# Senhas - Identificação e Autenticação para Redução de Vulnerabilidades na Rede Municipal de Informática - RMI

Evandro Luiz de Oliveira

2000

# Tecnologia de Informação e Gestão Pública

Senhas - Identificação e Autenticação para Redução de Vulnerabilidades na Rede Municipal de Informática - RMI

Evandro Luiz de Oliveira

2000

Evandro Luiz de Oliveira
Analista de Informática da Prodabel

# Tecnologia de Informação e Gestão Pública

## Senhas - Identificação e Autenticação para Redução de Vulnerabilidades na Rede Municipal de Informática - RMI.

Escola de Governo da Fundação João Pinheiro

Dissertação apresentada ao Curso de Mestrado em Administração Pública da Escola de Governo da Fundação João Pinheiro.

Área de concentração: Tecnologia da Informação.

Orientador: Prof. Márcio Luiz Bunte de Carvalho
Departamento de Ciência da Computação
UFMG.

Belo Horizonte
Escola de Governo
Fundação João Pinheiro
Abril de 2000

OLIVEIRA, Evandro Luiz de

Tecnologia da Informação e Gestão Pública; Senhas - Identificação e Autenticação para Redução de Vulnerabilidades na Rede Municipal de Informática - RMI. Belo Horizonte : Escola de Governo da Fundação João Pinheiro, 2000.

il. Dissertação de Mestrado

1. Informática 2. Administração Pública 3. Segurança 4. Senhas 5. Identificação 6. Autenticação

I. Título II CARVALHO, Márcio L. Bunte (Orientador)

*"Ad patres apud amicus, ab imo pectore"*

# Agradecimentos

À Prodabel, nas pessoas daqueles que acreditam e atuam na mudança da sociedade através da garantia de oportunidades a todos os que lutam por elas.

Aos companheiros da Prodabel e colegas do cotidiano, que apoiam e entendem que trabalhos de dissertação de mestrado vão além do individualismo que nos envolvem por um período às vezes longo, sendo parte de um processo de crescimento coletivo e não somente individual.

Aos parentes, próximos ou afastados, que sabem da importância de apoiar e valorizar trabalhos às vezes complexos e aparentemente sem sentido.

# SUMÁRIO

# LISTA DE GRÁFICOS

# LISTA DE FIGURAS

# LISTA DE TABELAS

# LISTA DE ABREVIATURAS E SIGLAS

**ADP -** Automatic Data Processing (Processamento Automático de Dados).

**AGM** - Auditoria Geral do Município (Órgão da Estrutura Administrativa da Prefeitura de Belo Horizonte).

**ANSI** - American National Standards Institute (Instituto Nacional Americano de Padrões). Desenvolve padrões de transmissão, armazenamento, linguagem, e protocolos.

**API** - Application Programming Interface (Interfaces de Programas de Aplicação). Mecanismo de comunicação entre programas de ambientes Windows®.

**BAC -** Biometric Control Access (Controle de Acesso Biométrico). Tecnologia de reconhecimento de características biométricas.

**CCITT -** Comité Consultatif Internacional de Téléphonie et Télégraphie (Comitê Consultor Internacional de Telecomunicações). Atual ITU, responsável pelo desenvolvimento de padrões de comunicação.

**CGM** - Corregedoria Geral do Município (Órgão da Estrutura Administrativa da Prefeitura de Belo Horizonte).

**Cepesc -** Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações. Órgão vinculado à Presidência da República responsável pelo sigilo das comunicações do governo brasileiro.

**CERT -** Computer Emergency Response Team (Equipe de Respostas a Incidentes em Computadores). Responsável por receber, responder e orientar administradores de segurança por incidentes em redes de computadores.

**CSC -** Computer Security Center (Centro de Segurança em Computação).

**DoD -** Department of Defense (Departamento de Defesa do Governo dos Estados Unidos da América).

**FTP -** File Transfer Protocol - Protocolo de Transferência de Arquivos.

**ID -** Abreviatura de Identificação. Utilizada para referenciar ao requisito de Identificação de usuário.

**IEEE -** Institute of Electrical and Electronic Engineers (Instituto de Engenheiros Eletrônicos e Elétricos).

**I&A -** Identificação e Autenticação.

**LAN -** Local Area Network (Rede de Computadores Local). Rede localizada fisicamente, na maioria dos casos, em um prédio, com tamanho, tecnologia de transmissão e topologia diferenciando-a das demais.

**NCSC -** National Computer Security Center (Centro Nacional de Segurança em Computadores).

**PIN** - Personal Identification Number (Número de identificação pessoal).

**PBH -** Prefeitura Municipal de Belo Horizonte.

**Prodabel -** (Empresa de Informática e Informação do Município de Belo Horizonte S/A). Empresa responsável pela RMI na PBH

**RMI -** Rede Municipal de Informática. Denominação da rede de longa distância ligando computadores de plataformas heterogêneas em funcionamento na PBH.

**TCB -** Trusted Computing Base (Base Computacional Confiável).

**WAN -** Wide-Area Network (Rede Remota de Computadores). Rede de computadores que utiliza comunicação de longa distância na área não abrangida pelas LAN.

# GLOSSÁRIO

**Esta seção tem como finalidade a definição de termos especificamente para este trabalho. Alguns dos termos assumem significados mais abrangentes ou mais completos, outros podem ter definições diferentes fora do ambiente de segurança em informática e em outras disciplinas.**

**Fontes: [4], [39], [48].**

**Acesso** - 1. Habilidade de se introduzir em área protegida. 2. Tipo específico de informações entre um sujeito e um objeto que resulta no fluxo de informações de um para o outro (Livro Laranja). 3. Processo de interação com um sistema ou conjunto de informações.

**Acesso remoto** - Comunicação entre computadores e uma estação, um terminal, ou outro dispositivo de conexão, que estão distantes e feita normalmente através de ligação telefônica comutada.

**Administração Municipal** - Conjunto de órgãos que compõem a administração da Prefeitura de Belo Horizonte.

**Administração de segurança** - As regras gerenciais e os controles suplementares estabelecidos para fornecer um nível mínimo aceitável da proteção para dados.

**Ambiente** - Reunião de circunstâncias externas, condições e eventos que afetam o desenvolvimento, operação e manutenção de um sistema (DoD).

**Ambiente de segurança aberta** - Ambiente em que uma das seguintes condições é verdadeira: 1. Projetistas de aplicações (inclusive pessoal de manutenção) não têm credencial suficiente para garantir que não introduziram programa nocivo. 2. O

controle de configuração não oferece garantia suficiente de que as aplicações estão protegidas contra a introdução de lógica maliciosa antes e durante a operação de aplicações do sistema (DoD).

**Ambiente de segurança fechada** - Ambiente em que os projetistas de aplicações têm credenciais e autorizações suficientes para fornecer indicação aceitável de que não introduziram lógica maliciosa.

**Aplicação -** O mesmo que aplicativo ou sistema.

**Aprovação/Credenciamento** - Autorização oficial concedida a sistema ADP para processar informações restritas em seu ambiente operacional, baseada em avaliação abrangente do projeto do hardware do sistema, *firmware*, e de segurança de software, configuração e implementação, além de outros controles administrativos, físicos, de pessoal e de segurança de comunicações.

**Ataque (Attack) -** O ato de tentar desviar dos controles de segurança de um sistema. Um ataque com pode ser ativo, tendo por resultado a alteração de dados; ou passivo, tendo por resultado a liberação de dados. O ataque sem sucesso pode acontecer dependendo do nível de vulnerabilidade do sistema, da atividade em si ou da eficácia das contramedidas aplicadas.

**Auditoria -** Revisão e exame de registros e das atividades do sistema, para confirmar sua consistência e veracidade. Procedimento adotado nas auditorias tradicionais.

**Auditoria de segurança computacional -** Avaliação dos controles utilizados para garantir a proteção adequada dos bens de informações de uma organização contra todas as ameaças ou perigos. Procedimento que fornece também subsídios para a garantia de confiabilidade operacional quanto à precisão e sincronia de todos os componentes do sistema computacional.

**Autenticação** - Processo de estabelecer a legitimidade de uma estação da rede de computadores ou de um usuário como pré-requisito da permissão de acesso às informações solicitadas.

**Autorização -** Delegação concedida a uma pessoa ou um sistema automático pela administração de segurança, permitindo que elas realizem transações ou procedimentos e possam também repassar esta delegação.

**Base computacional confiável ("Trusted Computing Base", TCB) -** A totalidade de mecanismos de proteção dentro de um sistema computacional - abrangendo *hardware*, *software*, *firmware* - cuja combinação é responsável por um ambiente a uma política de segurança confiável.

**Chave -** Em criptografia, uma seqüência de símbolos usados para codificar ou decodificar um arquivo. Pode introduzir uma chave em dois formatos: alfanumérico e condensado (hexadecimal).

**Código -** 1. Programa de computador. 2. (codificar) Criar programa de computador ou converter dados para um formato próprio para operação de programa.

**Comprometimento (Compromise) -** Uma violação da ***Política de Segurança*** de um sistema de tal maneira que divulgação desautorizada da informação sensível possa ter ocorrido.

**Confiabilidade -** A qualidade de produzir os mesmos resultados cada vez que o procedimento for repetido com as mesmas entradas, implicando em rotinas de processamento livres de defeito.

**Confidencial -** Um tipo de classificação para informações, que ao serem usadas por pessoa não autorizada, causam danos a uma organização ou pessoa.

**Confidencialidade -** Característica de ambientes computacionais em manter a informação confidencial.

**Controle de acesso (Access Control) -** Conjunto completo de procedimentos executados por *hardware*, *software* e administradores, para monitorar o acesso, identificar usuários solicitando acesso, registrar tentativas de acesso e conceder ou impedir acesso com base em regras preestabelecidas.

**Controle de acesso Biométrico -** Qualquer meio de controlar acesso para um local através de medidas humanas, como impressões digitais, impressões de voz ou determinação de padrões de retina.

**Criptografia (Cifragem) -** Processo de alterar as informações de arquivos ou programas, através de códigos, chaves específicas, tabela de conversão ou algoritmo. Um dispositivo ou *software* converte o texto para formato ilegível para quem não possui conhecimento dos mecanismos de decodificação.

**Defeito -** 1. Qualquer erro em um sistema ou processo automatizado, que permite o contorno de medidas de segurança. 2. Erro de autoridade, omissão, ou de imprudência que permite a passagem por mecanismos de proteção (Livro Laranja).

**Detecção de intrusão (Intrusion Detection) -** A detecção de ataque por processos manuais ou através dos sistemas que operam sobre os registros ou outra informação disponível na rede ou computador.

**Disfarce -** Ação considerada fraude onde uma pessoa se faz passar por usuário autorizado para penetrar em sistema computacional.

**Disponibilidade (Availability) -** Aspecto de segurança que lida com a entrega tempestiva de informações e serviços aos usuários. Um ataque na disponibilidade procuraria conexões de rede e promoveria paralisações de sistemas.

**Especificação -** Identificação das características de determinado recurso de informática, que pode ser um equipamento, um sistema ou um programa.

**Ferramentas -** Conjunto de programas de computador com finalidades específica. Por exemplo: Gerenciamento de senhas; Gerador de caracteres, Gerenciador de Tráfego. Para funcionarem exigem, na maioria dos casos, vários procedimentos de configuração (parametrização, customização).

**Firewall -** Um sistema composto de *software* e *hardware*, que protege a fronteira entre duas ou mais ***LAN***.

**Fraude -** Qualquer exploração de sistema de informações tentando enganar uma organização ou pessoas, para tomar ou fazer mau uso dos seus recursos.

**Funcionalidade -** Comportamento normal de um sistema. Um sistema funcional exige: confidencialidade, integridade, disponibilidade, autenticação e não repúdio.

**Hacker -** Estudioso das tecnologias, especialmente da informática, que utiliza boa parte de seu tempo na aplicação de técnicas sofisticadas para conhecer, utilizar, dominar ou modificar o funcionamento de programas e equipamentos.

**Hacking -** Uma tentativa desautorizada em alcançar informações de um sistema. Usado freqüentemente para referenciar a um *hacker*.

**Identificação de usuário -** É o processo pelo qual uma pessoa se identifica no sistema como usuário válido. Durante o processo de acesso, o usuário pode introduz número ou nome de conta (identificação) e senha (autenticação), além de reconhecimento de características biométricas.

**Integridade -** Exatidão e consistência de uma informação que pode estar submetida a processo de manipulação por sistemas de informática.

**Livro Laranja (Orange Book) -** Normalização do DoD - Department of Defense dos Estados Unidos da América. Trusted Computer System Evaluation Criteria. Fornece informações necessárias para classificar sistemas computacionais como A, B, C ou D, definindo seu grau de segurança.

**Logoff -** Terminar sessão de trabalho, iniciada com um *login*, através de algum procedimento simples que informa ao computador o fim da sessão.

**Login -** Procedimento inicial de uma sessão em estação de trabalho ou computador em que o sistema operacional ou aplicação pede ao usuário uma identificação.

**Nível de segurança -** Combinação de classificação hierárquica e um conjunto de categorias não hierárquicas que representam a restritividade das informações de um sistema ou recurso computacional, por exemplo as classificações do Livro Laranja.

**Padrão de impressão digital -** Qualquer característica de impressão digital usada em identificação pessoal.

**Password -** Também conhecida como senha, é formada por uma única palavra, ou seqüência de caracteres, usada para autenticar uma identificação. Deve ser confidencial, diferentemente da identificação do usuário.

**Penetração -** Em segurança computacional, uma tentativa bem sucedida e não autorizada de acesso a sistema computacional.

**Política de Segurança -** Conjunto de leis, regras e práticas que regulam como uma organização gerencia, protege e distribui informações restritas (Livro Laranja).

**Privacidade -** Direito de propriedade de informações pessoais ou corporativas e, portanto, o direito de determinar quem pode ter conhecimento destas informações e em que condições.

**Processo -** Programa em execução. É inteiramente caracterizado por ponto único atual de execução, espaço de endereço e conteúdo das memórias.

**Programa Nocivo -** Termo usado pela mídia de massa para indicar qualquer programa com o propósito de quebrar a segurança de sistemas de computadores.

**Proteção -** Qualquer medida projetada para defender informações de ataques.

**Rainbow Series (Série Arco-Íris) -** Conjunto de mais de 20 livros publicado pelo National Computer Security Center - NCSC, que promovem programas padrões de segurança. As cores são referências às cores das capas dos respectivos livros [55].

**Requisitos de segurança -** Necessidades de segurança identificadas. Estas necessidades devem ser expressas em leis e regulamentos, padrões e políticas definidas por órgãos e usuários.

**Risco -** A probabilidade de se efetivar uma ocorrência de ataque relacionada com ambientes computacionais.

**Risco aceitável -** Avaliação concluindo que um sistema ou atividade satisfaz os requisitos mínimos de segurança especificados, indicando que a probabilidade é menor que um limite indicado.

**Segurança -** Em sistemas computacionais, é o rendimento sincronizado, correto, autorizado de tarefas de computação. Engloba as áreas de confidencialidade, integridade e disponibilidade.

**Senha -** Código secreto designado a um usuário de serviço os sistema. O usuário introduz a senha e o *software* de gerenciamento verifica se a mesma é legitima e correta.

**Sistema -** Conjunto de programas destinados a automatizar funções do usuário. Funcionam através de programas em diferentes linguagens.

**Sistema computacional confiável ("Trusted Computing System", TCS) -** Sistema que emprega medidas de integridade de *software* e *hardware* suficientes para permitir processar, simultaneamente, uma faixa de informações restritas ou classificadas.

**Sistema de senha -** Parte de sistema computacional usado para autenticar a identidade de usuário. A garantia de identificação inequívoca se baseia na habilidade do usuário em introduzir uma senha privada que ninguém mais deve conhecer.

**Spoofing -** Ação caracterizada como fraude onde existe a tentativa de ganhar acesso ao sistema iludindo-o, passando-se por um usuário autorizado.

**Tentativa e Erro -** Procedimento em que alguma pessoa utiliza-se da repetição de um determinado roteiro de teste para achar um resultado que não conhece *a priori*. Algum indicador informará qual das repetições representa um resultado desejado.

**Texto Claro -** Texto ou informação escrita de forma a permitir a qualquer ser humano uma fácil leitura. Normalmente na linguagem falada pelo próprio homem. É o oposto de um texto criptografado.

**Uso de Senha -** O conhecimento da senha associado com uma identificação de usuário é considerado prova para uso das capacidades associadas com o ID do usuário.

**Usuário -** Qualquer pessoa que interage diretamente com um sistema computacional (Livro Laranja).

**Usuário não autorizado -** Usuário que utiliza um sistema computacional de forma ilegítima. Pode ou não ser usuário autorizado do sistema para outras tarefas. Suas ações violam mecanismos ou políticas de segurança, ou códigos de conduta estabelecidos.

**Validação -** Execução de testes e avaliações para verificar o cumprimento de regras de segurança.

**Vigilância -** Rotina de monitoração de equipamento e sistemas usada para garantir, através de procedimentos específicos, sua operação correta.

**Vulnerabilidade -** Qualquer área não protegida (ponto fraco) que deixa o sistema aberto a ataque potencial ou outro problema.

# RESUMO

Esta dissertação apresenta um estudo de caso a partir da premissa de vulnerabilidades das senhas em redes de computadores heterogêneas e descentralizadas, tema que tem significativa presença na pauta de discussão dos ambientes informatizados. O trabalho foi motivado pela experiência do Projeto de Descentralização dos Serviços de Informática [49], implementado através da Prodabel, empresa responsável pela infra-estrutura de serviços informatizados da administração municipal de Belo Horizonte. Esse projeto adotou procedimentos e soluções considerados radicais por diversos profissionais da área [2], ao substituir o computador centralizado por uma estrutura descentralizada, proporcionando uma ampla mudança nos conceitos vigentes sobre níveis de segurança, mecanismos de proteção e, sobretudo, nas políticas adotadas para proteção das informações, sistemas e serviços executados nas redes de computadores.

A meta principal do trabalho é apresentar e comprovar a importância da definição, desenvolvimento e implantação de políticas de identificação e autenticação (I&A). Esses dois conceitos são usualmente implementados através do uso de senhas e começaram a receber tratamento monitorado a partir da constatação de casos de vulnerabilidade na Rede Municipal de Informática (RMI).

Nesse contexto, são discutidos os mecanismos mais atualizados e as propostas para implementação de políticas de I&A em redes de computadores que atendam à órgãos públicos. Para posicionamento do trabalho, vários conceitos técnicos gerais sobre segurança são apresentados. Esses conceitos têm a função de esclarecer e

delimitar o escopo deste projeto. A maior preocupação foi permitir que as hipóteses propostas de implementação desses mecanismos de identificação e autenticação fossem aplicáveis em redes públicas e privadas.

O trabalho apresenta uma necessidade atual e bastante discutida no contexto da segurança em redes de computadores. As bases que o fundamentam estão centradas na fragilidade das senhas nos ambientes de Internet, correio eletrônico e sistemas da área tributária. Foram utilizadas técnicas de auditoria e de pesquisa não autorizada para obter informações, simulando uma situação de uso irregular.

Os resultados apresentados confirmaram a vulnerabilidade, que antes era mera suposição, e subsidiaram algumas contribuições para a administração da RMI no decorrer do trabalho. Mais do que apontar falhas, iniciou-se um processo de correção de problemas e diminuição de vulnerabilidades, além da apresentação de propostas de projetos futuros, importantes para a continuidade de trabalhos que objetivem o tratamento adequado de políticas e técnicas de identificação e autenticação.

## ABSTRACT

This dissertation discusses security in systems based on heterogeneous and decentralized networks presenting one study case on the fragilities of the passwords in the environment of Internet, electronic mail and systems of the tributary area. The motivation of this work is based on the platform migration implemented by Prodabel, the information technology company responsible for the infrastructure of computerized services of the municipal administration of Belo Horizonte. This migration was accomplished by the Project of Decentralization of the Services of Computer Science [49], with procedures considered by several professionals as extreme.

The project replaced the mainframe by a decentralized structure, which provided a wide change in the effective concepts of levels of safety, protection mechanisms and, what is more important, changed the policy adopted for protection of the information, systems and services avaiable in the networks.

The aim of this dissertation is to analise and confirm the importance of identification and authentication procedures in electronic systems. These two concepts, where passwords represent the most ordinary option, from certain moment, began to be treated with great importance in any process that uses systems and computerized procedures. In such a context, the most up-to-date mechanisms and policies are discussed for application in networks that are in use by public departments.

As a levelling and set to a common knowledge the work describes several general technical concepts on security. These concepts are helpful to bring light to the subject and to define the boundaries of this dissertation. One of the hypotheses is that these concepts of identification mechanisms and authentication are appliable in public

and private networks. The work treats the now existing need for safety in the context of networks.

The paradigm that sets up this work is one research wich proves the fragilities of passwords in the world of Internet, electronic mail and systems of the tributary area. Audit techniques and unauthorized accesses were used to get informations in the net through a simulated user with no authorization. The results confirmed the fragilities that were peviously mere supposition, assisted the implementation of some procedures and pointed out some proposals for future works.

# 1 - Apresentação

*"Esta obra, eu não a ornei nem a enchi de períodos longos*
*ou de palavras empoladas e magnificentes, ou de qualquer outro artifício de arte ou ornamento extrínseco,*
*com os quais muita gente costuma descrever e ornar as suas coisas;*
*porque não quis que artifício algum lhe valesse, mas, sim, que apenas a variedade do assunto*
*e a gravidade do tema a tornassem agradável."*
**Niccolò Machiavelli [36]**

Este trabalho discute a proposta de inserção de tecnologias a serem aplicadas em mecanismos de I&A, exigidos pelas evoluções e novas aplicações de redes de computadores. Fundamentando-nos em literatura técnica específica, além de artigos disseminadores e debatedores sobre tecnologias de ponta, apresentamos também conceitos gerais para esclarecimento e delimitação do escopo a ser abordado. A introdução desses conceitos é necessária para que se desfaçam mitos positivos e negativos referentes à segurança em redes descentralizadas e, em especial, à autenticação em sistemas de computadores. Através de um estudo de caso real, tendo como objeto o ambiente da Rede Municipal de Informática (RMI) da Prefeitura de Belo Horizonte (PBH), são analisadas as conseqüências e discutida a aplicabilidade deste trabalho como evolução para a RMI, gerenciada pela Empresa de Informática e Informação do Município de Belo Horizonte S/A - Prodabel.

# 2 - Introdução

*"Enquanto você lê estas páginas, alguns crimes estão sendo praticados via Internet no mundo todo."*
**Módulo Security [40]**

Inicialmente identificamos a administração pública como uma forma de organização complexa que deve atender, no plano principal, ao cidadão. É perfeitamente possível a compreensão dessa organização como um conjunto de sistemas e processos que, ao longo do tempo, foram se avolumando em relação ao crescimento da cidade e à demanda imposta pelo cidadão na busca de serviços. Essa evolução tem tornado as organizações, especialmente de administração pública, dependentes de diversas tecnologias, especialmente as de informática. Essas tecnologias sempre demandaram a adoção de requisitos de segurança para garantir ao cidadão confiabilidade e segurança em seu relacionamento com a autoridade pública.

Todavia, as organizações públicas têm sido colocadas à prova por vários motivos, especialmente pela ânsia de setores econômicos e políticos de tornar o Estado cada vez mais privatizado. O modelo de Estado centralizador, vigente à época da criação das empresas públicas de informática, propiciou o surgimento de empresas a partir dos modelos das grandes corporações de informática, os quais acabaram mostrando-se inadequados frente à rápida evolução tecnológica [1]. Com a decadência desse modelo, especialmente na Administração Municipal de Belo Horizonte, fez-se necessária uma reformulação organizacional, tendo a tecnologia sido utilizada como um dos argumentos para que as empresas buscassem novas propostas e formas de gestão.

No caso da Prodabel, a mudança de tecnologia, que teve como marco principal o mês de setembro de 1996, que consistiu na desativação do parque centralizado e início da operação de sistemas baseados em LANs e WANs, provocando uma grande alteração na cultura e na forma de trabalho dos profissionais de informática da organização [22]. No que se refere à segurança, foram inúmeras as vulnerabilidades e contradições vividas, sendo importante destacar o aumento de serviços distintos em relação ao volume de requisições de trabalhos anteriores, novas tecnologias adotadas no desenvolvimento de sistemas, e mais especificamente no tema I&A, a repetição de pontos de verificação de senhas. Essas questões nos convenceram da importância de examinar o assunto com maior profundidade.

Inicialmente, um dos temas sobre os quais o uso da informática tem repercussão é a vulnerabilidade social[1] vinculada à dependência da tecnologia. A associação da evolução tecnológica com esse tema leva o senso comum ao temor de que se fique cada vez mais à mercê de falhas totais[2] vinculadas às tecnologias, ao invés de se estar sujeito somente a falhas parciais[3], como as que ocorrem quando os processos decorrem sobretudo da intervenção humana [26] [14]. Caberia à disciplina de segurança em redes de computadores a responsabilidade de estudar os meios para minimizar esses riscos e de tentar evidenciar a existência de um patamar de segurança que possa ser associado à evolução tecnológica.

Como trabalhar com a totalidade da disciplina denominada "Segurança Computacional" é tarefa inviável na medida do trabalho a que nos propomos, optamos por abordar um tópico que consideramos inicial de todo processo de segurança em informática e do qual depende quase a totalidade de sua utilização: Identificação e

[1] Dependência da sociedade em geral de tecnologias desconhecidas ou herméticas [26].
[2] Falha que impede qualquer ação corretiva imediata.

Autenticação (I&A). Toda intervenção que requer a utilização de informática inicia-se a partir da requisição de um ser humano, ao solicitar a disponibilidade de determinado recurso, informação ou função informatizada. Essa solicitação, via de regra, requer uma identificação de usuário e uma autenticação do solicitante. É nesse início de processo que concentramos nossos esforços, a partir da convicção de que quanto mais seguro e confiável o processo inicial de acesso aos recursos informacionais, menores as possibilidades de estarem sendo liberados recursos indevidos ou de que tais recursos sejam liberados para usuários não autorizados. Ressalte-se que, no que se refere ao setor público, é força de lei que informações relativas aos cidadãos sejam mantidas íntegras [16] e que os serviços e sistemas sejam colocados em ambientes confiáveis (ver TCB em glossário e siglas) e livres de defeito.

O trabalho está dividido em quatro partes. A primeira parte, composta dos capítulos 3 e 4, está voltada para a conceituação genérica de segurança em informática, abordando a evolução das formas de acesso remoto e as possibilidades de controle físico e lógico dessas formas, além de sínteses contrapondo formas ideais de acesso e propostas aplicáveis ao caso da Administração Municipal.

No Capítulo 3, apresentamos a descrição das formas de acesso aos recursos informacionais existentes em redes de computadores. Nesse capítulo tratamos da classificação dos tipos de acesso, da evolução das forma de acesso contrapondo as vulnerabilidades em ambientes de grande porte (*mainframe*) e ambientes descentralizados (microcomputadores), abordando ainda a importância de uma política de segurança em ambientes informatizados.

No Capítulo 4 são detalhados e conceituados os controles físicos de acesso, diferenciando-os dos controles lógicos (de acesso) quando utilizados em ambientes

[3] Falha que pode ser corrigida com uso de tecnologia ou substituição da mesma.

centralizados[4]. Enfatizamos as vulnerabilidades dos controles de acesso lógico, especialmente as formas de ataque mais comuns, a visão do usuário em relação a segurança e os controles aplicados, em função da premissa de que às redes de computadores, atualmente, pouco importa a localização física do solicitante de qualquer recurso informacional, sendo, portanto, relevantes a forma de acesso à informação e não as condições de acesso físico à mesma. As considerações sobre as situações encontradas na maioria das redes de computadores e os tipos de controles considerados ideais e aplicáveis às novas tecnologias de rede, são apresentadas ao final desse capítulo.

Na segunda parte, constituída pelo Capítulo 5, detalhamos algumas questões que objetivam a melhoria de qualidade da segurança e do controle de acesso, com ênfase na I&A e utilização de senhas, tecendo ainda algumas considerações sobre o gerenciamento e a administração do acesso remoto através de I&A. Descrevemos, também, técnicas e métodos de auditoria aplicáveis e necessários a controles de acesso lógico, tratando também de apresentar algumas técnicas e ferramentas indicadas para procedimentos de I&A.

A terceira parte, constituída pelos Capítulos 6 e 7, refere-se ao caso da Prodabel e da RMI, onde fazemos um estudo comparativo com outros ambientes e analisamos as técnicas para monitoração, gerenciamento e proteção utilizadas em I&A. Adicionalmente, apresentamos uma fundamentação para a aplicabilidade da proposta a outros ambientes, notoriamente em organizações públicas, e discutimos a possibilidade de uma implementação piloto. Nessa parte, apresentamos as nossas conclusões sobre a questão e destacamos estudos mais específicos que consideramos necessários, bem como as suas possibilidades de aplicação. São apresentadas, também, as contribuições

[4] Ambientes informatizados com computador multiusuário baseado em *mainframe.*

trazidas por este trabalho e que formam uma base para o tratamento de I&A no ambiente informatizado da administração municipal de Belo Horizonte.

No Capítulo 6, analisamos o caso Prodabel - RMI a partir de experimentos realizados e da apresentação dos resultados mensuráveis e não mensuráveis, obtidos a partir do estudo comparativo entre o ambiente ideal e o ambiente existente e das condicionantes que impedem a implementação de um ambiente ideal, incluindo-se aí os fatores culturais presentes também nos ambientes informatizados. Ao final do capítulo descrevemos sucintamente um caso atual e polêmico que se consistiu em uma experiência adicional para o trabalho de pesquisa.

No Capítulo 7, discutimos e analisamos as ferramentas disponíveis, a funcionalidade de aplicação de políticas de segurança e as definições e ferramentas aplicáveis em outros ambientes informatizados das organizações públicas, tendo como referência a proposta de ambientes informatizados com acesso remoto mais amplo para o cidadão e usuário da RMI. Propomos, ainda, trabalhos essenciais ao aproveitamento do estudo, e, principalmente, à diminuição das vulnerabilidades da RMI.

Finalmente, apresentamos nossas conclusões sobre o trabalho, reforçando o argumento de que para aumentar a confiabilidade nos computadores e nas suas redes, procedimentos elementares de segurança, associados à I&A, devem ser implantados.

# 3 - Acesso e Segurança em Rede

*"Segurança tem início e termina com as pessoas"*
**Ællen Frisch [27]**

A conceituação de segurança é, talvez, a mais complexa da informática, por envolver, obrigatoriamente, todos os produtos e serviços associados aos computadores e processos automatizados, abrangendo políticas, ferramentas, tecnologias e procedimentos [61]. Iniciamos nosso trabalho abordando alguns dos conceitos utilizados no tema segurança para, em seguida, dedicarmo-nos à temática da I&A, à qual estaremos nos referindo em alguns momentos como senha, entendida como o processo normalmente utilizado pelos usuários de informática para se identificarem e receberem autorização para utilizar recursos computacionais. Destacamos que, mesmo que estejam surgindo novas tecnologias que contribuem para um maior controle da I&A de usuários junto às redes de computadores, consideramos básicos a qualquer sistemática de controle de acesso os mecanismos vinculados a políticas e procedimentos de I&A.

As definições mais importantes para I&A são descritas no chamado Livro Azul Claro[5] [42], documento orientador para implementação de políticas e procedimentos de tratamento de senhas. Tal orientação diz respeito a três modos clássicos pelos quais são tratados os mecanismos de I&A. Esses modos são aplicáveis com maior abrangência e intensidade nos sistemas informatizados multiusuário e referem-se às características de classificação, que podem ser utilizadas como determinantes do método de I&A a ser aplicado. Ressalta-se que os sistemas monousuários também podem ser considerados com as mesmas características apresentadas, mas não necessitam do destaque dado aos

multiusuários. São os seguintes modos pelos quais um sistema informatizado identifica e autentica um usuário:

1) **Algo que ele sabe** - É a classificação do esquema conhecido como I&A através de senha. A partir da inclusão do usuário em um sistema, ele recebe uma identificação e, associada a essa identificação, uma sequência de caracteres que constituem uma senha. A teoria fundamenta-se na suposição de que se alguém conhece a senha é porque esse alguém é seu dono e está autorizado a usar a respectiva identificação de usuário [42]. A fragilidade dessa premissa refere-se à possibilidade de que o usuário tenha a senha roubada por interceptação através de algum programa nocivo, por divulgação indevida através de anotações feitas por ele mesmo em função de não memorização, por programas de adivinhação[6] de senhas, ou, ainda, por divulgação voluntária.
2) **Algo que ele tem** - É a forma de identificar alguém através de algo que ele possui, tal como um cartão magnético, um cartão inteligente[7] ou uma chave específica. A premissa básica é bastante parecida com a anterior: se alguém apresenta alguma coisa que é sua propriedade para se identificar e obter autenticação, pressupõe-se que esse alguém seja o responsável e detentor autorizado dessa coisa. Da mesma forma que no modo anterior, se ocorrer a perda do elemento físico de identificação, perde-se a garantia de que o usuário seja realmente seu proprietário. Em adição à posse do objeto de identificação de usuário, pode ser necessária uma informação complementar para ocorrer a autenticação, como a exigência de que seja apresentada uma senha. Nesses casos ocorre o que é denominado modo de autenticação duplo [42].

---

[5] Documento do DoD que fornece informações sobre critérios de utilização de I&A de usuários de sistemas computacionais.
[6] Programas utilizados por processo de *hacking* que tenta descobrir uma senha a partir de testes sucessivos.

3) **Algo que ele é** - É a forma de I&A teoricamente mais forte. Parte do princípio de que a pessoa que solicita o recurso informacional é portador de alguma característica biológica que o sistema de identificação conhece antecipadamente, e que somente essa pessoa possui. São exemplos desse tipo de identificação, que pode também ser associado ao processo de autenticação, características físicas humanas como impressão digital, relevo da palma da mão, padrões da íris, voz, face e assinaturas [42]. Esses sistemas de reconhecimento, baseados em características fenótipas, são denominados sistemas biométricos e comparam as características particulares de cada usuário apresentando um nível de vulnerabilidade mais reduzido em relação aos outros modos de identificação. No entanto, não estão isentos de falhas, principalmente se considerarmos que o aumento da precisão de cada um desses sistemas corresponde à elevação dos custos associados à implantação e manutenção. Além disso, pesquisas apontam que os usuários de informática não se sentem confortáveis ao usar esse tipo de identificação [60]. Mesmo sendo forte, no sentido de dimimuírem as falhas, tais mecanismos não são imunes a elas. As falhas nestes mecanismos pdem ser verificadas, por exemplo, em função do custo de armazenamento das informações de cada usuário. Mesmo que não existam duas impressões digitais iguais, a diminuição dos critérios de digitalização podem fazer com que existam informações semelhantes, incorrendo na possibilidade de erro.

As classificações descritas são válidas para qualquer sistema de I&A. Sistemas devem se apropriar desses conceitos para definição de quais mecanismos devem ser implementados para sua segurança e para que se obtenha um sistema computacional

[7] Também conhecido como *Smartcard*, é um dispositivo semelhante fisicamente a um cartão de crédito que pode ser programado para várias funções e pode ter capacidade de processamento, identificando e qualificando seu usuário e portador.

confiável. A diferença básica na evolução dessas tecnologias é a mudança na caracterização do acesso. Nos sistemas centralizados[8], principalmente em função da tecnologia utilizada e da quantidade reduzida de pontos de acesso remoto, o foco era o acesso físico ao local onde se encontravam os terminais de computadores e/ou equipamentos essenciais às redes. No caso dos sistemas distribuídos[9], com pouco ou nenhum controle da localização física dos computadores, o foco da preocupação com segurança desloca-se para os controles de acesso lógico, fortalecendo a necessidade de que I&A sejam itens determinantes para o início de qualquer processo de compartilhamento de acesso[10].

Neste ponto, cabe destacarmos que em contraposição ao conjunto de normas e regras indicadas pelo Governo norte-americano, que aqui serão apresentadas genericamente como Livro Laranja[11], e mais diretamente relacionadas ao tema I&A, como o Livro Azul Claro, os governos de países europeus lançaram um conjunto de livros denominados Livro Verde e Livro Branco que abordam as questões de segurança, incluindo I&A. O Livro Verde foi publicado pela Agência de Segurança de Informação Alemã e o Livro Branco é um padrão europeu endossado pela Alemanha, França, Reino Unido e Holanda [58], adotando critérios de avaliação semelhantes aos que levaremos em consideração, mas que ainda não apontam para detalhes necessários às práticas de I&A.

Tratamos, em seguida, dessas classificações, levando em consideração as formas e os controles de acesso.

---

[8] Sistemas com características de funcionamento em um computador central e dotando os terminais com pouca ou nenhuma capacidade de processamento. Sistemas de grande porte nos equipamentos mais antigos.
[9] Sistemas onde o processamento pode ser realizado nos terminais com cooperação de um ou mais computadores denominados servidores. A utilização de microcomputadores, por si só, não determina que um sistema é distribuído.
[10] É a permissão de que dois ou mais usuários acessem simultaneamente arquivo ou recurso informacional.
[11] Ver *Rainbow Series*

### *3.1 - A Evolução das Formas de Acesso*

Historicamente, o controle de acesso a um recurso ou ambiente sempre foi um problema. As fortificações pré-históricas e medievais tinham a finalidade de permitir o acesso somente àqueles com autorização para tal, e tinham como foco as condições físicas desse acesso. Mecanismos engenhosos foram identificados nos túneis e labirintos das pirâmides egípcias, que aparentavam ter como objetivo garantir acesso exclusivo àqueles com conhecimento acerca do processo de autorização [10]. Até mesmo lendas e histórias referem-se a esse tema, e uma das mais famosas diz respeito diretamente ao que tratamos neste trabalho. Trata-se da história de "Ali Babá e os Quarenta Ladrões", que reproduz a temática em questão: "Abre-te, Sésamo" era a forma de I&A segura e, por que não dizer, premonitória da tecnologia de uso de senha numa época em que os computadores ainda eram impensáveis mesmo nos contos e lendas. Aquela expressão foi uma alternativa segura até o momento em que se tornou conhecida por pessoas não autorizadas, provocando um defeito irrecuperável para o sistema de segurança do acesso.

A preocupação em fornecer acesso seguro aos serviços nas redes de computadores para as pessoas apresenta sofisticação e precisão inimagináveis há algum tempo atrás. Técnicas como o reconhecimento da face e detecção de impressão digital, apresentados como ficção científica há três décadas, já podem ser encontradas em redes de algumas instituições [21], mesmo que ainda não sejam tão comuns já são aceitas e admitidas como possibilidade de aumento da segurança em redes de computadores e ambientes informatizados. A perspectiva é de que novos recursos de identificação eletrônica substituam o cartão magnético e desobrigue o cidadão a decorar seqüências numéricas, às vêzes estranhas e complexas [60]. Enquanto esta tecnologia não está

totalmente à disposição de todos os usuários de computadores, apresentamos um relato dessa evolução nos ambientes centralizados, existentes anteriormente, bem como nos ambientes distribuídos, implementados atualmente na RMI, objeto de nosso estudo. As diferenças de tratamento da I&A não são tão distintas nesses ambientes mas passaram a ser fundamentais nos ambientes descentralizados/

Nos ambientes centralizados, predominantes até o início da década de 80, prevalecia o sistema de senha por usuário para acesso remoto aos recursos computacionais. Havia algumas exceções, como nos ambientes baseados em *mainframes* Unisys® (na época denominada Burroughs) que podiam trabalhar com identificação por recurso. Ao precisar de um serviço ou recurso, o usuário se identificava e era autenticado por mecanismos próprios do ambiente em que estava trabalhando[59]. A ele era, então, concedido o acesso ao recurso em função de aceitação de sua I&A. Adicionalmente, tais ambientes eram, e ainda o são, cercados de um aparato de proteção do acesso físico. Para se ter acesso a terminais, impressoras, discos magnéticos, unidades de processamento, arquivos de segurança, dentre outros, são necessários procedimentos de autorização específicos, como reconhecimento por uma pessoa encarregada da liberação de determinado acesso, não existindo, nesse caso, um procedimento informatizado ou automático.

O usuário dos ambientes centralizados recebia uma identificação conhecida como *login* ou ID de usuário, geralmente de utilização individual, juntamente com uma senha associada a este *login*, que era seu instrumento de autenticação. Prevalecia nesses ambientes a tese do fator único de autenticação, ou seja, desde que informados o *login* e a senha, o usuário estava autorizado a utilizar os recursos do ambiente de acordo com seu privilégio de acesso. Este procedimento nos ambientes descentralizados promoveu

um dos fatores de aumento da vulnerabilidade, pois o usuário passou a ter identificação diferente em computadores diferentes e, até mesmo, para serviços e sistemas diferentes.

Os procedimentos típicos de um ambiente centralizado refletiam, e determinavam, em parte, o distanciamento dos usuários da informática em relação ao ambiente computacional e seus recursos. O advento e disseminação da microinformática, com os computadores conectados em redes remotas[12], transformaram essa relação de distanciamento, invertendo as práticas relativas aos fatores de segurança. Os recursos, na maioria dos casos, passaram a estar mais próximos dos usuários, com esse usuário assumindo o controle do acesso ao recurso e dependendo cada vez menos da autorização e concessão de um gestor centralizado. Nessas situações, o nível de segurança diminuiu por diversos fatores, especialmente o cultural, que deu a esse usuário oportunidades que ele não tinha quando o controle e gerenciamento de acesso eram centralizados. Confirmamos essa premissa em [11], quando o autor descreve os aspectos relevantes na proteção de bens de informação e as características de redes de microcomputadores, e confirma a diminuição das exigências dos usuários de redes descentralizadas no tocante a itens de segurança.

Embora os requisitos de segurança aplicados nos ambientes centralizados fossem utilizados como paradigma para os novos ambientes computacionais da década de 80, nem todos eles foram reproduzidos [58]. Na maioria dos casos, a cópia de técnicas utilizadas para terminais de redes centralizadas não produziu o efeito desejado nas redes de microcomputadores[13], independente da tecnologia adotada para montagem dessas redes. É certo que, dependendo da tecnologia, o nível de segurança da rede era, e ainda é, maior ou menor em relação aos problemas que discutimos. Uma das razões para

[12] Redes de computadores que utilizam comunicação de longa distância.

o aumento da vulnerabilidade é que a dispersão de equipamentos em um ambiente descentralizado não se restringe aos limites físicos das organizações; essa distribuição aumenta a possibilidade de uso indevido das redes de computadores [64]. As Figuras 1 e 2 tentam demonstrar um aumento da vulnerabilidade a partir da transformação de ambiente centralizado em descentralizado.

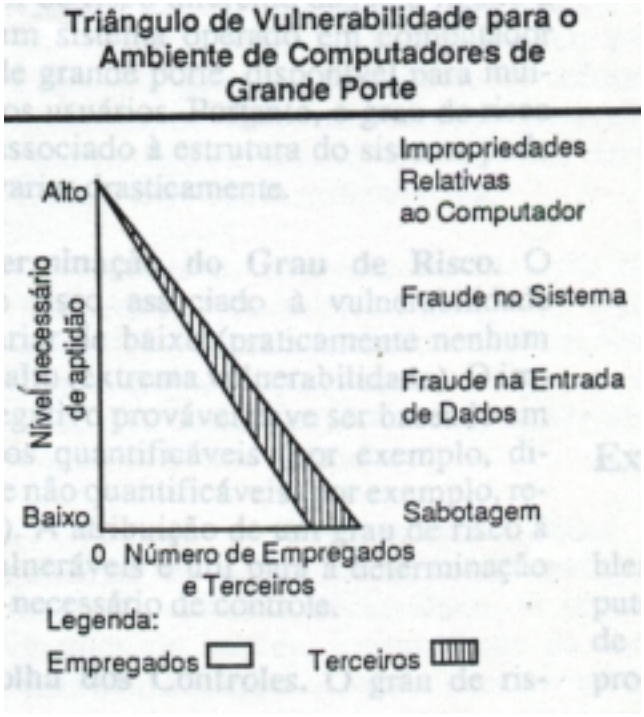


**Figura 1 - Vulnerabilidade em Ambientes de Grande Porte (extraído de [64])**

A Figura 1 associa a fragilidade da segurança de uma rede a fatores como: sabotagem; fraude na entrada de dados; fraude no sistema e impropriedades relativas ao computador de grande porte praticadas por empregados diretos e terceirizados. Exige-se um nível de aptidão dos usuários para que se diminua a possibilidade desta rede ficar vulnerável. A possibilidade de se cometer uma sabotagem é comum a um número maior de pessoas, decrescendo quando analisamos o nível de aptidão ou oportunidade para

[13] Chaves que trancavam teclados não tinham a mesma eficácia de chaves utilizadas em terminais 3278 da IBM®, podendo sofrer

fraudar entrada de dados, fraudar o sistema e aproveitar-se de impropriedades do computador [64].

Se nos ambientes centralizados as formas de acesso físico e lógico encontravam-se previstas em regras de segurança definidas e acompanhadas através de controles rígidos, os ambientes distribuídos trouxeram consigo a necessidade de se definir o que deveria estar acobertado por regras de segurança e qual forma de acesso deveria ser privilegiada.

A introdução e disseminação de microcomputadores em ambientes de escritório, a formação de sistemas em rede com compartilhamento de dados e recursos e o reconhecimento de que os dados e informações de qualquer corporação são bens valiosos levaram à constatação de que novos métodos de segurança precisavam ser definidos para proteger esses bens [58]. A transformação de sistemas monousuários[14], executados num único computador, para utilização numa rede de computadores deveria vir acompanhada da mudança de critérios para a nova situação de recursos compartilhados. Em [3] esta situação é claramente representada quando é feita a comparação entre as atividades para controle de senha em *mainframes* e àquelas necessárias aos ambientes de redes utilizando microcomputadores, onde nem sempre é definido um gerenciador centralizado. Isso explica o gráfico da Figura 2, onde é verificado um aumento da vulnerabilidade nesse ambiente em função do aumento de pontos de fornecimento de serviços e principalmente pela dispersão de gerenciamento de I&A. O aumento de pessoas tendo acesso a uma rede de computadores aumenta a vulnerabilidade da mesma se considerarmos as ameaças previstas nas Figuras 1 e 2. As

um ataque com maior facilidade em função do Sistema Operacional do microcomputador.

[14] Sistema ou aplicativo de computador onde somente uma pessoa trabalha ao mesmo tempo.

áreas dos triângulos representadas na Figura 2 relacionam-se ao aumento da condição de vulnerabilidade com o aumento dos microcomputadores.

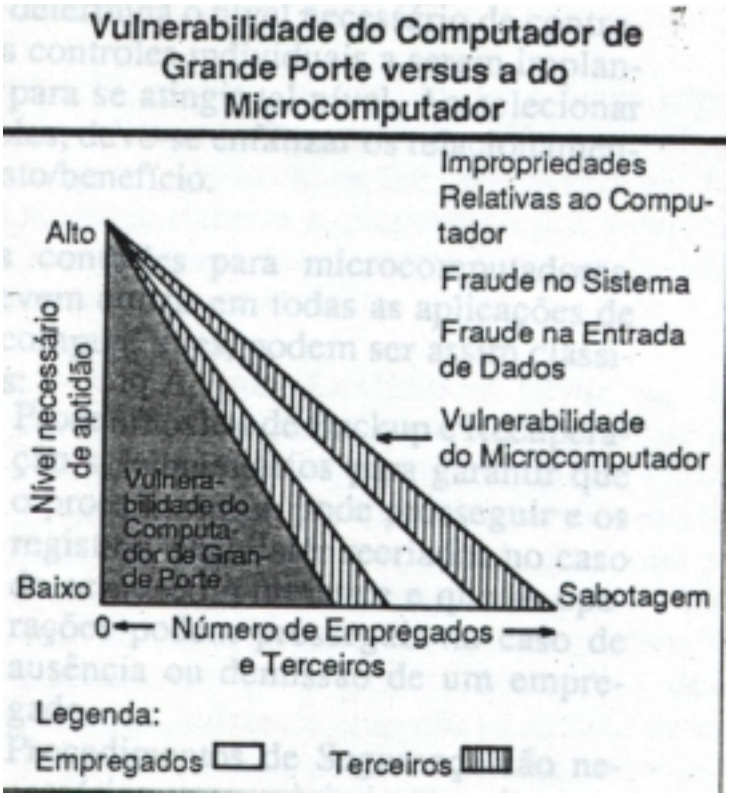


**Figura 2 - Vulnerabilidade de Microcomputador x Grande Porte (extraído de [64])**

Foi, portanto, a mudança das organizações, de seus respectivos negócios, do aumento no número de usuários e da forma de trabalho proporcionada pelas redes de computadores que provocaram uma alteração na concepção de como tais ativos da informação devem ser tratados e protegidos.

A partir desse momento, quando os computadores pessoais passaram a dispor de tecnologia que permite fácil comunicação com os demais computadores de redes descentralizadas com acesso público a qualquer cidadão, identificamos o aumento das ameaças, pois qualquer usuário externo às redes passou a ter condições técnicas de invadir determinada rede, colocando em risco a base computacional antes considerada

confiável. Ressalta-se que esta premissa não é automaticamente aplicável a qualquer rede descentralizada.

### *3.2 - Políticas de Segurança*

Neste trabalho, conforme mencionado no Capítulo 2, não trataremos do assunto segurança em redes de computadores como um todo. É essencial que se entenda a importância de alguns conceitos relevantes quando discutimos a questão específica de I&A. O conceito, ou estratégia, que destacaremos aqui, diz respeito à necessidade de se introduzir políticas antes da adoção de qualquer ferramenta que trate de segurança.

Sabe-se que a maioria dos ambientes de informática que se preocupam com segurança, adotam diretrizes seguindo as orientações descritas no Livro Laranja e seus complementos, pelo fato de seus administradores entenderem que a maioria das proposições ali contidas são aplicáveis e adequadas a qualquer rede de computadores. Mesmo que seja uma simples linha concedendo liberdade total de critérios para I&A é importante que se tenha documentação escrita para cada ambiente de informática, caracterizando assim uma política de segurança. É necessário que haja discussão e decisão sobre as políticas a serem implementadas e, *a priori*, não devemos considerar que uma política de segurança é correta ou incorreta. A adoção de uma política de segurança deve ser tomada a partir dos requisitos de cada ambiente, considerando, às vezes, que ambientes semelhantes requererem políticas diferentes.

Uma das motivações mais relevantes para se criar uma política de segurança destinadas ao uso de computadores é assegurar que esforços despendidos em segurança tragam benefícios consistentes. A adoção de políticas é necessária como prevenção à

ocorrência de problemas e é de difícil mensuração econômica e financeira pois trata-se de aplicar recursos para que não aconteçam situações indesejáveis.

A proposição de uma política deve fundamentar-se na análise do risco em que a rede de computadores está envolvida. É um processo de se ordenar todos os riscos, avaliar os níveis de gravidade caso os mesmos se tornem realidade. Normalmente uma política de segurança deve ser a base para que a administração de um ambiente operacional utilize os recursos financeiros objetivamente avaliando a tecnologia adotada e principalmente o custo do que se está protegendo. A evolução das redes tem tornado a avaliação de recursos de informática vinculados a tecnologia da informação cada vez mais complexa de mensuração, portanto as avaliações dos riscos estão cada vez mais difíceis de determinar, definir e quantificar.

No caso da I&A é fundamental o estabelecimento de critérios de acesso lógico, para que se tornem uma Política de Acesso Lógico a uma rede. O principal propósito de uma política de segurança é informar aos usuários, profissionais e gerentes, as suas obrigações para proteção da tecnologia e do acesso à informação. A política deve especificar os mecanismos através dos quais esses requisitos podem ser alcançados, sem contudo determinar os produtos que serão utilizados. Outro propósito é oferecer um ponto de referência a partir do qual se possa adquirir, configurar e auditar sistemas e redes, para que sejam adequados aos requisitos propostos. Uma política de segurança também deve expressar, tão explicitamente quanto possível, o que os usuários devem e o que não devem fazer evitando ambigüidades e maus entendidos.

A partir da participação de administradores de rede, técnicos de tecnologia da informação, representantes de usuários, profissionais diretamente ligados aos recursos

que serão protegidos, além das equipes de especialistas em segurança, uma boa política de segurança deve ter as seguintes características gerais:

- Deve ser implantada através de publicação de instrumentos administrativos e métodos apropriados de divulgação.
- Deve poder ser aplicada com ferramentas apropriadas e prever sanções onde as soluções técnicas não sejam implementadas.
- Deve definir claramente as áreas de responsabilidade para os usuários, administradores e gerentes de redes.

É importante reconhecer que sempre existem expectativas para cada regra de uma política, portanto este conjunto de regras deve permitir a flexibilidade de serem alteradas, excluídas além da inclusão de novas regras na política, de forma que a mesma não fique obsoleta nem tecnicamente inviável com o passar do tempo.

# 4 - Controles de acesso

*"As aparências enganam"*
**Dito Popular**

## *4.1 - Controles Físicos de Acesso*

As políticas e sistemas implementados para o controle de acesso físico aos ambientes centralizados mostram-se adequados às configurações de redes existentes, mesmo que falhas eventuais possam ser constatadas [59]. Esse sistema de proteção parte do pressuposto de que se uma pessoa não consegue entrar na sala onde estão os computadores, os sistemas e recursos informacionais estão suficientemente protegidos.

Consequentemente, poderíamos supor que essa segurança fosse suficiente, mas não é. Normalmente, empresas especializadas em segurança para ambientes informatizados iniciam seus trabalhos com testes de invasão física [31], e na maioria dos casos essa segurança é facilmente burlada através de disfarces ou ações simples que enganam as pessoas, como fazer-se passar por alguém que já trabalhou na empresa que está sofrendo o teste. Entretanto, são muitas as vulnerabilidades que crescem e se intensificam nesses ambientes e somente o controle de acesso físico não é suficiente para determinar a segurança, principalmente em ambientes que usam redes de computadores. A disseminação de redes distribuídas modificou a relevância do controle de acesso físico. A pulverização de pontos que passaram a ter equipamentos ligados às redes de computadores das empresas, ampliou a possibilidade de acesso lógico, esterilizando a infalibilidade das regras e políticas de acesso físico e reduzindo a eficácia de sua proteção. Essa nova conformação de vulnerabilidade remete à necessidade de novas formas de controle do acesso físico e lógico. O aumento das

facilidades remotas exigiu que os cuidados normalmente tomados em termos de acesso ao computador principal da rede fossem implementados para cada um dos computadores com possibilidade de acesso.


**Figura 3 - Principais Pontos de Invasão (extraído de [40])**

No entanto, é muitas vezes impossível controlar o acesso de pessoas aos locais onde há computadores conectados a uma rede, e ressalta-se o fato de que a maioria dos casos de invasão a servidores localizados internamente a uma organização e quebra de condições de segurança são provenientes de *insider attacks*[15], conforme a Figura 3, sendo que esta situação reflete pesquisa realizada no Brasil em 1999 [40]. Na figura, são considerados usuários internos mesmo aqueles que utilizam acesso remoto de serviços das redes. Informações do Computer Security Institute - CSI, de San Francisco (EUA), publicadas em março de 2000 [47], apresentam a tendência de que este parâmetro esteja se invertendo e os ataques a redes de computadores provenientes da Internet já representam 59% do total, contra 38% de ataques iniciados a partir dos computadores de redes internas.

No caso da RMI o quadro é reproduzido e pode acompanhar a tendência de que os ataques externos passem a ser maioria, à medida em que sistemas e serviços são

[15] Ataque originado por computador sem conexão remota, a partir ou do mesmo segmento rede protegida (WAN ou LAN),.

colocados na Internet. Uma estratégia que agrava o quadro apresentado é a necessidade de se conectar todos os computadores da Administração Municipa à RMI. Aliada à possibilidade de acesso a partir dos computadores de cada cidadão e da sociedade civil organizada, há ainda a possibilidade de que todos estes usuários passem a ser considerados como usuários internos de sistemas da RMI. A situação torna-se particularmente dramática ao se permitir que a rede interna da PBH possa ser acessada a partir da Internet e vice-versa. Essa possibilidade praticamente anula os cuidados com o acesso físico, tornando-se necessário o reforço nas regras e políticas de acesso lógico. A analogia que podemos utilizar aqui é com o controle das companhias telefônicas sobre os aparelhos de seus usuários e o uso que cada um deles dá aos serviços colocados à disposição pelas concessionárias. As antigas centrais telefônicas tinham as suas comunicações controladas manualmente por telefonistas ou operadoras de centrais e mesmo com os aparelhos telefônicos descentralizados o controle era central. A partir de sua evolução tecnológica, essas centrais telefônicas deixaram de ter o controle sobre os aparelhos e serviços utilizados e os usuários passaram a fazer conexões sem a supervisão de uma central, sendo a contabilização da utilização sua principal função. Os computadores em rede, contrapondo-se aos computadores e terminais gerenciados por um *mainframe*, foram ficando cada vez menos submetidos a um controle central.

Um aspecto importante de controle, que se reproduz no acesso físico em ambientes distribuídos, refere-se aos elementos usados para conexões de comunicação entre os principais pontos das redes. O aumento na quantidade de cabos, torres de comunicação, quadros de passagem, fiação e outras partes componentes dessas redes constituem pontos de acesso físico diferentes, os quais, em determinados casos, não estão sujeitos aos mesmos controles vigentes na localização física principal da rede. Se

associarmos a esse quadro as questões relacionadas ao controle de acesso aos equipamentos de comunicação, tais como roteadores, *hubs*, *switches* e suas respectivas conexões, o resultado é um ônus ainda maior no que se refere às responsabilidades de um sistema de segurança, com a distirbuição do foco da segurança física também por esses equipamentos periféricos de comunicação entre redes.

A evolução para as redes distribuídas e descentralizadas requer a ênfase na proteção física das redes especialmente destinadas ao gerenciamento e controle e nos locais onde se encontram os equipamentos utilizados para gerenciamento de seus elementos, além daqueles equipamentos utilizados como servidores em centros de informação vitais para os usuários.

Seria necessário que tais equipamentos estivessem sujeitos às mesmas especificações de segurança física dos tradicionais centros de processamento de dados que abrigavam os computadores de grande porte. Os equipamentos de conexão de redes são tão importantes, do ponto de vista das vulnerabilidades de acesso, quantos os servidores da redes. No entanto, os custos, as dificuldades relativas a procedimentos, as tecnologias diferenciadas e os recursos necessários à proteção das redes descentralizadas e de seus componentes, dificultam a implementação de níveis de segurança similares aos aplicados em ambientes físicos de *mainframe*.

Se nos ambientes centralizados o controle de acesso físico permite que se enfatizem menos os procedimentos e recursos relacionados com questões de acesso lógico, nos ambientes distribuídos, os recursos financeiros necessários para garantir o mesmo nível de controle podem inviabilizar a implantação de recursos computacionais ou mesmo sua utilização por parte dos usuários. Em função disso, os critérios de escolha para definir o que deve ser protegido, e em que níveis de rigidez, precisam ser

firmados para determinação do risco aceitável para o ambiente operacional, conforme citado nas políticas de segurança (Capítulo 3). Neste ponto, começamos a entender que a preocupação com o acesso lógico em redes descentralizadas deve aumentar para que se mantenham requisitos mínimos de segurança.

### *4.2 - Vulnerabilidades no Acesso Lógico*

Algumas condições que possibilitam a ocorrência de falhas de segurança nos sistemas de informação serão apresentadas a seguir para a continuidade do raciocínio que leva, mais uma vez, à integração entre controle de acesso físico em ambientes centralizados e controles de acesso lógico em ambientes descentralizados. Neste momento, devemos considerar a existência de perturbações potenciais, que colocam em risco os serviços de sistema de informação e que fundamentam, em grande parte, a preocupação com a segurança em computadores. A ênfase do tratamento desloca-se do conceito de acesso físico para as conceituações de acesso lógico, tornando menos importante o fato de o requerente do serviço de informática estar ou não fisicamente próximo do recurso por ele solicitado.

Inicialmente admite-se que o serviço prestado por qualquer sistema de informação ou recurso computacional deva estar plenamente disponível [5]. Nas figuras apresentadas a seguir, para esclarecer as possibilidades de quebra da normalidade dos serviços de uma rede de computadores, consideraremos o símbolo à esquerda como uma fonte de informação genérica ou representativa de qualquer recurso informacional, e que deve ser protegida pelos mecanismos de segurança; o símbolo à direita identifica o usuário ou destino da informação e é quem deve, e espera, receber todos os dados e

informações íntegras. O aparecimento de um terceiro símbolo ao centro caracteriza uma ameaça ou violação de segurança [5].

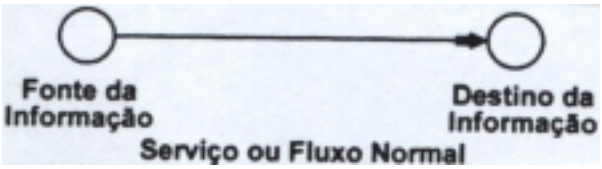


**Figura 4 - Fluxo Normal (extraída de [5])**

A Figura 4 representa essa condição de fluxo normal, em que o ponto denominado fonte da informação está ligado ao destino da informação sem que nenhuma barreira seja colocada entre eles. Como essa é a situação desejada para que se garanta a disponibilidade do serviço e das informações, podem ser estabelecidos mecanismos adicionais de segurança como identificação, autenticação, criptografia, dentre outros, para que a ligação entre as partes se mostre mais confiável.

A situação da Figura 4 demonstra o que se espera de qualquer recurso de informática. No exemplo, a parte da figura identificada como destino da informação precisa de autorização da fonte para ter acesso a essa informação.

Do ponto de vista do usuário, ou destino da informação, é requerida a garantia de que o serviço ou informação que ele solicita estará disponível, e que esse mesmo serviço ou sistema de informação seja confiável e íntegro. Não cabe a ele, usuário, em primeira análise, tomar providências para que o ambiente seja completamente seguro. Entretanto, veremos mais a frente que depende dele a execução de alguns procedimentos básicos para se garantirem níveis de segurança mínimos.

Na situação seguinte, é mostrada uma das possibilidades de quebra da normalidade. A Figura 5 apresenta a situação em que o serviço, ou sistema de informação, não pode ser acessado pelo possível destinatário. A interrupção, ou

indisponibilidade da fonte da informação, pode ser involuntária ou ainda o resultado de ações de quebra da segurança da fonte. Um exemplo dessa última situação é a impossibilidade de acesso, para qualquer usuário, a determinado recurso.

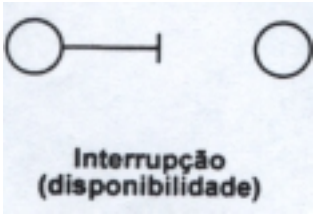


**Figura 5 - Interrupção (extraído do [5])**

A seguir, consideraremos todas as demonstrações como situação de vulnerabilidade proporcionada por sistemas sem a devida proteção. Tais anormalidades devem ser evitadas por sistemas de segurança e são, portanto, maneiras de quebra de confiabilidade possíveis entre computadores ligados em rede. A Figura 6 mostra mais uma dessas condições, conhecida como interceptação, na qual a fonte da informação mantém-se conectada com o destinatário, mas o fluxo deixa de ser confidencial. Um terceiro elemento, estranho à comunicação e não autorizado a ter esse tipo de acesso, passa a obter recursos e informações.


**Figura 6 - Interceptação (extraído de [5])**

Outra forma de ameaça é caracterizada pela perda do caráter confidencial e, adicionalmente, da integridade de qualquer sistema de informação. Essa hipótese é representada pela Figura 7 e mostra que, além de a informação deixar de ser

confidencial, um terceiro elemento envolvido promove a adulteração das condições iniciais e previstas.

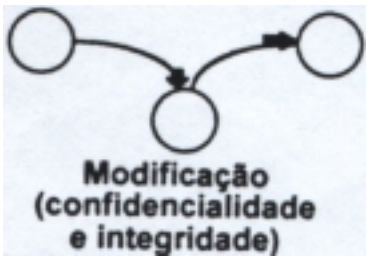


**Figura 7 - Modificação (extraído de [5])**

Nesse caso, o destinatário da informação a recebe de forma não confiável e, não havendo confirmação pelo emissor, não há garantias de que se trata de informação correta. Tal situação é também conhecida como modificação e representa uma vulnerabilidade adicional à interceptação.

Completando a lista de formas possíveis de vulnerabilidades, temos a fabricação, que está representada pela Figura 8 e mostra que um destinatário de sistema de informação não está recebendo as informações da fonte que ele deseja. No caso em que o emissor é diferente daquele desejado existem chances de alguém se passar por outrém [40], sendo que esta possibilidade é maior no mundo virtual do que no mundo real. A ausência de mecanismos de segurança como a certificação[16] proporciona ao solicitante de informações e recursos computacionais poucas garantias da integridade daquilo que ele recebe.

[16] Avaliação técnica dos recursos de segurança de um sistema, feita como parte e em apoio ao processo de aprovação/credenciamento de informação e recursos.

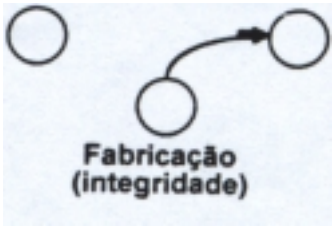


**Figura 8 - Fabricação (extraído de [5])**

Consequentemente, para que entendamos o trabalho que está sendo realizado, é necessário o dimensionamento das ameaças à segurança e das respectivas vulnerabilidades. As redes de computadores, cada vez mais, atuam com transferência de voz, dados, texto e imagem. Para cada um desses recursos devemos avaliar a forma de acesso, a tecnologia de transporte, as condições e recursos de armazenamento [5]. As vulnerabilidades existentes estão vinculadas à interrupção, à interceptação, à modificação e à fabricação, sempre considerando que os destinatários da informação podem ser sistemas computacionais e pessoas. Assim, cuidados devem ser tomados de parte a parte para que emissores e destinatários tenham garantias reais de que as trocas se sucedam da forma prevista, com ferramentas adequadas para garantir cada uma das condições de segurança desejadas.

### 4.2.1 - Disponibilizando uma Rede de Forma Segura

Nos ambientes informatizados onde sistemas de informação são utilizados, os recursos devem estar disponíveis o máximo possível para que se atenda a uma das vantagens da disseminação de redes de computadores, sendo que as ameaças previstas devem ser evitadas através de ferramentas e mecanismos de proteção.

Primeiro, devemos considerar os recursos a serem disponibilizados como uma relação de atividades, serviços de informação e recursos computacionais, utilizados para tratar e disponibilizar as informações estratégicas da organização.

Em segundo lugar, deve-se observar a disponibilidade dos serviços a serem oferecidos aos usuários. Qualquer condição adversa de falha dessa rede ou de seus serviços, provoca a falta de credibilidade em todo o serviço da rede. O simples fato de uma rede ficar indisponível provoca a quebra de confiança do usuário, independentemente da motivação da indisponibilidade da rede.

Finalmente, após esse conjunto de serviços estar preparado para funcionar adequadamente, devemos dar garantias aos usuários da rede quanto ao funcionamento dos serviços e à qualidade de informação proveniente dos mesmos, fazendo com que a confiança também seja refletida na troca de informações com outras redes de computadores, e provocando no usuário a sensação de que ele está trabalhando num ambiente de informática seguro e onde todos são identificados. Essa sensação deve ser confirmada a todo momento em que o usuário solicitar um serviço.

### 4.2.2 - Possibilidades de Obtenção Indevida de Senhas.

Nesse ponto é necessário aprofundar no tema do trabalho e destacar a utilização da senha como o principal recurso de I&A. Se admitirmos a hipótese de que somente a situação de fluxo normal é adequada (Figura 4), todas as demais situações de anormalidade só poderão ser confrontadas e verificadas caso seja feita a I&A dos usuários que solicitam serviços e informações. A tarefa principal é não deixar usuários se apropriarem de senhas que não sejam as deles.

Uma pesquisa sobre ambientes de informática indica que as senhas ainda são o tópico mais abordado em políticas de segurança [40]. Com base nesse trabalho, descreveremos algumas das várias formas possíveis de se obter senhas indevidamente. A credibilidade de uma rede de computadores pode ser determinada pela facilidade de obtenção das senhas de seus usuários. Existem diversas técnicas para obtenção de senhas, e as mais comuns estão descritas a seguir:

A) **Cavalo de Tróia (*Trojan Horse*) -** Nesta técnica, um usuário coloca um programa nocivo em determinado equipamento para que esse programa realize determinadas funções previstas e outras não previstas em situação de normalidade. Esse programa pode, por exemplo, executar funções de uma simples calculadora e ao mesmo tempo guardar IDes de usuários e senhas em um arquivo específico. Outro exemplo de programa que faz esse tipo de ação é aquele que grava tudo o que for digitado no teclado em um arquivo específico. O usuário que implantou o Cavalo de Tróia examina o arquivo de tempos em tempos e verifica a ocorrência de digitação de ID de usuário e senhas, fazendo com que os caracteres da senha estejam disponíveis para qualquer uso fraudulento. Essa técnica ainda é utilizada mesmo com a evolução de mecanismos de proteção às senhas [46].

B) ***Sniffer* em Redes -** O tráfego de informação entre os computadores permite a instalação, nos meios de transmissão, de programas que servem para verificar ou farejar (*sniff,* em inglês) o que transita nas redes. Esses programas têm a capacidade de verificar a presença de informações referentes a IDes de usuário e senhas, fazendo com que a ocorrência da mesma dispare uma cópia do pacote para que o *hacker* obtenha as

informações de que necessita. O mecanismo mais usado para combater essa vulnerabilidade é a criptografia de dados. Toda e qualquer informação que trafegue sobre um meio físico de ligação entre computadores ou redes de computadores e não esteja criptografada está sujeita a esse tipo de ataque. Ferramentas com essas características são encontradas na Internet e não requerem muitos conhecimentos para serem implantadas e utilizadas.

C) **Engenharia Social** - Uma das características presentes na informática é a de cunhar termos ou associá-los a termos emprestados de outras ciências. No caso de "Engenharia Social", esse tem sido o nome mais apropriado para caracterizar os subterfúgios usados pelos *hackers* para obter informações (inclusive senhas) e privilégios de outras pessoas desatentas ou inadvertidas. A Engenharia Social tem se tornado objeto de estudo das organizações [31] para que os trabalhadores e, especialmente os usuários de informática (por manusearem maior volume de informação organizacional), tenham cuidado com as técnicas de disfarce utilizadas. Um exemplo típico dessas artimanhas é relatado em [57], onde SHIMOMURA descreve as condições em que um rival cibernético apropriava-se de informações privadas de organizações ao ganhar a confiança de pessoas importantes nos ambientes informatizados, obtendo as informações de que precisava somente a partir dessa confiança. A Engenharia Social faz parte do cotidiano não só da informática, mas do mundo real. A cultura de certas profissões, os hábitos criados por muitos anos de determinado tipo de trabalho são alvos fáceis para técnicas simples utilizadas pelos que aplicam a Engenharia Social.

D) **Tentativa e Erro ou Força-Bruta** - É o jeito mais simples e mais antigo de desvendar senhas. Programas como o *Cracker*[17] vieram para facilitar a vida dos *hackers* e têm a função de examinar um determinado arquivo de senhas e testar as combinações de senhas candidatas, confrontando-as com as senhas necessárias a cada identificação de usuário. Esse método exige recursos de *hardware* e disponibilidade de tempo, pois gera ou assume seqüências variadas de caracteres testando cada uma dessas senhas candidatas para verificar se é a senha de um usuário. O aumento do tamanho da senha provoca um crescimento exponencial no número de possibilidades a serem testadas [58]. Com o aumento da capacidade computacional dos microcomputadores, os tempos necessários à descoberta de senhas têm diminuído drasticamente e as Tabelas 1 e 2 já têm, atualmente, seus tempos estimados diminuídos consideravelmente só em função da capacidade de processamento dos microcomputadores; mas ainda assim, elas servem para mostrarmos um exemplo obtido a partir de um equipamento com poder de processamento inferior aos existentes na atualidade. O equipamento utilizado foi de plataforma CISC, marca Intel®, modelo 386SX, com *clock* de 20Mhz. Computadores atuais (Pentium III, por exemplo) são até 100 vêzes mais rápidos e podem identificar senhas de 5 dígitos em aproximadamente 6 dias.

[17] Programa de domínio público (*freeware*) disponível em vários sites da Internet e que tem como objetivo descobrir senhas a partir de parâmetros pré-estabelecidos.

**Tabela 1 - Comprimento de Senhas e Tempo de Ataque (Força Bruta).**

| Comprimento da senha (caracteres) | Número de senhas candidatas | Tempo estimado para identificar todas as senhas |
|---|---|---|
| 1 | 36 | 36 segundos |
| 2 | 1.296 ($36^2$) | 21 minutos |
| 3 | 46.656 ($36^3$) | 12,96 horas |
| 4 | 1.679.616 ($36^4$) | 19,44 dias |
| 5 | 60.466.176 ($36^5$) | 1,9 anos |
| 6 | 2.176.782.336 ($36^6$) | 69 anos |
| 7 | 78.364.164.096 ($36^7$) | 2.484 anos |
| 8 | 2.821.109.907.456 ($36^8$) | 89.456 anos |

**Fonte: [58]**

Outra característica que aumenta o grau de dificuldade para o sucesso desses ataques é a utilização de um alfabeto de mais de 36 caracteres para a composição da senha. A Tabela 2 dá uma dimensão do aumento da dificuldade em se descobrir uma senha pela força bruta [58], onde a progressão geométrica se apresenta com maior ênfase.

**Tabela 2 - Número de Caracteres e Adivinhação de Senhas**

| Comprimento da senha (caracteres) | Número de senhas candidatas (36 caracteres) | Número de senhas candidatas (256 caracteres) |
|---|---|---|
| 1 | 36 | 256 |
| 2 | 1.296 ($36^2$) | 65.636 ($256^2$) |
| 3 | 46.656 ($36^3$) | 16.777.216 ($256^3$) |
| 4 | 1.679.616 ($36^4$) | 4.294.967.000 ($256^4$) |
| 5 | 60.466.176 ($36^5$) | 109.951.200.000 ($256^5$) |

**Fonte: [58]**

A evolução do poder de processamento dos computadores reduz essas dificuldades, mas isso pode ser compensado caso as senhas estejam criptografadas e tenham procedimentos de atualização e troca mais constantes, adotados através de política específica de proteção de senhas. Alguns destes procedimentos serão descritos em capítulo adiante. A falta de cuidado operacional com o acesso a um arquivo de senhas facilita o trabalho de descobri-las por força-bruta.

### 4.2.3 - Segurança Sob a Ótica do Usuário

Os conceitos de segurança e I&A apresentados até agora são dependentes de dois atores intervenientes. O primeiro é o provedor de sistemas de informação e recursos computacionais, a quem cabe tornar disponíveis as técnicas adequadas de proteção junto aos seus recursos, ferramentas e sistemas conforme as políticas estabelecidas. O segundo ator é o usuário dos recursos. Neste momento, faz-se necessário um detalhamento de como se processa a interface entre fonte e destinatário da informação, e como o usuário vê propostas para políticas de segurança.


**Figura 9 - Fases de Utilização de Senhas**

São quatro as fases esperadas, ressaltando-se que a ironia apresentada na Figura 9 não chega a ser absurda na vida real, observadas em várias situações do relacionamento entre os dois, no que se refere à segurança [38]. A primeira fase é conhecida como rejeição, quando o usuário não aceita facilmente as normas, regulamentos e procedimentos adicionais necessários para que se garantam certas condições de segurança. Após a fase inicial, entra-se numa etapa de adesão involuntária, quando o usuário, para não ser privado de recursos e serviços, na maioria dos casos adere aos procedimentos exigidos. A etapa posterior reflete uma mudança de comportamento, quando o usuário passa a entender que os procedimentos de segurança dizem respeito a garantias que ele mesmo exige. Finalmente surge o efeito da multiplicação, quando esse usuário entendendo a importância dos requisitos de segurança, passa a exigir e convencer outros usuários de que a melhoria das condições de confiança mútua são necessárias para evoluir nos procedimentos de segurança. Embora essas fases sejam tradicionalmente aceitas e verificáveis nas organizações, é possível que um usuário, ou grupo deles, não atue em determinada fase, indo diretamente a qualquer delas ou atuando em seqüência diferenciada da que apresentamos.

A partir dessas fases, a compreensão dos intervenientes sobre a responsabilidade coletiva de segurança da informação aumenta, ocasionando o comprometimento dos mesmos com as atividades-fim das organizações. Ocorre a inversão da visão individualista, muito difundida a partir do advento dos computadores pessoais nas residências, em benefício da visão coletiva e profissional. Conseqüentemente, as organizações durante as fases iniciais podem apresentar problemas técnicos e prejuízos

ocasionados pela falta de harmonia na aplicação dos requisitos mínimos de segurança [40].

## *4.3 - Controles Ideais e Aplicáveis*

Apresentadas as deficiências, podemos imaginar situações que minimizem as vulnerabilidades a que estão submetidas as redes de computadores. O controle ideal, do ponto de vista da segurança em informática e, especialmente, para adoção de critérios de I&A, seria aquele que não tivesse nenhum custo financeiro e que garantisse a inviolabilidade completa de qualquer rede ou dos computadores ligados a essa rede. Essa fórmula mágica ainda não está disponível para aplicação nas redes de computadores, tornando-se necessário seguir inicialmente políticas de segurança e implantar procedimentos (informatizados ou não) que sejam eficazes na implementação dessas políticas, permitindo estabilidade e confiabilidade ao ambiente de redes, a um custo aceitável para aquilo que se pretende proteger.

As possibilidades de uma maior efetividade de controle em I&A passam, principalmente, pela implementação de políticas de uso de senhas, que façam parte da cultura do usuário de informática e não gerem, na maioria dos casos, custos financeiros adicionais de proteção.

### 4.3.1 - Controles Físicos de Acesso.

A partir da descentralização dos equipamentos e da possibilidade de acesso lógico às redes independentemente da localização física, torna-se importante focalizar a proteção no acesso físico àqueles equipamentos e recursos vitais para o funcionamento da rede. As premissas e políticas estabelecidas para acesso aos *mainframes* devem ser

reproduzidas nos ambientes que abriguem computadores de controle da rede, nos locais onde existam impressões de informações estratégicas, nos compartimentos e salas que abriguem equipamentos de conexões de rede e nos espaços onde estejam armazenados os servidores de dados e aplicações [59].

A proteção desses componentes principais de redes descentralizadas, aliado à implantação de procedimentos de acesso lógico, contribui para a diminuição de acesso não autorizado ao ambiente. Adicionalmente, não pode ser desprezada a possibilidade de que vulnerabilidades físicas continuem existindo, mesmo que tenhamos detectado um movimento de ênfase ao acesso lógico. Do ponto de vista da segurança em geral, é essencial, sempre que possível, a manutenção de controles de acesso físico independente das possibilidades de acesso lógico.

### 4.3.2 - Controles Lógicos de Acesso.

Os controles lógicos de acesso, com a utilização adequada de senhas, identificam, verificam e restringem usuários para acesso ou não a atividades e recursos [58]. São importantes a determinação e implantação de critérios com previsão para:

Proteção seletiva de acesso às bases de dados;

Função administrativa com habilidade para concessão e outorga de acesso;

Identificação e documentação das tentativas e violações de acesso.

Assim, o administrador do ambiente deve ser capaz de identificar os recursos ofertados por ele, quem tem acesso a esses recursos e em quais condições, utilizando mecanismos que permitam identificar cada usuário univocamente. Deve, ainda, ser capaz de corrigir problemas no menor tempo possível e ter ferramentas e recursos para

tal, além de documentá-los para que não ocorram uma segunda vez, ou para que não tenham as mesmas conseqüências da primeira ocorrência.

### 4.3.3 - Outros Controles.

Para o bom funcionamento de uma rede de computadores, outros controles devem ser adotados para que a vulnerabilidade de uma rede não fique concentrada num ponto específico e coloque em risco os demais procedimentos e controles. Devem ser previstos, pelo administrador do ambiente, procedimentos discricionários[18] que permitam: A) Controle do pessoal autorizado a ter acesso aos equipamentos e pontos vulneráveis da rede; B) Controle no desenvolvimento de aplicações; C) Controle possível nas estações de trabalho; D) Controle dos servidores similar à proteção dada aos *mainframes;* e E) Procedimentos específicos para transmissão de dados.

No caso da RMI, a heterogeneidade dos ambientes e a dispersão física dos pontos de acesso aos recursos da rede justifica a delegação de responsáveis pelo controle das redes locais. Esses profissionais, administradores de segurança da rede, devem se orientar pelas políticas gerais de segurança e pelas condições de acesso físico e lógico que forem estabelecidas, além de propor controles com maior acuidade caso a rede sob sua responsabilidade requeira este tipo de procedimento. Ressalta-se que estes controles locais não devem ser menos exigentes que os controles da política de segurança geral para que pontos de vulnerabilidade específica não sejam criados devido a tolerância ao desrespeito das normas gerais estabelecidas.

[18] Forma de restingir acesso baseado na ID do usuário e/ou nos privilégios que ele pode possuir.

# 5 - Arquitetura de Segurança e Controle de Acesso

*"Você entrará num caixa eletrônico e*
*vai só olhar para o visor. Em apenas 2 segundos,*
*um scanner vai esquadrinhar seu olho ...*
*A identificação está feita."*
**Ricardo Setti [60]**

A partir das fundamentações e conceitos gerais sobre segurança apresentados, discutiremos temas ligados diretamente à questão de senhas ou, mais especificamente, sobre I&A, controles de acesso, administração desses controles, quesitos necessários à auditoria para manutenção do funcionamento de ambientes computacionais e, ainda, ferramentas para apoio à segurança de redes de computadores.

## *5.1 - Utilização de Senhas.*

O uso de senha como recurso de I&A tem sido o mecanismo mais utilizado nas políticas de segurança com vistas ao provimento de acesso aos recursos informacionais [40]. Tradicionalmente, as senhas associadas a um ID de usuário são conhecidas como senhas reutilizáveis[19]. Essas senhas, na maioria dos casos, exigem que o usuário seja autenticado através de terminais ou computadores centralizados. A utilização dessas senhas através de rotinas repetitivas de certificação provoca a necessidade de tratamento adequado às mesmas.

Utilizam-se senhas para provedor de acesso à Internet, para os vários sistemas nas redes das empresas, para cartões bancários, para *home banking*[20] e em outros

[19] Senha que não se altera a cada utilização feita pelo usuário.
[20] Serviço de acesso a serviços bancários feito da própria residência do cliente do banco utilizando teleprocessamento.

ambientes, dependendo do nível de tecnologia utilizado pelos cidadãos. Essa situação faz com que os usuários sejam compelidos a ter senhas fáceis de decorar e, geralmente, senhas iguais para os vários ambientes. Assim, fica facilitado o trabalho de quebrar o segredo das senhas por tentativa e erro e, por conseqüência, quebrar a segurança das redes de computadores.

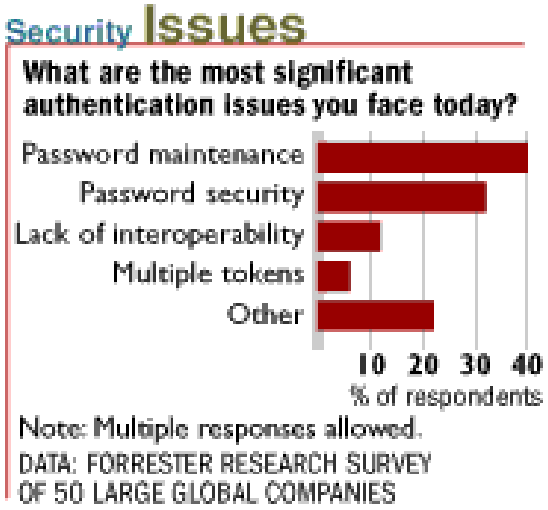


**Figura 10 - Uso de Senhas (extraído de [34])**

São fáceis de entender os riscos de segurança envolvendo senhas. A utilização de senhas associadas a um ID de usuário é a forma utilizada de aplicação de um mecanismo de I&A, pois é um recurso presente em todos os sistemas ADP, mas sua eficácia depende basicamente da maneira como são implementadas as políticas de segurança e da maneira como o usuário as utiliza. A Figura 10 reforça a informação de que senhas ainda hoje são bastante utilizadas pelas grandes corporações, possuídoras de grandes redes de computadores [34].


**Figura 11 - Problemas com Segurança (extraído de [40])**

Conforme mostrado na Figura 11, uma grande parte dos problemas está diretamente associado à utilização indevida dos recursos pelos próprios funcionários das organizações que utilizam os serviços e sistemas nos computadores [40]. O gerenciamento de redes permite usuários distantes dos centros gerenciadores, dificultando a identificação desses usuários, por ocorrerem situações em que a autenticação não pode ser feita ou é feita somente pela senha, sendo que nenhum programa de segurança irá detectar falhas se um usuário não autorizado estiver usando uma senha que não é a sua.

Um diálogo possível de se ouvir em ambientes de rede é reproduzido a seguir e, mesmo que em tom de brincadeira, dá uma visão de como são tratadas as questões relativas a senhas. É nessas possibilidades que devemos atuar para propiciarmos o uso adequado do mecanismo de acesso através de senhas.

"Segurança da Senha.

- Alô! É da segurança?
- Sim! Em que podemos servi-lo? Quem está falando?
- Aqui é do Departamento de Vendas da cidade de Ouricuri!
- Vocês são da nossa empresa?
- Claro! Somos o melhor departamento de vendas não-capital!
- Sim… fale!
- É que eu esqueci minha senha…
- Mas como esqueceu?
- Esquecendo, ora bolas! Esquecendo! Você já esqueceu seu guarda-chuvas em algum lugar?
- Claro que sim!
- Então? Esqueci minha senha!
- Tudo bem! Vamos… aguarda aí que vamos ligar de volta para você!

- ???? (alguns minutos depois…)
- Alô! Foi você que perdeu a senha?
- Sim. E liguei para vocês. Vocês acharam?
- O quê?
- A senha!
- Claro que não… olha vamos lhe dar uma nova senha e você vai trocar por uma senha sua. (alguns minutos depois…)
- Está dando senha incorreta? Qual é a senha correta?
- Não existe senha correta!
- Como não? O computador está dizendo senha incorreta. Se existe senha incorreta existe uma senha correta.
- Veja só, meu caro amigo, você tem que digitar a senha sob certas regras…
- Que regras?
- São regras simples… você não pode começar a senha com zero…
- Por que não pode começar com zero?
- Porque não pode! Definiram que não pode e não pode!
- E o que eu posso?
- Olha… a senha tem que ter um tamanho mínimo de 128 posições e um tamanho máximo de 1024 posições. Não pode ter vogal… a não ser que seja um conjunto de duas vogais seguidas de uma consoante que gere um som nasal!
- O quê!?!?
- É… e não pode deixar espaços, tem que conter 15 caracteres especiais, exceto se usar três caracteres iguais a partir da posição 64, não pode repetir as últimas 2048 senhas, … e … não pode ter siglas… e não pode… e não pode… e não pode…
- E a nova etiqueta? Vocês vão mandar?
- Etiqueta?
- Sim!
- Que etiqueta?
- A etiqueta para eu escrever a senha e colar no vídeo! A atual é muito pequena… e com essas novas regras de segurança… preciso de uma etiqueta maior…" [25].

Mesmo parecendo exagerado, esse é um ponto importante da questão da utilização de senhas como I&A. A dependência em relação à cultura dos usuários é alta e a ela está vinculada a segurança de toda uma rede. O equilíbrio da exigência ao usuário e a utilização de mecanismos de apoio podem contribuir para a melhoria desse tópico. Por exemplo, o usuário tem o direito de esquecer a senha e deve existir uma função na administração de segurança que possibilite a alteração dessa senha pelo próprio usuário ou por um administrador responsável. O acesso lógico deve ter características amigáveis aos usuários. Caso seja complicado o acesso aos controles de senhas, ou as regras de composição de senha sejam difíceis, fica comprometida a utilização dos mesmos.

### *5.2 - Administração de Acesso*

A forma mais simples de se obter acesso a computadores é através do uso de uma senha. Esse tipo de I&A é frágil e sofre várias vulnerabilidades [20] [21] [32]. Funções e regras, aplicáveis e de consenso geral reduzem algumas das vulnerabilidades já apresentadas e devem ser básicas em qualquer instalação de computadores.

Inicialmente, um fator importante a ser implementado é a separação das funções de gerenciamento de usuários e gerenciamento de acessos. As funções de cadastrar usuários, atribuir-lhes uma senha e bloquear o acesso devem ser distintas das funções de acesso do usuários à leitura, alteração, gravação ou remoção de informações. Essa premissa serve ao propósito de se garantir aos usuários que um administrador de ambiente operacional não adquirirá poderes além dos que lhe são permitdos nem utilizar-se de prerrogativas indevidas para se passar por um deles e, caso esse administrador tenha sua senha quebrada, um possível invasor não provocará danos em outros ambientes. Essa separação é útil, pois assim pode-se dar importância e destaque à função de Gestor de Usuário[21]. Estariam sendo aplicados alguns preceitos que dariam aos usuários garantias de que ninguém, além dele, tem conhecimento de sua senha e de que somente o Gestor de Usuários tem a prerrogativa de atribuir-lhe uma nova senha. Sugere-se que essa nova senha, por sua vez, deva ter como característica a atribuição de uma única utilização, ou seja, uma senha que perde a validade imediatamente após ser utilizada, sendo conhecida como senha única ou senha atribuída. Desta foram estaria sendo garantido que após a utilização pelo usuário, nem mesmo o Gestor de Usuários poderia ter acesso aos recursos através do conhecimento da senha criada anteriormente.

[21] Função específica que pode ser realizada por profissional com outras atribuições, mas distintamente.

### 5.2.1 - Cuidados com Senhas.

Mais do que sugestões, as regras de utilização de senhas devem nortear a utilização de recursos em ambientes de rede e sua implementação deve ser auditável. Descrevemos a seguir algumas dessas regras e os motivos para que sejam seguidas [3], [17], [42], [55]. Esses motivos dizem respeito à possibilidade de qualquer usuário não autorizado ficar testando condições de quebra de segurança e ao fato de as redes de computadores dependerem da segurança existente e aplicada pelos usuários, individualmente. Estas regras podem ser agrupadas por característica de usuário, algumas são destinadas aos gestores de usuários, outras aos usuários em geral e algumas são mais adequadas a sistemas. Embora todos usuários devam entendê-las e aplicá-las, algumas devem ser atribuição de profissionais em áreas específicas

- **Senhas devem ser robustas.**

Considerando que uma senha robusta é aquela senha que adota critérios variados na sua formação, e não se inclui no rol de senhas que são facilmente descobertas por ferramentas como o *Cracker*, a senha é considerada robusta quando não pode ser obtida a partir de algoritmos que tentem quebrá-la e não conseguem. Nomes de familiares, datas de nascimento, números de telefone, repetição de letras e siglas de nomes pessoais, dentre outras opções, são adivinhadas com pouca ou nenhuma técnica, por qualquer *hacker* iniciante, e não fazem parte das senhas consideradas robustas. Um exemplo de senha que atende ao requisito de robustez e não precisaria ser escrita pode ser extraída da frase: "Todo dia desde 80 acordo feliz", com o usuários utilizando-se da primeira letra de cada palavra formaria a senha "tdd80af", sendo que para dar mais uma característica de dificuldade à adivinhação da mesma algumas letras poderiam ser maiúsculas, transformando a senha em "Tdd1980AF". É

óbvio que essa senha com esta lógica de formação deixa de ser segura a partir da publicação deste trabalho.

- **Senhas devem ser de uso individual.**

Considerando que a senha é individual e que nos ambientes computacionais organizados os usuários têm seus privilégios vinculados à sua autorização de acesso[22], não deve ser permitida a utilização de senhas de usuários por empréstimo ou qualquer outra motivação. A auditoria deve ser sempre fundamentada na permissão de acesso dada pelo sistema e não pelo conhecimento da pessoa que utiliza. Os mecanismos de identificação biométricos contribuem para a eliminação dessa condição de vulnerabilidade e serão abordados posteriormente.

- **ID sem utilização de senha devem ser restritos.**

A idéia é de que qualquer ID de usuário que exista na rede não possa ser utilizado sem que tenha uma senha associada. Nos casos em que for necessária a utilização de usuários anônimos, como por exemplo em serviço de transferência de arquivos (FTP), os mesmos devem ter o acesso restrito ao ambiente do serviço requisitado e com o acompanhamento de auditoria mais detalhado.

[22] Permissão concedida a usuário, programa ou estação de trabalho, para usar certos programas ou conjunto de dados ou sistemas.

- **Senhas não devem ser anotadas indiscriminadamente.**

Procedimento a ser evitado, comum quando os mecanismos e regras para composição de senhas são complexos, ou quando a exigência por troca de senhas em curtos períodos de tempo é grande. O usuário utiliza-se do recurso de anotar sua senha em locais de fácil acesso (terminais, vídeos, teclado etc.) para que não a esqueça. Costuma ocorrer também quando a ID do usuário é de utilização coletiva. A melhor maneira de evitar esta situação é permitindo que o usuário tenha uma senha difícil de ser adivinhada mas fácil de ser memorizada. Como já exemplificado, uma boa técnica consiste em escolher um conjunto de palavras, ou uma frase que faça sentido para ele, e usar letras desta frase.

- **Senhas não devem ser digitadas na presença de outras pessoas.**

Esse procedimento simples, recomendado constantemente quando se trata de senhas de cartões bancários, nem sempre é observado pelos usuários de computadores em rede. O roubo de senhas numa rede chega a ter poder destruidor similar ao roubo de uma senha de cartão magnético bancário. Os usuários devem evitar que outras pessoas saibam suas senhas simplesmente olhando a sua digitação. Os usuários que costumam ter a mesma senha para várias funções (cartão bancário e sistemas de informática) correm risco maior ao exporem suas senhas no momento da digitação pois o fraudador pode fazer tentativas de utilizá-la em ambientes diferentes daquele em que o usuário deixou a senha vulnerável.

- **Programas de armazenamento devem criptografar senhas.**

A tecnologia permite que os dados armazenados sejam criptografados para maior segurança e para não permitir que usuários com privilégios de administrador de sistemas tenham acesso a estes dados. O custo desse tipo de tecnologia pode ser insignificante dependendo do sistema operacional utilizado. É importante que as senhas sejam sempre armazenadas com algoritmos fortes de criptografia.

- **Senhas devem ser trocadas regularmente.**

Tão logo o usuário suspeite que a sua senha esteja violada, ou ao constatar qualquer anormalidade, deve providenciar a substituição da mesma. Adicionalmente, o usuário deve ter o hábito de trocá-la em períodos regulares. Normalmente, os períodos para troca devem ser estabelecidos por normas gerais numa política de segurança e forçados pelo administrador do ambiente operacional, que possui ferramentas para tal procedimento.

- **Senhas originais devem ser substituídas.**

Os equipamentos e programas de computadores sempre vêm acompanhados de senhas *default* de seus fabricantes. É muito comum administradores de ambientes operacionais deixarem essas senhas em vigor. Esse procedimento é um dos primeiros a serem testados por *hackers* para invasão em roteadores e servidores. A mudança deve ser obrigatoriamente efetuada após a instalação do equipamento ou programa e sempre que uma nova versão do produto for atualizada.

### 5.2.2 - Soluções Propostas.

Durante o desenvolvimento deste trabalho, após o processo de implementação da RMI, sugerimos vários procedimentos para dotar os ambientes descentralizados de normas básicas de controle e acesso. O primeiro instrumento foi a "Norma de Controle de Acesso Lógico à RMI" (Anexo 3), que foi instituída para ser parâmetro para os usuários de serviços de informática. A Norma introduziu critérios distintos para usuário e gestor do ambiente operacional. Algumas diretrizes específicas foram publicadas para ambientes de sistemas operacionais diferentes, como Unix®, Windows NT® e OS/2®. Algumas recomendações presentes na norma são:

- Cada usuário tem uma única identificação para acesso definida de acordo com a Norma de Controle de Acesso Lógico à RMI.
- Cada identificação é associada a uma senha.
- A senha deve: (a) ter tamanho mínimo de seis caracteres; (b) possuir pelo menos dois caracteres alfabéticos distintos; (c) ser trocada a cada quatro semanas, no mínimo, e por uma senha diferente da anterior.
- A senha é de uso individual e intransferível, não devendo ser divulgada nem emprestada

Tal normalização não alcançou todos os servidores municipais e ficou restrita e passível de auditoria somente para o pessoal com vínculo trabalhista com a Prodabel. Uma legislação específica para o servidor municipal, potencialmente usuário de informática da RMI, talvez fosse necessária, mesmo avaliando que essa norma cumpriria somente o papel burocrático e não promoveria a mudança cultural, sendo pois

necessário uma campanha de conscientização para a importância da utilização correta das senhas de acesso aos computadores da RMI.

### *5.3 - Auditoria*

O processo de auditoria tradicional foi iniciado no século XIV, primeiramente na Inglaterra, quando foram apresentados relatos sobre exames feitos nas contas públicas. O aumento do volume das transações econômicas e financeiras levou os processos de auditoria para mecanismos formais e padronizados denominados "técnicas de auditoria". O trabalho conhecido como auditoria se ampara na utilização de técnicas próprias e procedimentos aplicados uniformemente durante o período determinado para auditoria. Neste sentido a auditoria tradicional procura trabalhar com as seguintes técnicas: (a) exame e contagem física; (b) exame de documentos originais; (c) conferência de cálculos; (d) exame de escrituração; (e) investigação minuciosa; (f) obtenção de informação de várias fontes; (g) exame de registros auxiliares; (h) estabelecimento de correlação entre as informações obtidas e; (i) estudos dos métodos operacionais.

Diferentemente da concepção de auditoria tradicional, que se fundamenta em fatos passados contrapostos a regras determinadas previamente, a auditoria voltada para I&A tem muito mais a contribuir na elaboração de normas e proposição dos itens que merecerão tratamento especial de armazenamento (trilhas de auditoria). É através das trilhas de auditoria que poderá ser feita a análise dos eventos de uma rede de computadores. Associados a essas trilhas de auditoria podem ser feitos planos de recuperação de desastres e apuração de responsabilidades [58]. Existe a necessidade de atuação de forma distinta da auditoria tradicional em função de que as técnicas

apresentadas por ela podem facilmente ser fraudadas pelo uso da tecnologia e da informática. É tarefa considerada simples a adulteração de registros auxiliares que possam comprometer a análise dos auditores.

No caso específico de I&A, a auditoria deve ter a garantia de que as pessoas que se identificam e autenticam são realmente quem dizem ser e que tudo aquilo feito nos ambientes operacionais, quando atribuído a um determinado usuário, foi realmente realizado por esse usuário. Dados de auditoria devem incluir desde a tentativa de se obter um nível de privilégio diferente do permitido para qualquer pessoa ou processo até o registro de alterações identificadas como relevantes para um sistema. Como exemplo aplicável à RMI, pode-se considerar que a auditoria deva criar alarmes que indiquem a possibilidade de falhas para rotinas específicas. Caso uma determinada rotina de alteração promova a mudança da alíquota de um contribuinte do IPTU acima de padrões considerados normais para o sistema, uma rotina de auditoria deve alertar os responsáveis pela segurança para que verifiquem as alterações efetuadas e certifiquem se são ou não corretas. Se o procedimento adotado foi o da auditoria tradicional, tal evento só será detectado no futuro, e possivelmente nem será detectado, caso não exista nenhum problema formal com o procedimento.

Todas as ocorrências de tentativas, bem sucedidas ou não, de mudança das condições de I&A devem ter suas ações registradas. Os dados colhidos pela auditoria devem estar rigorosamente protegidos, pois podem constituir valiosa fonte de informações para *hackers*, especialmente se na coleta contiverem ID e senhas de autenticação, mesmo criptografados. É, portanto, totalmente reprovável o armazenamento de senhas ou qualquer outro mecanismo de autenticação em trilhas de auditoria, sendo vital o armazenamento do ID de cada usuário.

Uma preocupação que deve estar constantemente ligada à área de auditoria, para constatação de problemas vinculados à I&A, é a verificação da legalidade dos mecanismos utilizados para coleta dos dados. Pelas experiências que acompanhamos no ambiente da RMI[23], a confirmação dos responsáveis por I&A é fundamental na resolução de dúvidas envolvendo ambientes informatizados. É factível, embora não seja um procedimento aceitável do ponto de vista da auditoria, que usuários da RMI realizem atividades nas bases de dados e, num momento posterior, repudiem o fato de a I&A serem deles. Nesse sentido, contribuímos para a redação e a publicação da "Instrução de Serviço" (Anexo 2), publicada pela Corregedoria Geral do Município - CGM, que dá tratamento de lei à utilização das senhas em redes de computadores da Administração Municipal de Belo Horizonte e que, em linhas gerais determina no seu art. 2º.: "O detentor de senha de acesso lógico a programa de computador da Prefeitura de Belo Horizonte deve: I - escolher senhas fáceis de lembrar mas difíceis de serem descobertas; II - manter absoluto sigilo, não divulgando, emprestando ou compartilhando com ninguém a sua senha, nem mesmo com secretária, chefe ou colega; III - memorizar a sua senha e não escrevê-la em nenhum lugar; IV - não digitar a senha quando alguém estiver observando; V - informar ao responsável pelo órgão as suspeitas de violação de segurança; VI - não deixar aplicativo ativo, desconectando-o da rede sempre que tiver necessidade de deixar o local de trabalho, mesmo que por pouco tempo; VII - pedir anulação da senha caso venha mudar de atribuições, for transferido para outro órgão, sair de licença, se exonerar, ou sempre que por qualquer motivo tenha que afastar-se do trabalho que exija a utilização de senha.".

### *5.4 - Técnicas Adicionais*

[23] CPI da Folha de Pagamento da Prefeitura de Belo Horizonte.

Por muito tempo o método de I&A orientou-se pelo padrão de senhas reutilizáveis. A necessidade de evolução das tecnologias fez surgir novas técnicas e ferramentas de apoio. Essas novas técnicas enfrentam o desafio de eliminar as senhas, como defendem alguns iniciados na informática [20], além de adotar tecnologias que estão se tornando mais acessíveis, trazendo também maior segurança [60]. Acreditamos, no entanto, que em vez de abolir a utilização de senhas, deve-se promover uma associação entre elas e as novas tecnologias e procedimentos, trazendo confiabilidade ao processo de I&A, mesmo porque as senhas reutilizáveis ainda são aplicadas na maioria dos ambientes de informática das empresas, mesmo que associadas às técnicas de reconhecimento biométrico [40].

Tratamos a seguir da discussão sobre mecanismos e procedimentos que demonstram a evolução para substituição ou aprimoramento da utilização de senhas como dispositivos de I&A. Os tópicos que trataremos não aparecem obrigatoriamente em ordem de importância ou facilidade para uso em redes de computadores. Apresentamos algumas possibilidades de evolução na I&A e entendemos que as mesmas podem e devem ser aplicáveis em maior ou menor grau, privilegiando as características positivas de cada uma em função dos recursos e necessidades de cada rede em que será aplicada. No caso da RMI, a discussão sobre qual a melhor ferramenta a ser utilizada será detalhada no Capítulo 7.

### 5.4.1 - *Kerberos*.

Kerberos é um método de autenticação para sistemas e redes de computadores. Desenvolvido pelo Projeto Athena no Massachusetts Institute of Technology - MIT, tem se tornado uma ferramenta consistente no processo de autenticação confiável [55],

provendo autenticação de redes[24] que apresentam possibilidade de falhas em itens de segurança com a proposta de fornecer integridade e recursos de criptografia. O método utiliza um banco de dados composto de chaves simétricas[25] armazenadas num centro de distribuição de chaves (KDC - *Key Distribution Center*), conhecido como o servidor *Kerberos*. O funcionamento é baseado na capacidade dos usuários da rede receberem convites para que se autentiquem e obtenham o acesso à rede. Vários parâmetros são atribuídos a esses convites como, por exemplo, seu tempo de validade e os locais da rede onde é possível utilizá-los. O mecanismo usado por Kerberos exige que os computadores tenham precisão no sincronismo em suas unidades de tempo. A maior facilidade de Kerberos está associada à integração com o nível de aplicação da camada de redes do modelo OSI [5]. Esta técnica apresenta características interessantes para aplicação à RMI, com fatores positivos, como a autenticação sendo realizada em pontos fisicamente distintos na rede, em posição de destaque sobre os fatores negativos como a necessidade de canais de comunicação velozes que são contemplados pela RMI.

[24] Abordagem específica de autenticação onde cada estação de trabalho prova sua identidade.
[25] Técnica de organização de chaves para utilização em Criptografia.

### 5.4.2 - Impressão Digital (*Fingerprint*).

A verificação de impressões digitais constitui uma das técnicas de BAC (*Biometric Acess Control* - Controle de Acesso Biométrico) mais exploradas. Técnicas de reconhecimento não informatizado da impressão digital remontam ao início do século 19 [55]. As marcas e traços nas pontas dos dedos são individuais e não se repetem; é como se tivéssemos a possibilidade de dar uma senha para cada ser humano do planeta e a garantia de que não haveria nenhuma senha repetida. A técnica para utilização informatizada dessa característica é simples e apoia nesse fator de não repetição dos padrões de desenho de cada dedo.

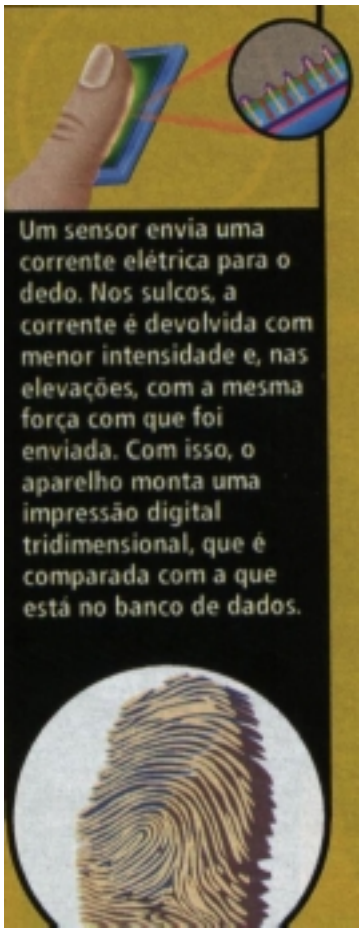


**Figura 12 - Impressão Digital [60]**

A impressão é transformada em um padrão binário onde a possibilidade de repetição é praticamente nula. As técnicas para se obter mais detalhes desses padrões têm se refinado e os programas estão aumentando sua capacidade de armazenamento. O processo digitalizado não reproduz exatamente a imagem da impressão digital, o mecanismo de leitura recebe as informações do desenho do dedo. Nos sulcos, um sensor devolve um sinal mais fraco e, nas elevações, devolve um sinal mais forte, formando uma codificação em sistema binário que é armazenada em arquivos que serão consultados no momento da autenticação. A cada autenticação do usuário, são devolvidos sinais que devem ser comparados com a informação binária armazenada. Qualquer diferença, por menor que seja, na forma da impressão digital pode levar à não autenticação.

É a **t**écnica de reconhecimento considerada mais promissora, pois o custo de sensores de leitura tem diminuído e sua precisão tem aumentado [60]. Já existem no mercado teclados de entrada de dados com leitores óticos de identificação das digitais dos usuários.

### 5.4.3 - Perfil da Palma da Mão (*Handprint*).

É a técnica de reconhecimento através do perfil da palma da mão e vem se desenvolvendo nos últimos 20 anos e tem a mesma característica da impressão digital. No corpo humano, o perfil da palma da mão também é único. Ao digitalizá-lo não significa que permanecerá único, principalmente devido ao fato de que a tecnologia a ser utilizada pode variar e ter características técnicas com menor acuidade, especialmente porque os programas disponíveis para a transformação da característica biométrica da palma da mão em informações digitais ainda tem custo elevado para os detalhes necessários à diferenciação completa [55].


**Figura 13 - Biometria da Palma da Mão [Fonte 60]**

Nesse método, a mão deve ser colocada num aparelho emissor de ondas com sensores que percebem a mudança das características das ondas em função do perfil da mão do usuário. Com base na informação dessas ondas, é construído um mapa único que pode ser mais detalhado em função da tecnologia dos leitores e dispositivos de armazenamento. Durante o andamento deste trabalho, identificamos que a Prefeitura Municipal de Natal implantou, em uma de suas redes locais, esse tipo de BAC.

### 5.4.4 - Padrão de Retina do Olho (*Retina Patterns*).

A exemplo das técnicas anteriores que reconhecem a possibilidade de identificação única no ser humano, o padrão da íris também é admitido como único. Esse tipo de identificação pode ser recente para a utilização de acesso a redes e recursos

computacionais, mas são antigos os métodos de análise dessas características biométricas. Considerada como uma das mais sofisticadas e seguras [55], a análise da íris do olho começou a ser usada em ambientes informatizados através de programas que faziam a comparação entre uma foto digitalizada no momento da I&A e uma outra armazenada previamente, o que levava um tempo inadequado à velocidade requerida para acesso a redes. Atualmente os sistemas transformam os padrões da íris em um conjunto de informações digitais que é comparado às informações já armazenadas [60] resultando na confirmação da I&A ou não. A grande discussão que ainda não chegou aos usuários porque a técnica ainda não é muito difundida, se dá entre os profissionais de informática que consideram esse tipo de identificação ameaçador em relação à perda da privacidade do usuário. Por exemplo, estudos feitos pelos chineses há muitos séculos conseguiram determinar várias ligações entre doenças genéticas e uso de drogas, simplesmente através da análise das características do olho [60]. A precisão da leitura da íris do olho pode levar à invasão da privacidade do ser humano, o que não é desejado pelos usuários que querem simplesmente acessar os recursos em redes públicas de computadores. Ressalta-se que apesar de conhecido como "padrão de retina" esta técnica utiliza-se de características da íris, que é uma membrana situada entre a córnea e a parte anterior do cristalino, enquanto a retina é uma membrana interna onde se projetam as imagens recebidas pelo olho.

### 5.4.5 - Voz (*Voice Patterns*).

Uma das propriedades da voz é que as suas características básicas não alteram nem com uma gripe; é praticamente impossível sua imitação, do ponto de vista do padrão digital produzido por ela. No processo de reconhecimento, a primeira análise é feita com comparação da freqüência e tamanho das ondas sonoras numa emissão vocal.

Essa característica permite uma aproximação confiável do processo. Adicionalmente, fatores como timbre, entonação e volume são agregados aos padrões anteriormente armazenados, o que garante uma diferenciação completa da voz de cada ser humano [55]. Mecanismos de reconhecimento da fala (*speech*), que não pode ser confundido com mecanismos de reconhecimento da voz (*voice*), tem sido utilizado em aplicações comerciais e amplamente difundido. O necessário é que o reconhecimento da voz consiga padrões técnicos de detalhamento e clareza necessários para usá-lo como ferramenta específica de I&A. Esta técnica pode ser fraudada a partir de amostras da voz digitalizada por não ser preciso reconhecer a fala. Teoricamente seria mais fácil de falsificar um padrão de voz, mesmo ele sendo único.

### 5.4.6 - Escrita (*Writing Patterns*).

A partir de parâmetros de pressão, forma e aceleração da escrita, pode-se identificar um usuário pela sua assinatura e padrão de escrita. Essa técnica de I&A exige mais recursos do que a simples utilização de senhas, e além disso, os mecanismos necessários à sua utilização são complexos, pois exigem a utilização de canetas e dispositivos de recepção da assinatura especiais [55]. Do ponto de vista do usuário, esses mecanismos seriam mais bem aceitos por tratarem de uma ação com a qual os usuários estão acostumados. As dificuldades de implementação de mecanismos como reconhecimento da escrita estão associados às dificuldades de comparação e aos mecanismos de transposição para autenticação.

### 5.4.7 - Outras Ferramentas e Técnicas.

Além das tecnologias descritas, inúmeras outras estão disponíveis para utilização em redes descentralizadas. Uma destas ferramentas que podemos destacar são os *tokens*[26], ou cartões de identificação, que armazenam informações sobre seus portadores e sobre os serviços e sistemas que as redes autorizam a utilização. Esses *tokens* funcionam normalmente com dois fatores de autenticação, o primeiro é o fato do seu portador ser identificado por um PIN, outro é a possibilidade do mesmo exigir uma senha que pode ser fixa ou variável, em função da aplicação do cartão. Uma das aplicações mais interessantes destes cartões é a utilização por usuários eventuais de redes descentralizadas e usuários que utilizam computação móvel, com a possibilidade de I&A de uso descartável. Outra técnica de reconhecimento baseada na biometria do dedo é apresentada na Figura 14.

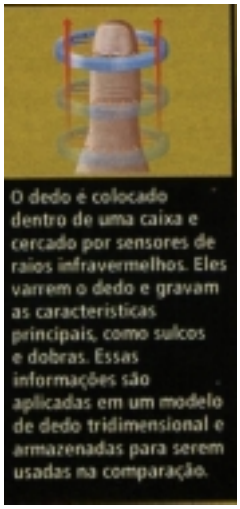


**Figura 14 - Biometria do Dedo [60]**

Para cada uma das técnicas apresentadas, ferramentas estão sendo disponibilizadas em profusão. Para cada uma delas existem mais de dois ou três fornecedores de reconhecimento mundial [58] que colocam no mercado, a cada ano, novas versões de suas ferramentas. Porém, mais importante do que a escolha de

[26] Dispositivo físico para ser utilizado como identicação, semelhante a um cartão de crédito magnético.

ferramentas é a determinação das políticas que serão implementadas em cada ambiente informatizado. A definição das políticas deve preceder a escolha de qualquer ferramenta, sendo que as ferramentas devem apoiar e facilitar a implementação das políticas escolhidas para a organização, podendo implicar na escolha de diferentes tecnologias e diferentes ferramentas até para o mesmo ambiente de rede de computadores.

A utilização das ferramentas disponíveis nos próprios sistemas operacionais garantem que vários itens descritos anteriormente possam ser implementados, como o que trata de administração de acesso. Mecanismos próprios para testar a expiração de senhas, inibir tentativas sucessivas de adivinhação, bloquear ID de usuário com ataques e induzir a mudança periódica de senhas, devem estar ativados pelos administradores de segurança em qualquer ambiente de informática. A elaboração de algoritmos para mudança de senha deve ser particularmente destacada e sugestões de resolução deste problema através de métodos numéricos[15] e equações matemáticas ajudam a elaborar senhas difíceis de serem descobertas, mas de fácil assimilação pelo usuário [15]. A determinação do que deve ser feito é estabelecida pela política de acesso lógico. A questão de como fazer deve se nortear pela mesma política, mas admite várias possibilidades de resolução.

# 6 - Ambiente Operacional da Pesquisa

*"A segurança na rede é um assunto tão recorrente como*
*as condições do tempo.*
*E como acontece com o tempo,*
*a segurança na rede nos faz sentir impotentes*
*diante de seus problemas"*
**Frank Barbetta**

Este capítulo apresenta as condições do ambiente operacional de pesquisa e os resultados da pesquisa aqui desenvolvida. Destacamos a metodologia adotada e as opções que complementariam o trabalho. Apropriamo-nos de técnicas utilizadas por *hackers* e comparamos com efeitos complementares que poderiam ser obtidos com a associação de outras técnicas. Apresentamos considerações sobre ferramentas que podem ser adotadas para diminuição das vulnerabilidades verificadas e colocamos em pauta argumentações e comparações que justificam a aplicabilidade dos resultados da pesquisa em outros ambientes de rede, além de descrevermos os resultados específicos do trabalho com avaliação dos resultados.

## *6.1 - O Caso Prodabel - RMI*

Nossa pesquisa estava planejada para ser realizada inicialmente com técnicas variadas de *hacking*. A primeira técnica proposta é conhecida como Engenharia Social; as segunda e terceira técnicas a serem consideradas são conhecidas como "força bruta" e foram realizadas em ambientes operacionais distintos para maior abrangência do público-alvo de usuários. O plano de trabalho foi inscrito formalmente no planejamento da empresa (Anexo 4).

### 6.1.1 - Ambiente Operacional da Pesquisa.

A escolha dos ambientes foi definida de comum acordo com os gerentes funcionais da empresa, no momento da elaboração do projeto, com posterior aprovação da diretoria. O critério principal definido foi o de que os ambientes deveriam ser aqueles denominados "de produção", ou seja, deviam estar completamente integrados com a realidade operacional da RMI, uma vez que a opção pela criação de ambientes fictícios tornaria sem efeito a simulação. Consideramos inadequada a realização da pesquisa em um ambiente de teste especialmente preparado para tais simulações, conforme recomendações contidas em [13]. Foram selecionados os seguintes ambientes: 1) Provedor de Acesso à Internet; 2) Servidor de Sistemas Tributários; e 3) Servidor de *Groupware*. Embora existam vários outros ambientes como Servidor de Sistemas de Trânsito, Servidor de Sistemas de Recursos Humanos, Servidor de Sistemas Urbanos, Servidor de Gerenciamento, Servidor de Desenvolvimento de Sistemas, dentre outros tantos, entendemos que as opções escolhidas reproduzem o conjunto dos demais ambientes operacionais em uso na RMI durante a realização deste trabalho.

### 6.1.2 - Pré-requisitos da Pesquisa.

Após a escolha dos ambientes operacionais, determinamos que os administradores dos ambientes de rede seriam co-responsáveis pelos trabalhos realizados, de forma que nenhum dos experimentos fosse efetuado sem acompanhamento de pessoa qualificada. O objetivo era garantir a inexistência de dúvidas sobre o propósito da realização da pesquisa. É importante observar que essas recomendações são previstas em [24], e são destinadas a evitar a ocorrência de mal-

entendidos, especialmente por usuários da PBH[27]. Desvios de entendimento são previsíveis, pois a pesquisa envolve segurança e os usuários poderiam sentir-se ameaçados nos trabalhos que realizam, reforçando com estes cuidados os requisitos de qualidade para órgãos públicos [41].

Não deveria fazer parte de nenhuma etapa da pesquisa qualquer procedimento conhecido como "teste de invasão", "teste de segurança" ou "quebra de segurança", mas admitimos que essas vulnerabilidades estão presentes em qualquer ambiente de rede. Esta opção foi adotada pelo fato de que não está vinculada diretamente às vulnerabilidades da I&A, sendo que se referem às questões gerais de segurança. Para a realização da pesquisa deveriam ser asseguradas todas as condições de funcionamento das redes onde seria realizada a pesquisa, inclusive com a hipótese de ataque ao ambiente por agentes ou programas maliciosos. Excepcionalmente, atividades de quebra dos controles de I&A poderiam requerer a utilização de técnicas de ataque *hacker*. Ao realizar a pesquisa firmamos o compromisso de que não seria feita nenhuma tentativa de assumir o controle do ambiente operacional com privilégios, pois esse tipo de ataque não faria parte do projeto. Mais uma vez, é importante a diferenciação do trabalho realizado voltado para problemas de I&A em contraposição à possibilidade de assumir o controle de todo o ambiente operacional através de uma falha do administrador da rede, sendo pois necessário assumir o compromisso de não se aproveitar de qualquer oportunidade.

### 6.1.3 - Operacionalização da Pesquisa.

Foram realizados alguns procedimentos básicos nos ambientes a serem pesquisados, os quais fundamentaram a proposta de que a correta utilização de senhas,

[27] Usuários da RMI podem ser servidores da PBH (Administração Direta) e das empresas e órgãos da Administração Indireta.

ou processos adequados de I&A, poderia ser vista como princípio para diminuição do problema de segurança na RMI. Essa forma de proceder é inerente ao processo de obtenção de informação dos ambientes operacionais estudados.

Foram considerados na operacionalização da pesquisa os levantamentos de situação da RMI feitos em [6], que previam a expansão da rede em termos de serviços de Internet, bem como os requisitos de evolução do ambiente de teleinformática constantes daquele documento. Mesmo que existissem decisões sobre a necessidade de implantação de técnicas de identificação e ferramentas de gerenciamento de autenticação anteriores à implantação de acesso Internet, essas ferramentas não estavam em funcionamento no momento da pesquisa, sendo assim, adotamos recomendações de segurança ali também descritas. Outro documento no qual nos orientamos para preparação da pesquisa foi o projeto funcional [7] e o projeto físico [8] da RMI, que descrevem totalmente o ambiente no qual os usuários seriam pesquisados na utilização dos serviços de correio interno, Internet e da aplicação específica de um sistema tributário. Preparamos ainda, para esta pesquisa, formulários de recebimento das indagações dos usuários para possíveis dúvidas ou esclarecimento de irregularidades (Anexo 1.4). No caso do correio eletrônico, utilizado na Internet, ressalta-se que as caixas postais são configuradas para recebimento e armazenamento das mensagens em texto claro, e as permissões de acesso são dadas exclusivamente pela classificação atribuída pelo sistema operacional reforçando a premissa de que um usuário sem nenhum privilégio teria a possibilidade de atuação idêntica à de um *hacker*. Caso se consiga acesso a uma caixa postal e seja possível a carga de alguns programas utilizados por hackers e facilmente encontrados na Internet, é tecnicamente facilitado a quebra do sigilo das correspondências de outras caixas postais no mesmo ambiente [37].

### 6.1.4 - Preparação da Pesquisa.

Foram planejadas duas pesquisas situacionais que fundamentariam a hipótese de vulnerabilidade das senhas utilizadas. A primeira pesquisa foi feita no ambiente de acesso à Internet, fraudando um *e-mail* (Anexo 1.1) do administrador do sistema em que o mesmo solicitava aos usuários que informassem, através de resposta, via ferramenta de *e-mail*, sua senha e identificação de acesso. O procedimento consistia em utilizar a conta y2k@pbh.gov.br que não tinha nenhum privilégio como receptora das mensagens de retorno. Para tanto foi forjado o remetente como root@pbh.gov.br e dentro da mensagem colocamos a orientação de "responder para todos" (*reply all*) fazendo com que as respostas fossem para o ID "*root*" e para o ID "y2k" do qual detínhamos a senha de acesso.

A segunda pesquisa utilizou-se de ferramenta do tipo *cracker* para descobrir senhas através do método de tentativa e erro. Essas pesquisas determinaram o nível de importância dada às senhas nos respectivos ambientes e comprovaram o pouco cuidado que se tem com elas. A importância dessas constatações fundamenta o propósito do trabalho, que, a partir da vulnerabilidade no tratamento com as senhas, ressalta que o problema de segurança pode ser diminuído com boas práticas de utilização de senhas. Além disso acreditamos que não seria a adoção de mecanismos sofisticados que mudaria os costumes dos usuários de serviços da RMI. A propósito dessa hipótese, [58] cita um exemplo aplicável ao caso: uma pessoa carregando pacotes e com as mãos ocupadas, pode facilmente ter a porta de entrada de uma sala de computadores aberta para ela sem que precise utilizar ou passar por nenhum mecanismo de I&A, bastando para tanto somente solicitar a gentileza a alguém solícito ou atencioso. Ainda em [58],

existem exemplos de invasão comprovando que a cultura dos profissionais de informática permite acesso fácil a qualquer ambiente, desde que o invasor atue com naturalidade. Kevin Mitnick, o mais conhecido *hacker*, atuou dessa forma por muito tempo [57].

### 6.1.5 - Resultados da Pesquisa.

Os resultados basearam-se na análise e quantificação das respostas obtidas nas pesquisas. Demonstramos quantos e quais os motivos que levam os usuários de uma rede interna a divulgarem suas senhas de acesso a pessoas não identificadas, reforçando a tese de vulnerabilidade de uma rede. A forma proposta para mostrarmos os resultados é colocar proporcionalmente o número de senhas fracas[28] em relação ao número de usuários para cada um dos ambientes.

### 6.1.6 - Engenharia Social por *e-mail*.

O *e-mail* forjado, conforme texto do Anexo 1.1, foi enviado utilizando-se uma técnica de *spoofing* que pode ser usada com qualquer ferramenta de correio eletrônico e que não exige conhecimentos técnicos especializados de quem é usuário desse serviço da Internet. Como dissemos anteriormente o *e-mail* forjado tinha a assinatura como se o remetente fosse o ID do *root* da Internet da Prodabel. O propósito do *e-mail* era ganhar a confiança de cada usuário que recebesse a correspondência e levá-los a responder de imediato. O horário e a data de envio para os usuários também foram objeto de estudo, as mensagens foram enviadas no dia 2 de junho de 1999, uma quarta-feira, entre 17 e 18 horas, na véspera de um feriado prolongado, em que vários usuários, dentre eles o responsável pelo ambiente operacional, só retornariam ao trabalho após quatro dias, ou

seja, em 7 de junho de 1999. Como o *e-mail* tinha um remetente forjado (root@pbh.gov.br), no caso para aparentar que a mensagem saía de alguém importante no ambiente operacional, a opção das datas e horários de envio foram planejadas de forma que as possíveis ações de um CERT-RMI[29] estariam limitadas e não pudessem ser realizadas de imediato. O endereço eletrônico que receberia as possíveis respostas não tinha nenhum privilégio (y2k@pbh.gov.br). A meta era receber algumas mensagens de retorno de usuários desprevenidos e, a partir da informação da senha de cada um deles, ter de três a quatro dias para fazer todas as operações possíveis a um *hacker* a partir de ID de vários usuários, inclusive com a possibilidade de implantação de programas que poderiam dar privilégios especiais para qualquer ID.

A estratégia principal ficou centrada no texto da mensagem, que trabalha a proposta de Engenharia Social, conquistando a confiança dos usuários e obtendo respostas sem que esses usuários se perguntassem sobre a correção daquela ação. Ressalta-se que as mensagens foram enviadas para todos os usuários cadastrados em 21 de maio de 1999, pois foi aproveitada uma falha do responsável pelo ambiente operacional quando o mesmo, ao fazer um *broadcasting*[30] de uma mensagem, que avisava todos os usuários cadastrados no serviço de Internet da PBH sobre a manutenção de um equipamento, deixou em texto claro todos os endereços eletrônicos cadastrados, que na maioria dos casos correspondem também às contas ou ID inscritos para acesso à Internet. Esse equívoco permitiu a obtenção de todas as identificações inscritas à época. Outra estratégia adotada, que contemplava a questão levantada em [24] e [28], foi a de darmos um prazo para a devolução das respostas e, a partir de determinada data, estipulada no próprio *e-mail* em 10 de junho de 1999, deveríamos

[28] Senhas que não suportam simples testes de quebra. Podem facilmente ser identificadas.
[29] Possível equipe de resposta a incidentes em computadores da RMI.

informar aos usuários os propósitos da pesquisa, principalmente para aqueles que infringiram normas e regulamentos pudessem se posicionar sem que tivesse se passado um tempo muito longo entre a divulgação da senha e a possível substituição da mesma. Esse procedimento ficou acertado antes da emissão da primeira mensagem, posto que, imediatamente após o final de semana, já poderíamos esclarecer às pessoas que estavam envolvidas com a pesquisa quais as finalidades e critérios da mesma. O texto dessa segunda mensagem também foi discutido com os responsáveis pelo ambiente operacional e a data de envio agendada previamente, sendo que o responsável pelo ambiente operacional e sua gerência não concordaram com o conteúdo da mesma (anexo 1.3).

Das mensagens enviadas recebemos um retorno correspondente ao gráfico apresentado a seguir:

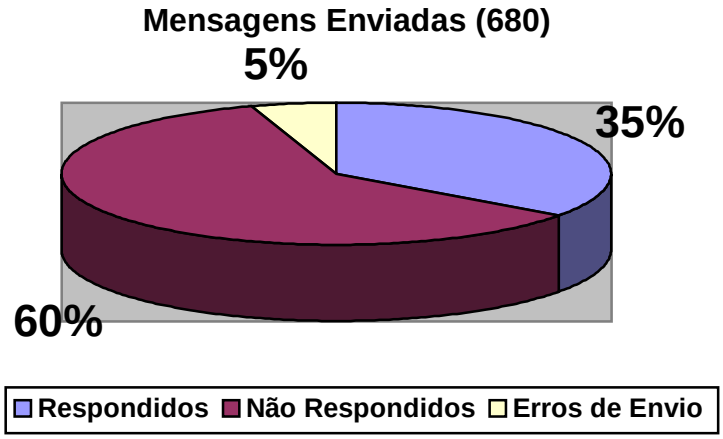


**Gráfico 1 - Aproveitamento de Mensagens**

[30] Numa rede, consiste na transmissão de uma mensagem para todos os usuários em atividade.

Comprovamos que a vulnerabilidade apresentada pelo fornecimento de senhas em 35% dos usuários que receberam a pesquisa, mesmo que em números absolutos não caracterize maioria dos casos, foi significativa para o experimento, pois permitiu a apropriação indevida das senhas e possibilidade de acesso através de várias identificações.

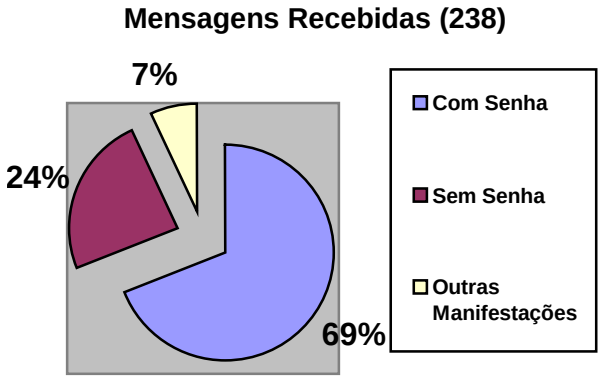


**Gráfico 2 - Mensagens Recebidas**

Ficamos surpreendidos com o número elevado de profissionais da Prodabel que responderam ao falso *e-mail*, enviando, inclusive, suas senhas. Esperávamos desses profissionais maior astúcia e cuidado com a possibilidade de invasão do ambiente da RMI, principalmente por serem tais profissionais co-responsáveis pela invasão e quebra de sigilo através da divulgação de senhas. Foram poucos os profissionais da Prodabel e usuários que questionaram aquela mensagem e obtivemos somente um caso concreto em que houve iniciativa para responder ao pseudo-ataque assim que o usuário identificou a possibilidade de quebra da segurança. A inexistência de um Centro Operacional de Resposta a Incidentes com Computadores, com procedimentos amplamente divulgados de seu funcionamento e como acioná-lo, pode ter contribuído para a pouca resposta obtida contra o processo. Excetuando-se as pessoas que estavam

avisadas previamente sobre o procedimento (inicialmente seis), as demais deveriam obedecer a Instrução de Serviço publicada pela PBH (Anexo 2), o que não foi possível comprovar pois não constatamos nenhum usuário da PBH se posicionando conforme descrito na norma. Ou melhor, constatamos que a maioria dos usuários deixou de cumprir ao menos um item da referida instrução. A exceção ficou por conta de três funcionários da Prodabel que registraram através de *e-mail* a estranheza com relação ao procedimento da pesquisa.

Confirmamos a facilidade de ser obter a informação sobre a senha, utilizada para I&A, e adquirimos a possibilidade de acesso aos ambientes informacionais da RMI. Adicionalmente aos procedimentos de recepção de senhas via *e-mail* identificamos um entrave à adoção da política de utilização de senhas no ambiente Internet, que consiste em uma dificuldade operacional para que o usuário altere sua senha sem que haja intervenção de outras pessoas.

O procedimento de atualização de senha consiste na solicitação por parte do usuário, através de e-mail ou contato telefônico para que sua senha seja alterada. Após a alteração, ou principalmente no fornecimento da senha inicial, esta senha é escrita num documento de solicitação de inscrição de identificação e um funcionário da Prodabel retorna a ligação telefônica ao solicitante e fala a ID e a senha para o mesmo.

Esse processo foi determinado pelos responsáveis do ambiente operacional da Internet, sem atender a Instrução de Serviço da CGM. A quebra de segurança possível a partir daí é intangível e vai desde a simples violação de correio até a adulteração de *homepages* e arquivos, sendo determinada, fundamentalmente, pela capacidade do invasor em alterar sua autorização de acesso.

A execução dessa pesquisa não foi realizada totalmente dentro do planejado em função da ocorrência de desentendimentos a partir da proposta do trabalho e dos encaminhamentos necessários.

**Impactos na execução do trabalho.**

Embora o projeto tenha sido inscrito oficialmente no planejamento da empresa e a diretoria e áreas com acesso ao planejamento tivessem conhecimento prévio do mesmo, o resultado do envio da primeira mensagem não foi bem entendido. Gerentes das áreas diretamente vinculadas ao ambiente operacional da Internet, que era a área diretamente atingida, se sentiram desrespeitados nas suas funções com as mensagens enviadas e questionaram os procedimentos previstos e adotados. Outros profissionais da empresa intercederam junto ao administrador do ambiente operacional, que não se manifestou formalmente sobre as intervenções destes usuários, mesmo que tivesse sido colocado a sua disposição um formulário para o registro de tais ocorrências, formulário este que foi devolvido em branco. A mensagem explicativa não foi enviada na data prevista (10/jun/1999), porque as gerências responsáveis pela Internet não aceitavam os procedimentos efetuados e previstos. A discussão foi levada à diretoria da empresa, que não encaminhou decisão a tempo para que a mensagem explicativa (Anexos 1.2 e 1.3) fosse enviada, mesmo considerando que essa mensagem foi enviada somente em 29 de junho de 1999 com atraso de dezenove dias da previsão inicial.

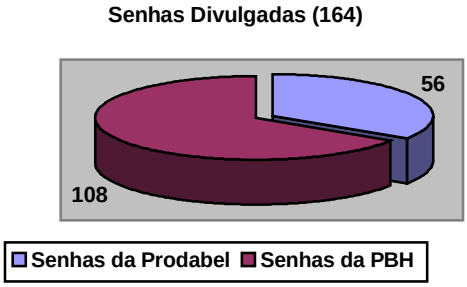


**Gráfico 3 - Senhas Divulgadas**

Em função dos resultados obtidos, nos quais os funcionários da Prodabel tiveram um índice de resposta ruim em relação aos funcionários da PBH, considerando que os usuários da Internet que são funcionários da Prodabel são mais qualificados e experientes na utilização de ambientes informatizados, a mensagem explicativa foi diferenciada, pois entendemos que caberia usar a oportunidade para destacar a importância do comportamento exemplar dos profissionais que trabalham pela segurança da RMI na empresa de informática da PBH. Os Anexos 1.2 e 1.3 mostram a diferença dos textos. A quebra de confiança demonstrada pela diretoria responsável pelo ambiente operacional obrigou a uma reforma nos procedimentos a serem adotados para as outras duas etapas da pesquisa.

### *6.2 - Quebra de Senha Através de Força Bruta*

Conforme já descrito, a segunda etapa da pesquisa estava prevista para ser realizada através da obtenção de um arquivo de senhas e, a partir da utilização de uma ferramenta denominada "cracker", que se encontra disponível na Internet, nosso objetivo era descobrir senhas. Como o arquivo que seria obtido é criptografado, conforme procedimento básico do sistema operacional, a primeira estratégia era usar o

"cracker" para testar se as senhas eram iguais ao ID do usuário. A segunda tentativa seria feita utilizando-se como senhas candidatas as palavras de um pequeno dicionário na língua inglesa. Caso obtivéssemos sucesso essas duas estratégias permitiriam que comprovássemos a fragilidade das senhas em uso.

Esta etapa não foi cumprida, pois reformulamos os procedimentos a serem realizados em função dos problemas na etapa anterior. Pedimos aos responsáveis pelo ambientes operacionais, nos quais a pesquisa se realizaria, que validassem todas as atividades e colocassem todas as observações que fossem necessárias para revisão da proposta apresentada e inscrita no planejamento da empresa. Alteramos inclusive o projeto junto à área de planejamento para participação dos novos profissionais envolvidos no projeto. Não obtivemos retorno das áreas que receberam o Plano de Trabalho para Pesquisa/Projeto a ser Incorporado à Dissertação de Mestrado (Segunda Parte) noventa dias depois de apresentarmos a proposta. O plano está reproduzido no Anexo 4 e não foi realizado, pois optamos por dar seqüência ao trabalho sem realizar essa atividade.

### *6.3 - Quebra de Senha Através de Tentativa e Erro[31]*

O ambiente operacional previsto é relacionado à ferramenta de correio do Notes® onde as senhas são dispostas num ambiente privativo da RMI, e com características específicas. O Notes® armazena as senhas em arquivos próprios, criptografados e disponíveis num equipamento central e com cópias em estações-cliente que utilizam o programa de correio. A seqüência de navegação para substituição de senhas é fornecida através de mecanismos da própria ferramenta (Anexo 6). Como o ambiente central não foi disponibilizado, nossas pesquisas se concentraram em

participar de uma lista de discussão hospedada no endereço eletrônico http://www2.uol.com.br/info/forum (Anexo 8) sobre o produto Notes®, para que pudéssemos constatar as vulnerabilidades daquele ambiente e fazer tentativas de quebra das senhas a partir do ambiente do usuário. Depois de algumas semanas participando da lista pudemos verificar a existência de vulnerabilidades associadas à senha da ferramenta de correio conforme cópias de e-mail de usuários e gestores do ambiente Notes® (Anexo 9). Focalizamos nossa pesquisa numa dessas vulnerabilidades e prosseguimos na tentativa de obter a quebra de senha no ambiente Notes®.

A vulnerabilidade enfatizada é que, com determinada ID, copiada de qualquer estação cliente, pode-se acessar a aplicação de qualquer local ou outro computador que esteja autorizado a executar o programa Notes®, mesmo que a identificação original fosse alterada na estação cliente ou no servidor posteriormente à cópia indevida. Utilizamos dessa vulnerabilidade e fizemos cópia de três identificações de arquivos com extensão .ID, ação esta que pode ser experimentada sem nenhuma restrição por qualquer pessoa que tenha acesso às pastas/diretórios dos computadores utilizados como estação-cliente.

A partir da posse desses arquivos, fizemos tentativas de adivinhação das senhas deles fundamentados nos conhecimentos que tínhamos de cada usuário. Conseguimos descobrir a senha de um dos usuários após doze tentativas, somente com técnica de adivinhação, ganhando assim acesso às aplicações e correio como se fôssemos proprietários dela. Dos outros dois usuários não foi possível descobrir a senha com menos do que as cinqüenta tentativas realizadas. Por questão de garantia de sigilo da caixa postal violada não divulgaremos a identificação da mesma, mas o Anexo 6 mostra uma imagem com as três identificações (ID) inseridas no meio de outras, juntamente

[31] Processo de tentativa e erro, onde experimenta-se à exaustão possíveis senhas de acordo com o conhecimento do usuário.

com a lista dos arquivos de identificação disponibilizados no computador alvo do ataque, servindo de amostragem de ID que pode ser livremente copiada.

Esta etapa do trabalho mostra que mesmo em ambientes com senhas criptografadas e com procedimentos claros para alteração de senhas, ainda assim é possível que senhas sejam quebradas com pouco esforço. Não foi possível mensurar a dificuldade com que um hacker pode assumir o controle operacional do ambiente a partir de uma ID submetida às vulnerabilidades em função da não disponibilização do ambiente operacional central do Notes®. Podemos concluir também que a política de acesso lógico bem implantada e seguida por todos usuários é mais forte e mais confiável do que ferramentas inadequadas e utilizadas sem critério e preparação. A utilização de ferramentas com inúmeros recursos e mal cofigurada pode trazer problemas adicionais àqueles que as redes teriam no caso de adoção de política que seja seguida e entendida por todos usuários da rede.

### *6.4 - Resultados e comparações*

Realizamos um estudo comparativo com a teoria apresentada sobre as vulnerabilidades e as hipóteses práticas comprovadas nas pesquisas realizadas.

Foi comprovada a vulnerabilidade através de quebra e divulgação de senhas. Os procedimentos realizados de engenharia social demonstram que, mesmo com a adoção de mecanismos modernos de I&A, é grande o risco de ocorrer mau uso de qualquer técnica de I&A fazendo com que usuários não autorizados acessem recursos previstos para outros usuários da rede. É mais do que relevante a constatação de que a implantação de políticas específicas de I&A são necessárias às redes descentralizadas de computadores, especialmente nos ambientes heterogêneos da RMI.

A falta de cuidado verificada no tratamento das senhas, aliada à possibilidade de quebra dessas senhas por tentativa e erro, mais a existência e evolução constante de programas com a finalidade específica de fraudar ambientes computacionais, levam à perspectiva de que a melhor estratégia para defesa dos ambientes informatizados descentralizados é a conscientização de cada um dos usuários para que exerçam seu papel de responsável pela parte de segurança que lhe cabe. Essa postura favorece a ampliação da cultura de segurança das organizações e proporciona maior confiança dos usuários internos nos serviços cujo suporte é o computador.


**Gráfico 4 - Principais Ameaças**

O gráfico 4 , que retrata as possibilidades de se evitar ataques por *hackers*, ainda é atual e pode ser confirmado através da Pesquisa Nacional sobre Segurança da Informação [40], quando verificamos que o tema "senha" ainda é colocado como ameaça constante a ambientes computacionais.

Ao compararmos a pesquisa realizada em [40], que abrange empresas públicas e privadas, e os resultados obtidos em nosso trabalho, confirmamos nossas hipóteses e reforçamos a necessidade de melhor tratamento e maiores investimentos em I&A,

especialmente com a utilização de senhas como mecanismos de controle de acesso, pois a aplicação desse método tem eficiência em quase todos os ambientes operacionais.

### *6.5 - O Caso da Urna Eletrônica Brasileira e Votação pela Internet*

Cabe aqui uma breve pausa para apreciarmos a situação que nos foi apresentada e que envolve fortemente uma questão de I&A. O sistema eleitoral brasileiro está adotando parcialmente, desde 1996, a chamada urna eletrônica e a partir das eleições de 2000 o sistema de votação estará totalmente informatizado. Uma das questões de direito do cidadão é o fato de que o voto não pode ser identificado, direito esse previsto na Constituição Brasileira. Em 1996 e 1998, considerando que realizava uma evolução com a urna eletrônica, o Tribunal Regional Eleitoral (TRE) promoveu a identificação do eleitor, juntamente com o voto, através do uso do número do Título de Eleitor. Este fato, que passou desapercebido quase que pela totalidade do eleitorado e partidos políticos, promove uma quebra dos requisitos de segurança [9] no sentido contrário ao da necessidade de I&A. Tal fato passa incólume também pela maioria dos usuários de informática quando constatamos que em [18] é apresentada a afirmação de que "… através da Internet, pode-se acompanhar processos eleitorais ao vivo, permitindo portanto um maior controle contra fraudes eleitorais durante a fase de processamento de resultados…", ressalta-se que o processo de I&A é completamente diferente do processo de apuração e fechamento, mas ao analisarmos todo o processo constatamos que, a partir do momento em que a votação através da Internet for uma demanda da sociedade, os procedimentos de I&A devem estar eficazes o suficiente para não permitir fraudes e dar garantias ao cidadão de que seu voto será sufragado efetivamente no candidato que ele deseja.

# 7 - Propostas de Proteção de Redes Descentralizadas

*"A recente invasão em massa dos sites do governo revela a fragilidade dos sistemas, colocando em risco operações críticas e, principalmente, a credibilidade das instituições."*

**Fernando Nery**

Este capítulo aborda as técnicas e ferramentas que consideramos mais adequadas para implantação na RMI, sem se descuidar da concepção de que estas ferramentas não devem ser apresentadas e implantadas antes de se fundamentarem numa política de segurança feita especialmente para o ambiente da PBH. Os exemplos e tecnologias apresentadas podem ter aplicação em outras redes públicas de informática semelhantes à de Belo Horizonte, fazendo com que as propostas e discussões apresentadas neste trabalho sirvam de referencial inicial à discussão de implantação de mecanismos de I&A em outras redes de computadores. A principal proposição aqui apresentada e as sugestões de trabalhos a serem realizados são importantes no contexto atual de vulnerabilidade da RMI e disponibilização de seus serviços ao ambiente Internet.

## *7.1 - Adequação de Ferramentas*

A proteção de redes de computadores de ferramentas requer mais do que a sua simples implantação. Quando se trata de proteção através de I&A, as ferramentas são mais específicas e dotadas de várias formas de apresentação. É necessário o estudo prévio do ambiente de redes a ser protegido e, depois de definidas as políticas e arquitetura do sistema de segurança, a implementação envolve uma combinação de

*hardware* e *software*, que pode ser obtida a partir de fornecedores diferentes para que atendam às políticas de segurança dos vários ambientes e sistemas.

A introdução de sistemas biométricos, que aparentam ser o caminho mais fácil de ser trilhado para a implementação das ferramentas de I&A, prejudica a conscientização de que a mudança de cultura dos usuários é o fator preponderante para a melhoria dos quesitos de segurança. Foram realizadas tentativas de contato junto a órgãos do Governo Federal, como o Serviços Federal de Processamento de Dados (Serpro), Câmara dos Deputados, e Ministério da Administração e Reforma do Estado (MARE), para saber sobre as condições em que poderiam estar implementado uma ferramenta de I&A através de reconhecimento biométrico para acesso a redes de computadores. O resultado foi negativo para os órgãos consultados. Foi possível, entretanto, observar o trabalho desenvolvido no Cepesc, órgão que cuida das comunicações da Presidência da República, em que foi confirmado, através da troca de mensagens com o responsável pelo setor de tecnologia, a utilização da impressão digital como mecanismo de biometria para implementar sua política de I&A.

A análise desse trabalho e, especialmente, da ferramenta utilizada para ele, possibilitou-nos dimensionar a relevância de definir previamente a política e arquitetura de segurança para que as ferramentas a serem utilizadas sejam adequadas, fazendo com que se torne essencial a escolha da técnica de I&A após a determinação das políticas de segurança.

A utilização de tecnologias suportadas somente por uma única plataforma pode levar à limitação da utilização de somente programas e sistemas específicos, colocando as redes públicas dependentes de um único fornecedor de *software* de gerenciamento e segurança. Observação neste sentido também foi efetuada na Prodabel, quando

determinado setor foi encarregado de pesquisar ferramenta que possibilitasse aos sistemas aplicativos a gerencia de senhas e permissões de acesso. A área, em seus estudos, encaminhou para solução que atendia somente a sistemas desenvolvidos para ambientes Windows 95® ou Windows NT®, além de limitar a linguagem de programação do sistemas em linguagens que suportassem a troca de APIs com o sistemas gerenciador de senhas de acesso. Ao adotar esta solução como ferramenta de gerenciamento de I&A é colocada a limitação de sistema operacional e linguagem de desenvolvimento, o que não é adequado para ambientes que se pretendem heterogêneos.

### 7.1.1 - Impressão Digital.

O custo por unidade computacional foi inibidor do uso da tecnologia de reconhecimento por impressão digital por algum tempo. Surgiram no mercado especializado opções que disponibilizavam esse recurso por um custo de aproximadamente U$250 (Duzentos e cinqüenta dólares)[32] por estação de trabalho. Embora esse custo seja aparentemente reduzido, sua aplicabilidade e benefício pode ser determinada pelo tamanho e os recursos da rede que se deseja proteger. Em uma rede como a RMI, que tem aproximadamente 3000 computadores[33] distribuídos em diversas redes locais, teria que investir em um número igual de equipamentos de identificação, caso a política assim o determinasse, além do processo de implantação e manutenção do procedimento e, mesmo que se considere a hipótese de implantação escalonada, representaria um montante fundamental aos cofres municipais que poderia ser destinado a outras atividades. A tecnologia é adequada e eficiente mas não viável para

[32] Dados de novembro de 1998 [44]
[33] Dados de janeiro de 2000 [Prodabel]

implantação em todos os pontos da rede, e tem características técnicas para ser considerada em projetos e justificativas específicas.

### 7.1.2 - Cartões Inteligentes.

Um fator a ser avaliado na implementação desse tipo de ferramenta é a análise da quantidade de usuários da rede a serem protegidos e quantos necessariamente devem possuir um cartão. Um caso exemplar na Administração Municipal é a necessidade de que os servidores municipais façam uso de seus privilégios de acesso à rede em qualquer dos prédios da PBH. O acesso à RMI poderia ter sua I&A possível em qualquer dos prédios a partir de leitoras de cartão que tivesse o poder de reconhecer o usuário e suas prerrogativas, sendo que o mesmo cartão pode ter outras finalidades relacionadas à função do usuário e suas características pessoais em relação ao seu ambiente de trabalho.

Redes de órgãos públicos que dêem acesso a usuários de difícil controle e que dispensem cadastramento prévio, como por exemplo cidadãos que procuram esporadicamente serviços da Administração Municipal e não são cadastrados previamente ,não têm nesse recurso de cartão inteligente uma solução adequada, mas, como no caso das demais tecnologias que abordamos, parte dos usuários podem utilizá-lo. Destacamos que o custo de implantação dessa ferramenta tem diminuído, como a maioria dos custos de produtos de informática, mas não o bastante para justificar um investimento que contemple toda uma rede com as características da RMI. Uma das maiores vantagens divulgada pelos fornecedores de *smartcards* é que a senha fica criptografada no próprio cartão [53] e, neste caso, o cartão está submetido às mesmas

características de uso descritas no Capítulo 5, o que não implica em grandes alterações nos procedimentos dos usuários ao cuidar do cartão.

### 7.1.3 - Outras Ferramentas.

A adoção de outras ferramentas ou tecnologias em redes de computadores, especialmente no setor público, requer estudo de viabilidade detalhado em função dos custos envolvidos e dos recursos a proteger. Aqui, mais uma vez, é relevante a determinação da política e da arquitetura a serem protegidas para que não se utilize uma tecnologia inadequada.

O setor pioneiro na utilização de ferramenta que usa tecnologia de ponta tem sido o financeiro, em função da necessidade de proteção a seus diversos ativos. Com a expansão do comércio eletrônico através da Internet, as grandes corporações e os órgãos públicos iniciarão um processo de adoção de tecnologias inovadoras, dentre elas as de reconhecimento biométrico, para prevenir a perda de senha por parte dos usuários e dar garantias de um processo de I&A mais eficaz. As argumentações de que os mecanismos e ferramentas que utilizam características biométricas são quase totalmente seguros e que a responsabilidade por uma possível má utilização não pode ser repudiada pelo usuário, ainda são insuficientes para a sua adoção em redes de órgãos públicos, especialmente em função do vácuo de legislação sobre o tema de autenticação e certificação digital.

Ao analisarmos o trabalho de identificação através de sistema biométrico, como o apresentado em [44], que trata do reconhecimento da face como tecnologia de identificação, constatamos que o mesmo ainda utiliza-se de senha para o processo de

autenticação; além da possibilidade de falhas de reconhecimento devido à configuração de sensibilidade no cadastramento de cada usuário.

Nesse sentido, é importante o trabalho que desenvolvemos, pois permite o estudo por terceiros e implantação das tecnologias e ferramentas de reconhecimento biométrico como conseqüência de uma adequada definição de políticas e arquitetura para I&A.

### *7.2 - Aplicação em ambientes descentralizados*

A partir da adoção de políticas e arquitetura de segurança que sejam determinantes para as propostas de I&A para uma rede de computadores, podemos indicar que a proposta aqui apresentada pode ser estendida para redes similares. A comparação técnica entre redes está no fato de políticas e arquitetura serem compatíveis e não na exatidão dos detalhes técnicos de topologia das redes. Os serviços de uma rede em órgãos públicos são parecidos e o acesso a essa rede, na medida em que há determinação política de torná-la de acesso amplo, ocorre de forma semelhante. Esse trabalho indica que as proposições e discussões aqui apresentadas são aplicáveis a redes do setor governamental em geral. Servem como início de parametrização para a necessidade de dotar essas redes de níveis mais elevados de segurança, ressaltando que não se aplicam necessariamente diretamente às redes educacionais utilizadas em universidades e centros de pesquisa, em função das características dos serviços utilizados nessas redes, que permitem maiores privilégios para a maioria de seus usuários.

No caso estudado, procedimentos de utilização trivial podem ser implementados com baixo custo e, na maioria dos casos, estão disponíveis nos sistemas operacionais

para serem utilizados como *default*. Descreveremos a seguir algumas situações recomendadas à utilização de senhas como mecanismo de I&A.

Apresentamos algumas regras básicas que asseguram a diminuição das vulnerabilidades nas redes descentralizadas através de acessos realizados por ID de usuário e senha em qualquer ambiente computacional. Algumas dessas regras foram divulgadas na Instrução de Serviço publicada pela PBH; outras regras e recomendações constituem boa prática de profissionais e usuários de informática na utilização de acesso lógico através de senhas, a se iniciar pelo indicativo de que senhas devem ser fáceis de lembrar, mas difíceis de serem descobertas ou adivinhadas. Além das recomendações relacionadas no Capítulo 5, especificamos mais detalhadamente procedimentos recomendáveis para utilização de senhas no ambiente de redes descentralizadas.

### *7.3 - Política de Identificação e Autenticação Única*

A partir dos problemas discutidos no Capítulo 4 com o uso de senhas, reforçados pela premissa da dificuldade dos usuários em tratar senhas diferentes para os mais variados serviços e sistemas, e com base na necessidade de que haja mecanismos fortes de determinação de privilégios e proteção de uma senha, entendemos que a arquitetura mais adequada para implementação em redes descentralizadas, como é o caso da RMI, ou mesmo redes locais, é a implementação de uma arquitetura conhecida como *single sign-on*[34] ou ID única de usuário. Embora reconhecidamente de difícil implantação, devido a grande variedade de mecanismos de autenticação, a partir dessa arquitetura devemos ter várias técnicas de I&A, desde que identificadas e implementadas com características de interoperabilidade entre plataformas diferentes de sistemas

operacionais, proporcionando a adequação dos serviços e sistemas às suas especificidades e necessidades, como procedimento que justifique a diminuição das vulnerabilidades no tratamento de senhas.

Alguns critérios devem ser seguidos como orientação para se implementar uma arquitetura ideal, os quais passamos a detalhar. Destacamos características fundamentais que uma ferramenta de ID única de usuário deve ter para que a arquitetura leve à solução da maioria dos problemas levantados em nosso trabalho, bem como a implantação, substituição ou evolução de ferramentas e técnicas de autenticação diferentes. A presença das características que apresentamos a seguir é essencial para a instalação de um sistema de ID única de usuário.

**Arquitetura Aberta** - A solução de ID única de usuário deve ser baseada em padrões de sistemas abertos. A ferramenta tem que ser capaz de absorver todas as políticas de segurança das organizações e não pode colocar nenhuma restrição à qualquer política implementada. A hipótese de uma política ser modificada ou excluída em função de limitações na ferramenta escolhida deve ser fator determinante para rejeição da ferramenta.

**Forma de I&A** - Característica fundamental, principalmente porque diz respeito diretamente ao trabalho aqui discutido. A ferramenta de ID única de usuário deve suportar várias técnicas de I&A. As organizações não devem implantar uma arquitetura ou política de I&A fundamentadas em restrições de ferramentas de ID única de usuário, o que dificultaria a possibilidade de heterogeneidade em ambientes operacionais. É ainda característica essencial a essas ferramentas o fornecimento de infra-estrutura de fácil manuseio para introdução de novas tecnologias de identificação. Nesse caso, as

[34] Conjunto de recursos, às vezes de *hardware* e *software*, que permite que o usuário seja autenticado por um único sistema de I&A.

tecnologias podem envolver a possibilidade de se utilizar senhas associadas a outras técnicas.

**Formas de Autenticação por Senha** - Na seqüência da característica anterior, a ferramenta de ID única de usuário deve ser implementada com a possibilidade de aceitar os diversos sistemas de autenticação em uso nas redes descentralizadas. A ferramenta deve ter capacidade de receber senhas simples, cartões inteligentes e *tokens*[35], detectar senhas transmitidas em texto claro e providenciar a segurança das mesmas através de criptografia. Esta característica é fundamental para que a transição dos mecanismos de I&A dos sistemas existentes não sejam impostas nem submetidas pelas novas tecnologias de I&A.

**Suporte a múltiplas plataformas** - A solução deve também ser capaz de operar em ambientes operacionais diversos, com reconhecimento e troca de informações entre ambientes computacionais de tecnologias e topologias distintas. Nesse sentido, os agentes de gerenciamento utilizados pela ferramenta devem ser compatíveis com os sistemas utilizados na RMI, ou qualquer rede descentralizada onde se implemente a solução, permitindo a adaptação dos sistemas legados, não esquecendo a necessidade de compatibilidade com os sistemas operacionais dos equipamentos servidores e estações cliente.

**Utilização de APIs**[36] - A solução de ID única de usuário deve ter a capacidade de aceitar programação de APIs com as mais diversas ferramentas, propiciando a construção de regras e interfaces com programas que não possuem comunicação natural com a própria ferramenta. Esta característica tem sentido quando é preciso que se faça o gerenciamento de senhas em ambientes operacionais diferentes, permitindo e facilitando

[35] Dispositivo eletrônico, normalmente codificado, com informações sobre a pessoa autorizada a carregá-lo.
[36] Forma de programação que permite a interface entre linguagens e ferramentas distintas.

assim que as funções e interfaces não disponíveis sejam programadas com a troca de informações entre esses ambientes através da utilização de API.

**Administração Centralizada** - Uma ferramenta de ID única de usuário deve ter a capacidade de administração centralizada e de distribuição de administração, à medida que o gestor central assim o determinar. Seus diretórios de administração e gerência devem ser centralizados e as cópias devem ser permitidas à medida que se façam necessários mecanismos de segurança para funcionamento ininterrupto da ferramenta. O padrão X.500[37], para os diretórios e arquivos, deve ser o paradigma da ferramenta que integra as aplicações, serviços e sistemas. Os procedimentos de gerência e manuseio da ferramenta devem ter interface amigável e de fácil utilização para ação rápida e eficiente da mesma. Reconhecemos que a partir da centralização de gerenciamento haverá um aumento considerável do tráfego de senhas em segmentos das redes por onde não passavam anteriormente, isto faz com que seja necessário a implantação de mecanismos que proporcione o tráfego destas senhas criptografadas.

Concluindo as características essenciais à uma ferramenta de ID única de usuário, entendemos que, para um problema complexo como a I&A em ambientes distribuídos, a solução passa pela simplificação de ferramentas e técnicas, apoiada fortemente na utilização de senhas como mecanismo de autenticação. A simplificação também passa pela centralização da gerência e auditoria dos controles de acesso, com distribuição de responsabilidades operacionais em função da quantidade de contas e identificações a serem administradas. A técnica de ID único de usuário permite a apropriação das características positivas apresentadas neste trabalho, das mais diversas técnicas e ferramentas, promovendo melhor controle e gerenciamento da segurança.

## *7.4 - Proposta de Implementação*

Embora vários dos sistemas em utilização na PBH ainda tenham características de sistemas centralizados, eles deverão, em breve, ser substituídos. A ampliação do número de sistemas e serviços disponibilizados para cada um dos usuários de informática também é fator importante na avaliação do quadro futuro das redes distribuídas.

Apoiados nesse quadro e nas constatações que realizamos durante todo o trabalho, podemos afirmar que se faz necessária a determinação de políticas de segurança e de uma arquitetura que implemente as estratégias de acesso e democratização das informações em redes de computadores públicas como a que está em funcionamento na PBH. Após definida uma política, poderemos ter detalhamento da arquitetura e as especificações para implantação de mecanismos de I&A. Não é adequado escolher um único mecanismo de identificação para toda a rede por imposição de elementos que não sejam provenientes da política de segurança, em função da especificidade de cada rede local e das características de cada usuário. Alguns locais e usuários demandam, exclusivamente, acesso através de ID de usuário e senha, enquanto outros serviços, destinados a usuários mais específicos, requerem I&A através de sistemas biométricos. Cada procedimento de I&A tem que ser analisado e deve ser implementado a partir da aderência à política de segurança e da infra-estrutura disponível, ressaltando que a arquitetura implantada é que deve determinar a utilização de qualquer mecanismo de I&A que for escolhido.

### 7.4.1 - Revisão da Política de Acesso Lógico

[37] Padrão desenvolvido pela ISO e ITU (ex-CCITT) para identificação de objetos (arquivos, usuários, equipamentos) e segurança.

A política de utilização de senhas para acesso lógico aos recursos de informática, implementada através da Norma de Controle de Acesso Lógico à RMI - NPBHTIAOSG00101 (Anexo 3) estabelece condições de uso que não estão sendo aplicadas em todos os ambientes de redes descentralizadas da RMI, sendo até inadequada para configurações de ambiente onde os mecanismos de I&A foram implantados anteriormente à publicação da norma. Essa norma deve ser revista e adequada às características dos sistemas e métodos de trabalho dos usuários dessas redes, proporcionando modernização da norma e o aumento à aceitação de utilização da mesma


**Gráfico 5 - Obstáculos para Implementar Segurança [40]**

O Gráfico 5 mostra que é fundamental a conscientização do usuário de informática, pois permite a diminuição dos obstáculos à implementação de segurança nas organizações, fortalecendo, assim, a proposta de revisão da política em vigor e proporcionando treinamento e informação aos usuários.

Além da revisão dessa norma, que não tem aplicação efetiva para todos os usuários da RMI e somente para aqueles com vínculo empregatício com a Prodabel,

deve fazer parte do trabalho a ser desenvolvido uma discussão com representantes da Administração Municipal, numa discussão que abrangeria diretamente a Corregedoria Geral do Município (CGM), a Auditoria Geral do Município (AGM) e a Procuradoria Geral do Município (PGM), visando a instituição de uma legislação municipal que trate o tema de acesso às informações do município através de computadores. Essa legislação deveria abordar a relação e responsabilização dos acessos feitos pelo servidor municipal e, também, pelos cidadãos, entidades privadas e não governamentais. Repetimos que o vácuo legislativo sobre a obtenção de informações do município, através de redes governamentais de computadores, não deve existir, e enquanto legislação federal não se apresente com abrangência suficiente a PBH deve apresentar sua própria legislação. A fundamentação técnica das formas de acesso lógico é essencial para que a legislação não seja produzida com vícios tecnológicos e com características técnicas que a tornem caduca, em função do avanço de tecnologias e ferramentas de acesso, sendo que como preceito básico essas normas devem conter diretrizes e ações genéricas para serem apicadas em qualquer ambiente operacional da RMI.

### 7.4.2 - Sistema de ID Único de Usuário

É necessária a implantação, no ambiente da RMI, de uma política que contemple características de ID único de usuário, ou qualquer outra nomenclatura que identifique este tipo de técnica. O principal requisito para este tipo de ferramenta consiste na capacidade de suportar e interoperar múltiplas plataformas.

São características técnicas essenciais dessa política e do sistema a ser implementado, além das já descritas na Seção 7.3, a operação com sistemas desenvolvidos em diversas linguagens e plataformas, a possibilidade de gerenciamento

detalhado desses sistemas e aplicações, feito por supervisores de segurança específicos e com a devida transparência para o usuário, de forma que ele tenha a sensação de que cada I&A é realizada pelo seu próprio sistema ou serviço.

A escolha correta, ou o desenvolvimento sob medida, de uma ferramenta de I&A com ID única de usuário permitirá ao administrador de segurança, e aos seus supervisores distribuídos pelas diversas redes descentralizadas, o melhor controle e gerenciamento da atribuição de privilégios de acesso e autorizações de utilização dos serviços da RMI. O simples fato das redundâncias, onde houver, serem controladas e a gestão dos acessos ser feita de maneira unívoca para cada um dos usuários, provocará diminuição de acesso através do controle lógico centralizado.

### 7.4.3 - Mecanismos de Auditoria

Nenhum processo de auditoria sobrevive sem que informações sejam armazenadas para posterior comparação. Estas informações são verificadas comparadas a partir de regras preestabelecidas, como as Normas de Acesso Lógico (Anexo 3) e a Instrução de Serviço (Anexo 2). O processo de gravar as atividades executadas não pode ser impeditivo para que serviços sejam implantados e disponibilizados para os usuários.

A proposta que apresentamos é a de que todos procedimentos de segurança vinculados à I&A sejam gravados e que rotinas de auditoria para esses processos sejam implementadas em todas as unidades com rede de computadores. Essas rotinas de auditoria devem ser discutidas com a AGM com o objetivo de que o órgão responsável pela auditoria tradicional na PBH incorpore técnicas, como as inicialmente identificadas na Seção 5.3, que lhe serão úteis no seu trabalho diário com ambientes informatizados.

### 7.4.4 - Rotinas de Quebra de Senhas

Um procedimento simples e que deve ser uma ferramenta corriqueira para os administradores de segurança das redes é a instalação de rotina periódica para verificação de senhas fracas, em atendimento às normas em vigor e como forma de se antecipar às possíveis verificações e constatações das auditorias que podem ser realizadas sobre I&A. A implantação de uma ferramenta do tipo "Cracker" em todos os ambientes de servidoras de aplicações e arquivos, mesmo que seja implantada a política e o sistema de ID única de usuário, é fundamental para a organização do ambiente de acesso e preparação dos usuários para uma possível implantação de sistema de ID única de usuário.

### 7.4.5 - Mecanismos de Alteração de Senhas

Um dos problemas mais característicos dos sistemas centralizados de controle de senhas é o fato de que o administrador de segurança e seus supervisores ficam constantemente com a responsabilidade e suposição, por parte dos usuários, de que estejam com o controle e conhecimento das senhas de todos os usuários. Alguns sistemas e serviços dispõem de mecanismos de criptografia que impedem que os administradores do próprio sistema vejam as senhas dos usuários.

Contrapondo-se a esse mecanismo, existe a necessidade de fornecimento de novas senhas aos usuários, seja no momento de um novo cadastramento ou porque esqueceram a senha que utilizam. Para esse problema, tão comum em ambientes computacionais, são necessários procedimentos especiais, tais como a adoção de uma sistemática para o envio da senha inicial exclusivamente ao usuário que requisitou sua inclusão. Essa senha só poderá ser utilizada uma única vez e, imediatamente após

utilizá-la o usuário deve alterá-la. Como no ambiente da RMI esse procedimento não é trivial (vários procedimentos são adotados dependendo do administrador de cada ambiente operacional), exceto no sistema de correio da Intranet, onde o procedimento de alteração é claro o suficiente para que os usuários alterem suas senhas a todo momento (Anexo 7), faz-se necessário também que sejam criados mecanismos de alteração de senhas na RMI, especialmente na Internet, onde a alteração é mais precária, em função de vários técnicos profissionais, especializados e não especializados, terem conhecimento das senhas fornecidas aos usuários. Uma possibilidade a ser considerada é a transferência da responsabilidade de criação de usuários seja realizada por pessoal vinculado ao setor de Recursos Humanos que colocariam esse procedimento como uma das atividades admissionais de cada funcionário e como tarefa do mesmo.

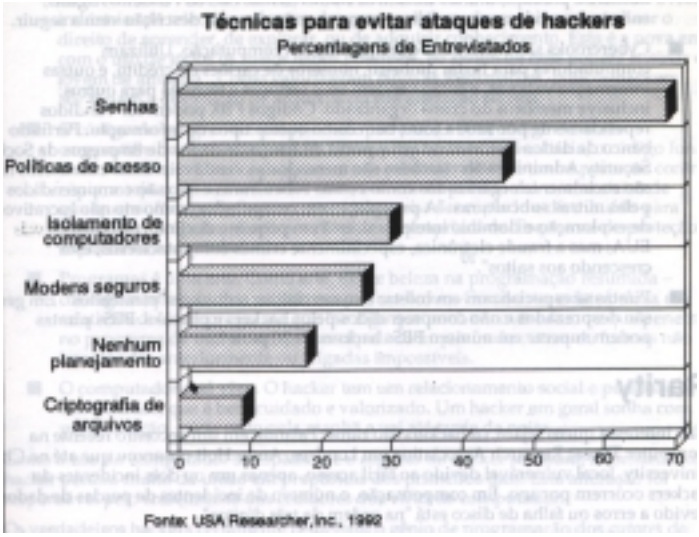


**Figura 15 - Técnicas para Evitar Ataques Hackers [40]**

A Figura 15 mostra que o tratamento e acompanhamento da utilização das senhas e de suas políticas podem evitar a maioria dos problemas de segurança, especialmente ataques de *hackers*. Esses mecanismos podem ser simples códigos de verificação desenvolvidos em linguagem como o "C" [3, 27, 35], que utilizam técnicas de programação simples como tabela de decisão [56], implementando rotinas para

verificação a cada mudança de senha e consultando arquivos para impedir senhas fáceis, senhas repetidas e fracas, ou seja fazendo exatamente o inversos do trabalho realizado pela ferramenta *cracker*, permitindo que as senhas não sejam, pelo menos, vulneráveis à ele.

# 8 - Conclusão

*"O problema de selecionar e usar adequadamente boas senhas está ficando mais importante a cada dia."*

**Francesco Bergadano [3]**

Dois fatores marcaram a opção que fizemos quando propusemos este trabalho: as mudanças implementadas pela Prodabel na RMI e o desafio de mostrar que a utilização de I&A não é um procedimento descartado, ou com o fim determinado em ambientes computacionais descentralizados [20]. A afirmação de que a utilização de senhas não existe mais nos ambientes informacionais modernos é parcial e inadequada, se feita desvinculada de estudos sobre esses ambientes. Comprovamos, e obtivemos avaliações externas à RMI, que o desafio apresentado era suficiente para justificar todo o estudo e trabalho que tivemos. As contribuições que demos à elaboração de Normas para Acesso Lógico à RMI e à Instrução de Serviço aplicável à Administração Municipal confirmaram a correção e aplicabilidade da opção que fizemos ao tratarmos do tema I&A. Um depoimento realizado na Câmara Municipal de Belo Horizonte para CPI da Folha de Pagamento da PBH, onde determinado usuário argumentava em sua defesa que sua senha era de conhecimento de várias pessoas, e que a ele não poderia ser atribuída nenhuma responsabilidade pelo uso fraudulento da senhas por outras pessoas, constitui uma comprovação da necessidade do trabalho que aqui concluímos.

Ao analisarmos o Grafico 6, apresentado numa recente pesquisa de segurança da informação [40], identificamos que é fator essencial a evolução no uso de técnicas de I&A para redes de computadores do setor público, além do avanço na discussão e implementação de políticas de uso de senhas nas corporações, públicas ou privadas, que têm redes de computadores locais ou remotas.


**Gráfico 6 - Tópicos de Política de Segurança [40]**

Da mesma forma, a avaliação do Grafico 7 mostra que essas mesmas organizações investem muito pouco nas medidas de segurança adotadas para a diminuição das vulnerabilidades. Sistemas biométricos não estiveram nem entre as dez medidas mais adotadas para melhoria da segurança nas redes de computadores no ano de 1999 [40].

As medidas vinculadas às questões culturais, que consistem na maior vulnerabilidade dos ambientes informatizados, devem ser reforçadas, o que corrobora também nossa hipótese de que o relacionamento social e cultural deve ser trabalhado para que não se percam os recursos aplicados em tecnologia e ferramentas.

São permanentes, e recebem destaque, os investimentos em procedimentos diretamente associados à I&A, *software* de controle de acesso, segurança no acesso físico de servidores, *software* de monitoração e auditoria nas trilhas de processamento, implementação de ID única de usuário e implantação de biometria estão presentes nas propostas de  medidas de segurança a serem implementadas pelas empresas.


**Gráfico 7 - Medidas de Segurança Adotadas [40]**

Finalmente, é essencial destacar que o estudo de caso componente deste trabalho fundamentou nossa teoria e mostrou que técnicas e ferramentas não são suficientes para dotar redes de computadores de segurança ilimitada, do ponto de vista de acesso e, em particular, para I&A. É necessário implantação das políticas mais adequadas a cada ambiente operacional, fazendo com que a adoção de qualquer técnica ou ferramenta deva ser obrigatoriamente precedida pela implantação de uma política clara de quesitos de segurança que seja aceita, seguida e disseminada pelos usuários dos recursos de informática. As políticas de uso de senhas não fogem a essas regras e podem, com uma mudança nas práticas culturais, ter utilidade inestimável para o controle de redes de computadores e à implantação de novas tecnologias de I&A.

# 9 - ANEXOS

## *1. Instrumentos da pesquisa.*

1.1 - Modelo 1 de e-mail enviado.

1.2 - Modelo 2 de e-mail enviado.

1.3 - Modelo 3 de e-mail enviado.

1.4 - Quadro de recebimento de respostas

## *2. Instrução de Serviço da Corregedoria Geral do Município.*

## *3. Norma de Controle de Acesso Lógico à RMI - NPBH TIAOSG00101.*

## *4. Plano de Trabalho para Pesquisa/Projeto.*

## *5. Plano de Trabalho para Pesquisa/Projeto (Segunda Parte).*

# *6. Identificação e Autenticação no Notes®.*

## *7. Como Alterar sua Senha no Notes®.*

## *8. Listas de Discussão em UOL/INFO.*

## *9. Reprodução de e-mails em UOL/INFO.*

## Referências Bibliográficas

[1] BARROS, Lincoln A. Informática Pública e Reforma do Estado: A Prodabel como experiência inovadora. *Dissertação de Mestrado em Administração Pública - Sistemas de Informação e Gestão*. Belo Horizonte: EGMG/FJP.1997.

[2] BARROS, Lincoln A. Informática Descentralizada: Um Modelo Alternativo; In: Prodabel - Espaço BH. Belo Horizonte. p. 11-16, Fev. 1998.

[3] BERGADANO, Francesco. High Dictionary Compression for Proactive Password Checking; In: ACM Transactions on Information and System Security. Londres. Vol. 1, n. 1, p. 3-25, Nov. 1998.

[4] BLACK BOX. Pocket Glossary of Data Communication Terms. Pittsburgh: Black Box Corporation.1994.

[5] BRISA. Gerenciamento de Redes - Uma Abordagem de Sistemas Abertos. Brasília: Makron Books.1993.

[6] BRISA. Rede Municipal de Informática - Levantamento da Situação Atual e dos Requisitos de Evolução do Ambiente de Teleinformática. Belo Horizonte: BRISA. Jun. 1995.

[7] BRISA. Rede Municipal de Informática - Projeto Funcional. Belo Horizonte: BRISA. Jul. 1995.

[8] BRISA. Rede Municipal de Informática - Projeto Físico. Belo Horizonte: BRISA. Nov. 1995.

[9] BRUNAZO Filho, Amílcar. A Segurança do Voto na Urna Eletrônica Brasileira. In: Simpósio sobre Segurança na Informática. São Paulo. ITA, 1999.

[10] BURNS, Robert. The Secret Of Pyramid [on line]. Disponível na World Wide Web: http://www.universalorder.com/pyramid.html, 1997.

[11] CARUSO, Carlos A.A. Segurança em Microinformática e em Redes. Rio de Janeiro : LTC Livros Técnicos e Científicos, 1993. 52p.

[12] COHEN, Frederick B. Protection and Security on the Information Superhighway. New York: Jonh Wiley & Sons, Inc. 1995. 19ª. Ed. 301p.

[13] COMER, Douglas E. Computer Network and Internets: Prentice Hall. 1997.

[14] CUNHA, Demerval R. R. Engenharia Social a La Ditadura [on line]. Disponível na World Wide Web: http://www.inf.ufsc.br/barata/engdit.html. 1999.

[15] DEL PICCHIA, Wálter. Métodos Numéricos para a Resolução de Problemas Lógicos. São Paulo : Edgard Blücher, 1993. 395p.

[16] DI PIETRO, Maria Sylvia Zanella. Direito Administrativo. 9ª. Ed. São Paulo : Atlas, 1999. 566p

[17] DoD. Department of Defense Password Management Guideline - CSC-STD-002-85. Maryland. CSC.1985.

[18] EISENBERG, José. Internet Popular e Democracia nas Cidades; In: Prodabel - Informática Pública. Belo Horizonte. p. 7-24, Jun. 1999.

[19] ELMASRI, Ramez. NAVATHE, Shamkant B. Fundamentals of Database Systems. 2ª. Ed. Menlo Park-CA: Addison-Wesley. 1994.

[20] O Fim das Senhas. ESTADO DE MINAS, Belo Horizonte, 06/set/1999. Caderno Informática. Pag.1.

[21] Adeus às Senhas Alfanuméricas. ESTADO DE MINAS, Belo Horizonte, 27/dez/1999. Caderno Informática. Pag.2.

[22] EUGÊNIO, Marconi. CAMPOS, Marconi O. Arquitetura da RMI (Rede Municipal de Informática); In: PRODABEL - Informática Pública: Uma Experiência Inovadora. Belo Horizonte. p.85-100, 1996.

[23] Truques e Cuidados ao Instalar o Sistema. Exame Informática. São Paulo. Vol. 7, n. 3, p. 38-40, Mar. 1992.

[24] FANTINATTI, João Marcos. Auditoria em Informática: Metodologia e Prática. São Paulo: McGraw-Hill. 1988.

[25] FONTES, Edison. I&A [on line]. Disponível na World Wide Web: http://www.jseg.net/identifi.htm.1999.

[26] FORESTER, Tom. MORRISON, Perry. A insegurança do computador e a vulnerabilidade social; In: FGV - Revista de Administração de Empresas. São Paulo. p. 73-83, Out/Dez 1991.

[27] FRISCH, Ællen. Essential System Administration. 2ª. Ed. Sebastopol - CA: O'Reilly. 1995.

[28] GIL, Antônio de Loureiro. Qualidade Total em Informática. São Paulo: Atlas, 1992.

[29] GRAHAM, Cole B. Para Administrar a Organização Pública. Tradução: Britta Lemos de Freitas. Rio de Janeiro : Jorge Zahar, 1994. 280p.

[30] GUENGERICH, Steven. Downsizing em Sistemas de Informação. São Paulo: Makron Books. 1993.

[31] HAFÉZ, Andréa. Pesquisa. GAZETA MERCANTIL - Caderno Tecnologia. p.16. São Paulo, Jul. 1999

[32] Segurança, "calcanhar de aquiles" na Internet. HOJE EM DIA, Belo Horizonte, 04/out/1999. Caderno Internet. Pag.2.

[33] IEEE. Distributed Computing: Concepts and Policies. New York: IEEE.1984.

[34] KAHANER, Larry. Companies Strive For Simpler Security. Information Week [on line]. Disponível na World Wide Web: http://www.informationweek.com. 2000.

[35] KERNIGHAN, Brian W. e RITCHIE, Dennis M. C, a linguagem de programação. Padrão ANSI. Tradução: Daniel Vieira. Rio de Janeiro: Campus. 1990.

[36] MACHIAVELLI, Niccolo. O Príncipe. Tradução: Antônio D'Elia. São Paulo: Cultrix. 1992.

[37] MARTINS, Ivan. Gurovitz, Hélio. Ilusão de Privacidade. Exame Informática. São Paulo. Vol. 7, n. 3, p. 134-146, Mar. 1997.

[38] MÓDULO. Políticas de Segurança da Informação em Redes Integradas à Internet; In: Seminário GI Sistemas Abertos. São Paulo. BRISA, 1996.

[39] MÓDULO. Glossário Módulo de Segurança da Informação [on line]. Disponível na World Wide Web: http://www.modulo.com.br/links, 1998.

[40] MÓDULO. Pesquisa Nacional sobre Segurança da Informação. São Paulo. Módulo, 1999.

[41] MONTEIRO, José A. Qualidade Total no Serviço Público; Questionamentos e Recomendações Segundo os 14 Pontos de E.W. Deming. Brasília - DF: QA & T Consultores Associados. 1991.

[42] A Guide to Understanding Identification and Authentication in Trusted Systems, NCSC-TG-017, National Computer Security Center, Set. 1991.

[43] A Guide to Understanding Object Reuse in Trusted Systems, NCSC-TG-018, National Computer Security Center, Jul. 1992.

[44] OLIVEIRA, Yuri G. Research on Face Recognitions; [on line]. Disponível na World Wide Web: http://www.prism.uvsq.fr/~anta/yuri.html, 1998.

[45] OLIVEIRA, Evandro L. As Armadilhas Virtuais; In: Prodabel - Diário de Bordo. Belo Horizonte. p. 2-3, Jul. 1999.

[46] PFAFFENBERGER, Bryan. Que: Dicionário dos usuários de microcomputadores: Português-Inglês e Inglês-Português. Tradutor e Consultor: Fernando B. Ximenes. - Rio de Janeiro: Campus, 1992.

[47] PILLER, Charles. Cyber-Crime Loss at Firms Doubles to $10 Billion; [on line]. Disponível na World Wide Web http://www.lantimes.com/business, 2000.

[48] PLATINUM. Glossary of Terms [on line]. Disponível na World Wide Web: http://www.platinum.com, 1998.

[49] PRODABEL. Descentralização da Informática na PBH. Belo Horizonte: Prodabel. 1994.

[50] PRODABEL. Proposta de Modelo Funcional da Informática da PBH. Belo Horizonte: Prodabel, 1995.

[51] SEMINÁRIO DE INFORMÁTICA PÚBLICA. 1, 1996, Belo Horizonte: Prodabel. 1996.

[52] PRODABEL. Topologia da RMI. Belo Horizonte: Prodabel/Diope, 1995.

[53] RANDALL, Neil. ROBERTS-WITT, Sarah L. Você está Seguro On-Line? PC Magazine Brasil. São Paulo. Vol. 9, n. 9, p. 66-99, set. 1999.

[54] RUMBAUGH, James. [et al.]. Modelagem e Projetos Baseados em Objetos. Tradução: Dalton Conde de Alencar. Rio de Janeiro: Campus. 1994.

[55] RUSSEL, Deborah. GANGEMI, G.S. Computer Security Basics. 2ª. Ed. Sebastopol - CA: O'Reilly. 1991.

[56] SEDGEWICK, Robert. Algorithms in C. Massachusetts: Addison-Wesley. 1990.

[57] SHIMOMURA, Tsutomu. e MARKOFF, John. The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw - By the Man Who Did It. Mass Market Paperback - Warner Books. Califórnia-USA.1996.

[58] STANG, David J. Segredos de Segurança em Rede / David J. Stang, Sylvia Moon. Tradução: Claudio Lobo. 1ª Edição. Rio de Janeiro : Berkeley Brasil, 1994. 986p.

[59] Summers, R.C. An Overview of Computer Security; In: IBM Systems Journal. Los Angeles - CA. Vol. 23 - n. 4. p. 309-325, 1984.

[60] SETTI, Ricardo B. Você é Sua Senha. Super Interessante. São Paulo. n. 143, p. 36-39, ago. 1999.

[61] TANENBAUM, Andrew S. Redes de Computadores. Tradução: [da 3a. edição original] Insight Serviços de Informática. 3ª Edição. Rio de Janeiro : Campus, 1997. 923p.

[62] TAROUCO, Liane M.R. Redes de Comunicação de Dados. 3ª Edição. Rio de Janeiro : LTC - Livros Técnicos e Científicos, 1985. 218p.

[63] VERHALEN, Berthold… [et al]. Procedimentos de Auditoria - Informática. Instituto dos Auditores Internos do Brasil. Rio de Janeiro: IAIB. 1993.

[64] Ward, Gerald M. e PERKINS, Willian. Controles de Segurança de Microcomputadores: Uma Abordagem em Três Etapas. São Paulo: MIPS. 1991.