JOSÉ GLADISTONE DA ROCHA

CONTROLE DE ACESSO A SISTEMAS DE INFORMAÇÕES

Dissertação apresentada ao Curso de Pós-Graduação em Criptografia e Segurança em Redes da Universidade Federal Fluminense / Centro de Estudos de Pessoal – Exército Brasileiro, como requisito parcial para obtenção do Grau de Especialista.

Orientador: Prof. Dr. RICARDO CAMPANHA CARRANO

Niterói
2006

JOSÉ GLADISTONE DA ROCHA

CONTROLE DE ACESSO A SISTEMAS DE INFORMAÇÕES

Dissertação apresentada ao Curso de Pós-Graduação em Criptografia e Segurança em Redes da Universidade Federal Fluminense / Centro de Estudos de Pessoal – Exército Brasileiro, como requisito parcial para obtenção do Grau de Especialista.

Aprovada em:_____.

BANCA EXAMINADORA

_____

Prof. Dr. RICARDO CAMPANHA CARRANO – Orientador

UFF

_____

Prof. Examinador

UFF

_____

Prof. Examinador

UFF

Niterói

2006

À minha esposa, por seu auxílio e paciência e aos meus filhos, simplesmente por existirem e, através de seus sorrisos, contribuírem para meu crescimento.

AGRADECIMENTOS

À minha esposa Vildécia que sempre me incentivou nos meus estudos e trabalho, com sugestões objetivas,

Aos meus filhos Brenner e Raquel que tiveram compreensão e paciência sempre que precisei,

Aos Professores Doutores Luiz Manoel e Ricardo Carrano que souberam transmitir orientações seguras na realização deste trabalho,

A todos os professores da UFF com quem tive o prazer de conviver no EB-Aula, passando orientações tão necessárias para o meu aprendizado neste curso.

RESUMO

Dentre muitas estratégias adotadas pelas empresas para obterem sucesso em suas áreas de negócio, merece uma atenção especial a implantação de uma Política de Segurança no trato com a informação, pois ela é o seu bem de maior valia, independente do ramo que atua. Com a evolução tecnológica dos sistemas de informação, surgiu a necessidade de se proporcionar segurança no tráfego e trato com as informações de forma que não fossem interceptadas por pessoas indesejáveis, que aliás, a cada dia vêm descobrindo novas técnicas de ataques e resultando em sérios prejuízos para as empresas. A falta de implantação de uma Política de Segurança bem definida, como parte de um processo vital para as empresas, pode se dar por desconhecimento ou descrédito de que elas venham realmente agregar valores como mecanismos de proteção de seus bens, pois a segurança é um produto de difícil mensuração, e somente percebida quando, na sua ausência, acarreta sérios prejuízos. Infelizmente, muitas empresas ainda não possuem uma mentalidade de investirem em um sistema global, que envolva a adoção de medidas passivas e ativas, com a participação de seus integrantes, para minimizarem falhas de segurança no fluxo, armazenamento e acesso às informações. O Objetivo que norteia este trabalho é de apresentar as principais medidas e mecanismos de segurança, que deverão ser observados, na proteção das informações organizacionais e que sirvam como elementos para constituírem numa Política de Segurança a ser adotada nas empresas, quanto aos controles ambientais e controles de acesso aos sistemas computacionais. Será enfatizada a necessidade das organizações adotarem uma Política de Segurança em TI, com base no levantamento de potenciais riscos, como elemento para identificação dos pontos vulneráveis do seu ambiente computacional e, assim, proverem um eficiente controle de acesso físico e lógico aos sistemas de informações. Em seguida, será mostrado como os sistemas biométricos podem ser utilizados na implementação de controles de acesso com maior precisão. Por fim, serão apresentadas as principais ameaças e suas origens, bem como, as medidas preventivas e corretivas no controle ambiental no qual os sistemas de informações estão inseridos.

Palavras-chave: Política de Segurança. Controle de Acesso. Riscos. Acesso Físico. Acesso Lógico. Biometria. Controle Ambiental.

ABSTRACT

Among many strategies adopted by companies to get success in its business area, the implantation of one Security Policies in information treatment deserves a special attention, because the information is its most value resource, independent of its business. With the technological evolution of the information systems, the necessity appeared to provide security in the traffic and treatment with the information to avoid interception by undesirable people, by the way, new techniques of attacks are discovered everyday and resulting in serious damages for companies. The lack of implantation of one defined Security Policies, as part of a vital process for the companies, must occur by the unfamiliarity or discredit that they really come to increase values, as mechanisms of protection, to its business, therefore the security is a product of difficult measurement, and only perceived when, its absence, causes serious damages. Unhappily, many companies not yet possess a mentality to invest in a global system, that it involves the adoption of passive and active measures, with the participation of its integrant ones, to minimize imperfections of security in the flow, storage and access to the information. The Objective that guides this work is to present the main measures and security mechanisms, that must be observed, in the protection process of information and support as elements to constitute in one Security Policies to be adopted by companies, related to the ambient controls and access controls to the computational systems. The necessity of the organizations to adopt one Security Policies in IT will be emphasized on basis of searching potential risks as element to identify vulnerable points of its computational environment and, thus, to provide an efficient control of physical and logical access to the systems information. After that, it will be shown as the biometrics systems can be used in the implementation of access controls to increase precision. Finally, the main threats and its origins will be presented, as well as, the preventives and correctives procedures in the ambient control in which the systems information are inserted.

Keywords: Security Politicies. Access Control. Riks. Physical Access. Logical Access. Biometry. Ambient Control.

SUMÁRIO

1. INTRODUÇÃO

A segurança da informação deixou de ser tratada como um assunto técnico, restrito aos profissionais de Tecnologia da Informação (TI), e vem sendo considerada uma real necessidade das empresas e instituições, tornando-se um requisito estratégico que interfere na capacidade das organizações em realizar transações e manter sigilo de suas regras de negócios vitais, para proteger-se de uma concorrência cada vez mais acirrada.

Apesar dessa mudança de postura, calçada na experiência e obtenção de resultados favoráveis pelas boas práticas no trato da gestão de segurança em TI, muitas empresas ainda não acordaram para a necessidade de proteger seu maior bem, a informação, fruto do desconhecimento da existência dessas técnicas ou mesmo por descrença nos resultados que elas podem proporcionar.

O aparato tecnológico, como rede de computadores, sistemas de armazenamento em massa, sistemas de comunicação e de gerenciamento, implantados nas empresas para responder prontamente e de forma eficiente o tratamento das informações, traz consigo a necessidade de protegê-las contra invasores, pois são alvos preferidos por sabotadores, espiões industriais e vários tipos de golpistas e *crackers*.

Uma Política de Segurança da Informação deve ser composta por regras claras e bem definidas, ser de fácil execução e estar sintonizadas com a cultura e o ambiente tecnológico da empresa. Deve proteger não só as informações vitais, mas também motivar o seu quadro de pessoal sensibilizando-os de sua importância e conscientizando-os da necessidade e do envolvimento de todos.

Segurança é, portanto, a proteção de informações, sistemas, recursos e serviços contra desastres, erros e manipulação não-autorizada, de forma a reduzir ou minimizar os impactos que delas possam advir.

Implantar mecanismos de proteção de informações exige altos investimentos, tanto em estrutura física dos bens mobilizados da empresa como na capacitação profissional de seu

pessoal. Há necessidade de medir o retorno que esse investimento trará à organização, o chamado *Return of Investiment* (ROI), para equilibrar as necessidades em segurança com os custos aplicados.

Deve-se considerar, também, que medidas de segurança resultam em certo desconforto para o usuário final, ou seja, existe uma relação inversa entre segurança *versus* conforto. Saber dosar qual o grau de segurança é o desejável, exige certa habilidade e conhecimento global do negócio da empresa e dos riscos potencias e vulnerabilidades existentes.

Um ambiente sem controle e proteção de suas informações, principalmente com usuários não comprometidos com o sigilo e a segurança, é altamente propício à perda de informações e fraudes. Mesmo que não sejam veiculadas na mídia, fraudes acontecem e dão prejuízos. Quando eventualmente vêm a público, desacreditam a organização vitimada perante seus clientes e parceiros comerciais.

A segurança física do ambiente de rede, bem como o seu controle de acesso, são fatores vitais para o sucesso de uma organização, por isso, a adoção de medidas e regras para sua implementação tem sido amplamente praticada, inclusive com suporte a outros campos da tecnologia como a automação predial e sistemas de combate a incêndio.

Com a criação de novas técnicas de invasão, muitas redes de computadores, particularmente aquelas mais antigas, não passaram por um processo de modernização tornando-se vulneráveis às atuais ameaças de segurança, pondo em risco os seus negócios e conseqüentemente ocasionando prejuízos incalculáveis.

Para a continuidade do negócio da organização, particularmente por ocasião de sinistros e desastres, devem ser previstas, nos planos de contingência, medidas alternativas para se evitar a paralisação dos sistemas, perda de dados, prejuízos à sociedade, levante de aspectos jurídicos de uma possível paralisação, queda nas ações da empresa e gastos elevados para as recuperações emergenciais.

Para os órgãos públicos, sejam da esfera federal, estadual ou municipal, a lei[1] determina que atendam às normas técnicas de segurança segundo a ABNT[2], e o novo Código Civil Brasileiro (Anexo B) impõe aos gestores da informação a solidariedade na reparação dos danos causados à sociedade e a terceiros, prejuízos em função de um ato ilícito, isto é, atribua-se diretamente a responsabilidade pela imperícia na gestão de segurança aos administradores dos sistemas de informação.

Neste contexto, pretende-se abordar os principais aspectos a serem observados para

[1] Lei 4.150/62, artigo 1° (Anexo A).
[2] ABNT: Associação Brasileira de Normas Técnicas.

que seja viável a implementação de controles ambientais e de acesso aos sistemas computacionais, como parte de uma Política de Segurança para organizações.

2. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Muitas vezes, questões de segurança da informação não são tratadas como uma ameaça direta e real ao negócio. Entretanto, se uma empresa está simplesmente conectada a Internet para leitura de *e mail*, ou com serviços de *e-commerce* 24 por 7 [3], o risco existe.

A necessidade premente do uso de tecnologia da informação pelas empresas para agilizar processos e tornar os negócios mais rentáveis, sob qualquer aspecto, trouxe consigo a necessidade de adoção de medidas que visassem evitar o roubo de recursos computacionais, a interrupção de serviços, a divulgação e a alteração não autorizada de informações.

A implantação de uma política de segurança da informação, vem a atender essas necessidades, ou seja, abrange um conjunto de leis, regras e práticas que regulam como os recursos, incluindo-se as informações sensíveis, são gerenciadas, protegidas e veiculadas dentro de uma organização. Essas leis e regras devem identificar critérios em concordância com a autoridade individual, intrínseca a cada usuário, e deve especificar condições as quais cada indivíduo deve exercitar suas funções dentro da empresa.

A segurança da informação visa preservar três princípios básicos pelos quais norteiam a sua implementação e devem estar bem consubstanciados na política de segurança:

> Confiabilidade – Toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo, visando à limitação de seu acesso e uso apenas às pessoas para quem elas são destinadas.
>
> Integridade – Toda a Informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-las contra alterações indevidas, intencionais ou acidentais.
>
> Disponibilidade – Toda a informação gerada ou adquirida por um individuo ou instituição deve estar disponível aos seus usuários no momento em que os mesmos delas necessitem para qualquer finalidade. (SÊMOLA, 2003, p.45).

A política de segurança não define procedimentos específicos de manipulação e proteção da informação, mas atribui direitos e responsabilidades às pessoas (usuários,

[3] 24 por 7: significa operar 24 horas por dia e 7 dias por semana, ou seja, horário integral, ininterrupto.

administradores de redes e sistemas, funcionários, gerentes, etc.) que lidam com essa informação. Desta forma, elas sabem quais as expectativas que podem ter e quais são as suas atribuições em relação à segurança dos recursos computacionais com os quais trabalham. Além disso, a política de segurança também estipula as penalidades às quais estão sujeitos aqueles que a descumprem.

Para ser significativo, este conjunto de regras deve indicar quando determinadas ações poderão violar ou ferir a política de segurança implantada na instituição.

A Política de Segurança da Informação deve envolver todos que trabalham numa organização e, no processo de gestão da informação, devem possuir responsabilidades bem definidas. Tais agentes podem ser classificados em (CARUSO, 1999, p. 34):

Gestor da Informação – indivíduo responsável para tomar decisões em nome da organização no que diz respeito ao uso, à identificação, à classificação, e à proteção de um recurso específico da informação;

Custodiante – agente responsável pelo processamento, organização e guarda da informação; e

Usuário – qualquer pessoa que interage diretamente com o sistema computadorizado, podendo ter autorização para adicionar ou atualizar a informação, inclusive podendo ser o proprietário da informação.

Uma Política de Segurança da Informação deve prover controles nos ambientes corporativos para detecção de vírus, controles de acesso lógico e mecanismos de controle de acesso físico envolvendo nesse processo o Gestor da informação, o Custodiante e os usuários do sistema.

É importante, também, a definição de procedimentos a serem adotados para as seguintes áreas:

- **Políticas de acessos externos à organização** – com a definição de Convênios para acesso às bases corporativas; procedimentos quanto ao uso de criptografia e certificação digital; controle e gerenciamento de *log*[4] de acessos e manutenção da configuração de *Firewall* para filtragem de acessos.
- **Política de uso da Intranet** – como a padronização de *Home Page*; definição de normas de gerenciamento de Rede; definição de padrões de distribuição de versões de *softwares*; mecanismos para facilitar a identificação de pirataria;

[4] Termo utilizado para descrever o processo de registro de eventos relevantes num sistema computacional

detecção e inatividade de *modens* ligados à rede e adoção de padrões de atualização de antivírus.

- **Política de uso da Internet** – fazer controle de acesso de funcionários ao Provedor Corporativo; estabelecer uma padronização da *Home Page* institucional e comercial; uso de criptografia e certificação digital; configuração de *Firewall* e Roteadores; definição de eventos mínimos a serem "logados" nos Sistemas Corporativos; procedimentos para execução de auditorias e definição de política de *backup*.
- **Política de acesso físico** – estabelecimento de controles de acesso físico; definição de ambientes físicos de alta criticidade e monitoração de ambientes.
- **Política de acesso lógico** – definição de uma política de senhas e de identificação de usuários; estabelecimento de perfis de acesso aos ambientes e aplicativos e registro de *logs* de eventos mínimos nas transações.

Quanto aos dois últimos tópicos apresentados acima, serão abordados com maior profundidade mais adiante, por serem objetivos delineados neste trabalho.

Para se tomar medidas pró-ativas, faz-se necessário classificar as informações corporativas, segundo seu grau de sensibilidade, sigilo e acessibilidade em: confidenciais, corporativas e públicas. Cada uma terá um tratamento diferenciado.

Uma política de segurança também significa delegar responsabilidades para funcionários, que passam a responder por seus atos (se colaboram para a disseminação de um vírus, por exemplo). A importância da conscientização da equipe de profissionais é consenso entre os especialistas em segurança (BARBOSA, 2001, p. 27).

Normas e regras devem ser claras e praticáveis, sintonizadas com a cultura e o ambiente tecnológico da organização. Deve não apenas proteger as informações confidenciais, mas também motivar as pessoas que as manuseiam, mediante a conscientização e destaque de sua importância neste processo. Em suma, garantir a segurança é um desafio de todos.

Alguns fatores importantes para o sucesso de uma política de segurança são:

- apoio por parte da administração superior;
- deve ser ampla, cobrindo todos os aspectos que envolvem a segurança dos recursos computacionais e da informação sob responsabilidade da organização;
- deve ser periodicamente atualizada de forma a refletir as mudanças na organização;

- deve haver um indivíduo ou grupo responsável por verificar se a política está sendo respeitada;
- todos os usuários da organização devem tomar conhecimento e manifestar a sua concordância em submeter-se a ela antes de obter acesso aos recursos computacionais;
- deve estar disponível em um local de fácil acesso aos usuários, tal como a *intranet* da organização.

Dentre os itens acima, o apoio por parte da administração superior é essencial. Se a política de segurança não for cobrada pela administração, será rapidamente negligenciada pelos demais setores da organização. Além disso, é importante que os seus membros dêem o exemplo no que diz respeito à observância da política de segurança.

Uma das maiores dificuldades na implantação de uma política de segurança nas organizações, repousa exatamente na falta de consciência de sua importância, por parte da classe dirigente (Figura 1), conforme aponta a pesquisa realizada pela Módulo Security.

Figura 1 - Obstáculos para Implementação da Segurança

Assim como existem fatores que contribuem para o sucesso de sua implantação, por outro lado, deve-se atentar para alguns fatores que podem influenciar negativamente na sua aceitação e levá-la ao fracasso, tais como:

- não ser demasiadamente detalhada ou restritiva. O excesso de detalhes pode causar confusão ou dificuldades na sua implementação;
- não devem ser abertas exceções para indivíduos ou grupos;
- não deve estar atrelada a *softwares* e/ou *hardwares* específicos.

3. CONTROLE DE ACESSO

Dentre as várias vertentes da segurança da informação, o controle a seu acesso, através de uma política bem consolidada, é um ponto crucial para a manutenção e proteção dos negócios de qualquer empresa, quer seja pelo público interno ou externo.

Em um sistema informatizado, entende-se como acesso, a capacidade de pessoas obterem informações quer seja fisicamente em contato com equipamentos computacionais ou remotamente através de uma rede.

Como dito anteriormente, as informações, armazenadas ou mesmo em trânsito pela rede, devem sofre um processo de segurança para proporcionar integridade, confidencialidade e disponibilidade, e o acesso a essas informações ou equipamentos deve ter um tratamento todo especial para atender à política de segurança das informações por seus usuários.

Antes mesmo de serem definidas as medidas a serem adotadas para controlar o acesso ao sistema de informação, é necessário ter conhecimento de toda estrutura física das instalações com base nos projetos de rede elétrica, hidráulica, climatização, identificação da localização de portas e janelas, tipo de revestimento, existência de forros e divisórias, entre outros fatores que caracterizam o ambiente a ser segurado.

É fundamental, também, fazer um levantamento da estrutura lógica e de equipamentos instalados na organização, tendo como base o projeto de redes para identificar a topologia de rede utilizada, a localização de Servidores e quais serviços são disponibilizados, quantidade de computadores instalados e identificação prévia de áreas críticas no trato com as informações confidenciais.

O profissional de TI, juntamente com a gerência da organização, deve atentar para a problemática do controle de acesso, vislumbrando possíveis ameaças e fazendo uma criteriosa análise dos riscos que poderão assolar a organização e assim decidir qual a melhor estratégia a ser adotada sem onerar excessivamente a instituição e atender a requisitos operacionais e de segurança, já estabelecidos na política da empresa.

Apesar de não ser objeto deste trabalho, merece destacar que a obtenção do acesso pode se dar por trabalho de engenharia social, a qual uma das táticas fundamentais é obter acesso a informações que os funcionários da empresa tratam como inofensivas e utilizá-las para ganhar a confiança de outros usuários e conseguir as informações que o atacante realmente deseja.

3.1 Gerência de Riscos

Quando se questiona quais ações devem ser adotadas objetivando o máximo de segurança para o controle de acesso ao sistema computacional, deve-se recorrer à técnica de gestão de riscos, pois, uma vez identificadas as possíveis vulnerabilidades e ameaças ao sistema e seus possíveis impactos, torna-se possível montar estratégias para aplicação de medidas de segurança efetivas sem ferir os objetivos organizacionais.

Os requisitos de segurança no acesso à rede devem ser identificados, por meio de uma análise e avaliação sistemática e periódica dos riscos de segurança da informação, baseadas nos critérios para aceitação de risco. Devem ser adotados, segundo prioridades de implementação dos controles, para assegurar que estes riscos sejam reduzidos a um nível aceitável pela organização.

Segundo Moreira (2001, p. 11):

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

Os gastos com os controles ou ações a realizar devem ser balanceados de acordo com os danos causados aos negócios gerados pelas potenciais falhas na segurança da informação e devem resultar no máximo retorno dos investimentos.

O processo de avaliação dos riscos e a seleção dos controles pertinentes devem ser realizados com certa freqüência, de forma a cobrir diferentes partes da organização ou de

sistemas de informação específicos, atendendo principalmente à evolução tecnológica e evitando a obsolescência dos procedimentos em uso.

A gerência de mudança de requisitos de segurança do acesso físico e lógico do sistema deve propor, continuamente, alterações de ações adotadas para que atendam a novos requisitos que anteriormente não eram contemplados e que, fruto de um trabalho metódico com base em novas tecnologias, necessitou-se de complementação.

Convém que, antes de considerar o tratamento de um risco, a organização deve submetê-lo aos critérios de aceitação para determinar se pode ser ou não aceito. Riscos podem ser aceitos se, por exemplo, forem avaliados como baixos ou se os custos dos seus tratamentos não são economicamente viáveis para a organização, cabendo ao gerente de requisitos registrar as decisões tomadas.

Para cada um dos riscos identificados, seguindo uma análise e avaliação, uma possível decisão a ser tomada é: aplicar controles apropriados para reduzi-los; conhecer e objetivamente aceitar os riscos, sabendo que eles atendem claramente à política da organização e aos critérios para a sua aceitação; evitar riscos, não permitindo ações que poderiam causar a ocorrência de riscos; e transferir os riscos associados para outras partes, por exemplo, seguradoras ou fornecedores.

Caso a estratégia a ser adotada seja a de tratamento do risco com aplicação de controles apropriados, deve-se atentar para que a medida de prevenção a ser implementada, atenda aos requisitos identificados pela análise e avaliação do risco em questão e assegurar-se de que, tal risco, seja reduzido a um nível aceitável, levando-se em conta:

- As restrições de legislações nacionais e internacionais;
- Os objetivos organizacionais;
- Os requisitos e restrições operacionais da organização;
- O custo de implementação e operação em relação aos riscos que estão sendo reduzidos; e
- A necessidade de balancear o investimento na implementação e operação de controles contra a probabilidade de danos que resultem em falhas de segurança da informação.

Deve-se ficar atento ao se aplicar medidas de controle para que não conflitem com a legislação nacional, como, por exemplo, o registro de eventos de *"logging"*, e a proteção à privacidade dos clientes ou a exercida nos locais de trabalho.

É fundamental que a especificação de requisitos para segurança seja realizada nos estágios iniciais dos projetos e sistemas para posterior implementação de controles de segurança da informação, pois caso isso não seja realizado, poderá acarretar custos adicionais e soluções menos efetivas, ou mesmo, na pior hipótese, incapacidade de se alcançar a segurança requerida.

Convém destacar que nenhum conjunto de medidas de controle pode conseguir a segurança completa ou ideal, em face de seu elevado custo de implementação ou por ser pouco amigável aos usuários do sistema, tornando-se fundamental ao gestor de segurança o monitoramento e avaliação dos riscos apontando a melhor solução, de forma eficiente e eficaz para apoiar as metas da organização.

Para se implantar medidas de segurança no controle de acesso, deve-se mapear todos os riscos através de uma análise criteriosa, e assim, identificar os recursos necessários para sua implementação, como: equipamentos de monitoração, energia elétrica, climatização, ambientes de segurança para equipamentos críticos, classificação do acesso às áreas da organização, política de segurança de acesso, dentre outros componentes que englobam um projeto de segurança da informação.

"Após realizar os investimentos e implementar o plano, a empresa deverá estar constantemente revendo o plano e modificando o que for necessário, o que demonstra ser um plano contínuo." (Barbosa, 2001, www.modulo.com.br).

Portanto, o processo de análise de riscos nos leva às respostas das seguintes perguntas: Quais os pontos vulneráveis? Quais as ameaças em potencial? Quais os possíveis danos que essas ameaças podem causar? Quais os impactos negativos para os negócios da organização em caso de incidente de segurança? Quais as medidas que devem ser adotadas para impedir ou minimizar o impacto de cada incidente de segurança?

Em entrevista ao *Web Site* da Módulo *Security* (www.modulo.com.br , acessado em 21 Out 06), Francesco Di Cicco[5] diz:

> "Nos últimos anos a Gerência de Riscos (GR), de maneira geral, tem buscado alcançar o adequado balanceamento entre aproveitar as oportunidades de ganhos e minimizar os impactos adversos. A GR "contemporânea" é parte integrante das boas práticas de gestão empresarial e é também um elemento essencial da chamada Governança Corporativa, sendo desenvolvida como um processo iterativo, composto de etapas seqüenciais, de modo a permitir a contínua melhoria da tomada de decisões e do desempenho da organização."

[5] Especialista em *Risk Management* e diretor executivo do QSP – Centro de Qualidade, Segurança e Produtividade. Entrevista realizada para a Módulo *Security Magazine* de 06 de fevereiro de 2006.

Francesco De Cicco propôs um processo estruturado de gerência de riscos para as normas AS/NZS 4360, versão 2004, conforme a figura 2.

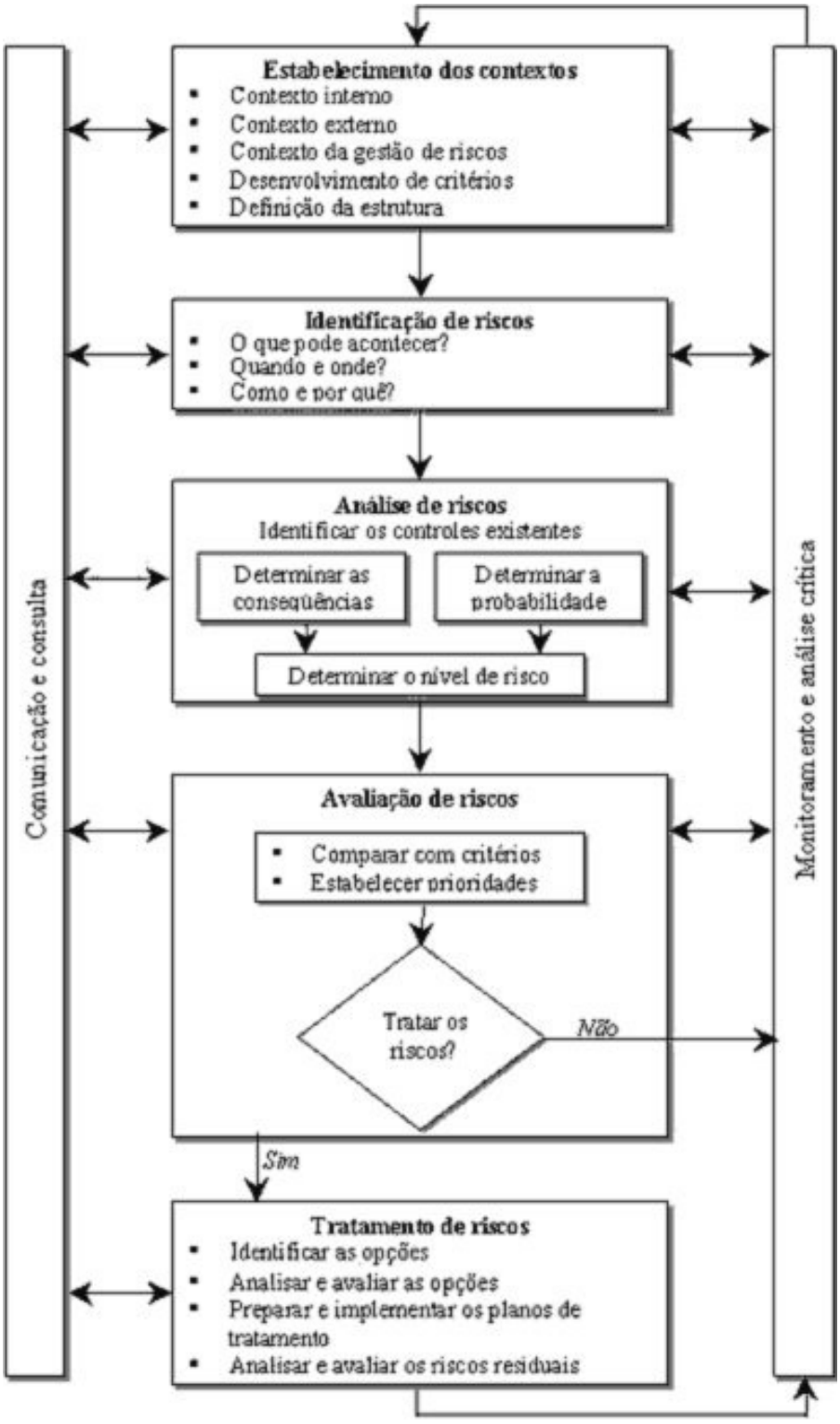

Figura 2 - Processo de Gestão de Riscos

Ressalta-se de importância no levantamento dos riscos a observância de alguns vetores que, bem identificados, podem ser combatidos, reduzindo as ameaças e vulnerabilidades a um custo mais acessível, tais como:

ERROS HUMANOS

Muitas pesquisas realizadas para avaliação de segurança em TI nas empresas, têm apontado o fator humano como sendo um dos que mais provocam incidentes de segurança, devido à falta de treinamento e suporte, desatenção no trabalho, omissão e descaso no trato com informações críticas e, principalmente, a vulnerabilidade à engenharia social[6].

Usuários impensadamente alteram configurações de equipamentos, divulgam contas e senhas de acesso, deixam sessões abertas na sua ausência, utilizam senhas frágeis facilmente descobertas ou mesmo contaminam seus arquivos e programas com vírus de computadores.

E MAIL

Outro recurso que tem se mostrado muito crítico é o uso de mensagens eletrônicas no ambiente de trabalho, que vai desde a falsificação até a contaminação por vírus. Isso se deve à facilidade proporcionada na troca de informações e, muitas vezes, não dizendo respeito aos propósitos do negócio das empresas, mas comumente utilizado para interesses particulares, que favorecem o recebimento de mensagens suspeitas contendo vírus ou mesmo *spam*[7].

Apesar de ter sofrido uma redução, a partir de 2005, dos registros de ocorrências de *spams*, reportados ao CERT[8] Brasil (Figura 2), ainda é muito alto o tráfego de mensagens dessa natureza. Tal redução, provavelmente, se deve ao fato de muitos usuários utilizarem programas *anti-spam* que reduzem substancialmente esse número e, principalmente o refinamento na configuração dos Servidores de Correio Eletrônico dos Provedores de Internet na tentativa de coibir essa prática.

[6] Atividade com objetivo de se colher informações de uma organização através de pessoas que nelas trabalham no intuito de tirar vantagem pessoal ou prejudicar a organização por meio de ataques.
[7] Envio, a uma grande quantidade de pessoas de uma vez, de mensagens eletrônicas, geralmente com cunho publicitário. Podem ser de origem desconhecida ou não.
[8] CERT: Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

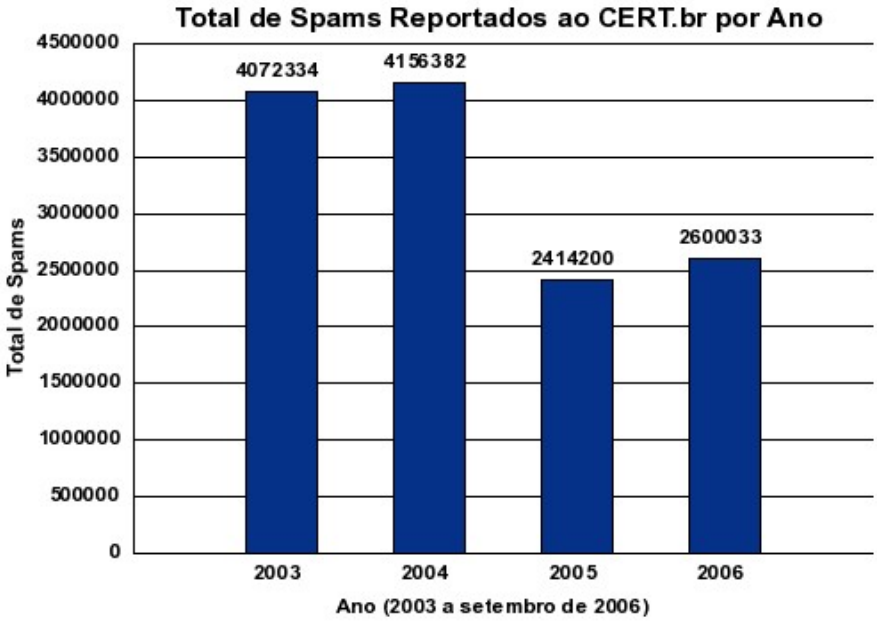

Figura 3: Total de *spam* registrados pelo CERT Brasil

Uma boa prática adotada nesse método de troca de mensagens é o uso da Certificação Digital, pois se evita o não repúdio e garante a integridade das mensagens e seus arquivos anexos.

Outra maneira de se controlar e policiar as trocas de mensagens dentro das empresas é a especificação na sua política de segurança do monitoramento do conteúdo dos *e mail* enviados pelos funcionários para fins de auditoria e/ou investigação.

Caso as organizações adotem o uso de Servidores de Correio Eletrônico próprios, devem fazer atualizações em seus Sistemas Operacionais e do próprio MTA[9], configurando inclusive *relays* para outros MTA, para se evitar proliferação de *spams*.

VÍRUS

[9] *Mail Transfer Agent* – programa responsável pelo gerenciamento do serviço de correio eletrônico, pelo recebimento e entrega de mensagens eletrônicas entre seus usuários e demais Servidores de mesmo serviço.

Um vírus de computador é um programa pequeno desenvolvido para alterar a forma como um computador opera, sem a permissão ou o conhecimento do seu usuário. Um vírus precisa atender a dois critérios. Primeiro, ele deverá executar a si próprio, freqüentemente inserindo alguma versão do seu próprio código no caminho de execução de outro programa. Segundo, ele deve se disseminar. Por exemplo, ele pode se copiar em outros arquivos executáveis ou em discos que o usuário acessa.

Algumas formas mais comuns para se infectar um sistema com vírus são: anexos de mensagens recebidas via e-mail; arquivos infectados armazenados em Servidores FTP; arquivos recebidos via ICQ; disquetes; CDROM e *newsgroups*[10].

Outra praga bastante comum nos dias atuais é a infecção de sistemas por cavalos de tróia, que apesar de não serem considerados vírus, são tão ou mais poderosos e destrutivos, pois, vêm acompanhados de um arquivo aparentemente inofensivo e se instala no computador com objetivos próprios para possibilitar uma futura invasão no sistema.

Segundo a 9ª Pesquisa Nacional de Segurança da Informação, realizada em outubro de 2004, pela Módulo Security (www.modulo.com.br), os vírus são as maiores ameaças à segurança da informação (Figura 3).

Figura 4 - Ameaças à Segurança da Informação

[10] Grupos de notícias onde se compartilham assuntos dos mais variados tipos pela Internet.

INVASORES

Os invasores são pessoas que se utilizam de conhecimentos em ferramentas e técnicas para burlarem esquemas de segurança computacional e causarem certos danos às vítimas, como a retirada de um serviço do ar, desconfiguração de Servidores, roubo de informações reservadas, fraudes financeiras, obtenção de senhas de acesso de administradores e outros.

Representam uma ameaça externa através de ataques oriundos de fora do ambiente da organização com o objetivo de explorar vulnerabilidades do sistema computacional para um determinado fim. Com a prática do comércio eletrônico, estes números vêm aumentando a cada dia, assim como as formas de ataques.

Outro ponto a ser destacado são os motivos, de cunho maldosos, pelos quais invasores praticam seus atos, que podem originar-se por interesses em ganhos financeiros, vingança, anarquia, idealismo, espionagem industrial ou mesmo pela sua auto-afirmação perante a comunidade dos *hackers/crackes*.

3.2 Controle de Acesso Físico

A preocupação com a segurança física dos sistemas de informação originou-se na década de 70 do século passado, motivado por atos de vandalismo praticados na Alemanha por estudantes que apontavam o processo de informatização das empresas como principal motivo de desemprego. Desde então, a preocupação pela segurança da informação no mundo tem se tornado cada vez mais crescente. No Brasil, essa necessidade se consolidou nos anos 90, com a publicação das normas de segurança da informação editadas pela Associação Brasileira de Normas Técnicas (REVISTA BRASILIANO, 2004).

A segurança física do acesso às informações pode ser abordada de duas formas: segurança de acesso, que trata das medidas de proteção contra acesso físico não autorizado, e segurança ambiental, que trata da prevenção de danos por causas naturais.

O controle de acesso físico tem como objetivo proteger equipamentos e informações contra usuários não autorizados, prevenindo o acesso a esses recursos. Apenas pessoal autorizado, previamente definido na política de segurança da organização, pode ter acesso físico aos sistemas computacionais. “Um dos pontos fundamentais da segurança física é o

controle de acesso. Ele está baseado no fato de que nem todas as pessoas devem ou precisam ter acesso a todas as áreas da organização" (LOSS CONTROL, 2001).

São componentes da segurança física:

- Instalação física de equipamentos;
- Uso de equipamentos;
- Customização de *Firewall*;
- *Backup*[11] de dados, aplicações, banco de dados, etc;
- Plano de contingência e de Recuperação por desastres;
- Projeto estrutural/arquitetural e manutenção do ambiente computacional.

Tratando-se de segurança no controle de acesso físico, existem duas áreas a serem consideradas: a primeira refere-se aos equipamentos que restringem o acesso indiscriminado internamente na organização, deste modo garantindo proteção aos terminais de computadores, unidades central de processamento, servidores, unidades de conversão de dados, fitas, discos, etc. A segunda refere-se a equipamentos que restringem o acesso a pessoas externas à organização, ou a quem tem interesse em acessar informações da organização e que não podem em virtude da falta de permissão física.

Algumas medidas que podem ser adotadas na implementação de segurança física do ambiente são (www.modulo.com.br):

- Construção de muros e grades no entorno da instalação para estabelecer um limite para inibir a presença de curiosos. As grades devem ter alarmes ou estarem sob vigilância de guardas, cachorros ou monitores de TV;
- Utilização de Guardas na entrada de instalações estratégicas para controlar o acesso e inspecionar pacotes e outros itens de mão, permitindo a entrada somente de pessoal autorizado. Para aumentar a sua eficiência, deve-se investir em recursos tecnológicos como instalação de alarmes, monitoramento de câmeras e outros dispositivos à sua disposição;

[11] *Backup:* rotina de salvar dados para um ou outro local/mídia, com o objetivo de recuperação em caso de danos aos dados no local original.

- Obrigar a utilização de Crachás por funcionários e visitantes para obterem acesso. Devem possuir poucas informações como assinaturas e detalhamento por escrito sobre privilégios de acesso, isso deve ser feito por uso de código ou cores, que são de fácil identificação pelo pessoal de segurança e dos próprios funcionários da organização. A instalação de leitores programados para permitir entrada é outro recurso que pode identificar facilmente intrusos;
- Uso de sistemas com portas duplas em áreas restritas para forçar as pessoas não autorizadas a se identificarem junto a um guarda posicionado na segunda porta;
- Instalação de travas e chaves do tipo *cipher lock*, ou seja, uso de combinação de travas com botões que abrem a porta após a digitação de uma seqüência;
- Controle de acesso biométrico para identificação de pessoas pela impressão digital, leitura da palma da mão, padrões de voz, escaneamento de retina, entre outras;

Os diversos ambientes da organização devem ser classificados segundo o seu grau de acesso físico pelos usuários internos e externos, levando-se em consideração a criticidade dos equipamentos e processos neles contidos. Com isso, restringe-se tacitamente o fluxo de pessoal nas áreas mais críticas, facilitando o seu controle.

Uma das áreas críticas em qualquer organização, onde são processados ou armazenados grandes volumes de informações, são os Centros de Processamentos de Dados (CPD) que devem ser localizados, de acordo com Caruso:

> *"O mais recomendável é a construção de um edifício exclusivo, localizado no centro de uma área exclusiva, acima do nível do solo, com as instalações sensíveis no centro do edifício e as áreas de apoio na periferia, seguindo o conceito das camadas concêntricas de segurança* (CARUSO & STEFFEN, 1999, p.210)."

A autorização de acesso aos ambientes de informações deve ser franqueada às pessoas somente em virtude de necessidade funcional e que seja de sua responsabilidade no trato com a manipulação da informação. Para tanto, áreas críticas como a sala dos Servidores e ativos de rede, devem ser classificados como de alto risco, com acesso restrito, e deve contar com um sistema de controle de acesso eletrônico, de preferência com mais de um nível de segurança, como por exemplo, uso de crachá de identificação, senha de acesso e identificações biométricas, como digitais e íris.

O ponto-chave é que as técnicas de proteção de dados por meio do controle de acesso lógico, por mais sofisticadas que sejam, tornam-se inócuas se a segurança física de acesso ao ambiente não for garantida.

Especial atenção deve ser dispensada aos serviços de terceiros contratados pela organização, como limpeza, bufês, pessoal técnico temporário, estagiários e outras contratações de curta duração, onde se deve prevenir contra a ação da engenharia social através de treinamento do quadro permanente de funcionários nos métodos, procedimentos e segurança da informação para assegurar sua conscientização nas questões e responsabilidades pela segurança da informação.

Com o uso de rede em fio (*wireless*), o controle de acesso físico de dispositivos que acessam a rede é inexistente. Neste caso, a implementação da segurança restringe-se ao enlace de dados, investindo-se fortemente no controle de acesso lógico através de mecanismos de autenticação de dispositivos e criptografia no tráfego dos dados. Cabe também, um judicioso estudo para definir os requisitos técnicos necessários para escolha e instalação dos *Access Point*[12] e antenas das estações de trabalho, como potência, localização física e configuração de recursos criptográficos.

O *backup* dos dados vitais da organização deve ser realizado e armazenado, segundo uma política de *bakcup*, em dispositivos isolados da rede e em outras instalações físicas e que devem estar previstos no Plano de Contingência da instituição, como medida de proteção e recuperação das informações em caso de incidente de segurança.

Ainda quanto ao *backup*, não basta simplesmente fazer a cópia dos dados, é necessário, periodicamente, testar se os dados provenientes do backup e as configurações dos Servidores são realmente recuperados como se esperado, tudo visando a continuidade do negócio em caso de contingência.

Cabe à gerência de redes identificar os terminais indisponíveis, salas ou escritórios vazios, e desconectá-los fisicamente do quadro de distribuição de cabos, monitorando toda tentativa de conexão não autorizada.

Ainda como procedimentos a serem adotados para a segurança física deve-se estabelecer mecanismos para avaliação do perímetro e áreas externa ao prédio, no aspecto vigilância velada, com uso de dispositivos de monitoração, de preferência, por câmeras com assistência de pessoal da segurança para avaliação de possíveis ameaças.

[12] Dispositivo de rede sem fio responsável pela retransmissão do sinal entre as estações de trabalho da rede.

Todo tratamento de incidente de segurança deve ser analisado por pessoal habilitado, na sala central de segurança, para a ação imediata pertinente.

Adoção de medidas para destruição de dados confidenciais devem ser implantadas, pois são de baixo custo e protegem contra ação de engenharia social, particularmente no trato com o lixo da organização.

Nas áreas de acesso restrito, particularmente na sala dos Servidores e Centro de Processamento de Dados, é recomendável a instalação de circuito fechado de TV para prover a vigilância no seu interior, nas portas de acesso e nas áreas externas, associado a um sistema de alarme sonoro e/ou por envio de mensagens aos administradores, que devem ser acionados por sensores de movimento. As imagens devem ser armazenadas para facilitar uma possível auditoria em caso de incidente de segurança.

Deve-se atentar para se evitar rotinas de trabalho, ligados à segurança, pois podem significar riscos na medida em que procedimentos repetitivos e mecânicos tornam-se monótonos e, muitas vezes, induzindo seus executores a relevar as medidas de segurança requeridas. Uma boa prática é a adoção de sistemas de rodízio de funções, cursos de reciclagem e pequenas alterações de procedimentos.

Caso seja necessária a contratação de serviços de terceiros em áreas de acesso restrito, deve-se fazer um registro dos funcionários autorizados e uma inspeção, com cautela, de seus materiais de trabalho, além de manter permanente acompanhamento de suas atividades por pessoal da organização responsável pelo setor.

Podem ser definidos três ambientes no que se refere à segurança física de um sistema computacional (HUNTER, 2001):

- Ambiente Global de Segurança: área sobre a qual a organização mantém alguma forma de controle ou influência, tal como estacionamentos ou áreas vizinhas à instalação computacional;
- Ambiente Local de Segurança: salas adjacentes ao local da instalação computacional. O controle de pessoas que entram ou saem deste ambiente deve ser feito de acordo com as medidas necessárias pré-estabelecidas. Dentro deste ambiente local, pode haver diferentes regiões com controles de acesso distintos; e
- Ambiente Eletrônico de Segurança: sala onde se localiza efetivamente a instalação computacional e todos seus equipamentos periféricos. Os recursos a serem protegidos e que se encontram no ambiente eletrônico de segurança são servidores, impressoras, terminais, roteadores, scanners, etc.

Como exigência de medidas de controle de acesso físico a ambientes é aconselhável a utilização de identificação biométrica por ser menos vulnerável, pois ao contrário de senhas e cartões, não podem ser esquecidos ou emprestados, uma vez que são partes inerentes às pessoas. Por este motivo, tais mecanismos vêm sendo muito empregados nas empresas.

Especial atenção deve ser dispensada ao local de guarda dos meios de armazenamento das informações, pois estão sujeitos a uma série de riscos que podem afetar a sua integridade, tais como: exposição a campos magnéticos; a calor; à umidade; a impactos mecânicos e à poeira. Não obstante, o transporte, a deterioração natural e falta de testes periódicos das mídias gravadas, figuram como pontos chaves para definição de procedimentos seguros para evitar a perda de informações.

3.3 Controle de Acesso Lógico

A segurança de acesso lógico diz respeito à proteção geral fornecida pelos recursos tecnológicos no ambiente computacional, impedindo acessos não autorizados de dados sensíveis por outros usuários do sistema, a exceção de seus proprietários. Normalmente a informação fica restrita à base de "precisa saber". Apenas indivíduos que têm necessidades operacionais de tais informações terão acesso lógico a elas.

Pode-se entender como segurança lógica os procedimentos adotados visando a proteção das informações para impedir a alteração, divulgação ou destruição, intencional ou não, por pessoas não autorizadas.

Cabe à política de segurança lógica estabelecer os controles de acesso a informação objetivando a integridade, autenticidade e manutenção da confidencialidade da informação protegida, definindo permissões de acesso àqueles previamente autorizados e negando aos que não gozem dos mesmos direitos.

A adoção de controles nesse ínterim visam garantir que apenas usuários autorizados tenham acessos aos recursos, e que se restrinjam aos estritamente necessários para o desempenho de suas funções, ou seja, impedir a execução de transações incompatíveis com o cargo que ocupam. Visam, ainda, garantir que o acesso a recursos críticos seja bem monitorado e restrito a poucas pessoas.

Na implementação da segurança lógica, deve-se levar em consideração qual a política de utilização de serviços de rede, cabendo ao administrador definir quais os serviços serão

disponibilizados, quem e de onde podem ser acessados. Cabe, ainda, estabelecer segurança aos serviços disponibilizados na rede, como uso de protocolos seguros, validação de usuários dos serviços e uso de criptografia na transmissão de dados.

3.3.1 - CUSTOMIZAÇÃO DE SOFTWARE

Deve ser estimulada entre os usuários a utilização de programas que não necessitem o estabelecimento de privilégios para o seu funcionamento.

O desenvolvimento e uso de rotinas de sistemas para a definição de perfil padrão, para uso de aplicações, deve ser implantadas de forma a evitar a necessidade de fornecimento de privilégios específicos aos usuários.

Após a instalação de novos serviços, deve ser alterada ou mesmo excluída as contas padrões desses serviços que vêm como *default*, pois previne contra a tentativa de acessos indevidos. É comum administradores de sistemas instalarem programas e não executarem esses procedimentos, deixando furos de segurança que poderão ser explorados por *crackers*.

Uma medida importante para permitir uma rápida avaliação da situação de *softwares* instalados é a documentação de suas instalações e configurações. A idéia é ter uma espécie de *logbook* (livro de registro), que detalhe os componentes instalados no sistema e todas as modificações na sua configuração global. O *logbook* deve ser armazenado e manipulado com cuidado, de acordo com a política para documentos sensíveis da organização.

Na instalação de softwares, principalmente aqueles que implementam serviços de rede, dever ter uma instalação mínima de pacotes e componentes que atenda estritamente ao funcionamento do serviço a ser disponibilizado, evitando-se assim a habilitação de outros serviços não desejáveis. É comum que serviços não utilizados não sejam monitorados por falhas de segurança, o que aumenta a possibilidade de não ser aplicada uma correção necessária. A redução no número de pacotes instalados diminui a chance de que o sistema possua uma vulnerabilidade que possa vir a ser explorada por um atacante.

Sempre que um serviço não estiver sendo utilizado pela organização, deve ser desabilitado. Caso não seja possível desativar serviços individualmente, uma alternativa é usar um filtro de pacotes para bloquear as portas TCP/UDP usadas por esses serviços, impedindo que eles sejam acessados através da rede.

3.3.2 – SENHAS

A Segurança no controle de acesso é obtida pelo uso de senhas, definições de perfis individuais para cada usuário autorizado a utilizar-se dos sistemas, bem como para cada usuário de domínio, atribuição de certos privilégios e restrições e direitos ou limitações de uso de determinados arquivos de dados, programas, sistemas, banco de dados, dentre outros.

Primeiramente, os mecanismos de segurança utilizavam-se unicamente das senhas como medida de controle de acesso, porém, nos dias atuais, elas se revelaram como um mecanismo muito frágil e são utilizadas apenas como recurso para autenticar a identidade dos usuários que desejem acessar determinado ambiente protegido.

O uso de senha é uma medida de proteção contra a busca casual de informações, e dificilmente irá conter um ataque criminoso. A senha de computador age como uma chave, se for permitido a várias pessoas usarem a mesma senha de acesso é como se todos usassem a mesma chave.

O gerenciamento de senhas deve seguir alguns princípios como:

- Serem individuais e confidenciais, evitando-se o compartilhamento com outras pessoas. A regra de ouro é: "uma pessoa – uma senha". Para usuários temporários que necessitem usar o sistema, basta adicioná-los à lista de usuários autorizados e após o término de seus trabalhos, devem ser excluídos os UID do sistema.
- Serem compostas por caracteres alfanuméricos e de tamanho mínimo de seis caracteres.
- Serem mudadas regularmente, pelo menos a cada trinta dias. Pode-se alertar os usuários que tiverem a validade de suas senhas expiradas. Para certificar-se de que houve a alteração de senhas expiradas, pode-se simplesmente bloquear o acesso ou conceder permissões mínimas para uso do sistema.
- Promover a alteração de senhas sempre que existir qualquer indicação de possível comprometimento do sistema ou da própria senha, principalmente se tiver sido vítima de uma invasão.
- Não incluir senhas em nenhum processo automático de acesso ao sistema, como armazenamento em macros ou funções-chave.
- Manter um histórico de senhas para se evitar o uso de senhas repetidas por um certo período de tempo.
- Manter uma lista negra de senhas que são freqüentemente utilizadas ou por serem

muito obvias de se adivinhar. Essa lista poderá ser usada da mesma forma que o histórico de senhas. Apenas o administrador do gerenciador poderá alterar o seu conteúdo.

- Ficar atento para o uso de senhas de manutenção remota para acesso à equipamentos que vêm de fábricas com senhas padrão, devendo ser alteradas pelos administradores de rede para evitar acessos indevidos.
- A gestão do sistema de *help desk* que trata de senhas perdidas ou esquecidas necessita de cuidado especial, pois este caminho pode ser também um dos meios de ataque ao sistema de senha.

3.3.3 - IDENTIFICAÇÃO DE USUÁRIOS E GERENCIAMENTO DE CONTAS

Deve ser estabelecido, na política de segurança lógica, um procedimento formal para o registro e cancelamento de usuário e contas além de garantir e revogar acesso em todos os sistemas de informação e serviços. Tal procedimento deve ser executado, particularmente, nos processos de admissão ou demissão de funcionários, ou em caso de promoção para outros cargos que exijam permissão de acesso diferenciados do cargo que exerciam anteriormente.

Convém a utilização de um identificador único de usuário (UID) para assegurar a responsabilidade de cada usuário por suas ações em caso de auditorias de acesso ao sistema. O uso de ID de grupos de usuários somente seja permitido em caso de necessidade para o negócio ou por razões operacionais, devendo ser aprovado e documentado na organização.

Para estabelecer um comprometimento formal do usuário quanto ao uso do sistema, é recomendável entregar um documento, por escrito, apresentando seus direitos de acesso e obter dele a assinatura em declaração indicando que entende as condições de acesso.

Deve ser considerada a inclusão de cláusulas nos contratos de usuários e de serviços, principalmente de terceiros, que especifiquem as sanções em caso de tentativa de acesso não autorizado pelos usuários ou por terceiros, para coibir qualquer tentativa de acesso não autorizado. O suporte a este requisito deve ser apoiado com o monitoramento freqüente dos *log* do sistema, confrontados com os perfis de acesso de cada usuário.

Adotar procedimento para desativação de contas para usuários que estejam afastados do serviço por um período considerável, como viagens a serviço, férias e outros.

3.3.4 - AUTENTICAÇÃO E AUTORIZAÇÃO DE ACESSO

Através do mecanismo de *logon*, o indivíduo passa por um processo de autenticação e autorização para certificar-se de que seja um usuário legítimo face ao conhecimento da senha ou por possuir características que foram previamente cadastradas.

Para o controle de acesso a ambientes protegidos, nos sistemas atuais, utilizam-se de mecanismos de listas de acesso, que descrevem os usuários que possuem permissão de acesso e o nível permitido, ou seja, os perfis dos usuários estão nelas definidos para utilização de todos os recursos do sistema de informação.

Em seguida, após obter o acesso ao ambiente, o sistema aloca para cada usuário acesso para certos recursos previamente estabelecidos, compatíveis com o nível de acesso como: aplicações que precisa se utilizar, arquivos de dados, programas, banco de dados, acesso remoto ou não, incluindo a propagação de acesso se necessário. Na essência, todos os recursos necessários para concluir sua transação. É importante saber que, em alguns casos, usuários têm acesso de somente leitura, não permitindo escrever ou modificar os bancos de dados.

Para o controle de acesso ao Sistema Operacional, é importante a identificação automática de terminal para se saber de onde o usuário acessa o sistema. Limitar o número de tentativas erradas para acesso sem fornecer ajuda ao usuário no processo de autenticação, definir um ID único para cada usuário que utiliza o sistema e ainda o uso de tecnologias mais avançadas de identificação como o *Smartcard* e autenticação biométrica.

Para que o usuário possa auxiliar no controle de acesso com o uso de sua conta, pode-se apresentar, após o *logon* ter sido efetivado com sucesso, data e hora do último acesso e detalhes sobre tentativas frustradas. Dessa forma, o usuário poderá identificar tentativas de uso não autorizado de sua conta e reportar o ocorrido à gerência de segurança para uma auditoria.

O fornecimento de privilégios a usuários para acesso a qualquer recurso do sistema só deve ser executado após a conclusão formal de todo o processo de autorização, devendo ser coibida a prática de liberar acesso enquanto tramita o pedido de autorização. Essa autorização deve ser devidamente registrada pelo pessoal de segurança para possíveis auditorias e monitoração.

Para sistemas de rede sem fio (*wireless*), o padrão IEEE 802.11 define duas formas de autenticação, que em ambos casos, o processo de autenticação se dá sempre entre duas estações e nunca *multicast*:

Open System – qualquer estação será aceita na rede, bastando requisitar uma autorização. Sistema de autenticação nulo. Ela foi desenvolvida visando redes que não necessitam de segurança para autenticação de dispositivos. Por esta razão, nenhuma informação sigilosa deve trafegar por nessas redes e é aconselhável que sejam separadas da rede interna por um *firewall*, à semelhança de uma zona desmilitarizada – DMZ.

Shared Key – neste processo, as duas estações compartilham uma chave secreta. A forma de obtenção dessa chave é implementada de variadas formas pelos fabricantes dos equipamentos. A troca de informações entre as estações, após a autenticação, se dá utilizando o protocolo WEP[13] que usa um sistema criptográfico baseado no RC4.

3.3.5 - CRIPTOGRAFIA DE DADOS

Devem ser adotados procedimentos para uso de sistemas criptográficos para a transmissão e armazenamento de informações críticas com uso de criptografia forte.

O uso do protocolo HTTPS para navegação de páginas *web* pode ser adotado como forma de prover segurança no tráfego de obtenção de informações ou acesso ao correio eletrônico via webmail ou IMAP.

A implantação de sistemas criptográficos na troca de mensagens eletrônicas como o *Pretty Good Privacy* (PGP) pode ser uma boa estratégia para a manutenção da segurança na troca de mensagens corporativas.

Os sistemas gerenciais devem possuir processos de criptografia de dados para a geração de informações criptografadas em arquivos antes de serem remetidos a seus destinatários.

Promover o uso de certificação digital para as áreas críticas da organização e, de preferência, seguindo as normas da ICP-Brasil para que a produção de documentos seja aceita legalmente fora da instituição e agregue valores de segurança como a integridade, confidencialidade, não-repúdio e a autenticidade.

Uma medida de segurança muito importante na operação de redes é a substituição de protocolos onde não haja autenticação através de senhas, ou onde senhas trafeguem em claro (Telnet, FTP, POP3, IMAP, rlogin, rsh, rexec), por outros que corrijam estas deficiências. A maioria dos protocolos citados pode ser substituída pelo SSH. Essa substituição, além de fazer

[13] Wired Equivalent Privacy – foi introduzido na tentativa de dar segurança na autenticação, proteção e confiabilidade na comunicação entre os dispositivos *wireless*. Porém é inseguro devido a sua arquitetura. Em 2001 a equipe do RSA sugeriu que para contornar as fraquezas do WEP fosse usada uma função de *hash* mais leve, que usasse uma chave temporária para criar chaves diferentes para cada pacote.

com que o tráfego entre cliente e servidor passe a ser criptografado, traz ainda outras vantagens, como proteção da sessão contra ataques do tipo *man-in-the-middle* e seqüestro de conexões TCP.

3.3.6 - TRANSFERÊNCIA DE DADOS

Quanto ao tráfego de informações e a política de gerenciamento lógico, deve-se definir quais as rotas de rede obrigatórias para canalizar o fluxo e obter maior controle e monitoração, exigir autenticação para conexão externa de usuários, autenticação de nós de rede, proteção de portas diagnóstico, implementação de segregação de redes, controle de conexões de rede e controle de roteamento.

Uma boa prática para estabelecer um controle de fluxo através de filtragem de pacotes por protocolos é a configuração da Lista de Controle de Acesso (ACL) nos roteadores e *firewall*, pois através delas pode-se permitir ou negar acesso a determinadas redes ou recursos disponíveis em outras redes.

3.3.7 - REGISTRO DE *LOG*

Logs são muito importantes para a administração segura de sistemas, pois registram informações sobre o seu funcionamento e sobre eventos por eles detectados. Muitas vezes, os *logs* são os únicos recursos que um administrador possui para descobrir as causas de um problema, comportamento anômalo ou tentativa de invasão.

Deve-se criar uma política de registro de *log* com estabelecimento de requisitos mínimos de informações a serem gravados nos *log* do sistema para os diversos serviços disponíveis na rede, como autenticação de usuários, uso de correio eletrônico, transferência de arquivos, acesso a aplicativos e bancos de dados, dentre outros.

Para que os *logs* de um sistema sejam úteis para o administrador de redes, eles devem estar com o horário sincronizado via NTP[14], ser tão detalhados quanto possível, sem no entanto gerar dados em excesso para não comprometer a sua interpretação ou mesmo exceder rapidamente a capacidade de armazenamento em disco.

Realizar periodicamente o *backup off-line* dos arquivos de *log* armazenando-os em local seguro para possíveis auditorias no sistema. Sem esse procedimento, os *logs* do sistema ficam vulneráveis a alterações em caso de invasão.

[14] *Network Time Protocol* – protocolo utilizado por serviço de sincronização de relógios de computadores.

A gravação de *logs on-line* deve ser realizada em uma partição de disco específica para esse fim, isso evita que em caso de ataque de negação de serviço, com geração de *logs* excessivos, venha a travar o sistema.

Os *logs* não podem ser mantidos *on-line* por tempo indeterminado, pois acabam por consumir muito espaço em disco. A melhor estratégia para resolver esta questão é transferir periodicamente os *logs* do disco para dispositivos de armazenamento *off-line*, tais como fita, CD-R ou DVD-R.

É recomendável gerar um *checksum* criptográfico (tal como MD5 ou SHA-1) dos *logs* que são armazenados *off-line*. Esse *checksum* deve ser mantido separado dos *logs*, para que possa ser usado para verificar a integridade destes, caso eles venham a ser necessários.

Uma boa estratégia a ser adotada é a utilização um *loghost* centralizado que é um sistema dedicado à coleta e ao armazenamento de *logs* de outros sistemas em uma rede, servindo como um repositório redundante de *logs*. Via de regra, o *loghost* não disponibiliza nenhum outro serviço, nem mesmo acesso remoto para os administradores, para minimizar a possibilidade de que ele seja comprometido. Outra vantagem de *loghosts* centralizados é que eles facilitam a análise dos *logs* e correlação de eventos ocorridos em sistemas distintos.

Outro ponto que merece atenção é a rotação automática de *logs*. Quando este recurso for utilizado, deve-se garantir que os *logs* sejam movidos para o armazenamento *off-line* antes que eles sejam removidos do sistema pela rotação, evitando assim a perda de registros.

3.3.8 – MONITORAÇÃO

Para eficácia da monitoração do sistema, é recomendada utilização de software de segurança ou analisadores de *logs*, os quais podem ser customizados para políticas de seguranças de diferentes organizações. A complexidade dos parâmetros de customização, neles existentes, deve ser configurada com base no conhecimento do administrador de rede e sua experiência em programas de segurança. Isso é importante, particularmente, para conter o acesso de invasores à organização.

Como forma de medida pró-ativa, para otimizar a segurança do sistema, deve ser adotada a geração periódica de relatórios de violação de segurança dos diversos serviços disponíveis, e que depois de analisados pelo pessoal de segurança da informação, devem propor a adoção de medidas corretivas em possíveis falhas de segurança.

Algumas práticas recomendáveis no que diz respeito ao monitoramento de *logs*:

- incorporar o hábito de inspecionar os *logs* como rotina de trabalho. Isso deve ser feito, pelo menos, uma vez por dia. Para sistemas muito importantes ou que gerem muita informação podem precisar ter seus *logs* analisados com maior freqüência;
- investigar as causas de qualquer registro que pareça incorreto ou anômalo, por mais insignificante que ele aparente ser;
- procurar identificar o padrão de comportamento normal dos sistemas, para poder encontrar eventuais anomalias com maior rapidez.

3.4 Sistemas Biométricos

Os sistemas biométricos deixaram de ser um produto de ficção científica, apresentados em muitos filmes, para tornar-se um verdadeiro aliado na prevenção de fraudes contra sistemas informatizados, principalmente na implantação de mecanismos de controle de acesso, físico e lógico, em ambientes computacionais e suas aplicações.

Não é objeto deste estudo aprofundar sobre as técnicas utilizadas nos diversos tipos de controles biométricos quanto à arquitetura, padrões de software, mecanismos de armazenamento/coleta de dados e estruturas de algoritmos utilizados, mas apontar as características mais importantes que devem ser observadas para adoção dessa tecnologia no controle de acesso aos sistemas de informações.

Segundo Kim (1995, p. 205):

> A definição mais geral de autenticação dentro de sistemas de computação engloba a verificação da identidade, autenticação da origem e conteúdo da mensagem. O conceito de verificação de identidade, especificamente, aplica-se a usuários humanos, sistemas de computação e processos executando nesses sistemas. A autenticação pelo conhecimento de uma informação secreta ou a pela posse de um dispositivo físico de autenticação único são igualmente válidos para todos os tipos de entidades descritos acima. Por outro lado, autenticação biométrica apenas tem sentido no contexto de seres humanos.

Estudos sobre a verificação de identidade baseado em características físicas e comportamentais do usuário vêm crescendo, principalmente nos últimos anos, com o objetivo de proporcionar mais segurança no processo de autenticação e suprir as deficiências dos métodos convencionais de uso de senhas, cartões e *tokens*, como o extravio, esquecimento, roubo e mesmo empréstimo a terceiros.

Os sistemas biométricos automáticos surgiram do processo manual de reconhecimento amplamente difundido como a análise grafológica de assinaturas e escritas, análise de

impressões digitais, reconhecimento de voz e, atualmente, análise de vasos sangüíneos da retina, que se utilizam de métodos e técnicas específicas para cada caso, inclusive com uso de tecnologia.

Seu princípio básico é de tomar como padrão alguma característica física e/ou comportamental e, de forma automatizada, fazer o reconhecimento do indivíduo com uma taxa de erro próxima a zero. Teoricamente qualquer característica pode ser utilizada, porém existem algumas limitações, pois a tecnologia deve ser capaz de medir, com precisão, determinada característica e identificá-la como única, inclusive em caso de gêmeos, além de não comprometer os direitos individuais e de não submetê-lo ao constrangimento.

De acordo com Jain (1997, p. 1388):

> Teoricamente, qualquer característica humana, física ou comportamental, pode ser usada para a identificação de pessoas, desde que satisfaça os seguintes requerimentos:
> **Universalidade**: significa que todas as pessoas devem possuir a característica;
> **Singularidade**: indica que esta característica não pode ser igual em pessoas diferentes;
> **Permanência**: significa que a característica não deve variar com o tempo;
> **Mensurabilidade**: indica que a característica pode ser medida quantitativamente.
> Na prática, existem outros requerimentos importantes:
> **Desempenho**: refere-se à precisão de identificação, os recursos requeridos para conseguir uma precisão de identificação aceitável e ao trabalho ou fatores ambientes que afetam a precisão da identificação;
> **Aceitabilidade**: indica o quanto as pessoas estão dispostas a aceitar os sistemas biométricos;
> **Proteção**: refere-se à facilidade/dificuldade de enganar o sistema com técnicas fraudulentas.

As técnicas[15] de reconhecimento por meio da biometria podem ser adotadas de duas formas:

- **Um-para-um** – o usuário apresenta como sendo uma determinada pessoa e o sistema confere a veracidade da informação com base na medida biométrica que foi registrada no banco de dados, por ocasião do cadastro (identificação) do usuário

[15] Sérgio Ricardo Teixeira. Gerente de Projetos de Segurança da SCUA Security, Jan/Fev 2002. Disponível em: http://www.scua.com.br/site/seguranca/artigos/biometria.htm. Acessado em 30 de outubro de 2006 às 07:46 hs.

- **Um-para-muitos** – a identificação de uma pessoa ocorre quando se tem o dado biométrico dela e se faz uma busca no banco de dados, comparando as informações até que se encontre (ou não) um registro idêntico ao que é procurado, com certa margem de erro inclusa.

Um dos problemas enfrentados por sistemas biométricos é sua alta taxa de erro, em função das mudanças das características dos indivíduos com o passar dos anos, devido a problemas de saúde e mudanças das características individuais, face à velhice, ou mesmo emocionais como o *stress*, medo, nervosismo, irritação, dentre outros. Uma forma de se minorar tais problemas é o uso de redes neurais (Anexo C).

A utilização da biometria tem basicamente dois propósitos: identificar e autenticar usuários. A identificação é o processo mais complexo e consiste em capturar, do usuário, as características biométricas de interesse do sistema, convertê-las em um modelo que as represente matematicamente e, finalmente, armazená-las em uma base de dados para futura autenticação e administração de usuário. A autenticação, resume-se na confrontação dessas informações armazenadas com os dados biométricos coletados do usuário, *on line*.

Uma aplicação imediata desse sistema é, sem dúvida, fazer o controle de acesso, tanto físico como lógico, aos sistemas computacionais de tecnologia da informação, e que, conjugado com outros sistemas, como o uso de senhas ou cartões, pode conferir alta segurança no controle de acesso.

Atualmente existem vários sistemas biométricos já em uso pelas organizações, cada um com características próprias, tanto no grau de segurança como no custo de implementação. A decisão de qual sistema implantar deve ser buscada através de requisitos básicos que a organização venha a definir, aliada às suas peculiaridades.

Para aumentar a eficiência contra fraudes e proporcionar maior robustez de algoritmos de identificação de pessoas, a tendência atual é a implantação de biometria multimodal que se utiliza de características de diversas modalidades, proporcionando múltiplas evidências do mesmo indivíduo, para serem submetidas, simultaneamente, ao processo de autenticação.

A seguir, serão apresentados os principais sistemas biométricos, seus princípios básicos de funcionamento, vantagens e desvantagem.

3.4 1 - IMPRESSÕES DIGITAIS

São características únicas e consistentes. Nos sistemas biométricos que utilizam essa opção, são armazenados de 40 a 60 pontos para verificar uma identidade. O sistema compara a impressão lida com sua base de dados de impressões digitais de pessoas autorizadas.

A impressão digital é composta por vários sulcos, que em sua formação apresentam diferenças chamadas de pontos de minúcias, ou seja, aquelas partes em que os sulcos se dividem (vales) ou onde terminam abruptamente (terminação). Cada um desses pontos tem características únicas, que podem ser medidas.

Ao compararmos duas digitais podemos determinar seguramente se pertencem a pessoas distintas, baseados nos pontos de minúcias. Há muitos anos os institutos oficiais de identificação de diversos países já realizam o reconhecimento de pessoas através do sistema de análise da impressão digital. Na Europa, judicialmente, são necessárias 12 minúcias para saber quem é uma pessoa. Os leitores biométricos são capazes de identificar mais de 40 minúcias de uma impressão digital.

3.4.2 - VOZ

Existem dois tipos de reconhecimento de voz: dependente-de-texto e independente-de-texto. No primeiro, o sistema é treinado para reconhecer um determinado texto, enquanto no segundo o sistema deve reconhecer qualquer texto. Sistemas dependente-de-texto geralmente tem melhor desempenho.

Os sistemas de reconhecimento de voz são usados para controle de acesso, porém não são tão confiáveis, em função da voz, como instrumento de medida, possuir uma componente comportamental que mudam com o decorrer do tempo devido à idade, condições de saúde, estado emocional, dentre outros. Além disso, podem ocorrer erros causados por ruídos no ambiente onde são operados.

3.4.3 - GEOMETRIA DA MÃO

Neste método, a leitura é feita por um digitalizador que possui guias, semelhantes a pinos, que se encaixam entre os dedos para facilitar o reconhecimento do desenho da mão. O

sistema calcula e registra as proporções entre os dedos e articulações, que são decisivas para identificar a pessoa.

O digitalizador captura uma imagem tridimensional dos dedos, que é convertida num modelo geométrico. No caso da palma da mão, o foco é direcionado ao desenho das linhas, saliências e outros detalhes, que o torna muito parecido com os sistemas de reconhecimento de impressões digitais.

Como a área da palma da mão é muito maior que a ponta do dedo, espera-se que sistemas biométricos baseados na palma da mão sejam mais discriminantes que aqueles baseados somente em digitais. Entretanto, são computacionalmente mais caros.

Também é usada em sistemas de controle de acesso, porém essa característica pode ser alterada por aumento ou diminuição do peso ou artrite.

Os dispositivos biométricos da mão são rápidos e de fácil operação. Ideal para ambiente onde o acesso a áreas restritas necessita ser rápido e seguro, como no controle de acesso de funcionários de uma empresa.

3.4.4 – CONFIGURAÇÃO DA RETINA

Os sistemas que utilizam essas características se propõem a efetuar identificação mais confiável do que as impressões digitais. Entretanto são sistemas invasivos, pois direcionam feixes de luz aos olhos das pessoas.

A biometria da retina é baseada na análise da camada dos vasos sanguíneos no fundo dos olhos. Para isto utiliza uma luz de baixa intensidade, que faz uma varredura para encontrar os padrões singulares da retina. É uma técnica de muita precisão e praticamente impossível de ser adulterada devido a forte relação com os sinais vitais humanos. Não é comumente bem aceita por seus usuários porque requer que este olhe em um visor e focalize um determinado ponto, trazendo alguma dificuldade se o usuário estiver de óculos.

3.4.5 – CONFIGURAÇÃO DA ÍRIS

Este método também se propõe a efetuar identificação mais confiável do que as impressões digitais. A segurança deste método é bastante eficiente, pois o ser humano, a partir de 18 meses de vida, não sofre mais alterações na íris. Entretanto são sistemas invasivos, pois direcionam feixes de luz aos olhos das pessoas.

Baseada nos anéis coloridos do tecido que circunda a pupila, é considerada a menos intrusiva das tecnologias que envolvem o uso dos olhos para identificação, pois não requer um contato muito próximo com o dispositivo de leitura como no caso da retina. Outro fator que agrada aos usuários é que não é necessário retirar os óculos ou lentes de contato para fazer a leitura da íris.

3.4.6 – RECONHECIMENTO FACIAL POR MEIO DE TERMOGRAMA

O termograma facial é uma imagem tirada com uma câmera infravermelha que mostra os padrões térmicos de uma face. Essa imagem é única e, combinada com algoritmos sofisticados de comparação de diferentes níveis de temperatura distribuídos pela face.

Constitui-se de uma técnica não invasiva e altamente confiável, não sendo afetada por alterações de saúde, idade ou temperatura do corpo. Para cada indivíduo, pode ser armazenado mais de 18.000 pontos de identificação, podendo distinguir gêmeos idênticos, mesmo no escuro.

3.4.7 – FACE

A autenticação neste processo é considerada de alta eficiência e se dá por meio do uso de uma câmera digital, que captura as características da face e de sua estrutura óssea, e toma por base alguns pontos específicos do rosto e não pela face em si. Por esse motivo, é possível efetuar o processo de reconhecimento ainda que a aparência do usuário sofra alterações com o passar dos anos. Entretanto, o uso de óculos, pode dificultar o processo de autenticação.

O programa de reconhecimento pode registrar vários pontos delimitadores na face, capazes de definir proporções, distâncias, tamanhos e formas de cada elemento do rosto, como olhos, sobrancelhas, nariz, lábios, queixo, maçãs do rosto, orelhas e outros. Esses pontos, em conjunto, identificam unicamente um usuário e, dependendo do grau de precisão que se deseje, pode-se reconhecer sósias como pessoas distintas.

Esta ramificação biométrica é a única que pode identificar à distância, sem a participação ativa do usuário, ou seja, sem mesmo saber que está sendo identificado. É composto basicamente de duas etapas: localização das faces na cena e o reconhecimento das faces localizadas.

Um fator de grande impacto nesse tipo de sistema é a iluminação, pois em ambientes com pouca luz, geralmente apresentam um desempenho relativamente fraco.

Este sistema é muito útil quando se deseja a identificação de pessoas, de forma discreta, em áreas de intensa circulação ou aglomerações, como em grandes eventos ou mesmo integrados a circuitos internos de TV para confrontação automática e rápida das imagens com fotografias ou retratos falados de suspeitos.

3.4.8 – ASSINATURA

A autenticação de assinaturas pode ser realizada de duas formas diferentes, que são as formas *off line* e *on line*. No primeiro processo, o usuário faz sua assinatura em uma folha de papel que posteriormente é digitalizada e submetida ao sistema que realiza a autenticação. Na autenticação *on line*, a assinatura é feita diretamente sobre um dispositivo de hardware, como uma mesa digitalizadora ou um *tablet*. Além deste dispositivo, pode ser utilizado computadores do tipo *Handheld*, que permitem a escrita diretamente sobre uma tela sensível.

O reconhecimento *on line* de assinaturas permite que sejam utilizadas diversas informações temporais e dinâmicas relativas à assinatura, como a velocidade e pressão da caneta e a trajetória dos traços, que permitem que se obtenham melhores resultados no processo de autenticação.

Os usuários desta tecnologia se identificam bastante com o processo, por já estarem acostumados a utilizar a assinatura como meio de autenticação. Apesar desta tecnologia ser de baixo custo e de boa precisão, surpreendentemente, poucas aplicações no mercado a adotam.

A desvantagem dos sistemas de reconhecimento de assinatura em sistemas biométricos é que eles dependem de uma cooperação adicional do usuário, pois o mesmo deve colocar sua assinatura em um dispositivo, os quais muitas vezes não são muito práticos e confortáveis.

Para uma visualização global dos métodos aqui apresentados, a tabela 1 mostra algumas vantagens e desvantagens dos sistemas biométricos mais utilizados no mercado.

Sistema	Como funciona	Vantagens	Desvantagens
Impressão Digital	Um scanner registra pontos da impressão digital do usuário	Praticidade e custo	Alterações como machucados podem atrapalhar o reconhecimento
Reconhecimento da Face	O programa mapeia características geométricas da face, pontos capazes de definir distâncias, proporções, tamanho e forma	Como registra características geométricas, o sistema aceita mudanças, como corte de cabelo	Não é dos sistemas mais seguros. De acordo com Scalco, é mais comum acontecerem erros de reconhecimento
Íris	Uma câmera registra a imagem da íris que, assim como a impressão digital, é exclusiva de cada ser humano	A íris praticamente não sofre alterações com o passar do tempo e não está tão sujeita a ferimentos quanto a impressão digital	Além de custo, há a questão da barreira cultural - afinal, não é todo mundo que quer ter uma luz entrando no seu olho
Voz	O programa analisa padrões harmônicos da fala	Praticidade	Ruídos e até mesmo o estado emocional podem alterar a voz
Geometria da Mão	É um sistema muito semelhante ao de impressões digitais. Ele registra pontos da mão, como desenho das linhas e distância dos dedos	Praticidade	Alterações como machucados podem atrapalhar o reconhecimento

Tabela 1 – Vantagens e desvantagens do métodos de Biometria.

A relação dos níveis de requerimentos que os sistemas biométricos exigem, segundo a tecnologia empregada, de acordo com Jain, é apresentada na tabela 2:

Biométricos	Universalidade	Singularidade	Permanência	Mensurabilidade	Desempenho	Aceitabilidade	Proteção
Face	Alto	Baixo	Médio	Alto	Baixo	Alto	Baixo
Impressão Digital	Médio	Alto	Alto	Médio	Alto	Médio	Alto
Geometria da Mão	Médio	Médio	Médio	Alto	Médio	Médio	Médio
Veias da Mão	Médio	Médio	Médio	Médio	Médio	Médio	Alto
Íris	Alto	Alto	Alto	Médio	Alto	Baixo	Alto
Retina	Alto	Alto	Médio	Baixo	Alto	Baixo	Alto
Assinatura	Baixo	Baixo	Baixo	Alto	Baixo	Alto	Baixo
Voz	Médio	Baixo	Baixo	Médio	Baixo	Alto	Baixo

Tabela 2 - Comparação de tecnologias biométricas quanto aos requerimentos

4. CONTROLES AMBIENTAIS

Assim como os controles de acesso físicos e lógicos, os controles ambientais também devem constar na política de segurança, pois estão diretamente relacionados com a disponibilidade e integridade dos sistemas computacionais.

Os controles ambientais visam proteger os recursos computacionais contra danos provocados por desastres naturais (incêndios, enchentes), por falha na rede de fornecimento de energia, ou no sistema de ar condicionado, ou seja, fatores que estão intimamente ligados ao ambiente físico e seus recursos para manter o sistema computacional funcionando perfeitamente.

4.1 Incêndios

O combate a incêndios, como medida de proteção e segurança ao sistema de informação, deve ser abrangente e seguir as seguintes fases: detecção, combate e medidas passivas.

A estrutura física do ambiente deve ser projetada visando-se evitar incêndios. Isso é, são adotadas técnicas de construção que evitam a iniciação de incêndios, quer sejam provocados por problemas na rede elétrica ou por descuidos de usuários. Estes são procedimentos preventivos que devem ser agregados nas construções que irão funcionar sistemas computacionais, como o uso de material resistente à ação do fogo, dispositivos de detecção de fumaça ou calor, e a instalação de pára-raios.

Em áreas sensíveis, recomenda-se a instalação de detector de fumaça do tipo iônico, pois possuem tempo de resposta menor, em conjunto com detectores inteligentes ópticos de fumaça, pois podem funcionar por mais tempo em condições de sujeira. É aconselhável também o uso de detectores de câmara de aspiração, pela precisão em diagnosticar um incêndio através da análise do ar com raios *laser* em uma câmara fechada.

Os detectores devem ser instalados na parte superior das instalações, obedecendo às distâncias regulamentadas na norma NBR 9441, editada pela ABNT, referente a sistemas de detecção e alarme de incêndio.

Todos os equipamentos devem ser ligados por laços tipo "Classe A[16]", a uma central de alarmes, onde se podem monitorar os níveis de poluição de cada uma. As sinalizações com sirenes e *strobes*[17] também são muito importantes para indicar a presença do sinistro e direcionar os funcionários às saídas de emergência.

As paredes do ambiente devem ser de alvenaria ou concreto, evitando-se o uso de fórmicas ou outro material comburente, e ser provido de portas corta fogo para isolar o fogo dos ambientes interligados por elas. É requisito técnico que o ambiente garanta, pelo menos, uma hora de resistência ao fogo a uma temperatura de até 1000° C, tempo necessário para acionamento do Corpo de Bombeiros para sanar o incidente.

Outros procedimentos a serem adotados são enchimentos nas paredes com material isolante como fibra de cerâmica, fibra de silício ou lã de rocha, além de utilização de tintas intumescentes[18], que aplicadas em estruturas metálicas agem como uma barreira contra o calor. Aplicação de massas corta-fogo são indicadas para cobertura de cabos elétricos e de dados.

Além dos procedimentos preventivos, deve-se prever procedimentos para se combater incêndio (controles supressivos), caso venham a ocorrer. Isto se dá com a instalação de mangueiras e/ou extintores de incêndio em número suficiente e do tipo adequado para cada categoria de incêndio; instalação de sistemas automáticos de combate ao fogo; treinamento dos funcionários na utilização dos dispositivos de combate a incêndio e vistorias freqüentes dos mesmos para certificar-se de que estão dentro do prazo de validade.

Na instalação de extintores em áreas críticas, preferencialmente, deve-se usar os compostos a base de CO_2 evitando-se os de água ou pó químico, pois podem danificar os equipamentos.

Sistemas de incêndios modernos utilizam-se de gás FM200[19] para extinção automática do fogo pois é eficaz e não tóxico para as pessoas, ao contrário do gás carbônico que é letal e, ao ser liberado, provocam mudanças bruscas da temperatura, podendo ser prejudicial aos

[16] Tipo de ligação em que existe um circuito fechado ligando os detectores à central de alarmes, aumentando a segurança do sistema.
[17] Lâmpada especial tipo *flash* para sistemas de incêndio que a luz emitida transpõe a fumaça.
[18] Impedem que o metal se aproxime dos 540ºC, temperatura que compromete a firmeza de estruturas de edificações.
[19] Gás do tipo inerte, incolor, não deixa resíduos e não nocivo à camada de ozônio nem ao ser humano.

equipamentos. Mesmo assim, ainda é encontrado em muitas organizações que possuem sistemas antigos, por serem mais conhecidos e de menor custo de manutenção.

Para a proteção física de mídias utilizar cofres a prova de fogo.

4.2 Energia Elétrica

Apesar de existir regulamentação específica sobre este tópico, será abordado apenas alguns procedimentos mínimos recomendados a serem observados para assegurar qualidade e confiabilidade em uma rede local.

Por ser um componente vital para o bom funcionamento dos equipamentos, falhas ou flutuações em seu fornecimento podem afetar consideravelmente a disponibilidade e a integridade dos sistemas da organização.

Faz-se necessário, assim, a instalação de dispositivos que minimizem os efeitos de cortes, picos e flutuações de energia como estabilizadores, *no-breaks*, geradores alternativos ou conexão a mais de uma subestação de distribuição de energia elétrica.

Em casos de fortes tempestades é aconselhável o desligamento dos equipamentos para se evitar a sua danificação por descargas elétricas naturais.

Toda alimentação de energia, em áreas críticas, deve ser fornecida por sistema *no-break*, que além de fornecer energia limpa para os equipamentos, atua também como fonte alternativa. Deve ser dimensionado para suportar 50% a mais da carga a ser utilizada, face aos picos de demanda e deve ser modular para possibilitar expansões para atender a novas demandas.

O cabeamento elétrico de entrada da concessionária deve ser duplicado na subestação local para servir como fonte alternativa, caso a primeira falhe. Na subestação devem existir transformadores que isolem a instalação interna da externa.

Preferencialmente, deve-se dispor de uma fonte de energia alternativa, independente da concessionária, através da instalação de grupo gerador a *diesel* com capacidade de alimentar os equipamentos vitais da organização, e que seja interligado à subestação local, com chave comutadora automática, para acionamento em caso de interrupção de alimentação externa.

Recomenda-se que o circuito elétrico para os equipamentos de rede seja exclusivo, com aterramento próprio e munido de proteção por disjuntores.

O sistema de aterramento da rede elétrica deve ser integrado em topologia estrela, por meio de malhas, ao longo de toda edificação, e dimensionadas para suportar as cargas a serem ligadas a fim de se evitar choques acidentais, além de instalação de pára-raios, tudo segundo as normas técnicas de instalação vigentes.

Em locais onde haja alta incidência de raios sugere-se, como proteção primária, a utilização de protetores de surtos de estado sólido[20], combinados ou não com tubos de gás[21], e como proteção secundária, filtros de linha. É absolutamente necessário que o sistema de aterramento, para esses casos, seja de excelente qualidade.

O ambiente deve possuir uma programação visual adequada que indique as tensões das tomadas, os espaços para passagem de cabos, a localização dos equipamentos de segurança, o caminho de saída e as portas, para prevenir contra a ocorrência de erros de operação e facilitar a aplicação de medidas corretivas em caso de incidente de segurança.

4.3 Sinistros

Como os equipamentos eletrônicos são sensíveis à água, deve-se instalá-los em locais pouco suscetíveis a esse tipo de ameaça ambiental. É presunção pensam que o ambiente não está exposto a esse tipo de ameaça, simplesmente pelo fato de nunca ter ocorrido uma enchente na localidade.

A água pode penetrar nas salas dos equipamentos de diversas formas, como telhados mal conservados, rede de esgotos e encanamento com problemas, condensadores, aparelhos de ar condicionado, janelas mal vedadas ou, até mesmo, em trabalhos de faxina sem a devida atenção de seus executores.

Para se defender contra danos provocados por água, deve-se instalar os equipamentos nos andares mais altos ou sobre suportes elevados. No entanto, essa medida preventiva não é suficiente no caso de goteiras ou estouro de encanamento. Deve-se fazer uma manutenção regular de todos os possíveis focos de problemas com água e utilizar detectores sob o piso falso, se for o caso.

[20] Os protetores de surto são projetados para proteção dos equipamentos de vigilância eletrônica, com finalidade de evitar a queima provocada por raios e outras sobre tensões transitórias injetadas no cabeamento. Fonte: http://www.teleson.com.br/index_arquivos/Page7761.htm.

[21] São constituídos de dois ou três eletrodos dentro de um tubo de vidro ou cerâmica, distando aproximadamente 1mm entre si, e com volume cheio de gás argônio. Fonte: http://www.jordanengenharia.com.br

A infiltração poderá ocorrer também pelo piso, nos casos em que o subsolo tenha características de ser bastante permeável, sendo necessária uma inspeção visual por ocasião, particularmente, dos períodos chuvosos. Deve-se atentar para o fato de que por baixo de pisos falsos, pode ter sido lançado cabeamento de dados e de alimentação elétrica.

Em princípio, deve ser evitada a instalação hidráulica em paredes diretamente pertencentes a salas que contenham equipamentos críticos, e caso isso ocorra faz-se necessário verificar as condições dos materiais utilizados nas tubulações para identificar possíveis infiltrações.

4.4 Condições Climáticas

O ambiente computacional, e em particular os Centros de Processamentos de Dados e salas de concentradores de rede, são totalmente dependentes das instalações de climatização, em função das exigências de níveis de temperatura e umidade inerentes aos equipamentos que o compõe, fruto de sua alta dissipação de calor.

O sistema de climatização destina-se a manter o ambiente isento de impurezas e estabilizar a temperatura ambiente (em torno de 22° C), proporcionando as condições ideais para a proteção e o perfeito funcionamento dos equipamentos nele existentes.

Atenção especial deve ser dispensada para a umidade do ar, pois ambientes muito seco podem gerar eletricidade estática e danificar os equipamentos (o ideal é em torno de 55%). Por outro lado, o excesso de umidade poderá ocorrer condensação nos circuitos dos equipamentos, provocando curtos. Para promover a ventilação necessária ao funcionamento adequados dos equipamentos, não se deve vedar suas canaletas de ventilação, nem dispô-los em ambientes muito apertados, que dificultem a circulação de ar.

Existem dispositivos que podem auxiliar no monitoramento do ambiente, registrando níveis de umidade e temperatura. Para que os aparelhos de ar condicionado e outros dispositivos de controle de temperatura e umidade funcionem perfeitamente, é aconselhável a sua manutenção periódica, de acordo com as recomendações dos fabricantes.

O controle da temperatura e umidade do ambiente pode ser obtido com eficiência através da utilização de caixas de volume de ar variáveis (VAV[22]), que possuem controles PID

[22] São aparelhos retangulares de controle de fluxo para sistema de volume variável, tanto para o insuflamento quanto para o retorno. A caixa VAV consiste de uma carcaça, *damper* de controle e sensor de diferença de pressão para medição da vazão de ar.

(Proporcional Integral Derivativo[23]). Deve-se contar também com um sistema de controle que feche os *dampers*[24] nas tubulações de insuflamento de ar-condicionado quando nível alto de poluição (fumaça) for detectado, para tanto será necessária a instalação de sensores nas tubulações, assim como a automatização dos *dampers*.

Como fonte de redundância e para proporcionar uma rotatividade no funcionamento dos aparelhos condicionadores de ar, deve-se prever a instalação de aparelhos reservas em ambientes críticos para que, em caso de contingência, não haja redução na qualidade do ar climatizado.

[23] Controles programáveis utilizados em sistemas hidráulicos e pneumáticos discretos.
[24] Dispositivos mecânicos de regulagem e fechamento.

5. CONCLUSÃO

A adoção de uma Política de Segurança da Informação é fator vital para as organizações, a fim de que a proteção da informação seja conduzida de forma racional e eficiente, servindo como um guia a ser seguido e aprimorado com a evolução tecnológica.

O apoio da cúpula dirigente quanto ao cumprimento das normas de segurança deve ter um posicionamento de cumplicidade com a execução da política de segurança para não cair na banalidade ou, o que é pior, achar que pratica segurança simplesmente por ter algumas normas documentadas. O importante é cumprir e fazer cumprir o que está escrito.

Para garantia da continuidade dos negócios, não resta dúvida que o "segredo institucional" seja preservado, e isso se dá com o planejamento e investimento em segurança de TI na medida necessária para equilíbrio do fator custo *versus* benefícios a serem obtidos.

É importante o envolvimento de todos os integrantes da organização através da conscientização de que, eles são os protagonistas no processo de segurança das informações. Treinamentos, palestras e informativos de alerta devem fazer parte da rotina de trabalho para atingir esse fim.

Saber avaliar os riscos de segurança que assolam a instituição é uma medida eficaz para identificar e buscar uma solução exeqüível e globalizada, neutralizando as principais vulnerabilidades de seu sistema computacional e assim contribuir para o sucesso dos negócios da organização, tornando-a competitiva e eficiente na concorrência do mundo atual.

O estabelecimento de controles de acesso ao sistema de informação, sejam físicos ou lógicos, merecem especial atenção pois, sendo mal configurados ou inexistentes atentam diretamente contra a segurança dos dados manipulados, pondo em risco a existência da própria organização.

Os controles de acesso ao sistema devem ser constantemente revisto para adequar-se às novas tecnologias, e mais especificamente, em se tratando de acesso lógico, prevenir contra ataques a novas vulnerabilidades descobertas em programas que fornecem serviços de rede.

O levantamento de requisitos para proteção a acessos a sistemas informatizados,

apresentado neste trabalho, não teve objetivo de esgotar o assunto, apenas aqueles de maior relevância foram destacados. É razoável aceitar que nem todos eles deverão ser implantados, face às peculiaridades de negócio e financeiras de cada instituição, e em virtude da definição das metas para se atingir o grau de segurança desejado.

As ameaças internas são apontadas como o maior causa de ocorrência de incidentes de segurança, particularmente oriundas dos próprios funcionários da organização. Cabe a adoção de medidas que regulamentem, por escrito, as responsabilidades e direitos de acesso dos usuários, associado a um trabalho de conscientização por meio de palestras e informativos versando sobre segurança em TI.

A implementação de mecanismos mais modernos para o controle de acesso, como os sistemas biométricos, merece um uma avaliação criteriosa pelos gestores de TI das instituições como forma de aprimorar e minimizar a ocorrência de incidentes de segurança.

Para a definição de qual sistema biométrico pode ser implantado na organização, deve-se levar em consideração as vantagem e desvantagens de cada um deles, custos de sua implantação e para qual fim se destina dentro da organização, além do grau de segurança requerido. Lembrando-se que sistemas multimodais são mais precisos e seguros.

Outro aspecto a ser observado e, não menos importante, são os controles quanto às condições ambientais onde os sistemas computacionais das empresas estão sitiados. De nada vale todo esforço tecnológico aplicado, se não estiverem amparados por uma infra-estrutura segura contra ocorrência de sinistros ou imprevistos provenientes do seu meio físico.

Por fim, ressalta-se que não existe uma organização 100% segura, pois as ameaças são muitas. Cabe um estudo judicioso para identificar aquelas de maiores riscos, para que seja priorizada a adoção de controles de segurança e assim reduzirem, ao máximo, suas vulnerabilidades a acessos indesejáveis ao sistema computacional, dentro dos recursos financeiros, previstos pela organização, para investimento em segurança.

6. GLOSSÁRIO

ABNT

Associação Brasileira de Normas Técnicas.

Ameaça

Fonte potencial de dano; elemento ou atividade que possui potencial de causar uma conseqüência.

Ataque

O ato de tentar desviar dos controles de segurança de um sistema. Um ataque pode ser ativo, tendo por resultado a alteração dos dados; ou passivo, tendo por resultado a liberação dos dados. Nota: O fato de um ataque estar acontecendo não significa necessariamente que ele terá sucesso. O nível de sucesso depende da vulnerabilidade do sistema ou da atividade e da eficácia de contramedidas existentes.

Auditoria

Revisão e exame dos registros e das atividades do sistema para avaliar sobre sua confiabilidade, executados com independência.

Autenticar

Verificação da identidade de um usuário, de dispositivo, ou de outra entidade em um sistema computadorizado, freqüentemente como um pré-requisito a permitir o acesso aos recursos em um sistema.

Backup

Rotina de salvar dados para um ou outro local/mídia, com o objetivo de recuperação em caso de danos aos dados no local original.

Biometria

É um conjunto de métodos automatizados para reconhecer uma pessoa, com base em características comportamentais ou fisiológicas.

Cavalo de Tróia

Programas que são aparentemente inofensivos, mas que, ao serem executados, iniciam de forma oculta, ataques ao sistema.

Checksum

É uma forma de verificação de redundância usando uma medida muito simples para proteger a integridade de dados por detecção de erros nos dados que são enviados pelos sistemas de telecomunicações ou redes de computadores.

Controle de Acesso

Prevenção e controle do uso não autorizado de um recurso. Tarefas executadas por hardware, software e controles administrativos para monitorar a operação do sistema, garantindo a integridade dos dados, identificando o usuário, registrando os acessos e as mudanças no sistema e permitindo o acesso aos usuários.

Controles

Procedimentos usados para controlar o sistema de tal maneira que ele esteja de acordo com critérios especificados. Qualquer ação, procedimento, técnica ou qualquer outra medida que reduza a vulnerabilidade de uma ameaça a um sistema.

Cracker

Termo usado para designar quem quebra um sistema de segurança, de forma ilegal ou sem ética. Este termo foi criado em 1985 pelos *hackers* em defesa contra o uso jornalístico do termo *hacker*. O uso deste termo reflete a forte revolução contra o roubo e vandalismo praticado pelo *cracking*. Pessoa que tenta acessar sistemas sem autorização, usando técnicas próprias ou não, no intuito de ter acesso a determinado ambiente para proveito próprio ou de terceiros.

Criptografia

Ciência que estuda os princípios, meios e métodos para tornar ininteligíveis as informações, através de um processo de cifração, e para restaurar informações cifradas para sua forma original, inteligível, através de um processo de decifração. A criptografia também se preocupa com as técnicas de criptoanálise, que dizem respeito a formas de recuperar aquela

informação sem se ter os parâmetros completos para a decifração.

DMZ

É uma sigla de *DeMilitarized Zone* ou "zona desmilitarizada", em português. Também conhecida como Rede de Perímetro, a DMZ é uma pequena rede situada entre uma rede confiável e uma não confiável, geralmente entre a rede local e a Internet. A função de uma DMZ é manter todos os serviços que possuem acesso externo (HTTP, FTP, etc) separados da rede local limitando o dano em caso de comprometimento de algum serviço nela presente por algum invasor. Para atingir este objetivo os computadores presentes em uma DMZ não devem conter nenhuma rota de acesso à rede local.

E-commerce

Comércio eletrônico ou comércio virtual, é um tipo de transação comercial feita especialmente através de um equipamento eletrônico, como, por exemplo, um computador.

Firewall

Dispositivo de rede que tem por função regular o tráfego de rede entre redes distintas e impedir a transmissão de dados nocivos ou não autorizados de uma rede a outra.

FTP

File Transfer Protocol, protocolo usado para transferência de arquivos entre computadores.

Gerenciamento de Mudanças

O conjunto de procedimentos apropriados para controlar mudanças num sistema de hardware e estrutura de software com o intuito de assegurar que as mudanças não permitirão violações da política de segurança de sistemas.

Gerenciamento de Riscos

O processo total de identificar, de controlar, eliminando ou minimizando os riscos que podem afetar recursos de sistema. Inclui a análise do risco, a análise de benefício de custo, a seleção, a execução e o teste, a avaliação de segurança das proteções, e a revisão total da segurança.

Help Desk

Forma de suporte à distância para usuários sanarem suas dúvidas quanto ao funcionamento de determinado sistema.

Home Page

Página inicial, normalmente em linguagem HTML de um *site* (também chamado sítio). Compreende uma apresentação do *site* e de todo seu conteúdo.

HTTPS

HyperText Transfer Protocol Secure, é uma implementação do protocolo HTTP sobre uma camada SSL ou do TLS, essa camada adicional permite que os dados sejam transmitidos através de uma conexão criptografada e que se verifique a autenticidade do servidor e do cliente através de certificados digitais. A porta TCP usada por norma para o protocolo HTTPS é a 443.

ICQ

É um programa de comunicação instantânea pela Internet que foi o mais popular durante anos. A sigla é um trocadilho feito baseado na pronúncia das letras em Inglês (*I Seek You*), em português, "Eu procuro você". O ICQ foi o pioneiro desta tecnologia tendo sua primeira versão lançada em 1997 por uma empresa israelense chamada Mirabilis, fundada por Yair Goldfinger, Arik Vardi, Sefi Vigiser e Amnon Amir.

IMAP

Internet Message Access Protocol é um protocolo de gerenciamento de correio eletrônico superior em recursos ao POP3 - protocolo que a maioria dos provedores oferece aos seus assinantes. A última versão é o IMAP4. O mais interessante é que as mensagens ficam armazenadas no servidor e o internauta pode ter acesso a suas pastas e mensagens em qualquer computador, tanto por *webmail* como por cliente de correio eletrônico (como o *Outlook Express*). Outra vantagem deste protocolo é o compartilhamento de caixas postais entre usuários membros de um grupo de trabalho. Além disso, é possível efetuar pesquisas por mensagens diretamente no servidor, utilizando palavras-chaves.

Intranet

É uma rede de computadores privativa que utiliza as mesmas tecnologias que são utilizadas na Internet. O protocolo de transmissão de dados de uma intranet é o TCP/IP e sobre ele podemos encontrar vários tipos de serviços de rede comuns na Internet, como por exemplo o *e-mail*, *chat*, grupo de notícias, HTTP, FTP, entre outros.

Logbook

Arquivo eletrônico destinado a fazer os registros de instalações e alterações de configurações de determinado programa para uso pelos administradores de sistemas.

Loghost

Sistema dedicado à coleta e ao armazenamento de *logs* de outros sistemas em uma rede.

Logon

Seqüência de operações para acesso a um sistema em que o usuário conecta-se, identificando-se com um nome de usuário (*username*) e uma senha própria.

Modem

Palavra oriunda de modulador demodulador. É um dispositivo eletrônico que modula um sinal digital em uma onda analógica, pronta a ser transmitida pela linha telefônica, e que demodula o sinal analógico e o re-converte para o formato digital original.

MTA

Mail Transfer Agent, é o programa de computador instalado em um servidor responsável por transferências de mensagens de correio eletrônico entre um computador e outro, também conhecido como servidor de *e-mail*.

Multicast

É a entrega de informação para múltiplos destinatários simultaneamente usando a estratégia mais eficiente onde as mensagens só passam por um link uma única vez e somente são duplicadas quando o link para os destinatários se divide em duas direções. Em comparação com o *Multicast*, a entrega simples ponto-a-ponto é chamada de *Unicast*, e a

entrega para todos os pontos de uma rede chama-se *Broadcast*.

PGP

Do inglês *Pretty Good Privacy* (privacidade bastante boa), é um programa de computador que utiliza criptografia para proteger a privacidade do e-mail e dos arquivos guardados no computador do usuário. PGP pode, ainda, ser utilizado como um sistema à prova de falsificações de assinaturas digitais, permitindo desta forma a comprovação de que arquivos ou e-mails não foram modificados.

RC4

Algoritmo simétrico desenvolvido por Ron Rivest que pode usar chaves de tamanho variável. Usualmente usado com 40 bits ou 128 bits.

Requisitos de Segurança

Tipos e níveis de proteção necessários para equipamentos, dados, informação, aplicações e instalações para atender a política de segurança.

Roteador

Dispositivo usado para fazer a comunicação entre diferentes redes de computadores que operam na camada 3 do modelo OSI. A principal característica do roteador é selecionar a porta mais apropriada para repassar os pacotes recebidos. Ou seja, encaminhar os pacotes para o melhor caminho disponível para um determinado destino.

Smartcard

Cartão semelhante aos cartões de créditos e que geralmente são utilizados na identificação do usuário para controle de acesso, convênios médicos e também como dinheiro eletrônico.

Spam

Envio, a uma grande quantidade de pessoas de uma vez, de mensagens eletrônicas, geralmente com cunho publicitário. Podem ser de origem desconhecida ou não.

Vulnerabilidade

Probabilidade de uma ameaça transformar-se em realidade.

7. REFERÊNCIAS

ABBAS, Rasha. *Backpropagation Networks prototype for off-line signature verification.* Minor thesis, RMIT, Department of Computer Science, Melbourne, March 1994.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). Norma ABNT NBR ISO/IEC 17799:2005 – Tecnologia da informação – Técnicas de segurança – Código de práticas para a gestão da segurança da informação, 2005, p.1-120.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). NBR 11515 - Critérios de Segurança Física Relativos ao Armazenamento de Dados. Rio de Janeiro: ABNT, 1990.

BARBOSA, Alexandre. E-Bussiness com Segurança. Internet Bussiness, São Paulo-SP, ano 5, 27 de setembro de 2001, 49p.

BRESSAN, Nadja Mench. Biometria. Trabalho apresentado à Universidade de Caxias do Sul. Caxias do Sul-RS, outubro de 2002.

CARUSO, Carlos A. A.; STEFFEN, Flávio Deny. Segurança em Informática e de Informações. 2ª ed. rev. e ampl. São Paulo: Senac, 1999.

CENTRO DE ATENDIMENTO A INCIDENTES DE SEGURANÇA DA RNP (CAIS). Relatório Anual 2003. Fevereiro de 2004.

CENTRO DE ESTUDOS, RESPOSTAS E TRATAMENTO DE SEGURANÇA NO BRASIL – CERT-BR. Práticas de Segurança para Administradores de Redes Internet. Versão 1.2, Mai 2003, 46p. Disponível em: http://www.cert.br/stats/. Acessado em: 10 de novembro de 2006, às 22:47 hs.

FIORESE, Maurício. Uma Proposta de Autenticação de Usuários para Ensino a Distância. Porto Alegre, 2000. 122 p. Dissertação (Mestrado em Ciência da Computação) – Instituto de Informática, Universidade Federal do Rio Grande do Sul, Porto Alegre, junho de 2000.

FREITAS, Marco Oswaldo da Costa. Artigo para revista TI Master, 18 maio 2001. Disponível em: http://www.timaster.com.br/revista/artigos/main_artigo.asp?codigo=357. Acessado em 14 de novembro de 2006, às 20:06 hs.

HEINEN, Milton Roberto; OSÓRIO Fernando Santos. Biometria Comportamental: Pesquisa e Desenvolvimento de um Sistema de Autenticação de Usuários Utilizando Assinaturas Manuscritas. Trabalho apresentado à Universidade do Vale do Rio dos Sinos. São Leopoldo-RS, 2004.

IEEE 802.11. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Disponível em: http://www em: http://standards.ieee.org/getieee802/. Acessado em 12 de setembro de 2006, às 23:32 hs.

IMONIANA, Joshua Onome. Validação de Modelos de Políticas de Segurança de Informação. Artigo apresentado na Universidade Metodista de São Paulo. São Bernardo do Campo-SP, 27 de setembro de 2004.

JAIN, A.K.et al. An Identity-Authentication System Using Fingerprints. Proceedings of the IEEE**,** New York, v.85, n.9, p.1365-1388, 1997.

KIM, Hyun-Jung. Biometrics, is it a viable proposition for identity authentication and access control ? Computers & Security, Oxford, v. 14, n.3, p. 205-214, 1995.

LEMOS, Aline Morais de. Política de Segurança da Informação. Monografia apresentada à Universidade Estácio de Sá. Rio de Janeiro-RJ, 2001.

LOSS CONTROL Consultoria e Assessoria Ltda – Autotreinamento em Segurança da Informação em CD-ROM da LOSS CONTROL.

MIELLI, Fernando. Dispositivos Biométricos. O que são e como funcionam. Módulo *Security Magazine*. Disponível em: http://www.modulo.com.br. 10 de janeiro de 2002.

MODULO SECURITY SOLUTIONS. Nona Pesquisa Nacional de Segurança da Informação - 2004. Disponível em: http://modulo.com.br. Acessado em 17 de junho de 2006, às 19:40 hs.

MODULO SECURITY SOLUTIONS. Glossário. Disponível em: http://www.modulo.com.br/pt/page_i.jsp?page=50&tipoid=12&pagecounter=0. Acessado em: 12 de novembro de 2006, às 21:12 hs.

MOREIRA, Stringasci Nilton. Segurança mínima: uma visão coorporativa da segurança de informações. Rio de Janeiro: Axcel Books, 2001.

RAMOS, Alice. Disponível em: http://www.aliceramos.com/segura/index.asp. Acessado em: 21 de junho de 2006, às 22:25 hs.

REVISTA ELETRÔNICA BRASILIANO & ASSOCIADOS. Antônio C. R. Artigo sobre **Conceito de Segurança em Áreas Computacionais – CPD.** Disponível em: http://www.brasiliano.com.br. Acesso em: 06 de agosto de 2004.

SANTOS, Luciano Alves Lunguinho. O Impacto da Engenharia Social na Segurança da Informação. Monografia apresentada à Universidade Tiradentes. Aracajú-SE, 2004.

SÊMOLA, M. Gestão da Segurança da Informação – Uma visão executiva. 3. Ed. Rio de Janeiro: Elsevier, 2003. 160p.

SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS - SERPRO. Disponível em: http://www.serpro.gov.br/publicacao/tematec/2002/ttec61. Acessado em: 07 de outubro de 2006, às 23:34 hs.

SOUZA, Leonardo Henrique Lima de. Segurança Física de Redes de Computadores. Monografia apresentada à Universidade Estácio de Sá. Rio de Janeiro-RJ, outubro de 2004.

THE SANS SECURITY POLICY PROJECT. Disponível em: http://www.sans.org/resources/policies/. Acessado em 21 de junho de 2006, às 19:46 hs.

UNIVERSIDADE DE SÃO PAULO – Centro de Computação Eletrônica. Norma Técnica – Redes Locais. Disponível em: http://www.usp.br/cce/normas/nt_indice.php. Acessado em: 13 de outubro de 2006, às 19:44 hs.

UNIVERSIDADE FEDERAL FLUMINESE E CENTRO DE ESTUDOS DE PESSOAL. Apostilas do Curso de Criptografia e Segurança em Redes. Rio de Janeiro, 2006.

WIKIPÉDIA. Disponível em: http://pt.wikipedia.org. Acessado em 21 de setembro de 2006, às 20:11 hs.

ANEXO A

Lei nº 4.150/62: Institui o regime obrigatório de preparo e observância das normas técnicas nos contratos de obras e compras do serviço público de execução direta, concedida, autárquica ou de economia mista, através da Associação Brasileira de Normas Técnicas e dá outras providências.

Art. 1º - Nos serviços públicos concedidos pelo Governo Federal, assim como nos de natureza estadual e municipal por ele subvencionados ou executados em regime de convênio, nas obras e serviços executados, dirigidos ou fiscalizados por quaisquer repartições federais ou órgãos paraestatais, em todas as compras de materiais por eles feitas, bem como nos respectivos editais de concorrência, contratos ajustes e pedidos de preços será obrigatória a exigência e aplicação dos requisitos mínimos de qualidade, utilidade, resistência e segurança usualmente chamados 'normas técnicas' e elaboradas pela Associação Brasileira de Normas Técnicas, nesta lei mencionada pela sua sigla “ABNT”.

ANEXO B

Artigos do novo Código Civil Brasileiro

Art. 186° - Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito.

Art. 187° - Também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes.

Art. 927° - Aquele que, por ato ilícito, causar dano a outrem, fica obrigado a repará-lo.
Parágrafo único: "Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem.

ANEXO C

BIOMETRIA COMPORTAMENTAL: PESQUISA E DESENVOLVIMENTO DE UM SISTEMA DE AUTENTICAÇÃO DE USUÁRIOS UTILIZANDO ASSINATURAS MANUSCRITAS.

Milton Roberto Heinen & Fernando Santos Osório
UNISINOS - Universidade do Vale do Rio dos Sinos
Ciências Exatas e Tecnológicas – Computação Aplicada
CEP 93022-000 São Leopoldo (RS)

(...)

3. Inteligência Artificial e Aprendizado de Máquina

Segundo Mitchell[25] [Mitchell (1997)], um programa aprende quando a sua performance melhora com a experiência em uma determinada tarefa. Para existir um problema de Aprendizado de Máquina bem definido devem-se identificar três características fundamentais: a tarefa a ser aprendida, a medida de performance e a fonte de experiência.

Também é necessário que se defina o conhecimento que será aprendido através da experiência, também chamado de função alvo. No caso do reconhecimento de assinaturas, o conhecimento que deve ser aprendido é como classificar de forma correta uma assinatura: autêntica ou não. A tarefa é a classificação das assinaturas, a fonte é a base de dados de assinaturas e a medida é a avaliação feita sobre a taxa de acertos na autenticação das assinaturas.

Existem diversas técnicas de Aprendizado de Máquina que podem ser utilizadas para a autenticação de assinaturas, como as Árvores de Decisão, os Sistemas Fuzzi, os Algoritmos Genéticos e as Redes Neurais Artificiais.

3.1. Redes Neurais Artificiais

Através de um modelo abstrato e simplificado dos neurônios humanos é possível desenvolver um simulador que seja capaz de classificar, generalizar e aprender funções

[25] [Mitchell (1997)] Mitchell, Tom. Machine Learning. WCB / McGrall-Hill – Computer Science Series. Boston, MA. 1997.

desconhecidas. Um dos modelos de aprendizado neural mais utilizados na atualidade é o modelo denominado *Backpropagation* [Rumelhart[26] et al. (1986)].

Para que ocorra o aprendizado, é necessário um conjunto de dados com exemplos de padrões e as respostas esperadas (padrões e classes correspondentes).

Esta base de dados de aprendizado é apresentada para a Rede Neural bhrtificial (RNA) de modo que esta possa aprender a responder de forma similar às respostas informadas na base de dados, passando a reconhecer os padrões. Utiliza-se também uma segunda base de dados, a base de validação (avaliação da generalização), que é usada unicamente para medir o desempenho do aprendizado (não é usada no ajuste da rede), sendo esta base um conjunto de dados diferente do usado no aprendizado [Osório[27] (1998)].

Este tipo de aprendizado é conhecido como aprendizado supervisionado com validação cruzada [Haykin[28] (2001)].

Através de um processo iterativo, são apresentados à Rede Neural diversos exemplos contidos na base de dados de aprendizado, para que ocorra a adaptação dos pesos, que simulam o reforço e a inibição das conexões sinápticas existentes entre os neurônios reais.

Desta adaptação de pesos surge o aprendizado, que fará com que a Rede Neural aprenda a responder aos estímulos de entrada de acordo com as respostas desejadas contidas nos exemplos apresentados.

(...)

[26] [Rumelhart et al. (1986)] Rumelhart, D.; Hinton, G.; Williams, R. Learning Internal Representations by Error Propagation. In: Parallel Distributed Processing: Explorations in the Microstructure of Cognition - Vol. 1. Cambridge: MIT Press, 1986.

[27] [Osorio (1998)] Osorio, Fernando S. INSS: Un Système Hybride Neuro-Symbolique pour l'Apprentissage Automatique Cons-tructif. Tese de Doutorado. INPG/IMAG - Grenoble, França. 1998.

[28] [Haykin (2001)] Haykin, Simon. Redes Neurais: Princípios e Prática. 2a. ed. Bookman. 2001.