados por hackers.

Foram criados scripts para automatizar todo o processo de backup. Eles automaticamente copiam e compactam os dados, que logo a pois são enviados para a estação que armazena esse backup em CD.

São realizadas cópias diárias e semanais, sendo que as cópias semanais são geradas com duplicidade.

Uma cópia fica disponível na própria instituição é a outra cópia é guardado no cofre. Dessa maneira essa cópia reserva fica protegida contra desastres naturais, roubo ou qualquer outro incidente físico que possa ocorrer na empresa.

As senhas são a forma de controle de acesso aos recursos de um sistema ou uma rede. Entre tanto, se elas forem aplicadas corretamente, podem deixar um sistema ou uma rede ainda mais vulnerável.

Sendo assim, foi necessário que alguns procedimentos referentes à escolha e utilização das senhas fossem reformulados na empresa.

Na segurança física os servidores estavam agrupados em uma sala onde acesso era controlado, onde só pode entrar pessoas autorizadas como administrador de sistema e gerente do CPD. Além disso, para garantir a segurança física dos equipamentos contra roubo, foi instalado mais em ponto de alarme nesse local.

Com base na segurança da ISO17799 foi realizado comparações de segurança nas instalações.

Nas instituição serão somente comentados os 09 itens que abrange a ISO.

Política de Segurança

- Revisões de avaliações periódicas do processo de segurança;

Segurança da Organização

- Existe total segurança nas instalações físicas da faculdade;
- Mantém a segurança organizacional mesmo quando o acesso aos recursos de processamento de informações for realizado por outras empresas;

Classificação e Controle de Bens

- Mantém proteção apropriada ao patrimônio físico da faculdade;
- Garante e que recebam níveis adequados de proteção;

Segurança de Pessoal

- Minimiza o risco de incidentes e criar mecanismos de aprendizado com os incidentes já foram registrado na faculdade;
- Existe treinamento de usuário ;
- Registra os incidentes de segurança;

Segurança Física e Ambiental

- Combate ao acesso não autorizado a dependência da faculdade;
- Prevenir quanto a retirada de informações não autorizadas e remoção de dispositivos que armazenam esses dados;
- Existe ambiente seguro onde estão localizados as máquinas da faculdade ;
- Há segurança quanto ao armazenamento de dados;
- Existe deslocamento dos equipamento entre setores de forma segura;

Gerenciamento da Operação dos Computadores e Comunicações

- Minimiza os riscos de falhas no sistema;
- Protege a integridade da informação e do software que está sendo operado;
- Garanti a guarda correta da informação nas redes e dispositivos de armazenamento;

Controle de Acesso ao Sistema

- Preven os funcionários dos usuários quanto ao acesso não autorizado aos sistema de informação;
- Há infra-estrutura administração e coordenação da segurança de informação;
- Existe atribuição de responsabilidade aos usuário quanto a segurança da informação;
- Existe avaliações constante dos dados, levando em consideração a confiabilidade das informações e consequência a sua informação;

Desenvolvimento e Manutenção de Sistema

- Protege a autenticidade, confiabilidade e integridade da informação;
- Exigê de segurança no sistema;

- o Garante que atividades de suporte projetos de TI(Técnica de Informação) sejam conduzidos de forma segura;
- o Há segurança de arquivos que compõem o sistema;

Confiabilidade

- o Registro de propriedade intelectual;
- o Existe proteção de dados e isolamento das informações pessoais;

ANEXO - QUESTIONÁRIO

4. CONCLUSÃO

O trabalho relacionado a segurança da informação envolveu a aplicação de conhecimentos de diversas outras áreas da informática. Nesse aspecto foram de grande valia as horas despendidas no processo de estudo das tecnologias a serem aplicadas e os conhecimentos obtidos através da Universidade. Foram aplicados conceitos relacionados as comunicação de dados e sistemas operacionais.

Como resultado, o estudo e aplicação dos conceitos expostos puderam ser concretizados em ações que trouxeram grandes benefícios para empresa onde a segurança foi realizado. Todos os objetivos iniciais foram atendidos, a eliminação das vulnerabilidades encontradas na empresa fortaleceu todos os elos que compõem segurança da organização, enquanto a aplicação de novas medidas e ferramentas de segurança criou um ambiente mais fácil de ser controlado e monitorado. As principais ameaças agora podem ser medida,, os ataques identificados, e as ações de resposta estão bem definidas e documentadas. Todos esses benefícios puderam criar um ambiente adequado para novos serviços lançados pela empresa, alem de aumentar a segurança da organização como um todo.

Não desmerecendo os benefícios obtidos, alguns problemas foram criados junto a essa nova realidade: Os equipamentos devido ao grande numero de regras de controle, e o excesso de informações e alertas gerados pelos sistemas de segurança que acabam por ocupar muito o trabalho dos administradores de sistema.

Ao termino das atividades, e gratificante constatar os bons resultados obtidos. Entretanto o trabalho não se encerra por aqui. Novas falhas e vulnerabilidades em sistemas são descobertas diariamente, os invasores possuem ferramentas cada vez mais automatizadas, e conforme o ambiente cresce, torna-a mais difícil controla-lo. Sendo assim pode-se concluir que segurança da informação deve ser um processo continuo que faça parte das atividades da empresa, sempre objetivando atender os seus princípios básicos: confiabilidade, Autenticidade, integridade e a disponibilidade.

ANEXO -QUESTIONARIO

1. Descrição do sistema, em que linguagem ?E qual e o banco de dados?
O sistema vestibular foi desenvolvido através da linguagem de programação Clipper e, utiliza o DBASE 1.0 como banco de dados,
2. Qual e o equipamento onde roda o sistema ?
Pentium III 550 Mhz, 128 MB RAM, HDD 20.2 GB
3. Qual e leitura da prova?
Com relação a leitura ótica dos gabaritos(folhas de respostas) do vestibular, a mesma e feita por intermedeio de serviço terceirizado especializado em concursos.
4. Qual o meio de armazenamento de backup?
O backup do sistema e feito em Zip Disk e repassado para CD, diariamente .
5. A onde e a divulgação da segurança na internet?
Divulgamos através da internet apenas os gabaritos das provas, após a sua realização.E, o resultado final e disponibilizado como forma de texto, apenas para consulta.
6. Se tem no-breaks por quantas horas?
Nossos servidores possuem no-breaks acoplados e com autonomia de 2 horas .
7. Que tipo de segurança temos no hardware?
Erros podem acontecer. Nunca estamos livres deles. Mas, fazemos de tudo para que não aconteçam .Caso aconteça, temos as ferramentas para depura-los e, conseqüentemente, encontrar a solução do problema.
8. Pode ocorrer erros de processamento ?
Pode sim, também não estamos livres disso.Uma maquina pode quebrar a qualquer momento. Mas caso isso aconteça, temos as copias de segurança para recuperação dos arquivos em uma outra maquinas .
9. Pode ocorrer erro na memória?
Não
10. Tem algum sistema computacional substituto?
Temos sim.
11. Tem identificação de senha ou long para as pessoas que tem acesso ao sistema do vestibular?
Trabalhamos para ter o Maximo de segurança possível do concurso.
- 12.Qual a notificação mau funcionamento do software ?
Fazemos backups (copias de segurança) diariamente .
13. No ato da inscrição se a pessoa pode se inscrever duas vezes?
Se, no ato da inscrição o candidato se inscrever mais de uma vez, o sistema detecta e, a inscrição valida e a ultima, ficando anuladas as inscrições anteriores.

REFERÊNCIAS BIBLIOGRÁFIA

1. ALMEIDA, Marcelo Cavalcanti, 1954-Auditoria: **um curso moderno e completo.** / 5.ed. São Paulo:Atlas,1996.
2. AUDITORIA de Sistema. Disponível em <<http://www.solution-assessoria.com.br/http>> Acesso em : 04 Abril 2002.
3. DIAS, Claudia **Segurança e Auditoria da Tecnologia da Informática.**/Auditoria Nacional Rio de Janeiro, axcel books 1999.
4. DUVIDAS MAIS FREQUENTES. Pesquisa sobre duvidas de inscrição do vestibular. Disponível em <www.faccat.br/vestibular/faq.htm#1> Acesso 10 Outubro 2002.
5. FONTES, Joaquim Rubens, **Manual de auditoria de sistema.**_FONTES- ed- Rio de Janeiro: Ciência Moderna-1991
6. GIL, Antonio de Loureiro, **Auditoria de computadores** Gil, .4.ed. . São Paulo:Atlas,1999.
7. IDGNOW. **Justiça indicia hacker de DVD.** Disponível em <<http://idgnow.terra.com.br>> Acesso 19 de Novembro 2002.
8. JT WEB. **Governos federais tentam deter o exércitos de hacker que ameaçam a internet e o mundo.** Disponível em < [http // www.jt.estadao.com.br](http://www.jt.estadao.com.br)> Acesso 19 de Novembro 2002.
9. MANUAL de Segurança. Disponível em:
<http://www.upis.Br/revista_múltipla/nr_003/neto.htm> Acesso em : 10 Abril 2002.
10. MODULO DE SEGURANÇA. **Security news** de segurança. Disponível em <<http://www.modulo.com.br>> Acesso em :12 Abril 2002.
11. PUTTINI, Ricardo S.; SOUZA, Rafael Tde. Principais Aspectos da Segurança obtido através da Internet. < <http://webserver.redes.und.br>> Acesso em : 18 Novembro 2002.
12. TRIBUNAL DE CONTAS DA ÚNIAO, **Manual de auditoria de sistema.** Procedimento de auditoria PA02-Sistema .1998.
13. TERRA. **Ataque na rede de computadores do pentágono.** Disponível em < [http // busca.terra.com.br](http://busca.terra.com.br)> Acesso 19 de Novembro 2002.
14. UMA ESTRATEGIA DE SEGURANÇA BASEADA NA ISO17799. **Pesquina sobre estratégia da ISO.** Disponível em <[http //www.modulo.com.br](http://www.modulo.com.br)> Acesso 14 Novembro 2002.
15. UOL. **Maior golpe financeiro pelo web já descoberto no Brasil.** Disponível em < [http //conjur.uol.com.br](http://conjur.uol.com.br)> Acesso 19 de Novembro 2002.
16. SCHNEIER, Bruce **Segurança.com: Segredos e mentiras sobre a proteção na vida digital** São Paulo Editora : CAMPUS,2001.