DENIS ROCHA DE CARVALHO

SEGURANÇA DA INFORMAÇÃO:
ESTUDO DE CASO DA APLICAÇÃO DA NORMA NBR ISO/IEC 17799

Trabalho de conclusão de curso apresentado ao Curso de Ciência da Computação.

UNIVERSIDADE PRESIDENTE ANTÔNIO CARLOS

Orientador: Prof. Elio Lovisi Filho

BARBACENA
2003

DENIS ROCHA DE CARVALHO

SEGURANÇA DA INFORMAÇÃO: ESTUDO DE CASO DA APLICAÇÃO DA NORMA NBR ISO/IEC 17799

Este trabalho de conclusão de curso foi julgado adequado à obtenção do grau de Bacharelado em Ciência da Computação e aprovado em sua forma final pelo Curso de Ciência da Computação da Universidade Presidente Antônio Carlos.

Barbacena – MG, 09 de dezembro de 2003.

_____

Prof. Elio Lovisi Filho - Orientador do Trabalho

_____

Prof. Eduardo Macedo Bhering - Membro da Banca Examinadora

_____

Prof. Emerson R. A. Tavares - Membro da Banca Examinadora

AGRADECIMENTOS

Agradeço a Deus, primeiramente, que me deu forças e sabedoria para alcançar meus objetivos, a minha família, que é meu pilar, pois sempre me apoiou nas horas ruins e boas, ao meu orientador, aos meus amigos de Carandaí que me ajudaram direta ou indiretamente e aos meus amigos e professores da UNIPAC, pelo convívio, pelo aprendizado e marcante amizade.

RESUMO

Neste trabalho, procurou-se desenvolver um estudo da aplicação da norma NBR ISO/IEC 17799. Para isso descrevemos os principais aspectos relativos à Segurança da Informação, descrevendo na Revisão bibliográfica, definimos alguns conceitos, demonstramos algumas ameaças e alguns elementos de Segurança de Redes de Computadores. Também, procurou-se mostrar na introdução a Política de Segurança a importância da informação para uma empresa. Bem como a importância política de segurança nos dias atuais, as etapas para construção de uma política confiável e que não fuja da cultura da empresa, e para tanto, nos baseamos na norma NBR ISO/IEC 17799. E no Capitulo referente ao estudo de Caso, foi determinado as responsabilidades, além de ter sido realizada uma análise de risco na empresa X Varejista e baseado nela apliquei a norma NBR ISO/IEC 17799, contendo todos os controles necessários para a segurança da informação da empresa em questão.

Palavras-chave: Informação, Segurança da Informação, Política de Segurança, NBR ISO/IEC 17799 ;

SUMÁRIO

LISTAS

TABELAS

1 INTRODUÇÃO

Em uma empresa moderna, a informação é tratada como um bem valioso da empresa, podendo estar de forma manuscrita, impressa, gravada em meios magnéticos, ou simplesmente, ser do conhecimento dos funcionários.

As informações adquiridas, desenvolvidas ou aperfeiçoadas, devem ser preservadas levando-se em conta a sua integridade, disponibilidade, privacidade e confidencialidade, evitando assim fraudes, violações, acessos, uso e divulgação indevida.

É nesse contexto que a definição de uma Política de Segurança da Informação deixa de ser custo associado a idéias exóticas, para se tornar investimento capaz de assegurar a sobrevivência da empresa e a continuidade dos negócios da organização. Para que as empresas possam ser competitivas, é imperativo que elas possam contar com um trabalho de

profissionais especializados e qualificados que saibam como alinhar Segurança à Tecnologia da Informação.

Com o crescimento da utilização da informática, percebe-se um aumento na armazenagem das informações, ou ativos das empresas, em meio magnético através de computadores ou redes de computadores.

1.1 CICLO DE VIDA DA INFORMAÇÃO

Como a informação é um bem valioso das empresas, temos que separar todos os aspectos ligados à segurança da informação, as propriedades que devem se preservadas e protegidas para que a informação esteja efetivamente sob controle, e, principalmente, os momentos que fazem parte de seu ciclo de vida. [Sêmola, 2003]

O Ciclo de Vida, por sua vez, é composto e identificado pelos momentos vividos pela informação que a colocam em risco. Correspondendo às situações em que a informação é exposta a ameaças que colocam em risco suas propriedades, atingindo a sua segurança, a figura 1, revela todos os 4 momentos do ciclo de vida que são merecedores de atenção.

Manuseio

Momento em que a informação é criada e manipulada, seja ao folhear um maço de papéis, ao digitar informações recém-geradas em uma aplicação na Internet, ou ainda, ao utilizar sua senha de acesso para autenticação.

Armazenamento

Momento em que a informação é armazenada, seja em um Banco de Dados compartilhado, em uma anotação de papel posteriormente postada em um arquivo de ferro, ou ainda, em uma mídia de disquete depositada na gaveta da mesa de trabalho.

Transporte

Momento em que a informação é transportada, seja ao encaminhar informações por correio eletrônico (e-mail), ao postar um documento via aparelho de fax, ou ainda, ao falar ao telefone uma informação confidencial.

Descarte

Momento em que a informação é descartada, seja ao depositar na lixeira da empresa um material impresso, seja ao eliminar um arquivo eletrônico em sua estação de trabalho, ou ainda, ao descartar um CD-ROM usado que apresentou falhas na leitura.

Temos que manter alinhado a Política de Segurança adotada aos momentos de Manuseio, Armazenamento, Transporte e principalmente Descarte. Pois não adiantaria cumprir todas as etapas da Política de Segurança e o momento de descarte as informações estiverem expostas. Comprometendo toda a Segurança do negocio a perder.

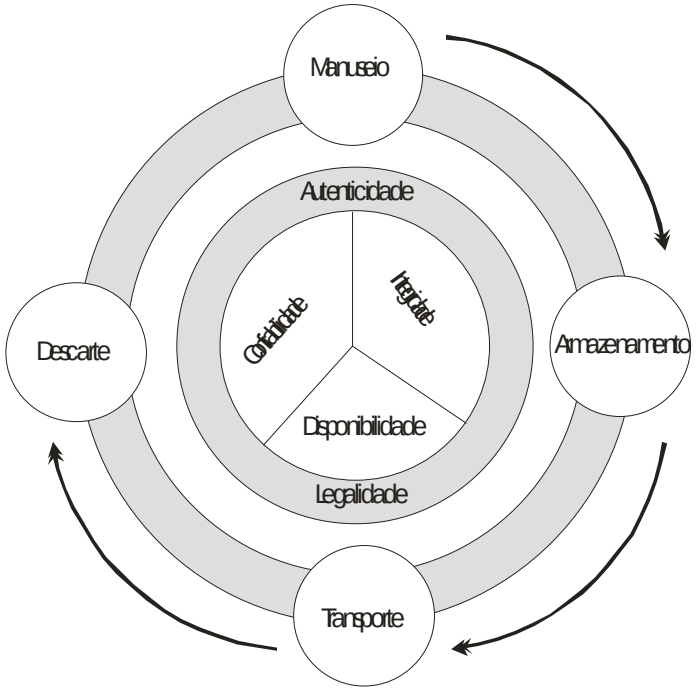

Figura 1 – Momentos do ciclo da vida da informação. [Sêmola, 2003]

1.2 A PROPOSTA

A presente proposta visa desenvolver um estudo da aplicação da norma NBR ISO/IEC 17799. O estudo de caso será referente à uma empresa do setor varejista, que vamos manter seus dados em sigilo para garantir sua confidencialidade e teremos atenção especial ao *Sistema XInfo* de tamanha importância para a empresa. O projeto visa analisar a situação atual, verificar patrimônio, instalações, estudo de mecanismos de segurança, métodos de monitoramento de segurança, métodos de auditorias de segurança.

Segundo Fábio [Axur, 2003], uma certificação NBR ISO/IEC 17799 evidencia a prática da melhor política de segurança, baseada no relato de auditores externos – portanto, imparciais. É uma declaração simples que apresenta a informação como parte do negócio, um bem valiosíssimo e que deve ser salvaguardado. “Este documento deve ser claro. Será dividido em grupos, conforme os enfoques estratégicos, táticos e operacionais. Deverá apresentar regras simples, sem o famoso ‘tecniquês’, utilizando sempre a NBR ISO/IEC 17799 como base”.

2 REVISÃO BIBLIOGRÁFICA

Nesse capítulo, procurou-se descrever os vários aspectos do tema Segurança de Redes de Computadores. Constantemente serão citadas definições retiradas da RFC 2828 (*Request for Coments* nº 2828). As RFC são documentos produzidos por professores, doutores e pesquisadores nas diversas áreas de tecnologia, que descrevem todos os detalhes das implementações dessas tecnologias, tanto de redes quanto de linguagens, protocolos de

comunicações, padrões de funcionamento de *hardware*, etc. Especificamente, a RFC 2828 é um Glossário de Segurança na Internet.

2.1 REDES DE COMPUTADORES

A RFC 2828, define rede de computadores como uma coleção de *hosts* interligados para troca de dados. *Host* é definido pela mesma RFC 2828 como sendo um computador ligado a uma rede de comunicação que possa usar os serviços providos pela rede para trocar dados com outros sistemas interligados.

A Figura 2, demonstra um esquema de redes de computadores. A definição de rede de computadores é utilizada para sistemas de todos os tamanhos e tipos, indo desde a enorme Internet até a um simples computador pessoal interligado remotamente como um terminal de outro computador.

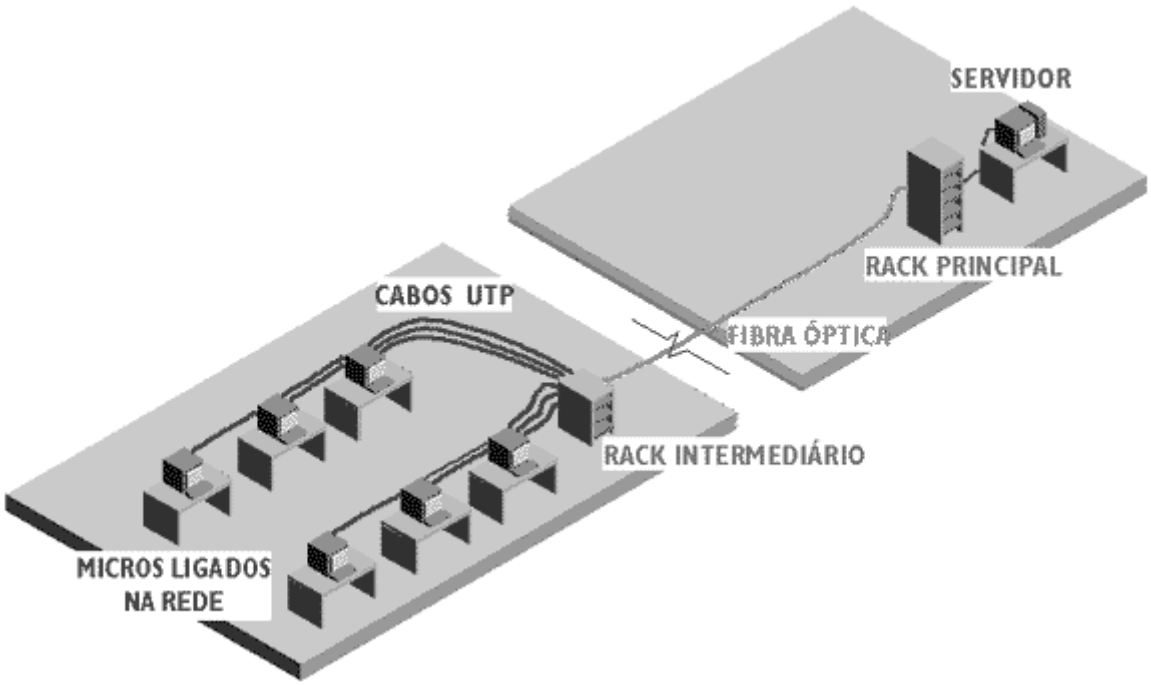

Figura 2 – Esquema de Redes de Computadores.[Tavares, 2003]

2.1.1 OBJETIVOS DAS REDES DE COMPUTADORES

Segundo Tanenbaum [Tanenbaum, 1994], define os objetivos da interconexão de computadores como sendo:

- **Compartilhamento de recursos:** fazer com que todos os programas, dados e equipamentos da rede estejam disponíveis a todos os usuários independentemente de sua localização física. Como exemplo, pode-se citar o compartilhamento de uma impressora por vários usuários;

- **Economia:** a substituição gradativa dos antigos *mainframes* para as redes de computadores de pequeno porte, significou uma redução muito grande nos custos de manutenção dos sistemas de informação, possibilitando uma verdadeira revolução nos CPDs. Esse fenômeno ficou conhecido mundialmente como *Downsizing*. Essas redes de computadores de pequeno porte possibilitam um aumento da capacidade de processamento a medida que a demanda cresce, ao contrário dos grandes *mainframes*, onde a sobrecarga só poderia ser solucionada com a substituição do mesmo por um *mainframe* de maior capacidade, a um custo geralmente muito elevado;

- **Prover um meio de comunicação:** As redes de computadores também são um poderoso meio de comunicação entre pessoas, possibilitando inclusive o trabalho em conjunto mesmo estando a quilômetros de distância.

2.2 PRINCÍPIOS BÁSICOS DA SEGURANÇA DA INFORMAÇÃO

Existem diversas definições para informação, a que melhor se adapta à nossa área é a definição do British Standards Institute, descrita abaixo:

Informação é um recurso que, como outros importantes recursos de negócios, tem valor a uma organização e por conseguinte precisa ser protegido adequadamente. [BS 7799]

A melhor definição para segurança pode ser obtida através do Dicionário Aurélio, conforme descrito abaixo:

Segurança. S. f. 2. Estado, qualidade ou condição de seguro. 3. Condição daquele ou daquilo em que se pode confiar. 4. Certeza, firmeza, convicção.

Seguro. [Do lat. securu.] Adj. 1. Livre de perigo. 2. Livre de risco; protegido, acautelado, garantido. 8. Em quem se pode confiar. 9. Certo, indubitável, incontestável. 10. eficaz, eficiente. [Aurélio, 2003]

A Segurança da Informação protege a informação de uma gama extensiva de ameaças para assegurar a continuidade dos negócios, minimizar os danos empresariais e maximizar o retorno em investimentos e oportunidades.

A Segurança da Informação é caracterizada pela preservação da confidencialidade, integridade e disponibilidade. [BS 7799]

[Pelissare, 2002] salienta outros três aspectos básicos da segurança de dados que se subdividem em vários tópicos:

1 - Prevenção: onde pretende-se evitar que aconteça:

- **Proteção de h*ardware*:** normalmente chamado de segurança física, é de vital importância. Negando acessos físicos inautorizados a infra-estrutura da rede, previne-se de possíveis roubos de dados, desligamento de equipamentos e demais danos possíveis quando se está fisicamente no local;

- **Proteção de arquivos e dados**: providenciado por autenticação, controle de acesso e antivírus. No processo de autenticação, é verificado se quem está pedindo acesso é realmente quem diz ser. No processo de controle de acesso, só são disponibilizadas as transações realmente pertinentes a essa pessoa (ex.: só leitura de arquivos, leitura e escrita, quais pastas ou arquivos a pessoa pode utilizar, etc.);

- **Proteção do perímetro da rede**: ferramentas *firewall* cuidam desse aspecto, mantendo a rede protegida contra invasões de usuários não autorizados.

2 - Detecção: onde detecta-se o problema o mais cedo possível:

- **Alertas**: sistemas de detecção de intrusos (IDS - *Intrusion Detection System* - Sistemas de Detecção de Intrusos), que podem avisar os administradores e responsáveis pela segurança da rede a qualquer sinal de invasão ou mudança suspeita no comportamento da rede que pareça um padrão de ataque ou mude o comportamento normal da rede. Os avisos podem ser via e-mail, via mensagem no terminal do administrador, etc.;

- **Auditoria**: periodicamente deve-se analisar os componentes críticos do sistema a procura de mudanças suspeitas. Esse processo pode ser realizado por ferramentas que procuram, por exemplo, modificações no tamanho nos arquivos de senhas, usuários com inatividade longa, etc.

3 - Recuperação: como voltar ao funcionamento normal após um incidente:

- **Cópia de segurança dos dados (*Backup*)**: manter completo, atualizado e testado, *backup* dos dados em meio diferente e separado dos servidores;

- **Aplicação para realizar o *Backup***: ferramentas que proporcionem recuperação rápida dos dados do *backup*;

- ***Backup do Hardware***: a compra ou utilização de *backup* de *hardware* (ex.: servidor reserva, *no-break* reserva, linhas de dados reserva, etc.) podem ser justificados levando-se em conta o custo de uma parada do sistema e determinando-se a importância da informática para a empresa.

[Sêmola, 2003] define que a segurança da informação tem como objetivo a preservação de três princípios básicos:

- **Confidencialidade**: Toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo, visando a limitação de seu acesso e uso apenas às pessoas para quem elas são destinadas.

- **Integridade**: Toda informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-las contra alterações indevidas, intencionais ou acidentais.

- **Disponibilidade**: Toda informação gerada ou adquirida por um indivíduo ou instituição deve estar disponível aos seus usuários no momento em que os mesmos delas necessitem para qualquer finalidade.

2.3 AMEAÇAS E PROBLEMAS DA SEGURANÇA DA INFORMAÇÃO

2.3.1 AMEAÇAS À SEGURANÇA DA INFORMAÇÃO

Podem ser classificadas em três tipos:

- ***Acesso não autorizado***: descoberta da informação de um dado utilizador, que é posteriormente utilizada por outro para aceder aos recursos disponíveis ao primeiro.

- ***Ataques por imitação:*** consistem em fazer que um dado utilizador ou sistema se comporte como um outro, para a obtenção de informação, recursos críticos ou perturbação do funcionamento de serviços. Nesta categoria incluem-se os *"Spoofing attacks"*, em que se utiliza informação falsa para obter acesso indevido a recursos e os *"Replay attacks"*, nos quais as mensagens que circularam na rede são copiadas e posteriormente repetidas de forma a simular um utilizador autorizado.

- ***Negação de serviços*** *(Denial of Service, DoS),* é uma forma bastante freqüente de ataque, cujo objetivo é a interrupção ou perturbação de um

serviço, devido a danos (físicos ou lógicos) causados nos sistemas que o suportam. Algumas formas de provocar um *"DoS"* são a disseminação de vírus, a geração artificial de grandes volumes de trafego, ou a geração de grandes volumes de pedidos a servidores, que devido a essa sobrecarga ficam impedidos de processar os pedidos normais.

2.3.2 VÍRUS

Para os usuários em geral, qualquer tipo de código malicioso que apague os dados ou atrapalhe o funcionamento dos computadores, é chamado de vírus. Mas atualmente, os chamados vírus de computador são classificados em vários tipos, cada um com suas particularidades de funcionamento, formas de contágio e disseminação. Os principais tipos são:

- **Vírus simples**: *é um vírus de computador como sendo um software com capacidade de se duplicar, infectando outros programas, usualmente com alguma intenção maliciosa*. Um vírus não pode executar-se sozinho, requer que o seu programa hospedeiro seja executado para ativar o vírus; [RCF 2828]

- **Cavalos de Tróia**: é definido pela mesma [RFC 2828], como sendo *um programa que aparenta ter uma função útil, mas possui alguma função maliciosa que burla os mecanismos de segurança.* Não possui a capacidade de se auto replicar. A Figura 3, demonstra a tela de controle do Trojan NetBus e com ela o invasor pode realizar várias ações maliciosas, como exemplo pode-se citar a função Open CD-ROM, que quando acionada abre ou fecha a sua bandeja;

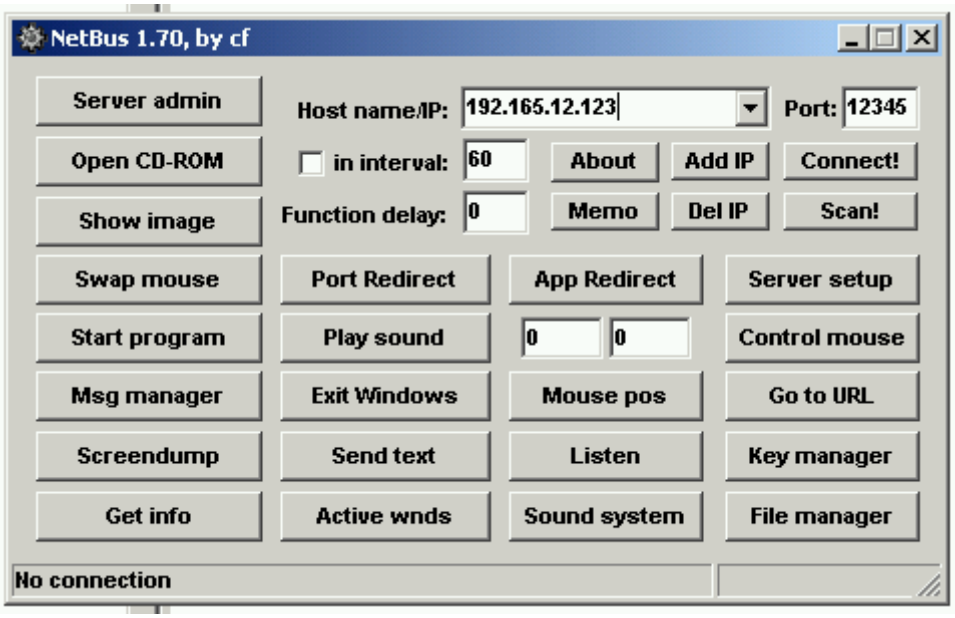

Figura 3 - Trojan NetBus 1.70, tela de controle [Anônimo, 2002]

- ***Worm* ou "verme"**: definido pela mesma [RFC 2828], *como sendo um programa de computador que pode se executar independentemente, propagar-se pelos computadores de uma rede sozinho, podendo consumir os recursos dos computadores destrutivamente*;

- **Vírus polimorfo**: tipo de vírus que modifica a si mesmo a medida que se dissemina, dificultando a sua localização e eliminação;

- **Vírus de Macro:** utiliza-se da linguagem *VBScript* dos softwares Microsoft e o de ser executado em qualquer computador que possua, por exemplo, o aplicativo *Word* instalado.

Os vírus propagam-se de várias maneiras: por disquetes infectados, por d*ownloads* feitos na Internet, executando-se arquivos anexos de *e-mail* e, ultimamente, apenas lendo-se um e-mail infectado. Esta última maneira, explorada pelo vírus *Scherzo*, descoberto em 27 de dezembro de 2001, segundo as empresas *Panda Software* e Sophos, ambas fabricantes de *softwares* antivírus [Anônimo, 2001] .

Seus malefícios podem ser desde uma simples mensagem de protesto na tela do computador infectado, a perda total dos dados gravados ou a sobrecarga da rede, impedindo seu funcionamento ou gerando lentidão.

A evolução dos vírus foi bastante rápida e devastadora. Segundo as empresas fabricantes de softwares antivírus *Symantec* e *McAfee*, o primeiro vírus de computador conhecido surgiu no ano de 1986 e era chamado *Brain*. Era um vírus de *boot* (atacava o setor de inicialização do disco rígido e se propagava através de um disquete de *boot* infectado).

Atualmente, estima-se que existam cerca de 58 mil tipos de vírus. Número que cresce diariamente a uma taxa de cerca de 10 a 12 novos vírus por dia, segundo as mesmas empresas fabricantes de softwares antivírus.

Vários fatores contribuíram para esse aumento exponencial da quantidade de vírus, dentre os quais pode-se citar:

- os *bugs* (erros de programação) encontrados nos *softwares* dos microcomputadores, desde os sistemas operacionais até mesmo nos servidores de Internet. Cita-se o caso dos vírus *Nimda* que se espalhou em setembro, e *Code Red* disseminado em julho, que exploravam falhas no servidor de Internet da *Microsoft* (IIS, *Internet Information Server*);

- a explosão do uso da Internet, onde pode-se trocar informações e experiências para construção e programação dos vírus;

- o surgimento de kits para fabricar vírus. Atualmente, existem ferramentas disponíveis gratuitamente na Internet que fabricam vírus, bastando o usuário fornecer os dados de como o vírus funcionará. O usuário não precisa nem saber programar para construir um vírus. Como exemplo, pode-se citar o vírus Antraz, feito a partir de um kit de criação de vírus que aproveitou-se da onda de medo em torno do bioterrorismo no mês de Outubro/2001. Não causou grandes danos por erros cometidos pelo seu criador devido a falta de experiência com programação.

2.3.3 ORIGEM DOS ATAQUES

2.3.3.1 Hacker

O termo *hacker* é definido pela RFC 2828 (*Request for Coments* nº 2828), como sendo alguma pessoa com um grande interesse e conhecimento em tecnologia , não utilizando eventuais falhas de segurança descobertas em benefício próprio. O termo é usado erroneamente, especialmente pelos jornalistas, como alguém que efetue crimes cibernéticos.

2.3.3.2 Cracker

O termo *cracker ou intruder*, esse sim, é definido pela mesma RFC 2828 como sendo alguém que tente quebrar a segurança ou ganhar acesso a sistemas de outras pessoas sem ser convidado. Não é obrigatoriamente uma pessoa com grande conhecimento de tecnologia como um *hacker*.

2.4 TIPOS DE ATAQUES

Invasão é a entrada em um site, servidor, computador ou serviço por alguém não autorizado. Mas antes da invasão propriamente dita, o invasor poderá fazer um teste de invasão, que é uma tentativa de invasão em partes, onde o objetivo é avaliar a segurança de uma rede e identificar seus pontos vulneráveis. Mas não existe invasão sem um invasor, que pode ser conhecido, na maioria das vezes, como *Hacker* ou *Cracker*. Ambos usam seus conhecimentos para se dedicarem a testar os limites de um sistema, ou para estudo e busca de conhecimento ou por curiosidade, ou para encontrar formas de quebrar sua segurança ou ainda, por simples prazer, mas também pode ser por mérito, para promoção pessoal, pois suas descobertas e ataques são divulgados na mídia e eles se tornam conhecidos no seu universo, a diferença é que o *Cracker* utiliza as suas descobertas para prejudicar financeiramente alguém, em benefício próprio, ou seja, são os que utilizam seus conhecimentos para o mau.

Muitas redes corporativas hoje em dia são implementadas com o objetivo de tirar o maior proveito dos serviços que as redes disponibilizam, esquecendo o aspecto da segurança dos dados que nela trafegam e a importância disso. É em umas dessas redes que o intruso poderá causar algum estrago ou roubar informações.

Para efeito de didática, vamos utilizar exemplos de comandos em Linux, por se tratar de um sistema operacional de mais recursos.

2.4.1 VULNERABILIDADES DE UM SISTEMA

Em um sistema, recomenda-se ter algum sistema de filtragem que estabelece um certo nível de segurança. Um intruso, ao atacar um servidor, está na verdade tentando se infiltrar na rede interna e ele terá sucesso se o *firewall* (programa para filtragem de pacotes) desta rede não estiver adequadamente configurado. É recomendado, então, para evitar estes tipos de intrusões, se ter sistemas de *firewall* bem configurados e executar alguma ferramenta que permita apenas computadores confiáveis acessarem à rede. [Gerlach, 1999]

Nessa situação, o intruso pode determinar em quais computadores foram estabelecidas conexões, verificando assim qual dos computadores contém confiança suficiente para dar condições favoráveis ao seu ataque.

A ferramenta “TCP Wrapers” (Ferramenta que registra em *Log* solicitações de sessão, estando instalada nos computadores de rede, poderá determinar quais computadores poderão ou não estabelecer conexões através de portas como: *ftp* (21), *ssh* (22), *smtp* (25), *named* (53), pop3 (110), *imap* (143), *rsh* (514), *rlogin*(513), *lpd*(515).

É possível um intruso usar um *exploit* Figura 4,(nome usado para generalizar programas de invasão) CGI (*Common Gatway Interface*) para visualizar o arquivo “hosts.allow” do computador e então verificar para qual domínio tem acesso as portas de *telnet* e FTP. Assim, ele pode tentar obter permissão a um domínio que seja confiável para aquele computador. Desta forma, ele obtém acesso facilmente. Em função disso, se recomenda verificar o grau de confiança que se tem com os outros computadores e quanto estes estão seguros perante algum ataque.

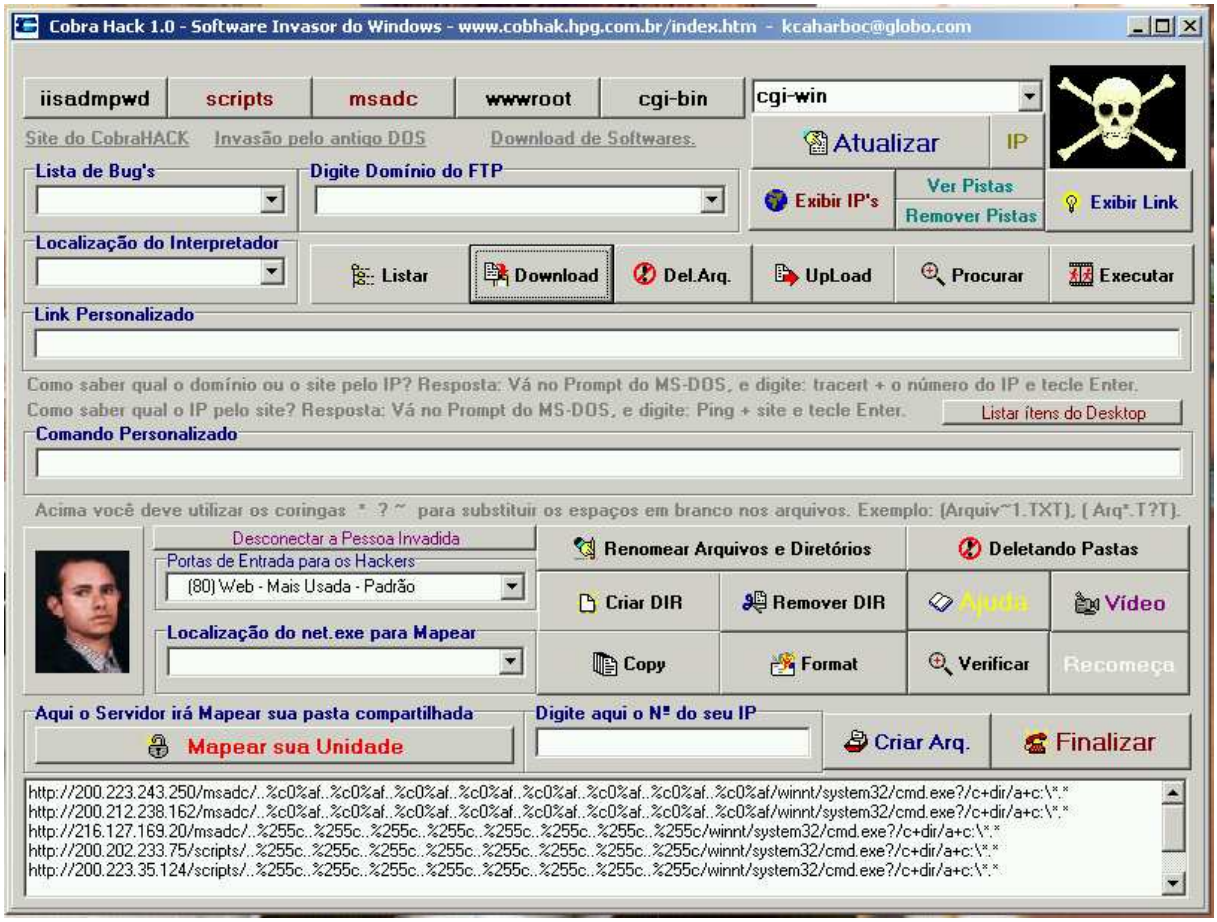

Figura 4 - Software Invasor do Windows. [Anônimo, 2002]

Corporações que não estruturam adequadamente a sua rede, com certeza possuirão vários computadores e roteadores mal configurados. Isto pode ajudar um intruso a ganhar o acesso à rede interna.

Outro ponto importante a ser observado é quanto à configuração dos servidores de DNS (*Domain Name Server*). O fato de se ter servidores de DNS mal configurados, permite com facilidade o mapeamento de rede interna. Empresas tiveram sucesso em testes de penetração, onde foi possível mapear a rede interna, utilizando servidores de DNS mal configurações. Devido a problemas como este, não se aconselha colocar servidores de DNS entre computadores de rede interna e externa.

Nos servidores de correio eletrônico, onde há conexões entre rede interna a externa para que ocorra a troca de mensagens, deve haver algum sistema de filtragem para evitar o ataque de um intruso.

Através do processo-servidor *finger* pode-se conseguir informações para identificar pontos de uma rede que são facilmente explorados por intrusos. As informações podem ser sobre usuários, computadores e sistema operacionais.

2.4.2 COLETA DE INFORMAÇÕES

A primeira etapa que um invasor executa em sua invasão, é tentar obter informações sobre a rede interna e externa para verificar quais computadores estão de alguma forma conectados à internet. Essas informações podem ser descobertas utilizando as seguintes técnicas: [Gerlach, 1999]

- Utilização de “nslookup”, ex.:

  nslookup

  >server <IP_do_DNS_primário_do_domínio_alvo>

  >set type = any

  >ls –d <domínioalvo.com.br>.

- Visualização do código HTML (Hyper Text Markup Language) nos servidores de *Web*, identificando os computadores;
  - Examinar código-fonte de páginas em busca de comentários.
- Obtendo informações do site com whois;
  - As informações coletadas em pesquisas whois podem trazer informações relevantes tais como:

- Quem registrou o domínio;
- O contato adminitrativo, etc.

Utilizando os itens descritos anteriormente, fica mais fácil para o intruso obter uma lista dos computadores com suas relações de confiança e entendê-las. Ao tentar a invasão, o intruso pode cometer algum erro, deixando alguma pista em *logs*. Se, por acaso, houver desconfiança de estar sendo atacado e se tiverem os registros de *logs* do sistema habilitados, então pode-se verificá-los para tentar descobrir o que está acontecendo.

2.4.3 IDENTIFICAÇÃO DE PONTOS VULNERÁVEIS DA REDE

Quando o intruso obtiver a relação de informações que identifica os computadores internos e externos, ele poderá utilizar ferramentas disponíveis para determinar as vulnerabilidades individuais de cada computador. Alguns programas podem ser utilizados para descobrir as vulnerabilidades em determinado computador, tais como: mscan, nmap, entre outros. [Gerlach, 1999]

Geralmente os programas que o intruso utiliza têm origem de máquinas com conexões com taxas de comunicação altas. Através dessas máquinas pode-se efetuar o ataque rapidamente, antes que seja notada a sua presença.

Outros *scans*, como o mscan e nmap já não exigem o acesso *root* para serem executados, porém são lentos e não conseguem se ocultar. O mscan explora os seguintes testes em computadores remotos:

- “TCP portscan”;
- “dump” do servido RPC executado pelo “portmapper”;
- verificações de vulnerabilidades em CGIs;

- localização de versões vulneráveis de *daemons* do tipo “sendmail”, “POP3”, “RPC staus”, “RPC mountd” e “IMAP” (*Internet Message Access Protocol*).

2.4.4 SNIFFERS

Após o intruso ter invadido e se apossado de um determinado computador da rede, o próximo passo será instalar *backdoors, trojans* em seguida *sniffers*. *Sniffers* são programas que trabalham, geralmente em rede *Ethernet*, utilizando uma interface de rede do computador em modo promíscuo. Esta interface “escuta” tudo o que passa pelo barramento e envia para o arquivo de *log* do *sniffer*.

Através dos *sniffers*, será capturado todo e qualquer dado que trafegar pelo barramento *Ethernet* onde estiver conectado o *sniffer*. Dados como nomes de usuários, senhas, seja senhas com “shadow” ou não, e informações que identificam os computadores podem ser coletadas da rede. O arquivo de *log*, que é armazenado no computador local que foi instalado pelo invasor, é regularmente consultado pelo mesmo.

Os *trojans* e *backdoors* costumam estar camuflados em arquivos binários do sistema (comentados no texto) para não serem descobertos. Os *sniffers* também utilizam este procedimento, instalando um *backdoor* no binário “ps” do sistema, por exemplo, para não ser percebido. Eles executam em *background* no sistema gerando como resultados os *logs*.

Existe uma ferramenta chamada “ifstatus”, que detecta a existência de interfaces de rede promíscua para o caso de execução de um *sniffer*. A Figura 5, demonstra a tela de controle do Win Sniffer. [Anômino, 2002]

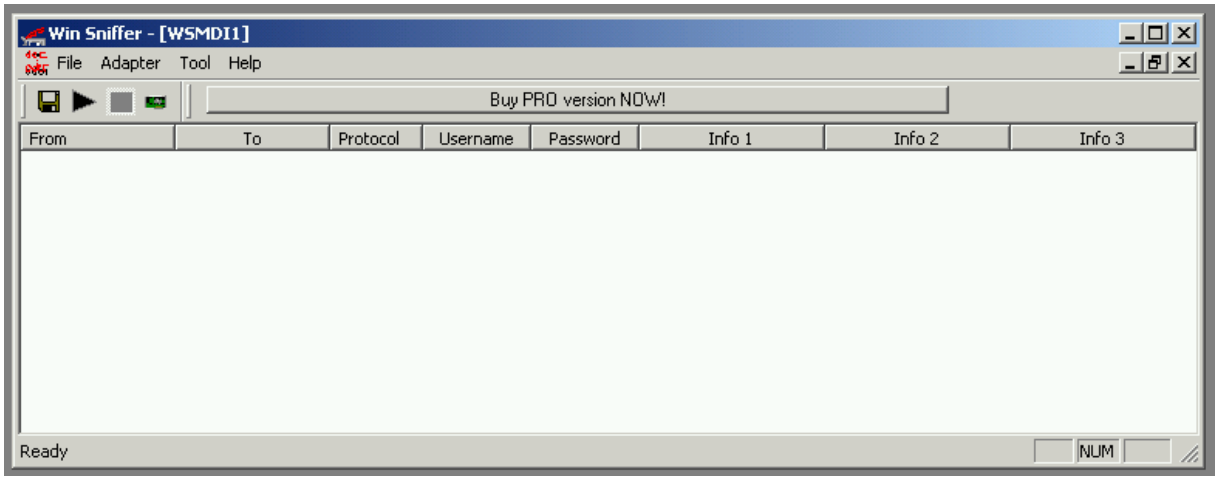

Figura 5 - Win Sniffer[Anônimo, 2002]

2.4.5 SPOOFING

O *spoofing* ocorre quando invasores autenticam uma máquina em nome de outra forjando pacotes de um *host* confiável (*trusted*). Nos últimos anos, essa definição foi expandida para abranger qualquer método de subverter a relação de confiança ou autenticação baseada em endereço ou em nome de *host*. [Anônimo, 2002]

2.4.6 ATAQUES DE RECUSA DE SERVIÇO - DOS

Um ataque de recusa de serviço (DoS) é qualquer ação iniciada por alguma pessoa que incapacitaria o *hardware* ou o *software* de um *host*, ou ambos, tornando o sistema inacessível e, portanto, negando serviço para usuários legítimos (ou mesmo ilegítimos). Em um ataque de DoS, o objetivo do invasor é simples e direto: derrubar o *host* da rede. Exceto quando as equipes de segurança testam *hosts* vulneráveis, os ataques de DoS são sempre maliciosos e, hoje em dia, ilegais.

A recusa de serviço é um problema persistente por duas razões: em primeiro, os ataques de DoS são rápidos e fáceis, e eles geram um resultado notável e imediato. Portanto, são populares e proliferam entre "*crackers*". E como isso, os administradores de sistema devem esperar freqüentes ataques de DoS.

Há uma razão mais importante para que ataques de DoS permaneçam problemáticos. A maioria dos ataques explora erros, limitações ou inconsistência em implementações de TCP/IP de fornecedores existentes, até que os fornecedores corrijam o problema. Nesse ínterim, todos os *hosts* afetados permanecem vulneráveis.

Um exemplo típico foi o ataque de “teardrop”, que enviava pacotes de “UDP” malformados para *hosts Windows*. Os alvos examinavam os cabeçalhos de pacotes malformados, engasgavam-se com eles e geravam um exceção fatal. Quando esse ataque surgiu, a Microsoft rapidamente reexaminou sua pilha de TCP/IP e gerou um correção e colocou as atualizações disponíveis para o público.

Entretanto, as coisas não são sempre tão simples assim. Quando se dispões do código fonte do Sistema Operacional, como usuários de Linux, à medida que surgem novos ataques de DoS, é de extrema importância corrigir o *software*, re-configurar o *hardware* ou filtrar as “portas” atacadas, dependendo da situação. [Anônimo, 2002]

2.4.6.1 Riscos impostos pelo Ataque DoS

Houve um tempo em que as pessoas viam os ataques de DoS como meros aborrecimentos. Eram problemas, certamente, mas não eram necessariamente críticos. Algumas pessoas ainda mantêm essa visão, argumentando que a maioria dos ataques de DoS eliminavam somente certos serviços que são fáceis de reiniciar. Mas, isso não é mais o ponto de vista predominante. Em vez disso, ataques de DoS agora estão sendo vistos de outra forma, principalmente porque os hábitos de computação da sociedade alteraram-se rapidamente. Os servidores hoje são os ingredientes essenciais no comércio eletrônico e outros serviços críticos. Nesse novo ambiente, incentivar ataques de DoS pode diminuir ou mesmo interromper lucros. De fato, poucas organizações podem ter recursos para um mal-sincronizado ataque de DoS. [Anônimo, 2002]

2.4.6.2 Ataques de DoS contra *hardware* de rede

A metodologia de DoS contra *hardware* de rede tem paralelos muito próximos de suas variedades comuns. De fato, em muitos casos, o mesmo ataque de DoS inutiliza tanto o *software* quanto o *hardware*. Alguns exemplos.

- Os invasores enviam solicitações de conexão a partir de endereços de IP forjados, inexistentes. Como a unidade receptora não pode resolver esses endereços, a sessão pode ficar pendente. (Essa condição pode incapacitar um único serviço ou porta, ou o sistema inteiro.)

- Os invasores comprometem todas as sessões disponíveis, evitando assim o alcance do roteador remotamente. Sendo assim, é necessário que o sistema seja reinicializado manualmente.

- Os invasores exploram estouros em rotinas de *login*, causando a queda da unidade ou reinicializando-a . Com isso, pode ser necessário a reinicialização do sistema.

- Os invasores inundam o sistema com pacotes ou estruturas peculiarmente malformados. O sistema não pode processá-lo corretamente e se auto-bloqueia.

2.5 FORMAS DE DEFESA

Os ataques a uma rede corporativa podem ser reduzidos consideravelmente se as portas de “smtp”, “name” e “portmapper” forem configuradas adequadamente. Deve ser reforçada a segurança nos roteadores de filtragem, evitando assim, ataques de “SMMP-Scanning” (*Simple Network protocol-Scanning*) e password *crackers*. Pois, se um intruso tentar se infiltrar, o roteador poderá servir como ponte para mais acessos não autorizados. [Gerlach, 1999]

2.5.1 SCANNERS

Um *scanner* é uma ferramenta de segurança que detecta vulnerabilidades de sistema. Seu objetivo é varrer arquivos, procurando campos de senhas vazios. Para cada campo vazio que ele encontra, ele adverte o usuário via correio eletrônico. Embora isso seja rudimentar, demonstra concisamente o conceito de *scanner*. [Anônimo, 2002]

Existem vários tipos de *scanners*, mas todos se enquadram em uma das duas categorias.

- *Scanners* de sistema, Figura 6;

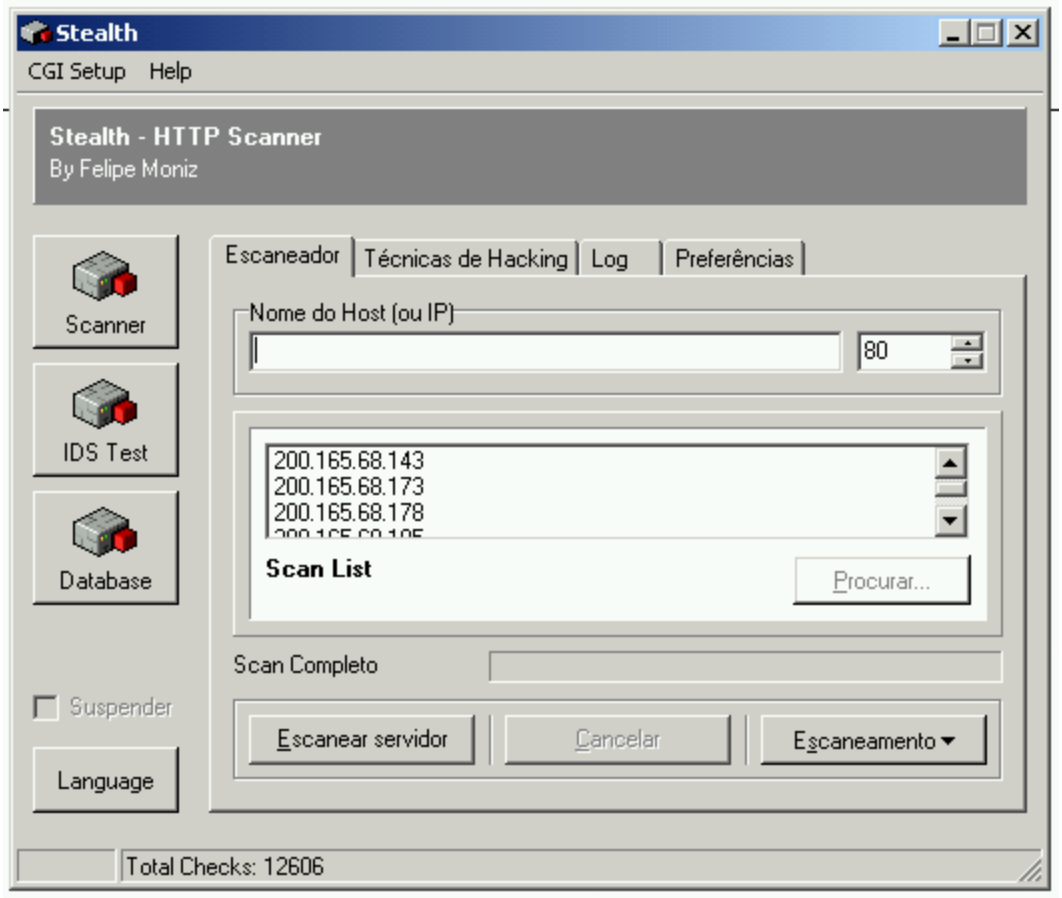

Figura 6 - Scanner de sistema[Anônimo, 2002]

- *Scanners* de rede, Figura 7;

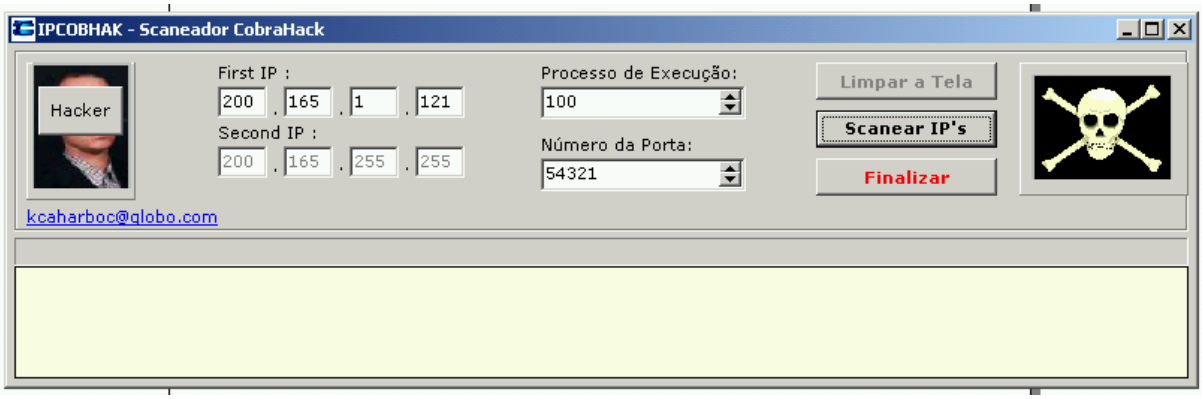

Figura 7 - Scanner de rede[Anônimo, 2002]

2.5.1.1 *Scanner* de Sistema

Varrem o por exemplo, *host* local, procurando vulnerabilidades óbvias de segurança que surgem de descuidos, pequenos deslizes e problemas de configuração que até usuários experientes às vezes perdem, por exemplo, permissões de arquivos excessivas, contas-padrão, entradas duplicadas de UID.

2.5.1.2 *Scanner* de Rede

Os *scanner* de rede testam *hosts* sobre conexões de rede, quase da mesma forma que um *cracker*. Eles investigam serviços e portas disponíveis, procurando as fraquezas mais conhecidas que invasores remotos podem explorar. [Anônimo, 2002]

2.5.2 FIREWALL

O *Firewall* consiste em um conjunto de componentes organizados de uma forma a garantir certos requisitos de segurança. Os componentes básicos para a construção de um *firewall* são:

- *Packet Filters*: são responsáveis pela filtragem (exame) dos pacotes que trafegam entre dois segmentos de rede.
- *Bastion Host*: computador responsável pela segurança de um ou mais recursos (serviços) de rede.

2.5.3 BASTION HOST

Bastion Host é qualquer máquina configurada para desempenhar algum papel crítico na segurança da rede interna. Essa máquina promove serviços permitidos segundo a política de segurança da empresa.

2.5.4 PACKET FILTERS

É de extrema importância dar-se atenção aos protocolos IP, TCP, ICMP e UDP. Estes são os principais protocolos a nível de rede e transporte (Modelo OSI) que são considerados e examinados ao se estabelecer regras de filtragem em um *packet filter*. Este mecanismo de filtragem a nível de roteador possibilita que se controle o tipo de tráfego de rede que pode existir em qualquer segmento de rede, conseqüentemente, pode-se controlar o tipo de serviço que podem existir no segmento de rede. Serviços que comprometem a segurança da rede podem, portanto, ser restringidos.

O *packet filter* não se encarrega de examinar nenhum protocolo de nível superior ao nível de transporte, como por exemplo, o nível de aplicação que fica como tarefa dos aplicativos *gatways* (*proxys servers*). Portanto, qualquer falha de segurança a nível de aplicação não pode ser evitada, utilizando somente um *packet filter*. O componente que realiza a filtragem de pacotes geralmente é um roteador dedicado, mas pode ser um *host* de propósito geral configurado como roteador e recebe a denominação de *screening router*.

2.5.5 REALIZAÇÃO DE AUDITORIA EM ARQUIVOS DE *LOGS*

Como em qualquer sistema operacional de rede, sempre soa necessárias auditorias periódicas, que têm o objetivo de conferir determinadas falhas de sistema. Através dessas auditorias, são avaliadas as necessidades de serem aplicadas novas técnicas de segurança. As falhas nas configurações dos serviços são uma das causas mais comuns nos sistemas. [Sloha, 1999]

É através de sistemas de *logs*, simples arquivos de textos, que um administrador poderá analisar a ocorrência de um incidente e poderá concluir se é ou não um ataque. A seguir são listados algumas discas sobre *logs* do sistema:

- Através do /etc/syslog.conf se tem uma grande variedade de opções para ativar *logs* para auditoria de sistemas;
- Consultar os arquivos de *logs* para auditoria periodicamente;
- Consultar os arquivos gerados pelos *daemons* como o xferlog (arquivo de *log* de transferências ftp), “syslog” (syslogd), *messages* (syslogd), *access log* (httpd);
- Verificar o arquivo de *log* “sulog”.

Para o caso de análise de algum problema no sistema ou da desconfiança de algum invasor estar tentando entrar no sistema, existe o serviço “syslog” comentado no parágrafo anterior, que registra através do *daemon* “syslogd”, os vários eventos que acontecem no sistema em arquivos de *logs*. Desta forma, o administrador conseguirá monitorar através destes, o que acontece no sistema. Há tempo o “klogd” que é o processo-servidor responsável por registrar tudo que acontece a nível de núcleo. Esses registros em arquivos de *logs* podem auxiliar na resolução de problemas.

A maneira que o *daemon* “syslogd” registra informações, em formato de *log* para os arquivos específicos, é de fácil entendimento para o caso de uma posterior análise. [Anônimo, 2002]

```
Information regarding the event(s) ORIGINATOR
_____________________________________________
Details on ORIGINATOR:
Best Name: UNKNOWN
NetBIOS: UNKNOWN
DNS Name: UNKNOWN
Network Address: 10.176.213.12
MAC: UNKNOWN
_____________________________________________
Information regarding the AFFECTED SYSTEM(S)
_____________________________________________
Alert List:
Issue: FTP port probe
Parameter: port=21,reason=RSTsent
Time Stamp: 1/6/02 3:25:36 AM (GMT)
Count: 1
Target: TLC3
Target IP: 192.0.2.5
Detector: TLC3
Detector IP: 192.0.2.5

Jan 2 21:38:06 host Feb 06 2080 02:32:53: %PIX-3-106010: Deny inbound
tcp src outside:10.216.10.3/4516 dst inside:192.0.2.81/21
Jan 2 21:38:07 host Feb 06 2080 02:32:54: %PIX-3-106010: Deny inbound
tcp src outside:10.216.10.3/4527 dst inside:192.0.2.85/21
Jan 2 21:38:07 host Feb 06 2080 02:32:54: %PIX-3-106010: Deny inbound
tcp src outside:10.216.10.3/4534 dst inside:192.0.2.87/21
Jan 2 21:38:08 host Feb 06 2080 02:32:55: %PIX-3-106010: Deny inbound
tcp src outside:10.216.10.3/4551 dst inside:192.0.2.88/21
Jan 2 21:38:08 host Feb 06 2080 02:32:56: %PIX-3-106010: Deny inbound
tcp src outside:10.216.10.3/4557 dst inside:192.0.2.89/21
Jan 2 21:38:08 host Feb 06 2080 02:32:56: %PIX-3-106010: Deny inbound
tcp src outside:10.216.10.3/4561 dst inside:192.0.2.90/21
Jan 2 21:38:09 host Feb 06 2080 02:32:56: %PIX-3-106010: Deny inbound
tcp src outside:10.216.10.3/4566 dst inside:192.0.2.91/21
Jan 2 21:38:09 host Feb 06 2080 02:32:56: %PIX-3-106010: Deny inbound
tcp src outside:10.216.10.3/4516 dst inside:192.0.2.81/21
```

Exemplo de Arquivo Log [Anônimo, 2002]

Há alguns diretórios que geralmente são utilizados para armazenar *logs* em sistemas UNIX: /usr/adm, /var/adm, /var/log, /etc e /etc/security, sendo que podem haver variações na localização destes conforme a versão e distribuição.

Qualquer serviço de rede, que seja inicializado pelo *daemon* “inetd” como (popd, imapd, ftpd, telnetd, sshd.), pode enviar mensagens de log, e estes *logs* poderão ser gerenciados por ferramentas como a “TCP Wrappers”.

Seguem alguns cuidados gerais:

- Criar uma política de *logs* séria. Verificar qual tipo de informação estará disponível para se registrar nos *logs*, quais mecanismos fazem tal registro, onde será executada a terefa e onde os *logs* serão armazenados;

- Verificar se as informações necessárias são registradas nos *logs* pelos mecanismos disponíveis pelo sistema;

- Habilitar todos os mecanismos de log disponíveis, e, aos poucos, ir filtrando quais são mais importantes para possíveis análises de detecção de intrusão;

- Monitorar regularmente todos os *logs* verificando registros não comuns e evidenciando possíveis ataques;

- Analisar toda e qualquer ocorrência estranha que ocorra no sistema, tal como: reinicialização do sistema;

- Se houver confirmação de intrusão pelos *logs*, deve-se compartilhar estas mensagens com a equipe de segurança ou com os administradores das redes comprometidas;

- Aconselha-se utilizar algum “script” ou ferramenta que auxilie o analisador, reduzindo o grande volume de informações e não retirando o essencial para a análise;

- Ao analisar sinais de intrusão, deve-se ter certeza que a intrusão esteja sendo realizada antes de passar a informação adiante;

- Efetuar cópias de segurança dos arquivos de *logs* regularmente, se possível em mídias não regraváveis;

- Mudar o local dos *logs* de tempos em tempos, para evitar que o intruso os localize com facilidade;

- Utilizar servidores de tempo para sincronizar todos os dispositivos da rede, inclusive computadores normais, para que se unifique os *timestamps* dos *logs*;

- Aconselha-se a instalação de uma máquina que deve centralizar os registros de *logs* e ter uma melhor segurança;

- Para o auxílio e automatização das tarefas, deve-se incluir utilitários para auxiliar em tarefas, como:

  - A procura de padrões de intrusão;

  - Para isolar *logs* que se destacam entre outros;

2.5.6 DETECÇÃO DE INVASÃO

A detecção de invasão é uma prática de utilizar ferramentas automatizadas para detectar tentativas de invasão em tempo real. Essas ferramentas são chamadas *Intrusion Detection Systems* (IDS).

2.5.7 CONCEITOS BÁSICOS DE DETECÇÃO DE INVASÃO

Em sistemas de detecção de invasão baseados em regras, há duas abordagens: preempitiva e reacionária. A diferença está relacionada principalmente com o tempo:

- Na abordagem preempitiva, a ferramenta de detecção de invasão ouve o tráfego de rede. Quando a atividade suspeita é observada (uma inundação de pacotes particulares, por exemplo), o sistema toma a ação apropriada.

- Na abordagem reacionária, a ferramenta de detecção de invasão observa os *logs* em vez de ouvir o tráfego de rede. Novamente, quando atividade suspeita é observada, o sistema toma a ação apropriada.

Essa diferença pode parecer sutil, mas não é. A abordagem reacionária é simplesmente um passo à frente do registro em *logs* padrão; ela faz um alerta para o ataque que acabou de acontecer. [Anônimo, 2002]

Ao contrário, a abordagem preempitiva realmente permite que o sistema emita uma resposta enquanto um invasor está montando o ataque. Além disso, certos sistemas permitem que os operadores testemunham e monitorem ao vivo um ataque em progresso.

É possível alcançar o modelo reacionário simplesmente utilizando ferramentas de segurança padrão do Linux. Teoricamente, é possível construir um sistema de detecção e resposta a pseudo-invasão assim:

- Utilizar “LogSurfer” (ferramenta de segurança) para observar certa atividade predefinida e ameaçadora nos *logs*.
- Um script que adiciona o endereço do invasor (ou mesmo sua rede inteira) a “hosts.deny” de modo que “tcpd” recuse conexões futuras.

Esse tipo de detecção é do tipo rápida. O invasor foi detectado e seu endereço agora será recusado. Entretanto, essa abordagem tem muitas deficiências. Uma é que os endereços de origem não são confiáveis. Eles são facilmente forjados, então um invasor pode continuar tentando, utilizando um endereço de origem diferente a cada vez.

Mas os modelos preemptivos também têm deficiências. Um, é que eles utilizam recursos intensamente. Isso realmente representa dois problemas: um, devido à interatividade inerente desses sistemas e outro, devido a limitações de *hardware* e *software*.

Primeiro, se um invasor sabe que é possível estar escutando um sistema preemptivo de detecção de invasão, ele pode fazer várias suposições. Uma, é que os IDS (*Intrusion Detection Systems*) empreenderá uma ação idêntica quando defrontado com um ataque idêntico. Portanto, inundando o *host* com múltiplas instancias do mesmo ataque de

diferentes endereços, ele pode realizar um ataque de saturação de processo e talvez derrube ou incapacite os IDS.

Segundo, dependendo da capacidade do processador e das limitações de memória, pode ser forçado a escolher análise de tráfego à análise de conteúdo. A análise de tráfego consome menos recursos porque está em processamento cabeçalhos de pacote e não de conteúdo. Isso protege contra muitos ataques, mas não todos. Não por muito tempo. Um número substancial de assinaturas de ataque está escondido no conteúdo do pacote e a simples análise de tráfego é insuficiente para esses casos. [Anônimo, 2002]

Por fim, ambas as abordagens podem gerar falso-positivo, o que pode ter conseqüências sérias. Por exemplo, muitas pessoas instruem o sistema de detecção de invasão a emitir um bip quando um ataque está em progresso. Depois de muitos falsos-positivos, os membros da equipe técnica começaram a ignorar esses avisos. Ou seja, os avisos não farão mais sentido.

De fato, a detecção de invasão não está cem por cento evoluída. Independentemente do sistema escolhido, pode-se ter um ou mais problemas. Além disso, a maioria dos sistemas de detecção de invasão disponíveis publicamente são mais um conjunto de ferramentas do que soluções finais.

3 INTRODUÇÃO À POLÍTICA DE SEGURANÇA

Quando se fala em "ter uma Política de Segurança", não estamos falando somente de ter um firewall e um antivírus, estamos falando de definir regras de negócios, muito mais do que pensar pura e simplesmente em tecnologia. É focar os negócios, ou melhor, no sucesso dos negócios da empresa que receberá a Política de Segurança. Basicamente, uma política de segurança são regras e práticas que especificam ou regulam como um sistema ou organização provê serviços seguros protegendo os recursos críticos do sistema.

Existem basicamente duas filosofias: Proibitiva (tudo que não é expressamente permitido é proibido) e Permissiva (tudo que não é expressamente proibido é permitido). Uma política deve descrever exatamente quais operações são permitidas em um sistema. Qualquer operação que não esteja descrita de forma detalhada deve ser considerada ilegal ao sistema.

Política de Segurança não se compra pronta, pelo contrário, tem de ser desenvolvida especificamente para a empresa.

A maioria dos profissionais da área de segurança concordam que uma Política de Segurança nada mais é do que um documento formal que define as diretrizes e normas em relação à segurança e os procedimentos a serem seguidos por toda a empresa, sem exceção. Aliado a esse documento, a tecnologia vem agregar a segurança física e lógica dos dados e do capital intelectual da empresa (apesar de muitas empresas ainda acharem que os funcionários são nada mais do que simples trabalhadores).

A Política de Segurança deve ser definida em conjunto com a alta direção da empresa e deve ser válida para todos, desde o presidente até o mais baixo escalão. É estritamente necessário que seja aprovada e apoiada pelo mais alto executivo da empresa.

Voltando ao documento que compõe a Política de Segurança, ele não precisa ser complexo e muito técnico. Deve apresentar regras e procedimentos bem claros e definidos como, por exemplo, como deve ser o uso do e-mail, o uso da Internet apenas para fins comercial e em prol do desenvolvimento da empresa, etc.

A Política de Segurança deve focar na segurança dos dados confidenciais da empresa, como por exemplo, as informações dos nossos clientes são confidenciais e não podem sair do domínio de nossa empresa.

3.1 PRINCIPAIS ETAPAS DE ELABORAÇÃO

Para que serve uma norma ISO? Muitos de nós nunca fizemos esta pergunta, apesar de estarmos cotidianamente em contato com produtos certificados, empresas que que possuem o reconhecimento de organismos certificadores e, em alguns casos, relações comerciais business to business que só ocorrem pela presença mútua de conformidade com determinada norma. Sendo didático, podemos dizer que uma norma tem o propósito de definir regras, padrões e instrumentos de controle que dêem uniformidade a um processo, produto ou serviço.[Sêmola, 2003]

Mas por que é que tantas empresas buscam adesão a essas normas? Em uma economia tradicional e saudável, as empresas representam engrenagens de um sistema complexo onde há trocas constantes de bens e serviços, através da utilização da moeda, para concretizar as relações financeiras. Diante disso, é saudável que todas as empresas procurem uma base comum que facilite a interação e a confiança entre elas e, oportunamente, busquem elementos que as projetem mais, conquistando diferenciais competitivos. Essa é a lei de mercado.

As normas surgiram para sugerir bases comuns, cada qual com a sua especificidade, como vemos na ISO9001 – Qualidade e a ISO14000 – Meio Ambiente. São exemplos de critérios, padrões e instrumentos de controle, aplicáveis parcialmente ou totalmente em função da natureza de cada negócio, que acabaram formando cultura e recebendo o reconhecimento mundial de segmentos específicos.

À medida que os negócios passaram a aplicar tecnologia da informação para suportar processos importantes da empresa e, muitas vezes, os mais críticos e representativos para a sobrevivência e continuidade operacional, a proteção da informação passou a ser fator crítico de sucesso.

A tecnologia da informação deixou de ser coadjuvante e passou à protagonista no desenvolvimento corporativo, servindo de base comum para a troca eletrônica de informações e para a intermediação de transações comerciais. Estamos falando de um parque tecnológico cada vez mais integrado, porém heterogêneo, que mantém custodiadas informações de seus parceiros da cadeia produtiva, informações de clientes, fornecedores e ainda informações estratégicas da empresa.

O mercado atingiu um nível de automação, de compartilhamento de informações e de dependência tal que motivou a elaboração e compilação de uma norma específica para orientar a padronização de uma base comum voltada para a gestão de segurança da informação. A ela dá-se o nome de BS7799: parte 1, que possui uma versão brasileira, a NBR /ISO17799:1.

Para os que desconhecem o assunto, a primeira parte da Norma Britânica BS7799 deu origem à versão ISO17799:1 após avaliação e proposição de pequenos ajustes. Em seguida, foi traduzida e disponibilizada pela ABTN – Associação Brasileira de Normas Técnicas. Tem o objetivo de definir na parte 1 um Código de Prática para a Gestão de Segurança da Informação. São ao todo 10 domínios reunidos em 36 grupos que se desdobram em um total de 127 controles. Por se tratar de um código de prática, esta parte da norma não é objeto de certificação, mas recomenda um amplo conjunto de controles que subsidiam os responsáveis pela gestão corporativa de segurança da informação.

Domínios

- Política de Segurança
- Segurança Organizacional
- Classificação e Controle dos Ativos de Informação
- Segurança de Pessoas
- Segurança Física e do Ambiente
- Controle de acesso
- Gerenciamento das Operações e Comunicações
- Desenvolvimento e Manutenção de Sistemas
- Gestão da Continuidade do Negócio
- Conformidade

Por hora, a parte 2 da BS 7799, que especifica um framework de segurança chamado SGSI – Sistema de Gestão de Segurança da Informação, está em consulta pública a fim de gerar a versão ISO correspondente e será, quando concluída, a base para a certificação das empresas. Enquanto isso não ocorre, a alternativa é buscar a conformidade e a certificação da BS 7799, que já poderia representar uma pré-certificação para a ISO 17799.

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

Vêm a seguir as principais etapas para elaboração de uma Política de Segurança. De acordo, com as normas internacionais ISO 17799.[Axur, 2003]

1 - Definição da equipe responsável pela implantação e manutenção da segurança

O primeiro passo para a elaboração de uma Política de Segurança é a definição das equipes responsáveis pela elaboração, implantação e manutenção da política. É importante que sejam definidas claramente as responsabilidades de cada colaborador, e também que sejam envolvidas pessoas da alta administração da organização.

2 - Análise das necessidades e procedimentos utilizados pela empresa

Nessa etapa devem ser levantados os procedimentos executados na organização, que tenham relevância para a segurança das informações. Devendo ser considerados todos os processos informatizados ou não, que possam afetar direta ou indiretamente a segurança.

3 - Identificação dos processos críticos

Após o levantamento dos procedimentos, devem ser identificados os processos considerados críticos à organização, ou seja, aqueles que contém informações sensíveis aosnegócios da organização. Esses processos deverão ser tratados de maneira diferenciada na política de segurança.

4 - Classificação da Informação

Tem como objetivo assegurar que as informações recebam um nível apropriado de proteção. As informações devem ser classificadas para indicar a necessidade, as prioridades e o grau de proteção.

A informação tem variados graus de sensibilidade e criticidade. Alguns itens podem requerer um nível adicional de proteção ou manipulação especial. Um sistema de classificação de informação deve ser utilizado para definir um conjunto apropriado de níveis de proteção, e comunicar a necessidade de medidas especiais de manipulação. A seguir descrevemos um exemplo de tipos de classificação da informação:

- **Uso Confidencial** - aplicada às informações de grande valor a organização, se divulgadas indevidamente podem causar danos e prejuízos a organização ou a seus parceiros. Seu uso e disseminação devem ser restritos e controlados.

- **Uso Interno** - aplicada às informações restritas aos funcionários e a terceiros.

- **Uso Público** - Informações que podem ser divulgadas para o público em geral, incluindo clientes, fornecedores, imprensa.

Também é importante definir um conjunto de procedimentos para a manipulação das informações de acordo com o esquema de classificação adotado pela organização. Estes procedimentos precisam levar em consideração a informação na forma física e eletrônica. Para cada classificação, procedimentos de manipulação devem ser definidos para cobrir os seguintes tipos de atividades no processamento da informação: cópia; armazenamento; transmissão por correio, fax e correio eletrônico; transmissão por voz, incluindo telefones celulares, correio de voz, secretárias eletrônicas; destruição.

5 - Elaboração de normas e procedimentos para técnicos e usuários

Nesta fase serão definidas, de acordo com as informações levantadas nas fases anteriores, as normas e procedimentos que devem ser seguidos pelos funcionários, estagiários, técnicos e colaboradores da organização.

Relacionamos os principais tópicos, que devem ser abordados na definição das normas e procedimentos: acessos externos; acessos internos; uso da Intranet; uso da Internet; uso de correio eletrônico; política de uso e instalação de softwares; política de senhas; política

de backup; uso e atualização de anti-vírus; acesso físico; acesso lógico; trilhas de auditoria; padrões de configuração de rede (nome de máquinas, etc.).

6 - Definição de um plano de recuperação a desastres ou plano de contingência

Plano de contingência ou plano de recuperação, é um plano que contém as diretrizes que a empresa deve seguir em caso de parada no processamento, decorrente de desastre.

Tem como objetivo auxiliar na recuperação imediata do processamento das informações, levando em consideração a criticidade, de modo que minimize eventuais prejuízos à organização.

7 - Definição de sanções ou penalidades pelo não cumprimento da política

Nesta etapa são definidas as punições aplicadas aos funcionários, estagiários e colaboradores pelo não cumprimento da Política de Segurança.

Devem ser definidas punições de acordo com a cultura da organização, algumas empresas optam por criar níveis de punições relacionados aos itens da política, sendo a punição máxima a demissão ou desligamento do funcionário ou colaborador, pode-se também definir uma punição generalista que geralmente é a demissão ou desligamento aplicada a casos extremos.

O principal objetivo de se estabelecer punições ao não cumprimento da política de segurança, é incentivar os usuários a aderirem a política, e também dar respaldo jurídico a organização.

8 - Elaboração de um Termo de Compromisso

O termo de compromisso é utilizado para que os funcionários, estagiários e colaboradores se comprometam formalmente em seguir a política de segurança, tomando ciência das sanções e 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

anualmente. O termo de compromisso deve ser implantado como um aditivo ao contrato de trabalho, para tanto deve ser envolvida a área jurídica da organização na sua revisão.

9 - Comunicado da diretoria / presidência aos funcionários

Para reforçar o aval da alta administração da organização, e reafirmar a importância da segurança, é importante que antes da implantação da Política de Segurança seja feito um comunicado da diretoria ou presidência, aos funcionários e colaboradores, comunicando a implantação da Política de Segurança na organização.

10 - Divulgação da Política

Um dos maiores desafios de uma Política de Segurança é conseguir grande aderência dos funcionários, isso acontece muitas vezes devido a cultura da organização e a falta de envolvimento da alta administração.

Para resolver esse problema utilizamos a divulgação como instrumento de conscientização dos funcionários e colaboradores, da importância da segurança das informações e da importância da adoção de uma política.

A Política de Segurança deve ser de conhecimento de todos os funcionários, estagiários e colaboradores da organização, portanto deve ser amplamente divulgada, inclusive e principalmente para novos funcionários e novos colaboradores.

Os métodos de divulgação da Política de Segurança variam de acordo com a empresa, abaixo listamos alguns dos métodos de divulgação mais utilizados: campanhas internas de conscientização; palestras de conscientização para os funcionários e colaboradores; destaque em jornal e folhetos internos; destaque na Intranet da organização; criação de manual em formato compacto e com linguagem acessível aos usuários; disponibilizar na Intranet ou na rede, em local comum a todos, a política na íntegra para consultas.

Independente do método de divulgação utilizado, uma característica fundamental é a linguagem utilizada, que deve ser de fácil entendimento, e a leitura deve ser estimulante

aos usuários. Lembre-se de que a política de segurança e todo o material de divulgação será direcionado tanto ao pessoal técnico quanto aos usuários, estagiários e colabores da empresa.

11 - Implantação

A implantação é a etapa final da política de segurança. Consiste na aplicação formal das regras descritas na política da organização, e a assinatura do termo de compromisso.

Deve ser realizada de forma gradativa e obrigatoriamente após ao programa de divulgação e conscientização dos funcionários.

12 - Revisão da Política

A política de segurança deve ser revisada periodicamente, para mantê-la atualizada frente as novas tendências e acontecimentos do mundo da segurança da informação.

O intervalo médio utilizado para a revisão de uma política de segurança é de um ano, porém deve ser realizada uma revisão sempre que forem identificados fatos novos não previstos na política de segurança vigente, que possam impactar na segurança das informações da organização.

3.2 BASES DE UMA POLÍTICA DE SEGURANÇA

Talvez algumas palavras nos ajudem compreender tamanha complexidade, e se tivesse de escolher uma para representar o desafio de uma solução de segurança – capaz de sinalizar todos os aspectos associados seria claramente: CONTROLE. [Sêmola, 2003]

Controle é absolutamente tudo o que se quer, claro sob a ótica da aplicação. Como, administrar as vulnerabilidades e reduzir os riscos. É com controle que podemos, por exemplo: autorizar ou bloquear pessoas que tentarem entrar em ambientes físicos restritos; registrar as tentativas de acesso ao site Internet; mensurar o prejuízo causado por ocorrências de quebra de segurança, dentre outras.

Com o apoio do Plano Diretor de Segurança, formaremos uma estrutura sólida, porém dinâmica e flexível que dará sustentação para a empresa construir um modelo de gestão de Segurança ajustado para superar os atuais e reagir adequadamente aos futuros desafios associados ao controle do risco de segurança da informação.

3.2.1 PDCA

Seguindo o modelo de organização proposto pela Norma BS7799 parte 2, que fora inspirada originalmente no modelo PDCA adotado na ISO 9001, e que tem sinergia com os estudos conceituais a segurança, temos as seguintes fases

- PLAIN (Planejamento)
- DO (Implementar)
- CHECK (Analisar)
- ACT (Monitorar)

Em geral podemos dizer que é necessário Planejar as ações executivas (Plano Diretor de Segurança) para realizar investimentos adequados e orientar o Administrador de Segurança (Security Office). Da mesma forma, é preciso Analisar os fatores de risco do negócio que apontarão as características e levantarão informações para apoiar o dimensionamento das ações. Implementar os controles físicos, tecnológicos e humanos é a próxima etapa, seguida da fase de Monitoramento, que fará a ligação com a primeira, subsidiando-a com informações de novas vulnerabilidades, ameaças e riscos.

3.2.1.1 Fases do PDCA

3.2.1.1.1 Planejar (Plain)

Compreende as atividades que objetivam definir arquiteturas, ações, atividades, alternativas de continuidade e critérios, abrangendo todo ciclo de vida da informação:

manuseio, armazenamento, transporte e descarte, aplicáveis desde os níveis mais estratégicos aos níveis operacionais. Como exemplos:

- Plano Diretor de Segurança
- Plano de Continuidade de Negócios
- Política de Segurança da Informação

3.2.1.1.2 Analisar (Check)

Compreende atividades que buscam gerar um diagnóstico de segurança, através do mapeamento e da identificação de particularidades físicas, tecnológicas e humanas da empresa como um todo ou de perímetros menores, vulnerabilidades, ameaças, riscos e impactos potenciais que poderão se refletir no negócio da empresa. Por exemplo:

- Analise de Risco
- Teste de Invasão

3.2.1.1.3 Implementar (Do)

Compreende atividades que aplicam mecanismos de controle nos ativos físicos, tecnológicos e humanos, que possuam vulnerabilidades, buscando eliminá-las, isso quando possível e viável, ou administrá-las, a fim de aumentar o nível de segurança do negócio. Esta fase que materializa as ações tidas como necessárias na Análise e organizadas pelo Planejamento. Por exemplo, algumas atividades:

- Implementação de Controles de Segurança
- Treinamento e Sensibilização em Segurança

3.2.1.1.4 Monitorar (Act)

Compreende atividades que visam gerir o nível de segurança, através de dispositivos que monitoram índices e indicadores, canalizando novas percepções de mudança

física, tecnológica e humana que provocam oscilação do grau de risco, a fim de adequar as ações de segurança ao contexto. Esta fase representa o elo de ligação com a primeira fase, formando assim um ciclo contínuo. Dando vida ao verdadeiro processo de gestão dinâmica.

- Equipe de Resposta a Incidentes
- Administração e Monitoração de Segurança

3.3 PLANO DIRETOR DE SEGURANÇA (PDS)

Planejamento é o fator crítico de sucesso para a iniciativa de gerir a segurança da informação e o Plano Diretor de Segurança é justamente o elemento específico para este fim. Ele é mais do que uma rubrica orçamentária destinada a investimentos tecnológicos, como sugere o já tradicional Plano Diretor de Informática, o PDS tem de ser dinâmico e flexível para suportar as novas necessidades de segurança que sugerem em virtude da velocidade como o contexto corporativo muda.

O PDS representa a bússola que irá apontar o caminho e os passos que irão formar o mosaico da solução e suprir as necessidades da segurança do negócio, conduzindo-o a operar sob risco controlado. È importante dizer que o PDS é específico para cada empresa, e não existe um PDS padrão capaz de atender a todos segmentos do mercado.

3.3.1 MODELAGEM DO PLANO DIRETOR DE SEGURANÇA

A modelagem do PDS está diretamente associada a ações de levantamento de informações do negócio, identificar ameaças, vulnerabilidades, riscos e impactos potenciais ao negócio. É fundamental entender os desafios do negócio, conhecer os planos de curto, médio e longo prazos. A modelagem consiste em 6 etapas:

1. Identificação dos processos do negócio;
2. Mapeamento da Relevância;

3. Estudos de impactos CIDAL;
4. Estudo de prioridades GUT;
5. Estudo de perímetros;
6. Estudo de atividades;

3.4 PLANO DE CONTINUIDADE DE NEGÓCIOS (PCN)

Garantir a continuidade do processo e informações vitais à sobrevivência da empresa, no menor espaço de tempo possível, com o objetivo de minimizar os impactos do desastre. Com este propósito e formado pelas etapas de Analise de Impactos no Negócio, Estratégias de Contingência e três planos de contingência propriamente. O PCN deve ser elaborado com o claro objetivo de contingenciar situações e incidentes de segurança que não puderem ser evitados.

Segundo o DRI – Disaster Recovery Institute, de cada cinco empresas que possuem interrupção nas suas operações por uma semana, duas fecham suas portas em menos de três anos. Seguem as etapas de modelagem de um PCN:

1. Analise de Impactos no Negócio (BIA);
2. Estratégias de Contingência;
    - Hot-site;
    - Warm-site;
    - Realocação de operações;
    - Bureau de serviços;
    - Acordo de reciprocidade;

- Cold-site;

3. Planos de Contingência;
    - Plano de administração de crise;
    - Plano de continuidade operacional;
    - Plano de recuperação de desastres;

4 ESTUDO DE CASO

4.1 AMBITO

A Empresa X varejista, tem 12 unidades em Minas Gerais. Sendo o CPD (Centro de Processamento de Dados) no escritório central em Barbacena, Minas Gerais. Possui uma linha dedicada via *Fibra Óptica* (Telemar). Os negócios da empresa são baseados no Sistema chamado *XInfo*, sendo este aplicativo executado sobre o protocolo Telnet de comunicação. O *Sistema XInfo* abrange todas as áreas da empresa. Cada usuário tem seu nível de visão,

baseado na sua função exercida na Empresa. Portanto o *Sistema XInfo,* é um possível alvo para invasões e posteriormente roubo de informações valiosas ou alterações. Causando enormes perdas financeiras para a empresa em questão. A Empresa X Varejista é uma empresa de comércio e distribuição em geral.

4.1.1 SITUAÇÃO ATUAL DA EMPRESA X VAREJISTA

A empresa X Varejista não possui hoje Política de Segurança e nenhum Plano de Continuidade de Negócios. Possui um Firewall na conexão com a linha dedicada Telemar, um no CPD no escritório central. Na empresa estão lotados 950 funcionários em 4 departamentos, sendo eles: Administração, Financeiro, CPD e R.H (Recursos Humanos). Estes funcionários trabalham 30 % na escritório e 70 % nas lojas. Como explicado antes, cada funcionário tem seu nível de visão no *XInfo,* de acordo com o departamento que ele está lotado e a sua função.

Na empresa temos 156 microcomputadores (Workstation), sendo a plataforma predominante a Microsoft Windows 98Se. Os servidores da empresa têm a plataforma Microsoft Windows 2000 Server. Todos os microcomputadores estão equipados com drive Disco Flexível, mas somente alguns têm CD-ROM.

Todos os departamentos possuem conexão à rede mundial a Internet via Proxy, as Workstation não possuem monitoração seja ela de e-mail ou mesmo bloqueio de acesso a Web sites Pornôs.

A situação atual é preocupante, segundo os Diretores da empresa no ano de 2003 foram contabilizados até meiados de novembro, 70 detecções de vírus.

4.2 POLÍTICA DE SEGURANÇA

4.2.1 RESPONSABILIDADES GERAIS

Responsável pelo desenvolvimento da política de segurança será de responsabilidade do Secutity Office com o apoio dos integrantes do Comitê Corporativo de Segurança da Informação.

Os gerentes são responsáveis pela proteção dos bens como, empregados, propriedade física e informações relativas a condução do negócio. São responsáveis pela identificação e proteção de todos os bens dentro de sua área de controle, por garantir que seus empregados entendam suas obrigações dentro do âmbito da empresa.

Os colaboradores são responsáveis por garantir a confidencialidade das informações bem como, garantir a excelência das sua obrigações na empresa.

4.2.2 ANÁLISE DE RISCO

A análise de risco consiste em um processo de identificação e avaliação dos fatores de risco presentes e de forma antecipada no Ambiente Organizacional, possibilitando uma visão do impacto negativo causado aos negócios. Através da aplicação desse processo, é possível determinar as prioridades de ação em função do risco identificado, para que seja atingido o nível de segurança desejado pela Organização. Proporciona também informações para que se possa identificar, antecipadamente, o tamanho e o tipo de investimento necessário para prevenir os impactos na Organização causados pela perda ou indisponibilidade dos recursos fundamentais para o negócio.[Calheiros, 2002]

4.2.2.1 Gap Analysis Light

Gap Analysis Light, é um instrumento que irá nos auxiliar a perceber o grau de aderência de sua empresa em relação às recomendações de Segurança da Informação a norma NBR ISO/IEC 17799, ver anexo B.

Esta análise é rápida, baseado em perguntas objetivas com pontuações associadas que irão revelar o índice de conformidade. O teste é baseado em 40 questões com uma visão geral de todos segmentos em que a NBR ISO/IEC 17799. [Sêmola, 2003]

Pontuação será a seguinte para cada resposta:

A – some 2 pontos;

B – some 1 ponto;

C – não some e nem subtraia pontos.

A amplitude dos assuntos abordados pela norma e, obviamente, a complexidade em planejar, implementar e gerir todos os controles de segurança, a fim de proteger os princípios básicos da segurança, confidencialidade, integridade e disponibilidade das informações.

O resultado da aplicação do questionário na Empresa X, foi direcionado aos gerentes de departamentos. Foram distribuídos 5 questionários, gerente de Financeiro, Contabilidade, R.H., Administração, Compras. O resultado em uma pontuação mínima de 0 e máxima de 80 pontos, foi 26 pontos, para determinar o resultado de forma correta, foi realizada uma média de todos os questionários.

Este resultado implica que a situação atual não é confortável para a empresa. A segurança não está sendo tratada como prioridade e indica ausência ou ineficácia de muitos dos controles recomendados pela norma NBR ISO/IEC 17799. As causas podem ser o desconhecimento dos riscos e a falta de sensibilização dos gerentes e da alta administração.

4.2.3 IDENTIFICAÇÃO DOS PROCSSOS CRÍTICOS

Nesta etapa como já foi dito na sessão 3.1, é a identificação dos riscos sensíveis aos negócios da empresa.

- Departamento Financeiro:
    - Risco de vazamento de informações;
        - Contas;
    - Risco de erro humano;
        - Digitação;
    - Acesso a Internet;
        - Vírus;
- Departamento Contábil:
    - Risco de vazamento de informações;
        - Conta de cliente;
    - Risco de erro humano;
        - Digitação;
    - Acesso a Internet;
        - Vírus;
- Departamento R.H:
    - Risco de vazamento de informações;
        - Salários;
    - Risco de erro humano;
        - Digitação;

- Acesso a Internet;
  - Vírus;

- Departamento Administrativo:
  - Risco de vazamento de informações;
    - Processos jurídicos;
  - Risco de erro humano;
    - Digitação;
  - Acesso a Internet;
    - Vírus;

- Departamento Compra:
  - Risco de vazamento de informações;
    - Valor de licitações;
  - Risco de erro humano;
    - Digitação;
  - Acesso a Internet;
    - Vírus;

Os riscos são comuns para todos os departamentos, pois eles usam o mesmo Software de gerenciamento o *XInfo* e utilizam a mesma configuração de Proxy.

4.2.4 CLASSIFICAÇÃO DAS INFORMAÇÕES

A classificação das informações é muito importante pois a parti dela nos poderemos avaliar onde será enfoque maior e quais controles adotar.

- Departamento Financeiro:
  - Confidencial:
    - Código de processos;
    - Valor de processos;
  - Interno:
    - Contatos;
    - Planejamentos;
    - Plano de vendas;
  - Publico:
    - Vendas;
- Departamento Contábil:
  - Confidencial:
    - Lucro líquido;
    - Contas de clientes
    - Debêntures;
  - Interno:
    - Financiamento;

        - Movimentação de bancos;
    - Publico:
        - Balanço contábil;

- Departamento R.H:
    - Confidencial:
        - Salários;
        - Informações pessoais;
        - Notificação de demissão;
        - Promoções de funcionários
    - Interno:
        - Quantidade de funcionários;
        - Seleção interna;
        - Calendário;
    - Publico:
        - Quantidade de funcionários;
        - Legislação trabalhista;
        - Benefícios que a empresa concede;
        - Abertura de vagas;

- Departamento Administrativo:
    - Confidencial:

        - Contratos;
        - Processos Jurídicos;
    - Interno:
        - Planejamento;
        - Política da empresa;
    - Publico:
        - Política da empresa;
- Departamento Compra:
    - Confidencial:
        - Contratos;
        - Valor das licitações;
    - Interno:
        - Licitações;
        - Compra;
    - Publico:
        - Abertura de licitações;

4.2.5 NORMAS E PROCEDIMENTOS

4.2.5.1 Política de Senhas

Uma senha segura deverá conter no mínimo 6 caracteres alfanuméricos (letras e números) com diferentes caixas.

Para facilitar a memorização das senhas, utilize padrões mnemônicos. Por exemplo:

eSus6C (eu SEMPRE uso seis 6 CARACTERES)

9SSgianc (9 Senhas Seguras garantem integridade a nossa corporação)

As senhas terão um tempo de vida útil pré-determinado pela equipe de segurança (90 dias), devendo o mesmo ser respeitado, caso contrário o usuário ficará sem acesso. Todas as senhas serão testadas diariamente pela equipe de segurança em busca de fragilidades.

Senhas como o nome do usuário, datas de aniversários, combinações simples como abc123, não são consideradas senhas seguras e por isso,dever ser evitadas.

Observações:
- Sua senha não deve ser jamais passada a ninguém, nem mesmo da equipe de segurança. Caso desconfie que sua senha não está mais segura, sinta-se à vontade para mudá-la, mesmo antes do prazo determinado de validade.

- Tudo que for executado com a sua senha será de sua inteira responsabilidade, por isso tome todas as precauções possíveis para mantê-la secreta.

4.2.5.2 Política de uso de e-mail

Nosso servidor de e-mail estão protegidos contra vírus e códigos maliciosos, mas algumas atitudes do usuário final são requeridas:

- Não abra anexos com as extensões .bat, .exe, .src, .lnk e .com se não tiver certeza absoluta de que solicitou esse e-mail;

- Desconfie de todos os e-mails com assuntos estranhos e/ou em inglês. Alguns dos vírus mais terríveis dos últimos anos tinham assuntos como: ILOVEYOU, Bug Beer, etc;

- Não reenvie e-mails do tipo corrente, aviso de vírus, avisos da Microsoft/AOL/Symantec, criança desaparecida, criança doente, pague menos em alguma coisa , não pague alguma coisa, etc;

- Não utilize o e-mail da empresa para assuntos pessoais;

- Não mande e-mails para mais de 10 pessoas de uma única vez (to, cc, bcc);

- Evite anexos muito grandes;

- Utilize sempre sua assinatura criptográfica para troca interna de e-mails e quando necessário para os e-mails externos também.

4.2.5.3 Política de uso de Internet

O uso e acesso a Internet será restrito aos seguintes tópicos:

- Somente navegação de sites é permitida. Casos específicos que exijam outros protocolos deverão ser solicitados diretamente a equipe de segurança com prévia autorização do supervisor do departamento local;

- Acesso a sites com conteúdo pornográfico, jogos, bate-papo, apostas e assemelhados estará bloqueado e monitorado;

- É proibido o uso de ferramentas P2P (kazaa, Morpheus, etc);

- É proibido o uso de IM (Instant messengers) não homologados/autorizados pela equipe de segurança;

Lembrando novamente que o uso da Internet estará sendo auditado constantemente e o usuário poderá vir a prestar contas de seu uso.

4.2.5.4 Política de uso da Estação de Trabalho

Lembramos que sua estação é sua ferramenta de trabalho, mas também é um importante componente de segurança. Por isso observe as seguintes orientações:

- Não instale nenhum tipo de software / hardware sem autorização da equipe técnica ou de segurança;

- Não tenha MP3, filmes, fotos e softwares com direitos autorais ou qualquer outro tipo de pirataria;

- Mantenha na sua estação somente o que for supérfulo ou pessoal. Todos os dados relativos à empresa devem ser mantidos no servidor, onde existe um sistema de backup diário e confiável. Caso não saiba como fazer isso, entre em contato com a equipe técnica.

4.2.5.5 Política de acesso ao servidor

Aos funcionários o acesso ao servidor será de acordo com seu login, ou seja, seu acesso depende de seu nível de usuário. Voltamos a lembrar, mantenha sua senha segura para evitar problemas.

Aos terceiros somente terá acesso mediante a pedido escrito por parte do gerente do departamento. Onde será concebido um login e uma senha provisória.

Lembramos que o acesso ao servidor será monitorado.

4.2.5.6 Política de acesso de terceiros

O acesso de terceiros será permitida somente após assinar o termo de confidencialidade.

4.2.5.7 Política de acesso à Internet por terceiros

Aos terceiros será imposta a mesma **Política de uso de Internet**.

4.2.5.8 Política de Monitoração de Logs

Fica estabelecido para fins de monitoração, é liberado o uso de leitura de Logs.

4.2.5.9 Política de uso de Drive de Disco flexível

No âmbito da empresa não será permitido o uso de discos flexíveis, sendo que, os dados mais importantes devem ser armazenados no nosso servidor.

4.2.5.10 Política de uso de Drive de CD-ROM

No âmbito da empresa não será permitido o uso de CD-ROM, sendo que, os dados mais importantes devem ser armazenados no nosso servidor.

4.2.6 PLANO DE CONTIGÊNCIA

Seguindo a análise de risco e a classificação das informações segundo seu critério de avaliação, podemos avaliar os ativos segundo sua importância para a continuidade dos negócios da empresa.

A estratégia adotada será a **Hot-site**, que é como o próprio nome já diz uma estratégia quente, pronta para entrar em operação assim que uma situação de risco ocorrer. O tempo de operacionalização desta estratégia está diretamente ligado ao tempo de tolerância a falha do objeto. No *XInfo*, por exemplo, o tempo de tolerância seria alguns milissegundos, garantindo assim a disponibilidade do serviço.

Isso por que todos os processos da empresa são dependentes uns dos outros, assim sendo esta estratégia é a que melhor se aplica às necessidades reais da empresa.

4.2.7 PENALIDADES ADOTADAS AO NÃO CUMPRIMENTO DA POLÍTICA

O não cumprimento dessas políticas acarretará nas seguintes penalidades que vão obedecer ao nível de risco da atividade, segue Tabela 1:

Nº.	Atividade	Punição
01	Uso de e-mail de forma maliciosa,contrariando a política de segurança de uso de e-mail.	Suspensão temporária ou definitiva da conta de e-mail.
02	Senhas, se contrariar a política de segurança de senhas.	Suspensão temporária de 1 a 2 semanas.
03	Uso de Internet, se contrariar a política da segurança de uso de Internet	Suspensão temporária ou definitiva do acesso à Internet.
04	Uso de Internet, se for início de infecção de vírus, invasão expondo a organização da empresa	Suspensão definitiva do acesso à Internet ou demissão por justa causa. Será aberto uma sindicância para apurar o fato.
05	Quebra de confidencialidade, vazamento de informações, espionagem industrial.	Demissão por justa causa. Será aberto uma sindicância para apurar o fato.
06	Uso da Estação de trabalho, se contrariar a política de segurança de uso de Estação de trabalho.	Suspensão temporária de 1 a 2 semanas.

Tabela 1 - Penalidades e punições

4.2.8 TERMO DE COMPROMISSO

Será criado um termo de compromisso, que todos os funcionários, estagiários se comprometem formalmente em seguir a política de segurança, tomando ciência das punições as seu não cumprimento. Ver Anexo C.

4.2.9 COMUNICADO DA DIRETORA

Para reforçar o aval da direção, e reafirmar a importância da segurança, é importante seja feito um comunicado da diretoria ou presidência, aos funcionários e colaboradores, comunicando a implantação da Política de Segurança na organização. Ver Anexo D.

4.2.10 DIVULGAÇÃO DA POLÍTICA DE SEGURANÇA

Será feita a divulgação da política por meio de e-mail, cartazes, folders. Ver Anexo E.

4.2.11 IMPLANTAÇÃO

Será determinado o dia que a Política de segurança for implantada.

4.2.12 REVISÃO DA POLÍTICA DE SEGURANÇA

Será determinada, seis meses após a implantação, para a revisão. E depois da primeira revisão, fica estipulado revisão de seis em seis meses.

4.3 SEGURANÇA ORGANIZACIOAL

4.3.1 COMITÊ CORPORATIVO DE SEGURANÇA DA INFORMAÇÃO

Será criado o Comitê Corporativo de Segurança da Informação, que será composto do gerente de cada departamento e como presidente deste Comitê o Security Office. Este comitê terá uma estrutura, funções e responsabilidades.

A estrutura do comitê é composta de Coordenação Geral de Segurança, Coordenação de Segurança, Planejamento e Avaliação, Controle e Execução. As funções e responsabilidades, são distribuídas conforme a posição na estrutura do comitê, por exemplo, membro lotado no nível de Controle terá que realizar análises de risco, conduzir ações de auditoria e monitoramento dentre outras.

4.3.2 FÓRUM DE DISCUSSÃO

Será criado um Fórum de discussão, onde todos os funcionários poderão ter livre diálogo com o Security Office.

4.3.3 TERCEIROS

Sempre que necessitar de serviços de terceiros, deverá ser efetuada uma análise de risco específica para determinar as implicações de segurança e requisitos de controles. A identificação de risco de acessos será feita com base em acesso físico o lógico.

Para os contratos de prestação de serviços, deveram existir obrigações de segurança a serem observadas.

4.4 CLASSIFICAÇÃO E CONTROLE DE ATIVOS

4.4.1 INVENTÁRIO DOS ATIVOS

O inventário dos ativos é um aspecto da gestão de riscos. Uma organização necessita identificar os seus ativos e o seu valor relativo e importância deste ativo. Baseado nestas informações a organização pode oferecer níveis adequados a todos os seus ativos. Exemplos de ativos:

- Ativos de informação: Banco de dados;
- Ativos de Software: Aplicativo *XInfo;*

4.4.2 CLASSIFICAÇÃO DA INFORMAÇÃO

O objetivo principal deste controle é garantir que a informação receba um nível adequado de proteção, para isso a classificação deve indicar a necessidade, prioridade e grau de proteção das informações. Aplica-se tanto no formato físico e eletrônico.

4.5 SEGURANÇA DE PESSOAL

O objetivo da segurança de pessoal é reduzir os riscos de erro humano, roubo, fraude ou mau uso. Responsabilidades de segurança devem ser tomadas no momento de recrutamento, incluindo no contrato, monitorizado durante o emprego.

4.5.1 ACORDO DE CONFIDENCIALIDADE

Será firmado um acordo de confidencialidade entre a empresa e funcionários e terceiros. O acordo será elaborado pelo departamento jurídico da empresa. Ver anexo F.

4.5.2 EDUCAÇÃO DA SEGURANÇA

Todos os funcionários deverão receber notas sobre a política de segurança. Será determinado períodos de treinamento para todos funcionários e terceiros, que estejam trabalhado pela empresa.

4.6 SEGURANÇA FÍSICA E AMBIENTAL

O objetivo é prevenir o acesso não autorizado, dano ou interferência da informação ou das instalações da empresa.

4.6.1 PERÍMETRO

Será estabelecido um perímetro da sala dos servidores. Para acesso à sala dos servidores, será disponibilizado uma copia da chave da porta e o código do alarme para o funcionário que realmente necessite de acesso aquela sala. Esta copia será pessoal e intransferível, o código será sempre trocado pelo Security Office, ficando o mesmo responsável a notificação para os funcionários envolvidos.

4.6.2 PROTEÇÃO DO LUGAR E EQUIPAMENTOS

Serão instalados extintores no perímetro da sala dos servidores e em pontos estratégicos de acordo com o técnico de segurança do trabalho.

Para o interior da sala dos servidores, será instalado um sistema especial de refrigeração para caso de incêndio.

4.6.3 FONTES DE ALIMENTAÇÃO

Será instalado No-break em todos os servidores.

4.6.4 MANUTENÇÃO DOS EQUIPAMENTOS

Será de responsabilidade do departamento de Informática, podendo contratar terceiros para efetuar serviços mais demorados.

Os funcionários deverão comunicar ao departamento de informática qualquer problema técnico, que esteja acontecendo.

4.6.5 CONTROLES GERAIS

Destinados a prevenir comprometimento ou roubo recursos de informações.

4.6.5.1 Controle contra Software malicioso

Objetivo proteger a integridade do software e da informação. É necessário prevenir e detectar a introdução de software malicioso. Os usuários devem estar cientes dos perigos do software malicioso ou não autorizado e os gestores devem, se apropriado, introduzir controles especiais para detectar e prevenir a sua introdução.

4.6.5.2 Manutenção da casa (Back-up)

O objetivo é manter a integridade e a disponibilidade do processamento da informação e serviços de comunicação. Procedimento rotineiros devem ser adotados para efetuar uma estratégia de back-up eficiente.

4.6.5.2.1 Back-up da Informação

O back-up será feito diariamente, sendo guardado fora das dependências da empresa. Por motivo de segurança, o lugar mais indicado é um cofre de um banco.

4.6.6 GERÊNCIA DA REDE

O objetivo é garantir salvaguarda das informações em redes e proteção da infra-estrutura de suporte.

A gerencia de rede temos a maior fronteira e que temos que ter maior atenção, especialmente às informações sensíveis trafegando em redes públicas.

4.6.7 TROCA DE INFORMAÇÕES

4.6.7.1 Correio eletrônico

Devemos considerar os riscos inerentes a informação, obedecer a política de uso de e-mail.

4.7 CONTROLE DE ACESSO

Terceiros antes de ter acesso à dependência da empresa deverá assinar o termo de confidencialidade.

O acesso será controlado para a sala dos servidores como já foi dito na seção 4.6.1. Terceiros somente terão acesso à sala dos servidores acompanhado por um gerente.

4.8 GERENCIAMENTO DE OPERAÇÕES E COMUNICAÇÕES

Visa proteger os serviços de rede. O acesso a serviços da rede interna e externa deve ser controlado.

Para isso, temos que nos apoiar na política de segurança. O aceso a rede interna depende da senha do usuário, logo o acesso a Internet, será monitorado pelo departamento de informática.

Os serviços de gerenciamento de redes devem garantir:

- Autenticação de utilizadores e equipamentos;
- Controle de acesso a rede
- Sistema de gestão de senhas

4.9 DESENVOVIMENTO E MANUENÇÃO DE SISTEMAS

O objetivo é garantir que a segurança da informação seja incluída no Sistema de informação.

Nesta etapa é garantir no Sistema de Informação alguns aspectos como o não repúdio, autenticidade, legalidade, dentre outros.

4.10 GERÊNCIA DA CONTINUIDADE DOS NEGÓCIOS

Para reagir a interrupções nas atividades do negócio e proteger as atividades críticas dos efeitos de grandes perdas ou desastres, temos que criar um plano de continuidade dos negócios.

4.11 CONFORMIDADE

Nesta etapa, observamos os termos legais, para evitar qualquer violação de lei cível ou criminal regulamento ou clausula contratual.

Devemos observar os seguintes aspetos:

- Identificação de legislação aplicável

- Direitos de propriedade intelectual
- Proteção de dados e privacidade de informação pessoal

5 CONCLUSÃO

5.1 REVISÃO

Na introdução foi exposto o escopo deste trabalho, a sua importância na atualidade e foi feita uma breve introdução ao ciclo de vida da informação. Na Revisão Bibliográfica, foi realizada uma revisão dos conceitos de segurança da informação, redes, identificação de, suas vulnerabilidades, os ataques mais comuns, formas de defesa como firewalls,Ids, logs de sistemas. Na Introdução à Política de Segurança, vimos quão importante, é a informação para uma empresa e por isso fizemos uma revisão dos pilares da segurança, confidencialidade, disponibilidade e autenticidade. Bem como a importância política de segurança nos dias atuais, as etapas para construção de uma política confiável e que não fuja

da cultura da empresa, e para tanto, nos baseamos na norma NBR ISO/IEC 17799, que é um código para boas práticas de segurança da informação. Nela contem 127 controles aplicáveis a empresa, de acordo com o nível de risco.

E no Capitulo referente ao estudo de Caso, foi determinado as responsabilidades, além de ter sido realizada uma análise de risco na empresa X Varejista e baseado nela apliquei a norma NBR ISO/IEC 17799, contendo todos os controles necessários para a segurança da informação da empresa em questão.

No anexo A, consta uma pesquisa da segurança da informação em empresas na versão 8 e no ano de 2003. Esta pesquisa é assinada pela empresa de consultoria de segurança Modulo Security S/A. No anexo B, consta o questionário apresentado para análise de risco, o Gap Analysis Light. No anexo C, temos um exemplo de Termo de Compromisso. No anexo D, temos um exemplo de Comunicado da Diretoria. No anexo E, temos um exemplo de panfleto para divulgação da política de segurança. E no anexo F, consta um Termo de Confidencialidade.

5.2 CONCLUSÃO

Na elaboração desse trabalho constatou-se que a Segurança de Informações é o elemento chave dentro da organização: envolve aspectos técnicos, humanos e organizacionais, sendo fundamental a definição e existência de uma Política para efetiva proteção das informações. O objetivo da segurança da informação é proteger a empresa contra riscos, apoiada em uma Política de Segurança e uma estrutura de Segurança, onde se podem identificar as vulnerabilidades e os controles para a proteção das informações.

Percebe-se que a tarefa de implementação das principais práticas de segurança da informação na empresa (NBR ISO/IEC 17799), não é uma tarefa fácil. Todavia, o ato de uma conscientização ampla da necessidade da adoção das práticas de segurança constitui-se em um grande passo tomado pela direção. Sempre lembrando que o melhor caminho não é a implantação compulsória, e sim a disseminação da cultura entre cada um dos ambientes da

empresa. Uma vez que, nem todos os colaboradores e funcionários entendem a necessidade de mecanismos de controle e de gerenciamento da segurança da informação.

Esse foi o objetivo principal deste trabalho foi demonstrar a aplicação da norma NBR ISO/IEC 17799 dentro do âmbito de uma empresa, indicando controles necessários para garantirmos um nível maior de Segurança da Informação. Visto que, todo este movimento deve ser em prol da defesa e fortalecimento do patrimônio intangível – a informação -, um dos bens mais valiosos de qualquer empresa.

5.3 RECOMEDAÇÕES

Após a elaboração deste estudo, minhas recomendações futuras são, a implantação deste padrão em outras empresas e na empresa X Varejista, um estudo mais a fundo na norma NBR ISO/IEC 17799 e BS 7799 2. Visto que, a BS 7799 parte 2 especifica um SGSI e o mundo da segurança da informação nunca para. Sempre teremos alguém descobrindo novas técnicas de invasão e nós que cuidamos da Segurança da informação, tentado impedi-los.

REFERÊNCIAS BIBLIOGRÁFICAS

[NBR ISO/IEC 17799] Coelho, Paulo.Tecnologia da Informação. Código práticas para gestão da segurança da informação - Uma versão resumida e comentada . Paulo Coelho.

[Sêmola, 2003]Sêmola, Marcos. **Gestão da Segurança Informação Uma visão executiva**. 2ª ed. Rio de Janeiro, RJ: Campus, 2003.

[Caruso & Steffen, 1999]Caruso, Carlos A. A. e Steffen, Flávio Deny. **Segurança em Informação e de Informações**. 2ª ed. São Paulo, SP: Senac, 1999.

[Tanenbaum, 1994]Tanenbaum, Andrew S. **Rede de Computadores**, 3ª ed. Rio de Janeiro, RJ: Campus, 1994.

[Gil, 1998] Gil, Antônio de Loureiro. **Segurança em Informática**, 2ª ed. São Paulo, SP: Atlas, 1998.

[Anônimo, 2001] Anônimo. **Segurança Máxima**, 3ª ed. Rio de Janeiro, RJ: Campus, 2001.

[Anônimo, 2002] Anônimo. **Hackers – Como ser e como evitá-los**, 3ª ed. Rio de Janeiro, RJ: Campus, 2002.

[Bauer, 2002] Bauer, Michael *Building Secure Servers with Linux*. Paperback, 2002.

[Neto, 2003] Neto, Cláudio de Lucena. **Segurança da Informação Corporativa: Aspectos e Implicações Jurídicas**, 2003. Monografia - Centro de Ciências Jurídicas, Universidade Estadual da Paraíba, Campina Grande.

[Seleguim, 2002] Seleguim, Guilherme Cestarolli. **Segurança da Informação: Perigos do Mundo Virtual**,2002. Monografia – Faculdade de Analise de Sistemas, Ponfícia Universidade Católica de Campinas, Campinas.

[Pelissari, 2002] Pelissari, Fernando Antônio Brossi. **Segurança de redes e Análise sobre a conscientização das empresas da cidade de Bauru (SP) quanto ao problema**, 2002. Monografia - Faculdade de especialização em Informática, UNESP, Bauru.

[Calheiros, 2002] Calheiros, Rosemberg Faria. **Segurança de informações nas empresas – uma prioridade corporativa**, 2002. Monografia - Universidade do Rio de Janeiro, Rio de Janeiro.

[Brasil, 2000] Brasil, República Federativa. **Decreto 3.505 de 14 de Junho de 2000 que Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal do Brasil**. <http://www.natlaw.com/brazil/topical/ec/dcbrec/dcbrec11.htm > Acesso em 11 fev. 2003.

[Segurança da Informação] Anônimo**,Segurança da informação;**

<http://geocities.yahoo.com.br/jasonbs_1917/seguranca/negocio.htm#segurança> Acesso em 05 jun. 2003.

[InfoGuerra - Segurança e Privacidade] InfoGuerra. **InfoGuerra - Segurança e Privacidade** <http://www.infoguerra.com.br/infoguerra.php?newsid=1037215495,16188,> Acesso em 10 jun. 2003.

[Modulo Security] Modulo Security Solutions S/A. **Modulo Security**

<http://www.modulo.com.br/empresa/site/modulo_interna_cursos_security_conteudo.jsp?pLinkMenu=Cursos&pMenuPai=3> Acesso em 11 jun. 2003.

[Security Handbook]Security Handbook. **Site Security Handbook** <http://penta.ufrgs.br/gereseg/rfc2196/cap1.htm> Acesso em 10 jun. 2003.

[Cisneiros, 1998] Cisneiros, Hugo. *The Linux Manual* [*online*]. 1998. Disponível em <http://www.netdados.com.br/tlm/> Acesso em 21 Set. 2003.

[BS 7799] BS 7799, Disponível em <http://www.bs7799.com.br> Acesso em 21 Nov. 2003.

[Axur Communications Inc] Axur Communications Inc. **Política de segurança – Principais etapas de elaboração**; <http://www.axur.com.br> Acesso em 15 mar. 2003.

[NIC BR Security Office] NBSO**. Cartilha de segurança para Internet;** <http://www.nbso.nic.br/docs/cartilha> Acesso em 10 mar. 2003.

[BS 7799 e ISO 17799] Anônimo**. Normas BS 7799 / ISO 17799 / NBR 17799**; <http:// www.iso17799.hpg.com.br> Acesso em 13 mar. 2003.

[Anônimo] Anônimo. **Política de segurança da informação**;

[RFC] RFC**. Requet for Coments**; <http://www.rfc.net> Acessado em 20 ago. 2003.

[Tavares, 2003] Tavares,Emerson Alves. Notas de aula da Disciplina Rede de Computadores, UNIPAC, Barbacena, 2003.

[Sloha, 2000] Sloha, Liliana Esther Velásquez Alegre. Os *logs* como ferramenta de detecção de intrusão <http://www.rnp.br/> Acesso em 8 out. 2003.

[Gerlah, 1999] Gerach, Cristiano. Técnicas adotadas por *Crackers* para entrar em redes corporativas e redes privadas <http://www.rnp.br/> Acesso em 25 out. 2003.

[Aurélio, 2003] Dicionário Aurélio. Dicionário Aurélio da Língua Portuguesa;

6 ANEXO A

6.1 8ª PESQUISA NACIONAL DE SEGURANÇA DA INFORMAÇÃO

A 8ª pesquisa Nacional de Segurança da Informação, foi desenvolvida pela Modulo Security Solutions S/A, em Setembro de 2002. A empresa desde 1994, publica sua Pesquisa Nacional de Segurança da Informação. Em 2002, sua 8ª edição, a pesquisa apresenta um panorama atualizado do segmento de segurança da informação no país, com dados estatísticos sobre o mercado, indicadores, melhores práticas e uma análise das informações através de gráficos dos resultados das diversas questões levantadas. A Figura 8 representa o ramo de atividades das empresas pesquisadas, 55% das empresas são integradas com certificação com ISO 9000/14000. A Figura 9 representa o perfil dos funcionários das empresas pesquisadas, 24% das empresas possuem entre 200 a 1000 computadores e 48% tem mais de 1000 unidades.

6.2 PERIL DAS EMPRESAS PESQUISADAS EM 2002

Figura 8 – Gráfico do Ramo de Atividades das empresas pesquisadas. [8ª Pesquisa Modulo]

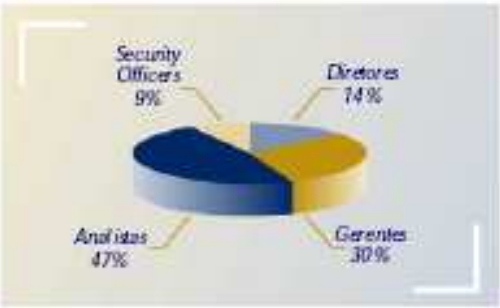

Figura 9 – Gráfico do Perfil dos Funcionários das empresas pesquisadas. [8ª Pesquisa Modulo]

6.3 ALGUNS DOS PRINCIPAIS DESTAQUES DA PESQUISA

- 43% das empresas entrevistadas sofreram ataques nos últimos 12 meses representando um aumento de 10% em relação a 2001, sendo que 24% nos últimos 6 meses.

- 78% das empresas no Brasil reconhecem que tiveram perdas financeiras. Porém, 56% ainda não conseguem quantificar o valor dos prejuízos causados pelos problemas com a segurança da informação. Em 22% das

organizações que conseguiram contabilizar estes valores, o total de perdas registradas foi de R$ 39,7 milhões.

- Os *hackers* (48%) foram os maiores responsáveis por ataques e invasões em 2002, representando um aumento de 15% com relação a 2001.

- A Internet continua sendo considerado o principal ponto de ataque com 55%. No entanto, o acesso remoto teve o maior aumento, passando de 9% em 2001 para 16% em 2002, um aumento de 78% em apenas 1 ano.

- A segurança da informação passou a ser fator importante para 45% dos executivos, sendo que 16% a consideram crítica e 32% entendem ser vital. Mesmo assim, a falta de conscientização dos executivos (45%) e dos usuários (38%) foram apontadas como os principais obstáculos para implementação da segurança nas corporações.

6.4 PRINCIPAIS AMEAÇAS À SEGURANÇA DA INFORMAÇÃO EM 2002

Funcionários insatisfeitos (64%), disseminação de vírus (55%), acessos indevidos (49%), e vazamento de informações (48%) foram consideradas as principais ameaças à segurança da informação nas empresas.

Contudo, quando solicitado a informar qual dessas ameaças seria considerado o fator mais crítico, o vazamento de informações aparece em primeiro lugar na opinião de 20% dos entrevistados, seguido por fraudes, erros e acidentes (18%), funcionários insatisfeitos (15%), acessos indevidos (10%), vírus (7%) e divulgação de senhas (6%). A Figura 10 demonstra as principais ameaças em 2002, Obs: O total de citações é superior a 100% devido à questão aceitar múltiplas respostas.

Figura 10 – Gráfica das principais ameaças em 2002. [8ª Pesquisa Modulo]

A pesquisa revela que 42% das empresas tiveram problemas com a segurança da informação nos últimos 2 anos, sendo que 33% destas sofreram algum tipo de ataque ou invasão nos últimos 12 meses.

A principal atitude adotada por 36% das empresas que sofreram ataques se limitou à correção do problema, enquanto 31% optaram por tomar providências internas e 19% providências legais. 14% não tomaram nenhuma providência.

6.5 MELHORES PRÁTICAS EM SEGURANÇA DA INFORMAÇÃO

- Política de Segurança: 55% das empresas brasileiras que participaram desta pesquisa afirmaram possuir uma Política de Segurança formalizada, embora 16% destas estejam com estas políticas desatualizadas. Em fase de desenvolvimento, encontram-se 30% das empresas, enquanto 15% informaram ainda não possuir nenhum tipo de política.

- Plano de Continuidade dos Negócios: 42% das empresas consultadas afirmaram possuir um Plano de Continuidade de Negócios. 32% informaram estar em desenvolvimento e 8% admitiram que seus planos estão desatualizados.

7 ANEXO B

POLÍTICA DE SEGURANÇA

1 – Política de segurança?

- Sim
- Sim, porém desatualizada
- Não

2 – Algum responsável pela gestão da política de segurança?

- Sim
- Sim, porém não esta desempenhando esta função
- Não

SEGURANÇA ORGANIZACIONAL

3 – Infra-estrutura de segurança da informação para gerenciar as ações corporativas?

- Sim
- Sim, porém desatualizada
- Não

4 – Fórum de segurança formado pelo corpo diretor, a fim de gerir mudanças estratégicas?

- Sim
- Sim, mas não está sendo utilizado atualmente
- Não

5 – Definição clara das atribuições de responsabilidade associadas à segurança da informação?

- Sim
- Sim, porém desatualizada
- Não

6 – Identificação dos riscos no acesso de prestadores de serviço?

- Sim
- Sim, porém desatualizada
- Não

7 – Controle de acesso específico para os prestadores de serviço?

- Sim

- Sim, porém desatualizada
- Não

8 – Requisitos de segurança dos contratos de terceirização?

- Sim
- Sim, porém desatualizada
- Não

CLASSIFICAÇÃO E CONTROLE DOS ATIVOS DE INFORMAÇÃO

9 – Inventário dos ativos físicos, tecnológicos e humanos?

- Sim
- Sim, porém desatualizada
- Não

10 – Critérios de classificação da informação?

- Sim
- Sim, porém desatualizada
- Não

SEGURANÇA EM PESSOAS

11 – Critérios de seleção e política de pessoal?

- Sim
- Sim, porém desatualizada
- Não

12 – Acordo de confidencialidade, termos e condições de trabalho?

- Sim
- Sim, porém desatualizada
- Não

13 – Processos para capacitação e treinamento de usuários?

- Sim
- Sim, porém desatualizada
- Não

14 – Estrutura para notificar e responder aos incidentes e falhas de segurança?

- Sim
- Sim, porém desatualizada
- Não

SEGURANÇA FÍSICA E DE AMBIENTE

15 – Definição de perímetros e controle de acesso físico aos ambientes?

- Sim
- Sim, porém desatualizada
- Não

16 – Recursos para segurança e manutenção dos equipamentos?

- Sim

- Sim, porém desatualizada
- Não

17 – Estrutura para fornecimento adequado de energia?

- Sim
- Sim, porém desatualizada
- Não

18 – Segurança do cabeamento?

- Sim
- Sim, porém desatualizada
- Não

GERENCIAMENTO DAS OPERAÇÕES E COMUNICAÇÕES

19 – Procedimentos e responsabilidades operacionais?

- Sim
- Sim, porém desatualizada
- Não

20 – Controle de mudança operacionais?

- Sim
- Sim, porém desatualizada
- Não

21 – Segregação de funções e ambientes?

- Sim
- Sim, porém desatualizada
- Não

22 – Planejamento e aceitação de sistemas?

- Sim
- Sim, porém desatualizada
- Não

23 – Procedimentos para cópias de segurança?

- Sim
- Sim, porém desatualizada
- Não

24 – Controles e gerenciamento de Rede?

- Sim
- Sim, porém desatualizada
- Não

25 – Mecanismos de segurança e tratamento de mídias?

- Sim
- Sim, porém desatualizada
- Não

26 – Procedimentos para documentação de sistemas?

- Sim
- Sim, porém desatualizada
- Não

27 – Mecanismos de segurança do correio eletrônico?

- Sim
- Sim, porém desatualizada
- Não

CONTROLE DE ACESSO

28 – Requisitos do negócio para controle de acesso?

- Sim
- Sim, porém desatualizada
- Não

29 – Gerenciamento de acesso do usuário?

- Sim
- Sim, porém desatualizada
- Não

30 – Controle de acesso à rede?

- Sim
- Sim, porém desatualizada
- Não

31 – Controle de acesso ao sistema operacional?

- Sim
- Sim, porém desatualizada
- Não

32 – Controle de acesso às aplicações?

- Sim
- Sim, porém desatualizada
- Não

33 – Monitoração do uso e acesso ao sistema?

- Sim
- Sim, porém desatualizada
- Não

34 – Critérios para computação móvel e trabalho remoto?

- Sim
- Sim, porém desatualizada
- Não

DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS

35 – Requisitos de segurança do sistemas?

- Sim
- Sim, porém desatualizada

- Não

36 – Controle de criptografia?

- Sim
- Sim, porém desatualizada
- Não

37 – Mecanismos de segurança nos processo de desenvolvimento?

- Sim
- Sim, porém desatualizada
- Não

GESTÃO DA CONTINUIDADE DO NEGÓCIO

38 – Processo de gestão da continuidade do negócio?

- Sim
- Sim, porém desatualizada
- Não

CONFORMIDADE

39 – Gestão de conformidades técnicas e legais?

- Sim
- Sim, porém desatualizada
- Não

40 – Recursos e critérios para auditoria de sistemas?

- Sim
- Sim, porém desatualizada
- Não

8 ANEXO C

TERMO DE COMPROMISSO

(nome da empresa)
_____, estabelecida à _____ n° _____, na cidade de _____, estado de _____, CNPJ/MF n° _____, designada **EMPRESA EMPREGADORA** e o **EMPREGADO**, Sr. _____, _____, residente à _____, na cidade de _____, estado de _____, e-mail _____, telefone _____, portador da Carteira de Trabalho e Previdência Social - série _____ n° _____, CPF n° _____, aluno do ___ semestre do Curso de _____, n° USP _____, celebram o presente **TERMO DE COMPROMISSO**, que se vincula ao Instrumento Jurídico (Prestação de Trabalho) firmado entre a Empresa Empregadora e o Empregado em ____/____/____, nos termos da Lei n° 6.494/77, conforme condições a seguir:

1. O funcionário seguirá as determinações da Política de Segurança da empresa, em razão deste Termo de Compromisso.

2. Em caso de descumprimento da Política de Segurança de forma intencional, o funcionário estará sujeito as punições impostas pela política em questão.

3. Salvo acidente de forma não intencional provado.

E, por estarem de acordo com os termos do presente instrumento, as partes o assinam em **3 (três) vias**, na presença de duas testemunhas, para todos os fins e efeitos de direito.

Barbacena, _____

Testemunhas

_____
Empresa

_____ _____
Funcionário

_____

9 ANEXO D

COMUNICADO DA DIRETORIA

A globalização da Internet aliada ao uso de tecnologias a ela associadas nas organizações tem originado, sob vários aspectos, uma verdadeira revolução na disseminação e acesso à informação dentro das corporações. Dentre estes aspectos, talvez o que gere maiores preocupações seja o que se relaciona às questões de segurança. E não é sem motivo, o uso das tecnologias representa uma mudança radical de paradigma, em que se sai de um modelo centralizador e de acesso restrito para um descentralizado com acesso universal.

Senhores colaboradores, venho através desta destacar a importância da segurança da informação para a nossa empresa. Com base nisto, saliento a importância da criação da Política de Segurança, com ela e com os senhores apoiando ela nos teremos uma empresa melhor e um nível de segurança maior, mais competitiva, dinâmica.

Desde já agradeço,

_____

Diretor da Empresa X Varejista

10 ANEXO E

MODELO DE INFORMATIVO SEMANAL X VAREJISTA – DD/MM/AA

POLÍTICA DA SEGURANÇA

Participe da nossa campanha de popularização da nossa Política de Segurança, observe:

DEFINIÇÃO

São regras e práticas que especificam ou regulam como um sistema ou organização provê serviços seguros protegendo os recursos críticos do sistema.

BENEFÍCIOS

Com as regras, ela vai nos proporcionar maior segurança, tanto física quanto lógica, . . .

NBR ISO/IEC 17799

Objetivo de definir um Código de Prática para a Gestão de Segurança da Informação. São ao todo 10 domínios reunidos em 36 grupos que se desdobram em um total de 127 controles.

CONTINUA . . .

11 ANEXO F

TERMO DE CONFIDENCIALIDADE

Eu _____, residente à _____, _____, _____, portador da célula de identidade n.º _____, CPF _____.Garante a completa confidencialidade das informações recebidas, comprometendo-se a somente utilizá-las para fins _____. Fica desta forma, vedada a divulgação total ou parcial, em caráter individualizado, de qualquer informação que venha receber ou descobrir.

_____ _____

Assinatura Terceiro Assinatura da Empresa