UNIVERSIDADE DO EXTREMO SUL CATARINENSE

CURSO DE CIÊNCIA DA COMPUTAÇÃO

EMERSON JOÃO DE SOUZA

APLICANDO CONCEITOS DE SEGURANÇA EM SISTEMAS VIA WEB PARA INSTITUIÇÕES DE ENSINO

CRICIÚMA, NOVEMBRO DE 2006.

EMERSON JOÃO DE SOUZA

APLICANDO CONCEITOS DE SEGURANÇA EM SISTEMAS VIA WEB PARA INSTITUIÇÕES DE ENSINO

Trabalho de Conclusão do Curso apresentado para a obtenção do Grau de Bacharel em Ciência da Computação da Universidade do Extremo Sul Catarinense.

Orientador: Prof. MSc. Rogério Antônio Casagrande

CRICIÚMA, NOVEMBRO DE 2006.

Emerson João de Souza

Aplicando Conceitos de Segurança em Sistemas Via Web para Instituições de Ensino

Submetido ao corpo docente do Departamento de Ciência da Computação da Universidade do Extremo Sul Catarinense como um dos requisitos para obtenção do grau de Bacharel em Ciência da Computação.

_____
Prof. M.Sc. Ana Claudia Garcia Barbosa
Coordenadora do Curso de Ciência da Computação

Banca Examinadora:

_____
Prof. M.Sc. Rogério Antônio Casagrande (UNESC)
Orientador

_____
Prof. M.Sc. Paulo João Martins (UNESC)

_____
Prof. M.Eng. Evânio Ramos Nicoleit (UNESC)

Dedico esse trabalho a todas as pessoas que acreditaram na minha capacidade, principalmente aos meus pais João e Lourdes por estarem sempre me incentivando a continuar os estudos e buscar novos desafios.

AGRADECIMENTOS

Em primeiro lugar, agradeço a Deus por estar sempre ao meu lado, principalmente nos momentos mais difíceis da minha vida. Dando forças para vencer os desafios e iluminando o meu caminho.

Aos meus pais por estarem sempre me incentivando a estudar e buscar novos aprendizados.

Aos amigos, pela compreensão da minha falta nos momentos em que estive fazendo esse trabalho.

Também quero agradecer aos professores do Curso de Ciência da Computação, pelo aprendizado adquirido durante esses anos, principalmente ao professor Rogério Antônio Casagrande que foi o meu orientador, me auxiliando na realização desse trabalho.

Enfim, agradeço a todas as pessoas que contribuíram para a realização e conclusão desse trabalho.

RESUMO

À medida que a Internet se dissemina entre as pessoas, causa uma grande preocupação com relação à segurança das informações que trafegam pela rede. Para amenizar esse problema existem várias técnicas, tais como: criptografia, assinatura digital, certificados digitais, protocolos seguros, controle de acesso, entre outras que possuem o objetivo de fornecer segurança as informações. Essas técnicas tendem a proporcionar ao usuário os princípios básicos de uma comunicação segura, caracterizada pelos itens de confidencialidade, autenticação, integridade e disponibilidade. Esse trabalho descreve os conceitos relacionados à segurança de informações, assim como os métodos existentes para implementar segurança, principalmente em sistemas voltados para Internet. Para demonstrar a aplicação de algumas dessas técnicas, foi desenvolvido um protótipo de software via web destinado a instituições educacionais, onde são aplicadas as técnicas de níveis de acesso e protocolos seguros, a fim de disponibilizar de forma confiável as informações referentes aos alunos e professores de uma escola.

Palavras chave: Segurança de Dados, Criptografia, Protocolos Seguros, Certificado Digital.

ABSTRACT

As the internet spreads among people, the security of the information that goes through requires a great concern. To diminish this problem there are plenty techniques available such as: cryptograms , digital signature, digital certificates, safe protocols, access control, among others that present the same purpose, to guarantee the security the information. These techniques tend to provide to the user the basic principles of a safe communication, characterized by classified information, authenticity, integrity and availability. This describes the concepts related to the security of information, as well as the existing methods to implement security, mainly in systems directed toward Internet. To demonstrate how some of these techniques have been applied to the softwares on line , it was developed specially to the educational institutions, where the safe techniques of access levels and protocols are applied, in order to make the information about the students and teachers available in a safety way.

Keywords: data Safeness , locking, Criptograms, Protocols, Digital Certificate

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

AES	*Advanced Encryption Standard*
CA	*Certification Authority*
DES	*Data Encription Standard*
HD	*Hard Disk*
HTTP	*Hiper Text Transfer Protocol*
HTTPS	*Hiper Text Transfer Protocol Security*
IDEA	*International Data Encryption Algorithm*
IP	*Internet Protocol*
KDC	*Key Distribution Center*
MD	*Message Digest*
NIST	*National Institute of Standards and Technology*
PGP	*Pretty Good Privacy*
SERIE	Sistema Estadual de Registro e Informações Escolares
SGBD	Sistema Gerenciador de Banco de Dados
SSL	*Security Socket Layer*
TCP	*Transmission Control Protocol*
TSL	*Transport Security Layer*
UNESC	Universidade do Extremo Sul Catarinense
VPN	*Virtual Private Network*
WAN	*Wide Area Network*

SUMÁRIO

1 INTRODUÇÃO

Várias organizações de médio e grande porte estão entrando na era da Internet, ou seja, estão direcionando seus negócios ao ambiente virtual, como o e-business, por exemplo. A migração de sistemas clássicos cliente/servidor para a plataforma web é uma grande realidade. Sendo assim, as organizações que ainda não aderiram a esse processo tendem a perder competitividade e mercado.

A evolução da Internet é uma realidade, que pode ser observada devido aos serviços oferecidos. Sendo assim, a Internet está deixando de ser uma mera ferramenta para exibição de páginas e se tornando uma grande área para aplicativos web. Isso tudo devido a questões de portabilidade, interface amigável, controle de transações e o que é mais importante, à segurança dos dados.

A segurança dos dados voltada a aplicativos web é de grande importância, principalmente se o aplicativo conter informações confidenciais, secretas ou de uso restrito.

Nesse trabalho, foram abordados tópicos relacionados a segurança que é o foco do sistema proposto, o qual chama-se: Aplicando Conceitos de Segurança em Sistemas via Web para Instituições de Ensino.

Nas Instituições de Ensino, como em qualquer outra organização, ocorre um grande fluxo de informações. Essas informações são referentes aos seus alunos e professores.

Todas essas informações são controladas por meio de cadastros, diário de classe e freqüência, histórico escolar, boletins, entre outros. Em muitas das instituições de médio e pequeno porte, esse controle é realizado de forma manual, por meio de fichas que ficam armazenadas em arquivos não muito seguros, podendo ocorrer

deterioração e perda de dados, outras, em implementações de sistemas corporativos internos.

Fundamentado pelas razões expostas acima, este trabalho apresenta o desenvolvimento de um protótipo de software via web para fazer o controle dessas informações. Este sistema, além de transformar o processo manual em eletrônico, também disponibiliza de forma “segura”, os dados referentes aos professores e alunos da instituição que podem acessar via web, por exemplo: diário de classe, boletins, históricos, entre outros.

O foco em segurança, não se refere somente a segurança lógica das informações, mas sim a segurança de todo o parque tecnológico que a cerca, como por exemplo, computadores e máquinas.

O tratamento da segurança envolvido nessa proposta, foi realizado por meio de protocolos seguros, criando-se um canal seguro para o tráfego de informações na rede, proporcionando integridade e confiabilidade das informações.

Uma outra vantagem relacionada a aplicativos desse porte é a facilidade de acesso a ele a qualquer momento, sendo necessário apenas que o usuário possua um computador conectado a Internet e um navegador instalado.

O custo relacionado ao desenvolvimento de um aplicativo desse tipo é relativamente baixo, tendo em vista que a implementação deles se dá com ferramentas gratuitas, disponíveis na Internet.

1.1 OBJETIVO GERAL

Aplicar alguns conceitos de segurança em um protótipo via web para instituições de ensino, a fim de proporcionar um meio de comunicação segura,

principalmente em relação às informações que trafegam na rede. Entre cliente e servidor, proporcionando confidencialidade, integridade e disponibilidade das informações pertinentes aos professores e alunos da mesma.

1.2 OBJETIVOS ESPECÍFICOS

Os objetivos específicos desse trabalho são:

a) aplicar as tecnologias de desenvolvimento para web;
b) desenvolver um protótipo via web para instituições de ensino;
c) descrever a importância da segurança da informação em sistemas via web.
d) aplicar alguns conceitos de segurança no protótipo SMAAE para preservar a confidencialidade e a integridade das informações que trafegam na rede.

1.3 JUSTIFICATIVA

Em uma análise realizada, conforme item 5.2 em algumas escolas municipais de médio e pequeno porte do município de Morro da Fumaça, em especial a Escola Municipal Pietro Maccari (onde foram coletadas as informações necessárias para o desenvolvimento do trabalho), percebeu-se a necessidade de um sistema de gestão para controlar as informações internas, como: diário de classe e freqüência, cadastramento de professores e alunos, histórico e boletim escolar do aluno. Alguns processos ainda são realizados de forma manual, sendo muito lento e cansativo, dificultando assim o trabalho dos professores e administradores da instituição. Além disso, não há confiabilidade, podendo vazar informações.

O item segurança é de fato muito importante, principalmente em sistemas voltados para o ambiente WEB, onde as informações estão trafegando na rede. Em outros projetos de mesmo porte já pesquisados, a questão segurança não foi levada em consideração, ou seja, não foi implementada nenhuma técnica de segurança, assim como: criptografia, protocolos seguros, assinaturas digitais, entre outros a fim de proteger as informações do sistema.

A segurança da informação é o foco desse projeto, proporcionando acesso aos dados por meio da Internet, tanto de professores quanto de alunos com maior confiabilidade.

Esses foram os fatores determinantes para a escolha do tema, proporcionando o desenvolvimento do sistema nas escolas, tendo-se também um ganho social para a região.

2 SEGURANÇA DE INFORMAÇÕES

A segurança das informações, principalmente nos dias de hoje, é a base de todas as organizações (sociais, governamentais, educativas, entre outras) modernas. Todos dependem da informação. Seja para vender seus produtos, para controlar estoques, para a tomada de decisões, ou até mesmo por questões de marketing. Sendo assim, conforme Caruso (1999), o bem mais valioso de uma organização pode não ser o produto em sua linha de produção ou o serviço prestado, mas as informações relacionadas com esses bens de consumo ou serviço.

Desde os tempos antigos, o ser humano se preocupava com o controle das informações e sempre buscou de alguma forma, registrar as informações que eram importantes. Segundo Caruso (1999), o que mudou desde então foram somente as formas de armazenamento, manipulação e disseminação dessas informações, que antes eram gravadas na memória humana e divulgadas por meio de papiros e pergaminhos.

> Atualmente, não há organização humana que não seja altamente dependente da tecnologia de informações, em maior ou menor grau. E o grau de dependência agravou-se muito em função da tecnologia de informática, que permitiu acumular grandes quantidades de informações em espaços restritos. (CARUSO, 1999, p.22)

Hoje, toda essa gama de informações é manipulada por recursos tecnológicos, agilizando os processos, dando maior praticidade e velocidade no acesso às mesmas. Por outro lado, existe certa vulnerabilidade em relação a riscos de invasões, acessos não permitidos, perda de dados importantes, entre outros. Atendendo ao fato de que hoje as pessoas são extremamente dependentes dessas informações, uma falha computacional nos sistemas de empresas do mercado financeiro, de assistência médica ou de telecomunicações, por exemplo, poderia de várias formas afetar a população, causando danos irreversíveis.

O mesmo pode ocorrer em caso de um acesso não autorizado, onde os dados podem ser apagados ou corrompidos. Também pode haver o vazamento de informações de uma dessas organizações, podendo essas informações cair em mãos erradas. Pois nesse caso, a organização pode perder a credibilidade dos clientes e gerar oportunidade competitiva aos seus concorrentes.

Esses sistemas, por serem na maioria das vezes, conectados em redes externas, correm maior risco a ataques, mesmo porque conforme Dias (2000) “as ferramentas utilizadas antigamente por agências de inteligência, hoje estão disponíveis a qualquer pessoa”.

Os usuários comuns, no entanto já estão bem conscientes de que correm riscos de perda de informações, por isso já estão mais exigentes quanto à qualidade nos serviços prestados, pois para eles quando um dado é perdido, não importa como isso aconteceu. O que importa para ele é que o sistema esteja funcionando corretamente, lhe proporcionando privacidade, gerando integridade e disponibilizando os dados de que necessita.

Os sistemas computacionais são desenvolvidos, com o objetivo de atender as necessidades dos usuários, considerando aspectos de segurança, tentando proteger esses sistemas de qualquer ameaça, para que não haja nenhum dano que comprometa o seu funcionamento. Sendo assim, segundo Dias (2000) devem ser realizados testes de hardware e software a fim de prevenir erros que possam ser cometidos pelos usuários.

É muito difícil imaginar na atualidade, uma organização de grande ou médio porte que não utilize tecnologia para administrar seus negócios, controlando todo o trafego de informações através de sistemas e computadores conectados em redes. Mesmo porque, é inviável a manipulação de tanta informação de forma manual.

A informação, também faz parte dos ativos de uma organização, assim como os bens e produtos gerados pela mesma. E conforme Caruso (1999), esses ativos são gerados através dos três fatores de produção tradicionais, que são: Capital, mão-de-obra e processos (Figura 1).

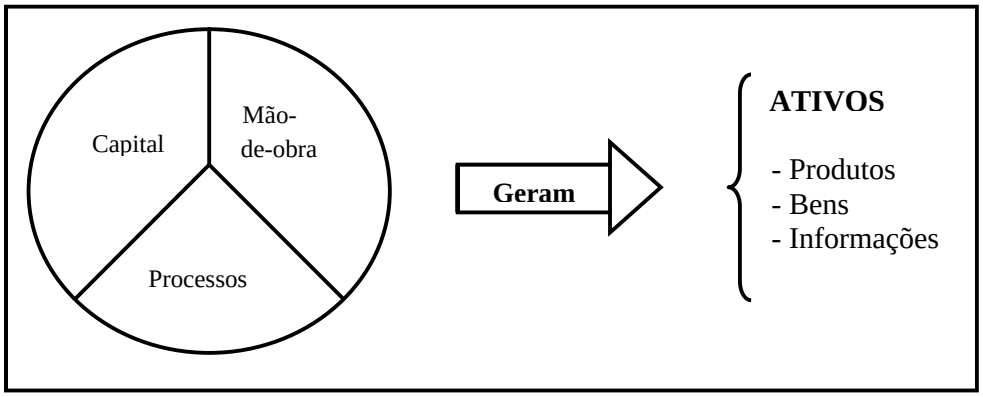

Figura 1. Fatores econômicos de produção
Fonte: CARUSO, C. (1999).

Dessa forma, mesmo que as informações não entrem na contabilização da organização (como é o caso dos outros ativos), elas devem ser protegidas. Isso vale tanto para a informação propriamente dita, como também para todo o ambiente de informação. Por isso, é necessário que sejam levadas em consideração, várias questões relacionadas à segurança, visando à proteção da mesma.

Para isso, fica a cargo da gerência a responsabilidade de buscar a melhor forma de controlar e proteger não somente a informação em si, mas também todo o parque tecnológico que a cerca, visando segurança tanto lógica quanto física. Segundo Dias (2000), essa é a garantia para que não ocorram falhas, acessos não autorizados (hackers, espionagem industrial, venda de informações confidenciais para a concorrência) e outros.

Já para Gil (1998), a segurança não é apenas responsabilidade da gerência e/ou dos profissionais de informática. O usuário também deve ser responsável pelas

informações das quais ele manipula, ou seja, aquelas informações das quais ele tem acesso.

"Segurança é portanto, a proteção de informações, recursos e serviços contra desastres, erros e manipulação não autorizada de forma a reduzir a probabilidade e o impacto de incidentes de segurança". (DIAS, 2000, p.41)

Segundo Gil (1998), para administrar a segurança, pode-se focar em quatro fases: Planejamento, Operacionalização, Acompanhamento e Avaliação (Figura 2).

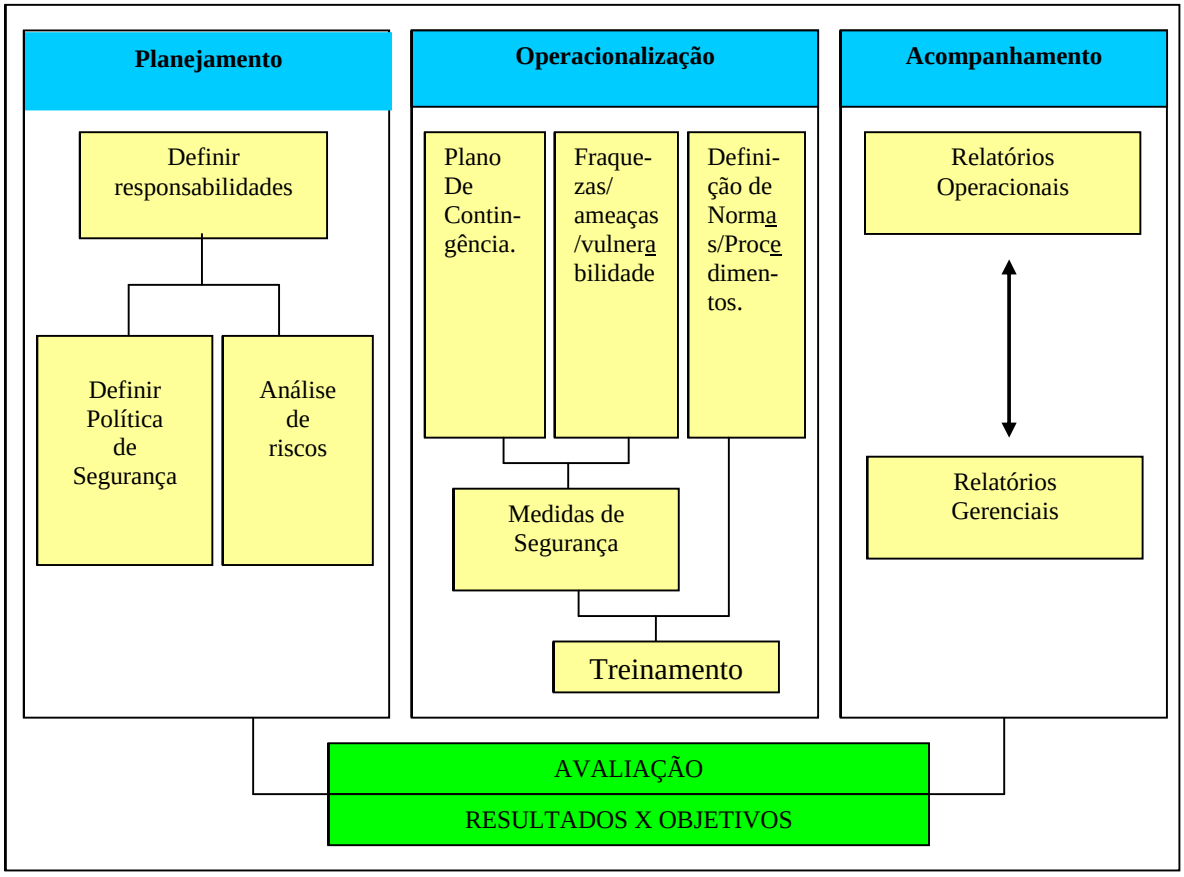

Figura 2. Ciclo da administração da segurança empresarial.
Fonte: Gil, C (1998).

A finalidade de cada fase pode ser descrita da seguinte forma:

a) planejamento: deve-se planejar as atividades a serem executadas:

- definindo as responsabilidades, ou seja, distribuindo responsabilidades aos envolvidos no processo de implantação da segurança;

- definir uma política de segurança, de forma a tratar o controle da informação;

- realizar análise de riscos, ou seja, saber quais as ameaças que a organização pode sofrer e de que forma isso vai prejudicar o bom andamento da mesma.

b) operacionalização : a parte operacional trata das seguintes etapas:

- analisa o atual plano de segurança e de contingência;

- analisa as fraquezas, ameaças e vulnerabilidades existentes no sistema atual, a fim de desenvolver medidas de segurança para proteger a organização contra os agentes agressores;

- aplica na organização as normas e procedimentos necessários para a segurança do patrimônio da organização: a informação e os meios de suporte da mesma.

c) acompanhamento : possui a seguinte finalidade:

- analisar os relatórios operacionais, táticos e estratégicos, a fim de aplicar as medidas de segurança necessárias à organização no que se refere a segurança das informações.

d) avaliação : é a ultima fase e possui a seguinte função:

- a quarta e ultima fase, corresponde à avaliação, comparando-se os resultados alcançados com os objetivos que haviam sido definidos. É nesse momento que se pode concluir se a administração está sendo

eficiente, caso contrário deve-se reavaliar as falhas encontradas e aplicar as técnicas de correção necessárias.

A chamada Política de Segurança de Informações, se implantada em uma organização, tem o objetivo de fazer o controle básico de segurança, seja ela física, lógica ou ambiental. Além disso, serão fornecidas sugestões para a elaboração de um plano, ao qual possui o objetivo de dar continuidade aos negócios da organização.

2.1 POLÍTICA DE SEGURANÇA DE INFORMAÇÕES

Como visto anteriormente, a implantação de uma Política de Segurança de Informações, visa o controle da informação de forma lógica, física e ambiental.

> A política de segurança é um mecanismo preventivo de proteção dos dados e processos importantes de uma organização que define um padrão de segurança a ser seguido pelo corpo técnico e gerencial e pelos usuários, internos e externos. Pode ser usada para definir as interfaces entre usuários, fornecedores e parceiros e para medir a qualidade e a segurança dos sistemas. (DIAS, 2000, p.48)

Sendo assim, é a política de segurança que vai estabelecer os princípios dentro da organização, de como serão feitos os controles, a organização, o monitoramento e a proteção dos recursos computacionais existentes e utilizados dentro da mesma. Estabelecendo também responsabilidades referentes a cada um que trabalhe em funções relacionadas à segurança, descrevendo também quais as principais ameaças e riscos que podem ocorrer naquele setor.

> A política de segurança deve ser claramente definida, as responsabilidades devem ser corretamente atribuídas e deve haver relacionamento entre todas as políticas da organização, tais como: Política de Segurança Empresarial e Patrimonial, Política dos Negócios Empresariais e Política de Informática. (GIL, 1998, p.16).

A política de segurança deve ser muito bem discutida dentro de organizações, mesmo porque a vida delas depende do resultado de decisões políticas

(Caruso, 1999). Qualquer organização sempre estabelece regulamentos políticos a serem seguidos por todos que se relacionem com ela.

Em uma política de segurança, são estabelecidos regulamentos para a proteção dos ativos dessa organização. Esses regulamentos são traduzidos em um conjunto de diretrizes gerais, destinadas a governar a proteção a ser dada a esses ativos.

A melhor maneira de implementar uma política de segurança, conforme Caruso (1999) pode ser resumida em três pontos principais, que são:

a) redução da probabilidade de ocorrências de desastres: as medidas de segurança devem ser de cunho preventivo, ou seja, os riscos devem ser previstos ou eliminados antes de se manifestarem. Isto porque a prevenção geralmente possui menos custo do que a restauração dos danos provocados pela falta de segurança;

b) redução dos danos provocados por eventuais ocorrências de desastres: se vier a ocorrer algum tipo de dano à organização, mesmo depois de aplicada as medidas preventivas, deve se reduzir os danos resultantes ao mínimo possível. As medidas tomadas para se fazer essa redução vai depender dos danos causados e dos riscos envolvidos;

c) recuperação dos danos provocados por ocorrências de desastres: se caso acontecer alguma ocorrência danosa à organização, mesmo depois que todas as medidas de prevenção tenham sido tomadas, então deve se criar um plano de recuperação dos danos, ou melhor dos ativos atingidos pela ocorrência. Esse plano também dependerá do porte da organização em questão, e dos ativos que a mesma possui além dos riscos envolvidos.

Em linhas gerais pode-se dizer que não existe uma receita que sirva para todos os tipos de organizações, pois dependendo do porte ou do tipo de organização a

política de segurança deve ser implementada de maneira que se encaixe ao perfil da mesma.

Além disso, uma política de segurança não abrange somente aspectos computacionais, mais sim todos os aspectos relacionados à segurança em geral, bem como metas e planos estratégicos de informática. Pois, talvez são esses os pontos mais críticos em uma organização.

Como afirma Dias (2000), “uma boa ou má política de segurança de informações gera impactos sobre todos os projetos de informática, tais como planos de desenvolvimento de novos sistemas, plano de contingências, planejamento de capacidade, entre outros”.

“A Política de Segurança será efetiva, se for comunicada a todos com ênfase adequada” (GIL, 1998, p.16), ou seja, cada executivo deve mostrar aos seus subordinados, evidências sólidas que justifique a necessidade e as vantagens de se implantar uma Política de Segurança.

Mas para obter resultados são necessários primeiramente saber os conceitos básicos de segurança, seus padrões e orientações a fim de alcançar os objetivos esperados.

2.2 OBJETIVOS DE SEGURANÇA

Sabe-se que a segurança da informação visa proteger os dados em seus diferentes locais de armazenamento (HD, disquetes, papel, entre outros). E também, que um sistema ou um computador só é considerado seguro funcionando corretamente e de acordo com os propósitos do usuário.

Para o usuário, seus dados estão seguros se estiverem sempre no mesmo local onde foram armazenados, e estejam sempre disponíveis assim que ele necessitar, não sendo permitido qualquer acesso indesejável. Essas são as expectativas dos usuários em relação à segurança.

Os objetivos de segurança então, estão relacionados e moldados a essas expectativas. Ou seja, tem o objetivo de proporcionar ao usuário a possibilidade de acesso a seus dados no momento e no local onde ele desejar, garantindo a fidelidade e restringindo o acesso aos mesmos.

Conforme Dias (2000), os objetivos de segurança variam de acordo com o tipo de ambiente computacional e a natureza do sistema ao qual se deseja implementar, seja ele administrativo, financeiro, militar, entre outros. É necessário então que se faça uma análise para saber quais os riscos que o sistema corre e dos impactos que podem vir a acontecer a partir desses riscos, qual a sua real importância além de sua aplicabilidade.

É partindo desse princípio, que tanto usuários como técnicos em informática devem se preocupar com os seguintes objetivos de segurança;

d) confidencialidade ou privacidade: um sistema confiável ou que mantém a privacidade dos dados, é aquele que restringe o acesso de algumas pessoas ao sistema, disponibilizando as informações a apenas pessoas autorizadas. A segurança nesse caso é realizada através de alguns métodos de controle de acesso e criptografia, principalmente se essas informações trafegam pela rede;

e) integridade de dados: o objetivo de segurança em relação à manutenção da Integridade de dados se diferencia da Confidencialidade conforme Dias (2000), porque “o objetivo da Confidencialidade está mais voltado à leitura de dados enquanto que a integridade se preocupa com a

gravação ou alteração de dados". Ou seja, manter a integridade é não permitir que pessoas sem autorização apaguem ou alterem algum dado no sistema, protegendo também os programas, fitas magnéticas, documentação, e outros recursos pertinentes ao mesmo;

f) disponibilidade: para o usuário um sistema deve estar disponível sempre que ele necessitar. Sendo assim, se deve proteger os serviços de informática de forma que não seja danificada nenhuma máquina ou os dados que elas contem. Para isso é importante que se tenha sempre mais de um equipamento para determinada tarefa e que se faça o backup dos dados regularmente. A disponibilidade como afirma Dias (2000), pode ser definida como sendo "a garantia de que os serviços prestados por um sistema, são acessíveis sob demanda aos usuários ou processos autorizados". A segurança de informações nesse caso visa prevenir possíveis ataques, que possam prejudicar o acesso de pessoas autorizadas a utilizar o sistema. Por exemplo, alguns internautas ficam fazendo várias requisições ao mesmo tempo a fim de bloquearem o servidor de Internet;

g) consistência: um sistema é considerado consistente se estiver sempre funcionando de acordo com o que o usuário espera. Por isso deve-se ter muito cuidado ao fazer alterações, que possam modificar o comportamento do mesmo. Essas alterações dizem respeito tanto a hardware quanto a software, onde qualquer falha pode causar sérios danos, por exemplo, a perda de um arquivo contendo dados importantes;

h) isolamento ou uso legítimo: quando se fala em isolar um sistema, está se tratando em restringir o acesso à somente pessoas autorizadas. Pois os

acessos indevidos sempre acabam trazendo transtornos, sendo toda vez que ocorre um ataque ou um acesso não autorizado fica a cargo do setor de informática saber, quem foi o invasor, como conseguiu entrar no sistema, quais os danos causados por aquele acesso, como impedir para que ele não retorne a fazê-lo. Tudo isso, envolve tempo e dinheiro, tendo em vista que se ocorrer algum dano referente a essas invasões, terão que ser feitas às devidas correções;

i) auditoria: a função da auditoria em relação aos objetivos de segurança da informação, é monitorar os usuários, sendo eles autorizados ou não, para que não cometam nenhum tipo de erro ou falhas mal intencionadas ao sistema. Para isso os auditores utilizam as chamadas trilhas ou *logs* de auditoria, os quais registram tudo que foi executado no sistema, por quem e quando. Essas trilhas, além de evitar ações indesejáveis dos usuários, auxiliam na reconstrução do sistema em caso de um incidente, sendo que pode até mesmo voltar ao estado inicial. Também é função do auditor responsabilizar ao final da auditoria, os culpados pelos danos causados;

j) confiabilidade: um dos principais objetivos da segurança da informação, é a existência de um sistema confiável, funcionando sempre como o esperado e possuindo sempre dados atualizados e confiáveis. Isso é muito importante para sistemas de grandes organizações;

Segundo Dias (2000), todos esses pontos referentes aos objetivos de segurança das informações são importantes, mas dependendo do sistema ao qual se deseja implementar, alguns serão mais relevantes do que outros.

Os sistemas de acesso à Internet, por exemplo, necessitam estar disponível 24 horas, nesse caso a prioridade levada em consideração é a disponibilidade dos dados, deixando a privacidade em segundo plano. Já os sistemas militares, que armazenam informações altamente confidenciais, levam em consideração os objetivos de segurança que envolve confidencialidade, confiabilidade, isolamento, entre outros. Sendo a disponibilidade o objetivo menos importante.

Por esse motivo é que sistemas de diferentes finalidades devem ser tratados e protegidos de diferentes formas, conforme os objetivos dessas informações.

2.3 PROCESSO DE IMPLANTAÇÃO

Toda política de segurança, para ser aplicada, deve passar por um longo processo de implantação, sendo que ao longo desse processo a mesma deve-se adequar de acordo com as necessidades ou atualizações que possam vir a acontecer.

Segundo Dias (2000), as principais fases de um processo de implantação são:

a) identificação dos recursos críticos;
b) classificação das informações;
c) classificação dos sistemas;
d) analisando riscos.

2.3.1 Identificando os recursos

O primeiro passo a ser dado ao implantar uma política de segurança, é saber identificar quais os recursos mais importantes a serem protegidos em uma organização. Além disso, tem-se que saber qual a forma de armazenamento de informações que essa organização utiliza (disquetes, HD, papel, fitas, entre outros), para saber o que proteger.

Em geral, segundo Dias (2000) os recursos de informática mais utilizados são:

a) hardware: processadores, placas, teclados, terminais, estações de trabalho, computadores pessoais, impressoras, unidades de disco, linhas de comunicação, servidores, roteadores;
b) software: utilitários, programas de diagnósticos, sistemas operacionais, programas de comunicação, aplicativos;
c) dados: em processamento, em trânsito nos dispositivos e linhas de comunicação, armazenados *on-line* e *off-line*, *backups*, *logs* de auditoria, bases de dados;
d) pessoas: usuários e funcionários necessários para o funcionamento dos sistemas;
e) documentação: sobre programas, hardware, sistemas, procedimentos administrativos;
f) suprimentos: papel, formulários, fitas, disquetes, *CD-ROMs*.

2.3.2 Classificação das informações

A forma utilizada para se proteger uma informação, segundo Dias (2000) vai depender do tipo de informação a ser protegida, ou seja, depois de saber que informações serão protegidas, deve-se classifica-las a fim de saber os métodos de segurança mais adequados para tratá-las.

O responsável para fazer a classificação dessas informações será o proprietário da mesma, pois ele é a pessoa ideal para afirmar quais as que são mais relevantes à organização. O proprietário nesse caso é a pessoa que manipula diariamente essas informações, pois ela possui conhecimento profundo sobre a mesma.

Nos sistemas atuais de médio e grande porte, é muito comum se encontrar diferentes classes de informações, nesses casos se deve tratar esses sistemas, considerando a classe de maior nível, ou seja, a que exige mais segurança.

Conforme Dias (2000) a classificação mais comum é aquela que as divide em quatro níveis:

a) públicas ou de uso irrestrito: as informações e os sistemas assim classificados podem ser divulgados a qualquer pessoa sem que haja implicações para a instituição. Exemplos: serviços de informação ao público em geral, divulgadas à imprensa ou pela Internet;

b) internas ou de uso interno: as informações e os sistemas assim classificados não devem sair do âmbito da instituição. Porém, se isso ocorrer, as conseqüências não serão críticas. Exemplos: serviços de informação interna ou documentos de trabalho corriqueiros que só interessam aos funcionários;

c) confidenciais: informações e sistemas tratados como confidenciais dentro da instituição e protegidos contra acesso externo. O acesso a esses sistemas e informações é feito de acordo com sua necessidade, ou seja, os usuários só podem acessá-los se eles forem fundamentais para o desempenho de suas funções na Instituição. Nesses tipos de informações, o acesso não autorizado pode prejudicar o funcionamento da organização, causar danos financeiros ou perda de fatias de mercado para concorrentes. Exemplos: dados pessoais de clientes e funcionários, senhas, informações sobre as vulnerabilidades de segurança dos sistemas institucionais, contratos, balanços, entre outros;

d) secretas: são as informações que necessitam de maior segurança, por isso o acesso tanto interno como externo de pessoas não autorizadas a essas informações é extremamente critico para a instituição. Sendo assim, deve-se restringir o número de pessoas a quem se deve dar acesso a essas informações, obtendo um controle total. Exemplos: dados militares e de segurança nacional;

2.3.3 Classificação dos sistemas

Os sistemas de informações, por serem muito complexos também devem passar por uma classificação, os quais serão subdivididos em partes, visando uma melhor forma de implantar a segurança, podendo assim ser controlado de acordo com cada camada.

Segundo Dias (2000), os sistemas de informações também devem ser divididos em quatro camadas:

a) programas aplicativos: projetados para atender as necessidades específicas do usuário;
b) serviços: utilizados pelos aplicativos, como por exemplo os serviços prestados por um Sistema Gerenciador de Banco de Dados (SGBD);
c) sistema operacional: presta os serviços de mais baixo nível, tais como gerenciamento de impressora e gerenciamento de arquivos;
d) hardware: o processador e a memória que suportam o sistema operacional.

Analisando cada camada de forma individual, fica mais fácil configurar um nível de segurança obtendo-se também um maior controle sobre cada camada. Como resultado disso, se tem no final do processo de implantação, um sistema "seguro" por completo, ou seja, foram tomadas medidas de prevenção em todas as partes componentes do mesmo.

2.3.4 Analisando riscos

Os riscos normalmente se referem às ameaças em que um sistema pode sofrer. Segundo Dias (2000) "na verdade, risco é uma combinação de componentes, tais como ameaças, vulnerabilidades e impactos".

"A mecânica da análise de risco compreende a identificação das ameaças e vulnerabilidades dos ativos de informática, via análise qualitativa dos eventos e agentes agressores" (Gil; 1998; p.16).

A análise de riscos então, significa o processo de analisar as ameaças que um sistema pode sofrer, a vulnerabilidade que esse sistema possui e os impactos que

podem vir a acontecer em caso de uma ameaça se concretizar, gerando custos ao usuário do mesmo.

Para prevenir contra tais ameaças é necessário tomar varias precauções, começando com a identificação da ameaça, para saber com que tipo dela está se lidando (roubo, incêndio, vírus, entre outras). Após isso, é necessário saber a probabilidade dessa ameaça vir a se concretizar. E posteriormente verificar qual a gravidade do dano que possa vir a ocorrer, comparando com os custos necessários à prevenção ou recuperação das informações perdidas.

Segundo Gil (1998), pode-se quantificar o risco por meio do algoritmo para a quantificação dele, que é composto pela formula R = A X B, onde A corresponde a mensuração das causas e B a mensuração das conseqüências. Cada constante dessas, possui uma escala de um a dez (valor pré-estabelecido pelos profissionais responsáveis pela apuração do risco). Com isso pode-se obter um risco R na escala de “um” a “cem”.

Dependendo do custo envolvido para a prevenção de determinadas ameaças, pode-se chegar à conclusão de que o custo para a prevenção de uma ameaça pode ser mais alto do que o custo de seus impactos a organização. Não sendo viável então a prevenção de tal ameaça. Por isso é necessário fazer uma relação de custo/benefício, onde se deve levar em consideração àquelas ameaças que de alguma forma prejudiquem o andamento da organização.

Além disso, deve-se levar em consideração de que os riscos não podem ser eliminados, apenas reduzidos. “Tomando medidas de segurança mais rígidas, os riscos podem ser cada vez menores, mas nunca serão totalmente anulados”. (DIAS, 2000, p.54). Isso significa que não importa quanto tempo isso pode levar, mas com a ajuda de recursos técnicos mais sofisticados, um dia essa segurança pode ser quebrada.

Mesmo assim, é importante que se tenha o conhecimento sobre as ameaças aos recursos informacionais de uma organização, para que se possa aplicar uma maneira mais eficaz de reduzir as ameaças, juntamente com a vulnerabilidade e os impactos que elas podem trazer.

> Portanto, o objetivo da análise de riscos é medir ameaças, vulnerabilidades e impactos em um determinado ambiente, de forma a proporcionar a adoção de medidas apropriadas tanto às necessidades de negócios da instituição, ao proteger seus recursos de informação, como aos usuários, que precisam utilizar esses recursos, levando em consideração justificativas de custos, nível de proteção e facilidade de uso. (DIAS; 2000; p. 54)

Com isso, pode-se afirmar então que a análise de riscos, pode atender as necessidades tanto da organização quanto dos seus funcionários, além de garantir que o custo envolvido para se prevenir uma ameaça não seja maior do que o recurso que se deseja proteger.

3 SEGURANÇA NA INTERNET

Supondo-se que existem duas entidades que desejam se comunicar. Por exemplo: entidade A e entidade B. E que a entidade A deseja se comunicar de forma segura com a entidade B.

Para isso, a entidade A precisa ter certeza de que somente a entidade B consiga interpretar e/ou entender a informação enviada pela entidade A. Da mesma forma, a entidade B precisa ter certeza de que a informação ou a mensagem que recebeu foi realmente enviada pela entidade A e vice-versa.

As entidades A e B também desejam que o conteúdo de suas mensagens não seja alterado durante a transmissão e de que o acesso a essa comunicação não seja negado.

Segundo Kurose e Ross (2006), esse é o principio básico para se iniciar uma comunicação segura, ou seja, a segurança na rede é caracterizada pelos seguintes itens: Confidencialidade, Autenticação, Integridade e Disponibilidade.

O modo mais “seguro” para garantir a segurança de uma comunicação é não permitir que intrusos consigam invadir a rede, ou melhor dizendo, que seus pacotes não entrem na rede.

Conforme Kurose e Ross (2006), o Firewall é um mecanismo que pode ser utilizado para exercer essa função. Ele fica situado entre a rede e o resto do mundo. Portanto funciona como uma barreira, onde pode-se configura-lo para definir quais os pacotes podem passar para dentro ou para fora da rede.

Essa é tarefa do administrador da rede, que na prática não envolve apenas a proteção da rede, mas sim a detecção de falhas nas comunicações e ataques que podem comprometer a infra-estrutura, bem como reagir a esses ataques. Para isso, são implementados mecanismos de proteção, como aqueles que foram mencionados nas seções anteriores. Para ilustrar uma comunicação segura, segue abaixo (figura 3):

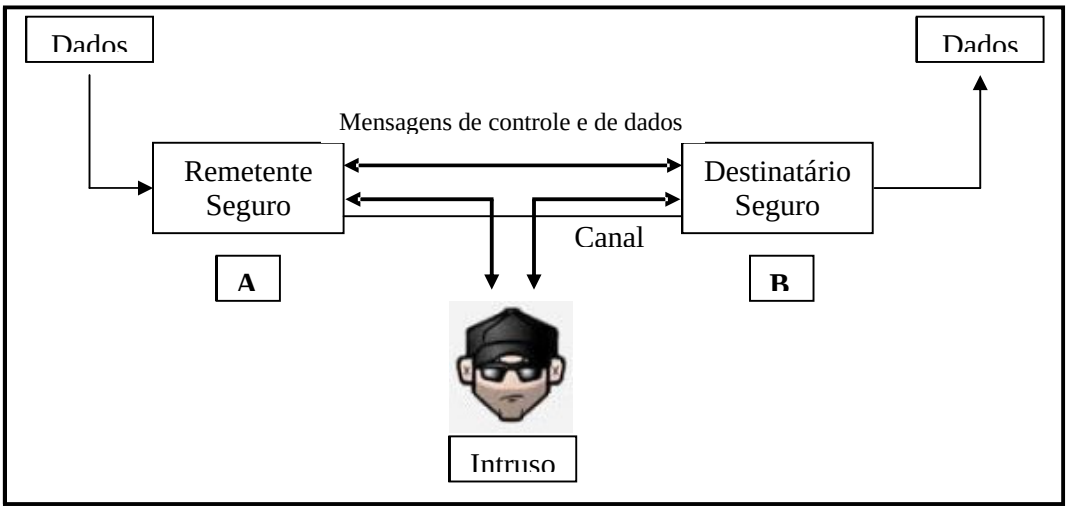

Figura 3. Remetente, destinatário e intruso.
Fonte: Keith, Ross (2006).

Nesse caso a entidade A esta tentando enviar dados a entidade B. Sendo assim, para que essa comunicação seja “segura”, além dos requisitos básicos de confidencialidade, autenticação e integridade de mensagens, também será necessário fazer um controle dos dados. Segundo Kurose e Ross (2006) todas ou algumas informações serão criptografadas, pois algum invasor pode:

a) monitorar: Ouvir e gravar as mensagens;

b) modificar: Inserir ou eliminar mensagens ou o conteúdo da mesma.

Dessa forma, o invasor pode roubar senhas e dados, fazer-se passar por outra entidade, recusar serviço a um usuário legítimo da rede sobrecarregando os recursos do sistema, entre outros desastres.

Para entender melhor à gravidade dessas ocorrências ou das conseqüências que elas podem trazer, podemos comparar as entidades A e B como sendo duas grandes organizações fazendo uma transação de comércio eletrônico. Ou até mesmo um cidadão comum querendo comprar um produto via Internet e que para isso necessita transmitir o número do seu cartão a um servidor WEB.

Essas são algumas das justificativas, que pode-se citar para ilustrar a importância e da necessidade da segurança na Internet.

Um dos principais métodos utilizados para esse fim na área da segurança é a criptografia, que além de prover Confidencialidade pelo fato de que sua função é transformar a mensagem em algo ilegível, a criptografia conforme Kurose e Ross (2006) também pode prover autenticação, integridade de mensagem, além da não repudiação e controle de acesso.

A criptografia foi um dos métodos aplicados ao protótipo desenvolvido, pois é fundamental na segurança da rede.

3.1 CRIPTOGRAFIA

Segundo Martini (2001) a criptografia existe desde que o homem se agrupou em sociedades, as quais eram mais ou menos organizadas. Ela surgiu a partir do

momento em que o homem desenvolveu a linguagem como uma forma de comunicação entre as pessoas. Desde então, utiliza-se a criptografia com a finalidade de ocultar textos ou informações a uma parte da sociedade.

Conforme Martini (2001), o uso maciço dessa técnica sempre foi característico de grupos militares que precisavam ocultar suas estratégias do inimigo. Tudo isso, para guardar em segredo dados que são considerados críticos ou sensíveis.

Para que essa técnica funcione é necessário criar códigos ou cifragens, com o objetivo de ocultar as informações, tornando-as incompreensíveis ao invasor. Em contrapartida, também é necessário fornecer ao receptor dessa informação uma chave, para decifrar tais códigos.

Dentre as várias formas de criptografia existentes, a mais simples é a chamada Cifragem ou Sistema de César, que foi inventada pelo imperador Julio César. Sendo assim, este é um dos mais antigos sistemas criptográficos documentados pela história, cuja cifragem consiste em substituir uma letra do texto por outra letra que se encontra três posições à frente no alfabeto. Dessa forma: A significa D, B significa E, C significa F e assim por diante.

“Essa forma de criptografia é chamada de criptografia monoalfabética ou substituição monoalfabética” (MARTINI, 2001, P.2).

Utilizando esse método, pode-se escrever a palavra “jogo” como segue:

J O G O

N R J R

Em sistemas desse porte, a chave para decifrar uma palavra ou uma frase é saber que deve-se avançar três letras. Mas mesmo sendo um texto ilegível, um invasor não levará muito tempo para decifrar a mensagem se souber que foi utilizada a cifra de César para codificá-la. Pois há somente 25 valores possíveis para cada chave.

Houve então, um aprimoramento dessa técnica chamada de Cifra Monoalfabética, que também substitui uma letra do alfabeto por outra. Porém, com uma significativa diferença, em vez de substituir as letras seguindo um padrão de deslocamento, a cifra monoalfabética permite substituir uma letra por outra qualquer sendo que a letra substituta deve ser previamente determinada antes do processo de encriptação, conforme figura 4.

Letra no texto aberto:	a b c d e f g h i j k l m n o p q r s t u v w x y z
Letra no texto cifrado:	m n b v c x z a s d f g h j k l p o i u y t r e w q

Figura 4. Uma cifra monoalfabética
Fonte: Kurose, Ross (2006).

Nesse caso, as possibilidades de se conseguir decifrar a mensagem foi elevada para n^2 , onde n é a quantidade de letras (as repetidas não são contadas) que a mensagem possui.

Segundo Kurose e Ross (2006), uma segunda evolução da cifra de César é a criptografia polialfabética, que faz uma mescla das duas técnicas anteriores. E possibilita substituir uma letra do alfabeto por duas ou mais letras conforme uma seqüência pré-definida. (Figura 5).

Letra no texto aberto:	a b c d e f g h i j k l m n o p q r s t u v w x y z
C_1(k=5):	f g h i j k l m n o p q r s t u v w x y z a b c d e
C_2(k=19):	t u v w x y z a b c d e f g h i j k l m n o p q r s

Figura 5. Uma cifra polialfabética que utiliza duas cifras de César.
Fonte: Kurose, Ross (2006).

Conforme (Figura 5), pode-se observar que para cada letra do alfabeto existem duas possibilidades de substituição que podem ser k=5 ou k=19, ou seja 5 ou 19 posições à frente, caracterizando uma cifra de César.

Existe também uma seqüência, onde determina-se a cifra a ser utilizada. Por exemplo, se utilizar a seqüência C1, C2, C2, C1 a palavra TESTE será transformada em: YXLYJ.

Pode-se observar que a letra E aparece duas vezes na palavra TESTE, porém a seqüência de substituição não foi à mesma, deixando duas letras com substituição alfabética diferentes.

É lógico que nos dias de hoje, esse tipo de criptografia já não é mais utilizado. “A criptografia moderna é um conhecimento científico, sistemático, coerente e formulado matematicamente” (MARTINI, 2001, P. 2).

Os algoritmos criptográficos desenvolvidos atualmente envolvem técnicas matemáticas avançadas como a fatoração de números inteiros, logaritmos discretos, entre outras que associadas ao poder computacional que existe atualmente, podem criar sistemas com um excelente nível de segurança.

“A criptografia é literalmente, o estudo da grafia secreta, ou seja, é o estudo de métodos que servem para esconder o conteúdo de mensagens ou dados armazenados” (DIAS, 2000, p.74).

Segundo o dicionário Aurélio, a criptografia é a escrita em códigos ou em cifras. Em resumo, pode-se dizer que a principal função dessa técnica é tornar um texto legível em um texto incompreensível, sendo que também são usadas regras especiais que permitem reverter o processo, voltando ao texto legível novamente. (Figuras 6 e 7).

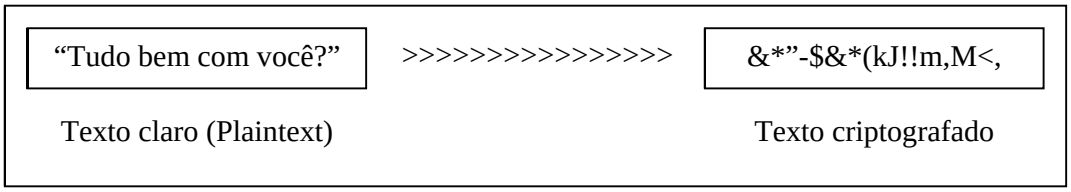

Figura 6. Processo de Encriptação.
Fonte: (Martini, 2001).

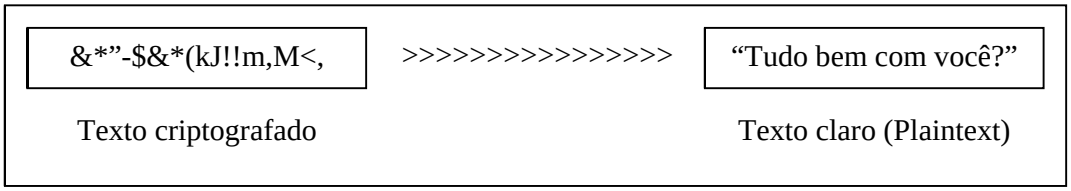

Figura 7. Processo de Desencriptação.
Fonte: (Martini, 2001).

Essas regras são chamadas de algoritmos de criptografia. “Algoritmo é um conjunto bem definido de regras que se destinam à solução de um problema qualquer e que, para isso, utilizam um conjunto finito de etapas” (MARTINI, 2001, p.3).

Um texto antes de ser criptografado, chama-se texto limpo ou texto claro. E depois de criptografado é chamado de texto criptografado ou texto cifrado. A esse processo de transformação, em que uma informação é criptografada chama-se de algoritmo de criptografia, ou cifra.

Os sistemas criptográficos utilizam esses algoritmos para proporcionar confidencialidade de dados e de informações de fluxo de dados. A vantagem da utilização desses algoritmos é que mesmo que os métodos de proteção de informações como: senhas, permissões de acesso, controle de roteamento, entre outros, falhem, os invasores não conseguirão ler a mensagem capturada.

Isso ocorre porque os dados ali contidos estão de certa forma ilegível ao invasor. Para recuperar ou disponibilizar para outra pessoa os dados que foram

criptografados, temos que reverter o processo. Sendo assim, para conseguir decifrar o que está escrito na mensagem criptografada, o invasor terá que possuir duas coisas: a chave e o algoritmo de criptografia utilizado para cifrar a mensagem.

Todos os textos referentes à criptografia mencionam a palavra chave. “As chaves são os valores secretos para codificar e decodificar mensagens” (NORTHCUTT, 2003, p.617). Esses valores variam de acordo com o tamanho da segurança que se deseja aplicar a uma informação, ou seja, quanto maior a segurança aplicada a uma determinada informação, maior também será a chave criptográfica que ela contém.

“É a chave que vai determinar como um texto legível será criptografado” (MARTINI, 2001, P.4). Sendo assim, para recuperar o texto original deve-se possuir essa chave.

Conforme Martini (2001), toda chave possui um tamanho que é expresso em *bits*. É o tamanho da chave que vai determinar o grau de segurança do texto criptografado, ou seja, quanto maior a chave maior também será a dificuldade de decifrar por criptoanálise um texto criptografado.

“Criptoanálise é um conjunto de métodos e procedimentos para decifrar uma mensagem sem o conhecimento da chave” (MARTINI, 2001, P.4).

Segundo Martini (2001), se uma chave possui um tamanho de n bits, então tem-se 2^n. Sendo assim, pode-se comparar uma chave que possui 56 bits com outra que possui 2048 bits. Logicamente considera-se que a chave de 2048 bits é computacionalmente muito mais segura. Mesmo que tentar quebrá-la por força bruta, seria necessário um grande poder de processamento e muito tempo para encontrar todas as combinações possíveis.

Utilizar força bruta, significa tentar quebrar a criptografia com várias combinações. Nesse caso, uma chave de 2048 *bits* ou seja 2^{2048} possui uma quantidade gigantesca de combinações possíveis. O fato é que o importante não é o algoritmo em si, mas sim o tamanho da chave que ele comporta.

A quantidade de chaves que o algoritmo implementa também é importante, pois dependendo da quantidade de chaves pode-se obter dois tipos diferentes de criptografia, que são: criptografia convencional ou simétrica e a criptografia assimétrica ou de chave pública, as quais serão estudadas mais a fundo nos tópicos posteriores.

A criptografia é um dos principais mecanismos de segurança existentes, que conforme Northcutt (2003) serve para dar suporte a quatro serviços de segurança importantes, que são: confidencialidade, integridade, autenticação e não rejeição. É a prática e o estudo da codificação e decodificação de informações.

Conforme Dias (2000, p. 75), “os componentes básicos que compõem um sistema criptográfico são: texto em claro, algoritmo, chave e texto cifrado”.

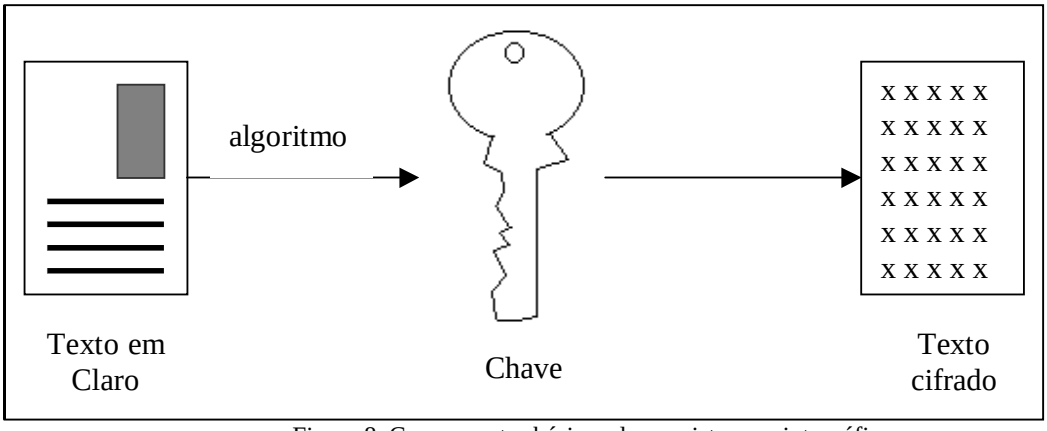

Figura 8. Componentes básicos de um sistema criptográfico.
Fonte: (DIAS, 2000).

O texto em claro corresponde à mensagem original antes de ser criptografada, ou seja, sem tratamento nenhum, que no caso pode ser lido por qualquer pessoa, por meio de qualquer editor de texto comum como o Word, por exemplo.

O texto cifrado corresponde à mensagem criptografada chamada de criptograma, depois de sofrer o processo de criptografia decorrente do algoritmo que foi executado. Nesse caso, somente poderão ler o texto as pessoas que possuem a chave e o algoritmo para decifrá-lo.

“O algoritmo nada mais é do que uma seqüência de passos e operações matemáticas que transforma o texto em claro em texto cifrado”. (Dias, 2000, p. 75).

Existem vários algoritmos com essa finalidade, entre eles os mais conhecidos segundo Peterson e Davie (2004) são: *Data Encription Standard* (DES) – Desenvolvido na década de 70 pela IBM, o Triple DES (variação do DES que utiliza três chaves criptográficas diferentes), o *International Data Encryption Algorithm* (IDEA) – desenvolvido em 1990 pelo Instituto Federal Suíço de Tecnologia e considerado um dos mais rápidos algoritmos disponíveis no mercado. O algoritmo desenvolvido por Rivest, Shamir e Adieman (RSA), capaz de implementar tamanhos variáveis de chaves, o conjunto de algoritmos que utiliza chaves de tamanho variável (família RC) e o *Message Digest* (MD), conjunto de algoritmos utilizado para garantir a integridade de dados, atualmente padrão para correio eletrônico, (*firewalls* e redes VPN).

A criptografia é um dos mais importantes mecanismos de segurança existentes, pois quando utilizada pode realizar vários serviços de segurança ao mesmo tempo, como por exemplo, uma mensagem criptografada está oculta aos olhos de pessoas não autorizadas, por isso não pode ser alterada, proporcionando integridade de

dados, e ao mesmo tempo confidencialidade de dados, pois se sabe que a mensagem está de certa forma “segura”.

Segundo Dias (2000), existem mais dois termos relacionados à criptografia, que são: a criptoanálise e a criptologia. Onde a primeira estuda as formas para poder invadir sistemas criptografados, enquanto que a segunda realiza as duas coisas, a criptografia e a criptoanálise, ou seja, tanto estuda formas para criptografar uma informação, como também para decifrá-la.

Depois da criptografia, ainda existem muitos outros mecanismos de proteção utilizados para proporcionar segurança de informações.

Conforme Dias (2000) entre os mais conhecidos estão:

a) assinatura digital: esse mecanismo é formado por um procedimento de assinatura propriamente dita e outro de verificação de assinatura, permitindo assim, a proteção das partes envolvidas quanto à violação da autenticidade de uma delas e da integridade da mensagem;
b) mecanismos de controle de acesso: com esse mecanismo, o proprietário é quem determina quem e como vai poder acessar determinados recursos da organização. Para isso, ele utiliza listas com permissões, capacidade de cada um, entre outras informações;
c) mecanismo de integridade de dados: é o mecanismo que provê a proteção contra modificação de dados;
d) mecanismo de disponibilidade: são mecanismos que servem para disponibilizar os dados ao usuário, mesmo quando ocorrer um incidente, como uma falha ou invasão ao sistema. Entre os mecanismos de disponibilidade mais conhecidos, temos o backup e recuperação de dados, sistemas e a replicação de equipamentos.

e) trocas de autenticações: é a troca de mensagens criptografadas entre duas entidades, formando uma espécie de protocolo, onde uma entidade faz a autenticação de uma outra entidade, que necessita solicitar o acesso a algum recurso.

f) enchimento de tráfego: é um mecanismo que gera varias mensagens (sem nenhuma utilidade) aleatórias na rede, confundindo os invasores e dificultando na identificação dos nós mais importantes da rede, pois aumenta o tráfego de dados. Esse mecanismo é utilizado em conjunto com sistemas criptográficos para proporcionar confidencialidade das informações de fluxo de dados, impedindo a análise de tráfego na rede. Porém não é muito utilizado, pois causa uma queda no desempenho do sistema, decorrente do número imenso de mensagens inúteis que são geradas.

g) controles de roteamento: é o mecanismo utilizado para impedir que dados importantes trafeguem por rotas inseguras. Esse controle escolhe o melhor caminho a ser trafegado pelo dado, impedindo a sua entrada em caminhos que não sejam confiáveis.

3.2 ALGORITMOS DE CRIPTOGRAFIA

Os algoritmos de criptografia, como mencionado nos tópicos anteriores, utilizam-se de fórmulas matemáticas para transformar uma mensagem ou um texto legível em algo ininteligível aos olhos do invasor. Ocultando assim, informações importantes, protegendo os dados de pessoas não autorizadas, proporcionando integridade e confiabilidade das informações.

Existem duas categorias de algoritmos, que segundo Northcutt (2003), são técnicas de criptografia muito importantes que são: o algoritmo de chave simétrica e o algoritmo de chave assimétrica.

3.2.1 Algoritmo simétrico – chave compartilhada

Uma chave compartilhada ou chave simétrica é aquela que utiliza o mesmo valor para codificar e decodificar uma informação. Nesse caso para aplicar um algoritmo simétrico, considera-se que as organizações envolvidas na troca de mensagens conheçam com antecedência o valor da chave utilizada.

Como os valores das chaves são sempre as mesmas, esse processo de criptografia se torna bastante rápido, tendo em vista que a matemática utilizada nesses tipos de algoritmos para se criar um texto cifrado a partir de uma chave secreta compartilhada, não é tão complexo quanto à implementação dos algoritmos assimétricos.

Porém, segundo Northcutt (2003) “existe a desvantagem de que com a utilização desse tipo de algoritmo fica difícil trocar mensagens ou iniciar uma troca simétrica com um parceiro desconhecido”.

Essa questão é complicada, pois nesse caso seria necessário possuir um canal seguro para enviar essa chave compartilhada, caso contrario não teria o porque de criptografar uma mensagem utilizando esse método, pois se a chave compartilhada estiver disponível na rede, qualquer pessoa com conhecimentos apurados na área computacional, pode utilizar a mesma para decifrar a informação.

Mesmo assim, o algoritmo simétrico é um método que proporciona confidencialidade dos dados, enquanto sua chave permanecer secreta.

Entre os vários tipos de algoritmos simétricos existentes e disponíveis, os mais utilizados atualmente pelas Redes Privadas Virtuais (VPNs) são: *Data Encription Standard* (DES) e uma versão atualizada do DES, chamada de 3DES. O DES segundo (NORTHCUTT, 2003, p.618) “é um padrão de criptografia definido pelo *National Institute of Standards and Technology* (NIST) em 1977. O DES é um algoritmo simétrico com uma chave de 56 bits, parecia invencível com a tecnologia da época”.

Com o avanço da tecnologia associada ao grande poder de processamento hoje existente, o DES já foi vencido várias vezes. A partir desse fato, fica difícil dizer se o DES continua sendo adequado para se utilizar em VPN.

Tudo vai depender do custo/beneficio que esse algoritmo vai trazer a organização, ou seja, é necessário pesar o valor gasto nessa tecnologia, com o valor gasto para recuperar as informações que se deseja proteger. Pois muitas vezes não compensa investir muito em informações rotineiras, sem muita importância.

“Muitas organizações ainda utilizam o DES para transação de informações do tipo padrão como seus algoritmos de VPN” (Northcutt; 2003, p.619). Por outro lado, sendo que esse tipo de algoritmo já foi quebrado várias vezes, também não é recomendável a utilização do mesmo para instituições financeiras ou para a troca de mensagens altamente secretas, como é o caso das organizações militares.

Para organizações desse tipo o meio termo é a utilização do 3DES, que utiliza três chaves de 56 bits cada uma, gerando uma chave de 168 bits. Isso garante uma maior segurança. Mesmo assim, como o DES foi quebrado, surgiu à necessidade da criação de um novo algoritmo criptográfico para trazer uma maior proteção às informações.

Segundo Kurose e Ross (2006), em Novembro de 2001 foi lançado o sucessor de DES, também chamado de Padrão Avançado de Criptografia, originado da denominação em inglês *Advanced Encryption Standard (*AES).

O AES é um algoritmo simétrico criado por Rijndael, que processa dados em blocos de 128 bits e que também pode funcionar com chaves de 128, 192 e 256 bits de comprimento.

"O NIST estima que uma máquina que conseguisse quebrar o DES de 56 bits em 1 segundo (isto é, experimentar 2^{55} chaves por segundo), levaria aproximadamente 145 trilhões de anos para quebrar uma chave AES de 128 bits". (KUROSE; ROSS, 2006, p.520). Portanto é considerado o futuro da criptografia simétrica.

Por enquanto, o 3DES é ainda uma das melhores opções de algoritmo simétrico existente, porém não significa que todas as empresas necessitam utilizá-lo, pois como foi mencionado anteriormente, isso vai depender da aplicação ou da informação que esse algoritmo vai proteger.

Conforme afirma Northcutt (2003), os algoritmos simétricos são importantes porque fornecem o componente de confidencialidade que a VPN oferece. Além disso é o algoritmo de proteção mais rápido, para a vasta quantidade de informações que trafegam na rede de uma VPN.

3.2.2 Algoritmo assimétrico – chave pública/ privada

Desde a época da cifra de César, até a década de 1970 a comunicação cifrada utilizava a chave simétrica. A dificuldade que essa técnica apresentava é que as

duas partes (remetente e destinatário) teriam que concordar com a chave a ser compartilhada.

Para isso, seria necessária uma comunicação pessoal de forma segura, para depois se comunicar de forma cifrada.

Atualmente isso pode ser até mesmo impossível, sendo que o mundo está ligado à rede e a comunicação pessoal é quase impossível. As duas partes comunicantes podem nunca terem se conhecido a não ser pela rede.

Portanto, a necessidade agora era achar uma forma de comunicação, sem compartilhar a chave secreta e conhecida pela rede.

Foi na época de 1976, que Diffie e Hellman apresentaram um algoritmo com esse propósito e que segundo Kurose e Ross (2006), levou ao desenvolvimento dos sistemas criptográficos de chaves públicas existentes atualmente.

Os algoritmos assimétricos, são aqueles que possuem duas chaves diferentes. Uma pública que serve para criptografar a informação, ou texto claro em texto cifrado. E uma privada para decifrar essas informações ou transformar o texto cifrado no texto original novamente.

> As vantagens de criptografia por chave pública são usadas para permitir a criação de uma conexão externa sem conhecimento anterior. Essa conexão é usada para se passar informações vitais de chave simétrica e dados de configuração que não podem ser transferidos com segurança de outra maneira. Depois poderá ser iniciada a comunicação com algoritmo simétrico. (NORTHCUTT, 2003, p.620).

O relacionamento entre essas duas chaves acontece da seguinte forma: A chave pública não pode ser usada para reverter o processo da chave privada. Porém, qualquer informação criptografada por uma cópia da chave pública, poderá ser decifrada pela pessoa que possui a chave privada da mesma.

Para exemplificar esse conceito, digamos que as entidades A e B desejam utilizar a criptografia de chave pública. Ao invés das duas entidades compartilharem

uma única chave (como acontece no caso do sistema de chave simétrica), a entidade B (destinatário) vai possuir duas chaves. Uma pública, que pode estar à disposição de todos (inclusive de invasores), e uma privada que apenas a entidade B conhece.

Para iniciar a comunicação, a entidade A utiliza a chave pública da entidade B e um algoritmo criptográfico (padronizado) para criptografar a mensagem e posteriormente enviar a entidade B.

A entidade B por sua vez, ao receber a mensagem criptografada utiliza sua chave privada, juntamente com um algoritmo de decriptação (também padronizado) e obtém a mensagem original. Nesse caso, não foi preciso haver a troca da chave secreta entre as partes comunicantes.

Por essa razão, a implementação desse tipo de algoritmo é muito mais difícil do que a dos algoritmos simétricos, sendo que a matemática utilizada nos algoritmos assimétricos é muito mais profunda e complexa. Por isso, os algoritmos assimétricos também são mais lentos e requerem um maior poder de processamento.

Com esse tipo de algoritmo pode-se garantir a confidencialidade dos dados, pois a chave pública não compromete o texto cifrado. Porém, não resolve o problema da troca de mensagens entre desconhecidos.

Existem portanto, duas preocupações quando é utilizado esse tipo de criptografia. Primeiro, além de ser um algoritmo lento em termos de processamento, um intruso que consiga interceptar a comunicação entre a entidade A e B, pode não entender a mensagem, mas pode utilizar o algoritmo de criptografia e a chave pública (disponível a todos), para criptografar qualquer tipo de mensagem e enviar a entidade B.

A segunda preocupação é que o intruso pode se fazer passar pelo remetente (no caso, a entidade A). Na criptografia simétrica isso não ocorre, sendo que

compartilhar uma única chave secreta, fica implícito o reconhecimento do remetente ao destinatário.

Mas com a utilização da criptografia de chave pública, qualquer um pode cifrar uma mensagem utilizando a chave pública da entidade B.

Para isso foi criado o conceito de Autoridades Certificadoras (CA) e Assinatura Digital, que vincula o remetente a uma chave ou a uma mensagem respectivamente.

Um exemplo dado por Northcutt (2003) sobre criptografia assimétrica é o *Pretty Good Privacy* (PGP). Esse é um meio de trocar mensagens com segurança, além de poder conhecer a pessoa com quem se está comunicando. Para isso ele utiliza um servidor de chaves públicas, a fim de disponibiliza-las publicamente. Então no momento em que alguém pretender realizar uma comunicação enviando uma chave publica, e este tiver colocado sua chave nesse servidor, será possível identificar a pessoa através de seu e-mail ou até mesmo pelo próprio nome. Depois disso pode-se começar a comunicação entre as partes.

Conforme (NORTHCUTT, 2003, p.620) “entre os algoritmos assimétricos existentes, os mais conhecidos e usados são: o Diffie-Hellman e o algoritmo de chave publica criado por Rivest, Shamir e Adelman (RSA)”.

O primeiro foi criado por Whitfield Diffie e Martin Hellman em 1976, esse foi o primeiro algoritmo assimétrico desenvolvido. Ele faz parte de um protocolo de troca de chaves chamado de Oakley, sendo bastante utilizado na tecnologia VPN.

O RSA (criado por Ron Rivest, Shamir e Adelman) é um dos principais algoritmos assimétricos, que segundo (KUROSE e ROSS, 2006) se tornou quase um sinônimo de criptografia de chave pública. Portanto, é importante um conhecimento mais profundo de como ele funciona.

Primeiro, é necessário saber que a chave pública e a chave privada estão respectivamente relacionadas ao algoritmo de criptografia e decriptação. Sendo assim, segundo (KUROSE e ROSS, 2006), deve-se seguir os seguintes passos: Para escolher as chaves pública e privada, a entidade B (destinatário) deve:

a) escolher dois números p, q. Sendo que quanto maior o valor de ambos, mais lento será o processo para codificar e decodificar uma informação;
b) computar $n = p.q$ e $z = (p - 1).(q - 1)$;
c) escolher uma letra *e* menor do que *n* que não tenha fatores comuns (exceto o 1) com *z*. A letra *e* será utilizada na encriptação dos dados;
d) escolher um numero *d* tal que $e.d - 1$ seja divisível exatamente (sem que haja resto) por *z*. A letra *d* será utilizada na decriptação dos dados. Em outras palavras, pode-se dizer que dado *e*, escolhe-se *d* tal que o resto da divisão de *e.d* por *z* seja o numero inteiro 1.

A chave pública nesse caso é o par de números (*n*,*e*), a qual a entidade B coloca a disposição de todos. E a chave privada é o par de números (*n*,*d*), que deve pertencer somente à entidade B. Sendo assim o processo de criptografia e decriptação funciona da seguinte forma:

a) caso a entidade A queira enviar um numero *m* tal que $m < n$, para codificar a entidade A calcula a potência m^e e então, determina o resto inteiro a divisão de m^e por *n*. Assim, o valor cifrado *c* da mensagem em texto aberto *m*, que a entidade A envia é: $c = m^e \bmod n$.
b) para decifrar a mensagem do texto cifrado recebido *c*, a entidade B processa: $m = c^d \bmod n$, (que exige o uso de sua chave secreta (*n*,*d*)).

O RSA só não é totalmente seguro pelo fato de ainda não se conhecer um algoritmo para fatorar rapidamente um número. Pois se alguém conhecesse os números *p* e *q*, dado o valor publico *e*, poderia achar a chave secreta *d*.

A fusão dos dois algoritmos, o simétrico e o assimétrico é uma ótima saída para fazer a troca de informações de chave utilizando a tecnologia VPN. Pois o algoritmo assimétrico, apesar de ser lento, possui um meio mais confiável na troca de chaves na fase inicial da negociação. Enquanto que os algoritmos simétricos são exatamente ao contrário, eles possuem problemas nas trocas de chaves, mas é um algoritmo veloz durante a comunicação.

Nesse caso, basta unir a confiabilidade dos algoritmos assimétricos, com a velocidade dos algoritmos simétricos, para adquirir uma troca de chaves e uma comunicação de forma excelente.

3.3 CERTIFICADOS DIGITAIS

O certificado digital é um método considerado muito importante na área de segurança em sistemas desenvolvidos para web. Um certificado digital, garante ao usuário que a comunicação realizada entre ele e o servidor de um site seja feita de forma segura.

Essa segurança é conseguida por meio do processo de autenticação, que será solicitada no início do acesso, antes mesmo da troca de informações pela rede.

3.3.1 Autenticação

Os seres humanos autenticam-se uns aos outros por meio de várias maneiras, pelo rosto quando se encontram, pela voz ao telefone ou por documentos.

“Autenticação é o processo de provar a própria identidade a alguém”. (KUROSE; ROSS, 2006, p.525).

Isso é muito importante durante uma comunicação pela rede e muito utilizado, quando uma parte deseja se autenticar a uma outra parte quando ambas estão se comunicando.

Nesse caso é necessário que se utilize um certificado digital, onde as partes envolvidas, não mais podem confiar em informações como a aparência visual ou a voz. Mas ao invés disso, a autenticação deve ser feita com base em mensagens e dados trocados como parte de um protocolo de autenticação.

Muitas vezes, os participantes dessa comunicação são os próprios componentes da rede, como roteadores e processos Cliente – Servidor que devem se autenticar mutuamente.

O protocolo de autenticação, segundo Kurose e Ross (2006) é executado antes que as duas partes executem qualquer outro protocolo. Sendo assim, primeiro é garantida a identidade das partes para depois serem executadas as tarefas dos outros protocolos, como o protocolo de transferência confiável de dados, protocolo de troca de informações de roteamento ou o protocolo de e-mail.

3.3.2 Integridade

No mundo real, quando se assina um cheque, um comprovante de operação de cartões de créditos, documentos ou cartas, esta se atestando de que o conteúdo é conhecido e/ou de que concorda se com o que está escrito.

No mundo digital, também existe uma técnica que comprova o verdadeiro dono de um documento. Essa técnica chama-se assinatura digital.

Essa técnica tem a função de comprovar a veracidade de um documento, assim como acontece com as assinaturas por escrito. “A Assinatura Digital deve ser verificável, não falsificável e incontestável”. (KUROSE; ROSS, 2006, p.531).

Isso significa dizer que, será possível provar que um documento assinado por um indivíduo, foi na verdade assinado por ele e que somente aquele indivíduo poderia ter assinado o documento.

3.3.3 Geração de assinaturas digitais

Supondo-se que a entidade B queira assinar digitalmente um documento (arquivo ou mensagem) e enviar para a entidade A. Para isso, basta à entidade B utilizar uma chave privada.

Isso pode parecer estranho, pois se sabe que a chave privada é normalmente utilizada para decriptar uma informação cifrada pela chave pública.

Mas conforme Kurose e Ross (2006), tem-se que lembrar de que a criptografia e a decriptação, nada mais é do que um cálculo matemático e que a intenção da entidade B não é embaralhar o documento. É somente assiná-lo para que o destinatário tenha certeza de que foi ele quem o enviou.

Nesse caso, a entidade B tem o documento *m* e sua assinatura digital do documento $K_b^-(m)$. Figura9:

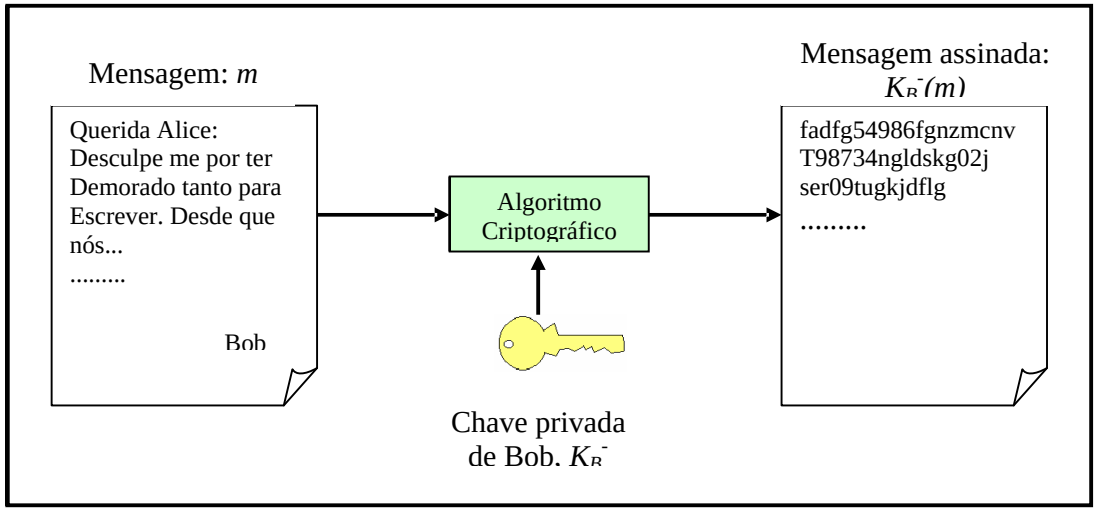

Figura 9. Criação de uma assinatura digital para um documento
Fonte: Kurose, Ross (2006).

Ao receber o documento, diga-se que a entidade A quer provar a veracidade do documento para se certificar de que não esteja falsificado e de que o remetente foi realmente à entidade B.

Para isso, segundo Kurose e Ross (2006) basta aplicar a chave pública (aquela que a entidade B disponibilizou para todos) na assinatura digital que esta associada ao documento. Dessa forma, a entidade A consegue fazer o processo inverso, obtendo o documento original novamente.

Portanto, agora a entidade A tem a certeza de que foi realmente a entidade B que enviou o documento e pode provar o seu argumento pelos seguintes motivos:

a) somente a entidade B é quem possui a chave privada, à qual foi utilizada para processar o documento;
b) somente uma cópia da chave pública disponibilizada pela entidade B é que pode decifrar o documento.

3.3.4 Resumos de mensagem

A preocupação da aplicação da técnica de assinatura digital através da criptografia é que criptografar e decriptografar uma informação, podem dispender um longo tempo de processamento em termos computacionais.

Portanto dependendo da importância do documento, não seria necessário criptografar o documento inteiro, pois os requisitos principais nesse caso são:

a) garantir que o remetente é realmente quem diz ser e que essa assinatura possa ser verificada;

b) garantir que os dados não foram alterados desde que o remetente os criou e assinou.

Nesses casos, como afirma Kurose e Ross (2006) a aplicação da criptografia no documento inteiro seria considerado um exagero.

Uma solução adequada e que atinge os mesmos objetivos é aplicar a criptografia em apenas um pedaço do texto, ou como é chamado segundo Kurose e Ross (2006) resumo de mensagem.

> "O resumo de mensagem é muito parecido com uma soma de verificação. Algoritmos de resumo da mensagem pegam uma mensagem *m*, de comprimento arbitrário e calculam uma "impressão digital" dos dados, com comprimento fixo, conhecido como resumo de mensagem H(m)". (KUROSE; ROSS, 2006, p.533).

Sendo assim, o resumo da mensagem protege os dados originais, pois caso algum dado seja modificado transformando a mensagem de *m* para *m*', então a mensagem H(*m*) (resultado do processo do resumo da mensagem) não será compatível com o resumo H(*m*') (modificado) processado sobre os dados modificados *m*'.

O intento nesse caso é ilustrar que ao invés de criptografar todo um documento, pode-se apenas criptografar parte dele e mesmo assim poder obter os mesmos resultados de confidencialidade, integridade e autenticação.

3.3.5 Distribuição de chaves e certificados

Uma outra forma para se resolver os problemas encontrados com a criptografia simétrica e assimétrica, são os conceitos de distribuição de chaves e certificação respectivamente.

Como verificado anteriormente, a comunicação de chave simétrica necessita de que as partes envolvidas concordem com a chave secreta previamente e que a transmissão da chave deve passar por um canal seguro, visto que a mesma serve tanto para criptografar como para decriptar a informação.

Conforme Kurose e Ross (2006) uma outra alternativa para a comunicação segura através da criptografia simétrica é a Central de Distribuição de Chaves (*Key Distribution Center* – KDC), que conforme Kurose e Ross (2006) é uma entidade de rede única e de confiança com a qual o usuário estabelece uma chave secreta a ser compartilhada. Sendo assim, uma entidade A pode utilizar a KDC para obter as chaves secretas que necessitam e estabelecer uma comunicação segura com outras entidades da rede.

A KDC é um servidor que compartilha uma chave simétrica única com seus usuários. Mas para isso, o usuário necessita ser registrado. A chave é instalada manualmente no servidor no momento em que o usuário se cadastrar pela primeira vez.

Dessa forma, a KDC conhece a chave secreta de cada usuário registrado. E após o usuário se cadastrar utilizando sua chave, o usuário pode se comunicar com segurança com a KDC usando essa chave.

Então, quando algum usuário desejar se comunicar com outro usuário (ambos registrados), este vai entrar em contato com a KDC que por sua vez, vai fornecer uma chave única para que a comunicação seja feita com segurança. Mas como

o próprio nome diz, a chave é única, ou seja, a chave que a KDC fornece vale apenas durante aquela comunicação.

Já o problema que ocorre com a criptografia assimétrica é outro. Como mencionado anteriormente, na comunicação utilizando uma criptografia de chave pública, não é necessário fazer uma troca de chaves entre as partes envolvidas.

Pois para enviar uma mensagem criptografada à entidade B, a entidade A utiliza a chave pública da entidade B, sem ter que conhecer a chave secreta de B e nem a entidade B, necessita conhecer a entidade A. Portanto o KDC não é necessário nesse tipo de comunicação.

Porém, por se tratar de criptografia de chaves públicas, as entidades comunicantes (principalmente o destinatário) precisam trocar chaves públicas na rede.

Sabendo que essa chave esta disponível a todos, um invasor pode utilizar essa chave para criptografar uma informação e fazer-se passar por outra pessoa.

Por essa razão, quando as entidades estão se comunicando, é necessário que a entidade A tenha certeza de que a chave pública, a qual esta utilizando é realmente da entidade B.

Para essa finalidade, foi criada uma entidade chamada de Autoridade Certificadora (*Certification Authority* – CA), cuja função é validar identidades e emitir relatórios. Ou melhor dizendo, verifica se uma entidade é quem diz ser.

Assim que a CA identifica a identidade da entidade, ela cria um certificado que vincula à entidade à identidade verificada.

“O certificado contém a chave pública e a informação exclusiva que identifica mundialmente o proprietário da chave pública.” (KUROSE; ROSS, 2006, p.540).

Agora a entidade A pode começar a comunicação segura com a entidade B. Então ela recebe um pedido da entidade B, obtém o seu certificado e usa a chave pública da CA para verificar a validade do certificado de B assinado pelo CA.

Essa é a forma da entidade A saber se realmente esta se comunicando com a entidade B.

3.4 PROTOCOLOS SEGUROS

Os algoritmos criptográficos, são apenas uma parte do processo para a implementação da segurança em uma rede. O próximo passo conforme Peterson e Davie (2004) que se deve fazer é vincular esses mecanismos em conjunto com protocolos para solucionar os diversos problemas de segurança, tais como: Autenticação de participantes, técnicas para garantir a integridade das mensagens e algumas técnicas para solucionar o problema da distribuição de chaves.

3.4.1 Protocolos de autenticação

Antes que duas entidades estabeleçam um canal seguro para iniciar uma comunicação, ou seja, utilizando por exemplo um algoritmo simétrico como o DES, elas geralmente desejam saber se a outra entidade é realmente quem diz ser.

No contexto de protocolos, pode-se substituir as duas entidades como sendo um relacionamento entre cliente e servidor. Onde o acesso remoto do cliente para excluir ou alterar algum arquivo vai depender da certificação do servidor, que vai autorizar ou não esse processo, dependendo do resultado da sua autenticidade.

Da mesma forma, um cliente também pode querer se certificar que está enviando dados ao servidor desejado, pois pode correr o risco de pensar estar mandando dados ao servidor de arquivos, mas que na verdade é um processo intruso.

Conforme Kurose e Ross (2006), pode-se implementar serviços de segurança em rede através das quatro camadas superiores da pilha de protocolos da Internet, que são: aplicação, transporte, rede e enlace.

Deve-se saber, a importância da implementação da segurança, tanto nas camadas mais baixas, como também nas camadas mais altas.

Começando pela camada mais alta da pilha, ou seja, a camada de aplicação, onde pode-se exemplificá-la através da troca de e-mails seguros entre duas entidades A e B.

Considerando que a entidade A deseja trocar e-mail seguro com a entidade B e que o objetivo principal dessa segurança, seja somente a confidencialidade (que ninguém consiga ler a mensagem).

Uma forma mais prática é a utilização de um algoritmo de chave simétrica, como por exemplo o DES, que possuindo uma chave grande e que somente A e B possuírem a chave, então um intruso não conseguira ler a mensagem.

Outra forma, seria a utilização das chaves públicas, onde o remetente A criptografa a mensagem utilizando a chave pública (disponível pelo destinatário B). Assim o destinatário B ao decriptar a informação com sua chave privada pode admitir que a mensagem pertence ao remetente A.

Mas dependendo do tamanho da chave, visto que a implementação da chave pública envolve na maioria dos casos uma chave muito longa. Ela torna o processo, um tanto quanto ineficiente. Principalmente nos dias atuais, onde as mensagens de e-mail

estão cada vez maiores em decorrência dos anexos que envolvem imagens, áudio e vídeo.

A solução mais completa para se adquirir confidencialidade na troca de e-mails, seria mesclar os dois tipos de chaves: simétrica e assimétrica. Dessa forma segundo Kurose e Ross (2006), a entidade A executa os seguintes passos:

a) escolha uma chave simétrica Ks;
b) criptografa sua mensagem *m* com a chave simétrica;
c) criptografa a chave simétrica com a chave pública;
d) concatena a mensagem criptografada e a chave simétrica criptografada formando apenas um pacote;
e) envia o pacote ao endereço de e-mail da entidade B.

Assim, quando a entidade B recebe o e-mail, deve executar os seguintes passos:

a) usar sua chave privada K_b^- para obter a chave simétrica Ks;
b) utilizar a chave simétrica Ks para decriptar a mensagem *m*.

Observe a Figura 10:

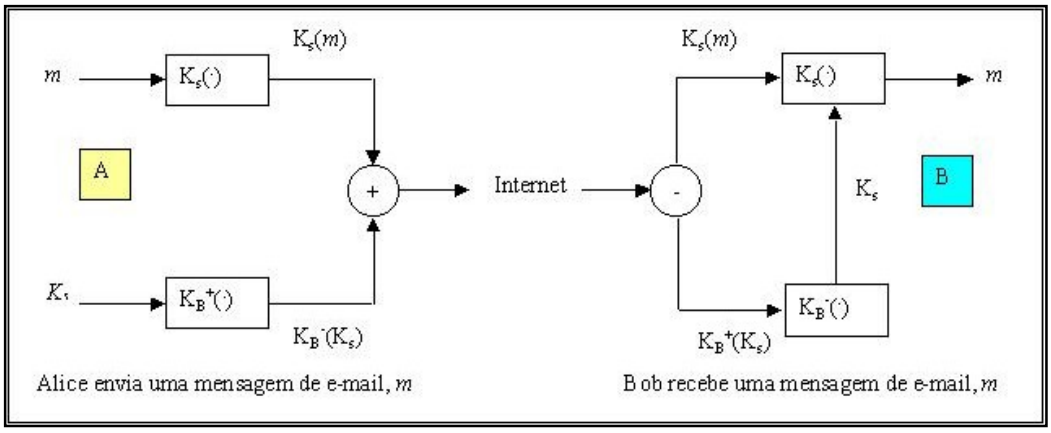

Figura 10. A usa uma chave Simétrica KS, para enviar um e-mail secreto para B
Fonte: Kurose; Ross (2006).

Sendo assim, tem-se um sistema de e-mail seguro que nos fornece confidencialidade. Portanto, podemos criar outro que nos forneça os requisitos de autenticação e integridade, para que o destinatário B tenha certeza de que a mensagem que recebeu, tenha vindo de entidade A e que seu conteúdo não tenha sido alterado durante o trajeto.

Nesse caso, a confidencialidade dos dados não é levada em consideração. Para isso, é utilizada a assinatura digital, juntamente com resumos de mensagem. Dessa forma, o remetente A executará os seguintes passos:

a) aplica a função de hash H a uma mensagem *m*, para obter o resumo da mensagem H(*m*);
b) assina o resultado da função de hash com a sua chave privada K_A^- para criar uma assinatura digital $K_A^-(H(m))$;
c) concatena a mensagem original com a assinatura digital formando um pacote;
d) envia o pacote ao endereço de e-mail da entidade B.

B por sua vez, ao receber o pacote executa os seguintes passos:

a) aplica a chave publica de A K_A^+, ao resumo da mensagem assinado;
b) compara o resultado dessa operação com o próprio hash H da mensagem.

Segundo Kurose e Ross (2006), se os dois resultados forem iguais, então B terá uma garantia de que a mensagem é da entidade A e que seu conteúdo não foi alterado. Figura 11:

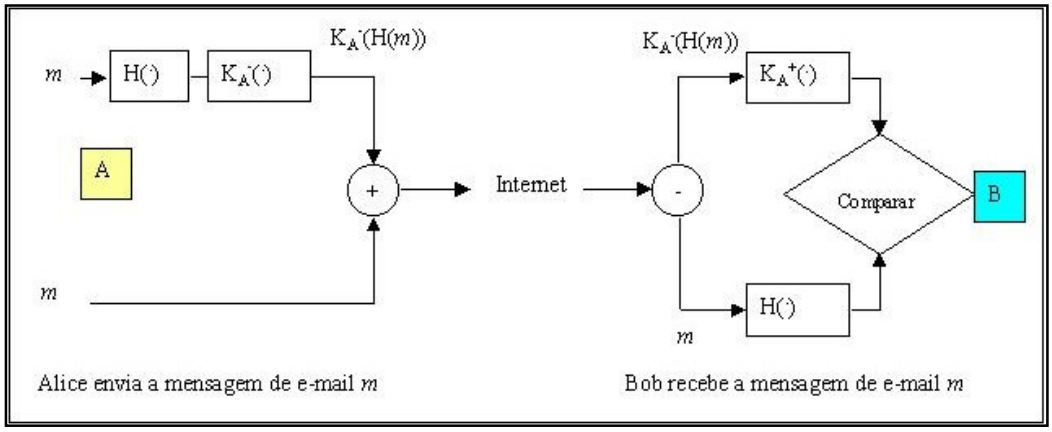

Figura 11. Utilização de funções de hash e assinaturas digitais.
Fonte: Kurose; Ross (2006).

Por fim, também se pode criar um sistema de e-mail seguro por completo, ou seja, que fornece todos os requisitos de confidencialidade, autenticação e integridade de mensagem. Para tanto basta combinar os procedimentos executados nas Figuras 10 e 11. Para isso, são executados os seguintes passos:

a) a entidade A cria um pacote idêntico ao da Figura 11, ou seja, com a mensagem original junto com o hash da mensagem assinado digitalmente;
b) após isso, a entidade A trata esse pacote como sendo uma mensagem comum e envia a mesma em conjunto com os processos utilizados na Figura 10, criando assim um novo pacote;
c) envia o novo pacote a entidade B;

A entidade B então, recebe o pacote e aplica primeiramente os mesmos processos da Figura 10 e posteriormente os processos da Figura 11.

Sendo assim, temos um sistema de envio de e-mail que atende a todos os requisitos: confidencialidade, autenticação e integridade. Porém, conforme Kurose e Ross (2006) não se pode definir como sendo seguro por completo, pois nesse esquema existem várias trocas de chaves públicas entre remetente e destinatário.

Conforme abordado nas seções anteriores, um intruso pode utilizar a chave pública de uma das entidades para criptografar a mensagem e fazer-se passar por uma delas. Esse tipo de problema, conforme já visto, pode ser solucionado com a utilização de uma Autoridade Certificadora.

3.4.2 Camada de sockets de segurança (SSL) e segurança na camada de transporte (TSL)

A camada de transporte esta localizada logo abaixo da camada de aplicação. Através de sockets seguros (SSL) e uma camada de transporte segura (TSL), pode-se obter um protocolo de transporte seguro HTTPS.

Para ilustrar na prática uma aplicação com esse tipo de protocolo, pode-se abordar o seguinte tema: Comércio na Internet.

Supondo-se que uma entidade A deseja fazer uma compra via Internet. Para tanto, a entidade A entra em um site e encontra o produto que deseja.

Para comprar esse produto é apresentado um formulário onde à entidade A deve fornecer várias informações, tais como: endereço, quantidade desejada, número do cartão de crédito, entre outras.

Após confirmar essas informações, a entidade A então aguarda o recebimento do produto através do correio, bem como a cobrança na próxima fatura de seu cartão de crédito.

Segundo Kurose e Ross (2006), todo esse processo parece seguro se forem tomadas às medidas de segurança. Do contrário, podem ocorrer os seguintes problemas:

a) um intruso pode interceptar esse pedido de compra, juntamente com o número do cartão e as outras informações. Sendo assim, poderá fazer compras na conta da entidade A;

b) o site pode conter o logotipo de uma empresa famosa, mas que na verdade foi desenvolvido ou esta sendo mantido por um intruso, se fazendo passar pela empresa designada. Dessa forma, o intruso pode roubar ou fazer compras enviando a fatura para a conta da entidade A.

O protocolo SSL se propõe a resolver esses problemas. Segundo Kurose e Ross (2006) a SSL é um protocolo projetado para fornecer criptografia de dados e autenticação entre cliente e um servidor WEB.

O SSL começa com uma fase de apresentação que autentica o servidor ao cliente através da troca de algoritmos criptográficos e suas respectivas chaves. O Cliente também pode ser autenticado junto ao servidor com a mesma técnica.

Após a apresentação, então inicia-se a transmissão dos dados de forma criptografada, usando chaves de sessão negociadas durante a apresentação.

O protocolo SSL é à base da Segurança da Camada de Transporte - *Transport Layer Security* (TLS). Fica situado entre a camada de aplicação e a camada de transporte.

“No lado remetente, o protocolo SSL recebe dados (como uma mensagem HTTP ou IMAP vinda de uma aplicação), criptografa-os e direciona os dados criptografados a um socket TCP. No lado receptor, o SSL lê socket TCP, decripta os dados e os direciona a aplicação” (KUROSE; ROSS, 2006, p.555).

4 AMBIENTE EDUCACIONAL

Basicamente, o ambiente educacional é composto pelas pessoas e pela própria estrutura física. Em relação às pessoas, o ambiente educacional é formado por alunos, professores, diretores, secretárias, coordenadores, faxineiras, entre outros componentes. Sobre a estrutura física se pode citar as salas de aula, diretoria, secretaria, ginásio de esportes, departamentos, biblioteca, lanchonete, entre outros recintos.

Toda instituição de ensino é um ambiente educacional, tendo como objetivo primordial à aquisição e construção de conhecimentos, seja essa instituição uma escola de ensino fundamental, médio ou superior. A informação então é passada do professor para aluno, o qual será cobrado pelo aprendizado adquirido.

A forma de cobrança vai depender do professor e da instituição a qual ele está lecionando, cujos meios são: avaliações, participação em sala de aula, entre outros.

Para registro desses meios avaliativos, tem se o chamado diário de classe, onde o professor registra e controla as notas e ao final de cada bimestre ou semestre (dependendo da instituição em questão), gera-se a média resultante a partir do processo de soma e divisão das notas obtidas pelo aluno no decorrer de cada período. Normalmente, a média, na maioria das instituições de ensino não pode ser inferior a 7 (sete).

A assiduidade do aluno também é levada em consideração, conforme artigo 7º da resolução nº 23/2000/CEE/SC o aluno precisa ter freqüentado 75% (setenta e cinco por cento), das aulas dadas. Caso contrário será reprovado por faltas. O controle de faltas geralmente é realizado através do diário de freqüência, contendo o nome do aluno, a data em questão e a quantidade de presença e faltas do mesmo nas aulas.

Ao final de cada bimestre ou semestre (isso dependo da instituição em questão), será entregue um boletim ou um relatório com todas as notas (médias de cada aluno), seguido também da quantidade de faltas obtidas pelo aluno. Se ao final do ano letivo, todas as médias de cada matéria forem maior ou igual a 7 (sete) e a assiduidade for maior ou igual a 75% (setenta e cinco por cento), então o aluno está aprovado, ou seja, está apto a freqüentar o próximo nível, também chamado de série ou fase. Caso contrário, terá de repetir o ano ou a disciplina em questão, dependendo do projeto político pedagógico de cada instituição.

Ao final do ensino fundamental, o aluno receberá um diploma, o qual certifica a sua aprendizagem em determinada instituição, mostrando estar apto a seguir em frente nas próximas fases ou seguir para o mercado de trabalho. Também ao final de cada curso, o aluno recebe o seu histórico escolar, onde constam todas as médias finais do aluno durante todas as fases e em todas as disciplinas. Nesse histórico também vai a porcentagem total de aproveitamento na freqüência do curso.

Ao concluir o ensino fundamental, o aluno já formado em determinado curso, tentará ingressar no mercado de trabalho, levando consigo toda a bagagem adquirida no processo de aprendizagem. No seu curriculum também estará em anexo o seu diploma, comprovando o seu rendimento no curso.

Por trás de todo esse processo, existe um aglomerado de informações que transitam pela instituição, mas que, na maioria das vezes, não se dá conta da importância que elas representam para a instituição.

Quando o aluno entra em uma instituição de ensino, a secretaria recebe seus dados para fazer o cadastro e armazená-lo em fichas ou arquivos eletrônicos. Nesse cadastro serão informados nome, endereço, telefone, cidade, estado, cep, entre outros.

Na matrícula será feita mais uma ficha ou mais um arquivo, contendo alguns dados sobre a situação escolar do aluno.

Ao iniciar as aulas o professor de cada disciplina terá em suas mãos o diário de classe e o diário de freqüência, contendo o nome de todos os alunos matriculados na mesma. Sendo assim, todas as informações referentes às notas e às freqüências de cada aluno serão controladas pelos professores por meio desse documento, que ao término de cada bimestre ou semestre será entregue à secretaria para o registro dessas informações e emissão dos boletins escolares.

A secretária também é a responsável pela emissão dos históricos. Para isso, é necessário que ela aglutine todas as informações contidas durante o curso do aluno, para montar a carreira escolar do aluno no decorrer de sua vida escolar.

Ao término do curso, o aluno também deve receber o seu diploma, confirmando a sua presença e a sua atuação regular no curso em questão. Nesse caso o responsável pelo diploma não necessariamente será a secretária, pode ocorrer uma possível prestação de serviços terceirizados que executarão essa tarefa.

Os diretores, por sua vez, têm como tarefa administrar todos os setores da instituição, bens, recursos, serviços e, principalmente, as informações da instituição que circulam na secretaria e em todos os setores. Essas informações devem ser armazenadas e manipuladas de forma segura, para o bom funcionamento da instituição.

4.1 TRABALHOS CORRELATOS

Os trabalhos correlatos são trabalhos que possuem certa semelhança ou os mesmos objetivos do trabalho realizado. Envolvendo estudos feitos na mesma área e contendo alguns assuntos em comum já pesquisados.

Dentre todos os trabalhos pesquisados, um dos mais interessantes e condizentes com o trabalho aqui desenvolvido foram:

4.1.1 Reserva de matricula on-line

O aplicativo Reserva de Matrícula on-line é um trabalho de conclusão de curso, desenvolvido em 2001 pelo acadêmico Frabrizio Colombo Machado, da Universidade do Extremo Sul Catarinense (UNESC).

Esse trabalho proporciona aos acadêmicos da instituição, à comodidade e a facilidade para fazerem a matrícula em semestres subseqüentes da própria casa, ou seja, via Internet.

Esse aplicativo se encontra no site da Unesc (www.unesc.net) e está disponível a todos os acadêmicos que desejem realizar a sua matrícula semestralmente sem sair da comodidade da sua casa.

Para obter acesso ao ambiente de reserva, o aluno necessita colocar o seu código de matrícula e a sua senha de acesso que se encontra no kit de reserva. Depois o aluno seleciona as disciplinas que deseja cursar, colocando os dados que forem requeridos.

Após o processo ser finalizado, o aluno recebe um comprovante de reserva e espera até o dia em que sair o resultado da reserva, na Internet ou no respectivo departamento.

4.1.2 Segurança de dados digitais utilizando esteganografia

Esse foi mais um trabalho de conclusão de curso, realizado em 2004 pelo acadêmico Fernando Warmeling Feldhaus da Universidade do Extremo Sul Catarinense (UNESC)

Esse trabalho, descreve os conceitos relacionados a segurança de dados digitais na Internet, tendo-se como foco principal os assuntos relacionados a esteganografia e a criptografia de dados.

Além disso, utiliza-se dessas duas técnicas como objetivo de desenvolver um protótipo, capaz de ocultar uma mensagem criptografada dentro do conteúdo de uma imagem, ou seja, mesmo que se alguém descobrir que a imagem possui uma mensagem embutida, precisara da chave criptográfica para ler o seu conteúdo.

4.1.3 Protótipo para assinatura digital de informações médicas

Esse é outro trabalho de conclusão de curso que foi desenvolvido em 2004, pela acadêmica Regiane Pizzetti Borges, da Universidade do Extremo Sul Catarinense (UNESC).

Com estudos relacionados a segurança de informações, em particular de pacientes em um prontuário médico e tendo como ênfase uma pesquisa realizada em torno de técnicas de criptografia e assinatura digital.

O trabalho desenvolvido, teve como objetivo a criação de um protótipo para digitalizar as informações pertinentes aos pacientes do hospital regional de Araranguá. Bem como garantir a segurança e a autoria dessas informações, por meio da aplicação de técnicas de criptografia e assinatura digital.

Nesse caso, os dados referentes ao paciente, tais como: diagnóstico, acompanhamento, tratamento, entre outros, serão de responsabilidade dos profissionais da área da saúde, assim como acontece hoje nos prontuários em papel.

Além de reduzir os custos com papel (impressão de relatórios impressos, carimbados e assinados manualmente), esse protótipo fornece ao prontuário, um certo grau de segurança as informações contra alterações não autorizadas e após assinar o documento eletrônico o profissional não poderá negar a sua autoria.

5 TRABALHO PROPOSTO

Nesse trabalho desenvolveu-se um protótipo de *software*, nomeado como SMAAE (Sistema para Monitoramento de Alunos no Ambiente Escolar), que tem por finalidade gerenciar e disponibilizar via web, as informações relacionadas a uma escola, em particular a Escola de Educação Básica Municipal Pietro Maccari, onde foram coletadas as informações necessárias para a construção do projeto e implementação do protótipo. Portanto, tornou-se necessário um estudo de caso, para analisar o cenário.

5.1 ESCOLA MUNICIPAL PIETRO MACCARI

A escola Municipal Pietro Maccari, cujo nome é em homenagem ao pai dos doadores do terreno, Senhor Antônio Maccari e Mansuetto Maccari, foi inaugurada no dia 07 de maio de 1977, na gestão do Sr. Prefeito Jorge Silva e tendo como 1ª professora a Sra. Maria das Dores Bittencourt Maccari.

No início de sua fundação, localizava-se no atual bairro Menino Jesus e contava com uma pequena clientela de alunos.

Atualmente, este estabelecimento de ensino é denominado de Escola de Educação Básica Municipal Pietro Maccari e está instalado com sede própria na Avenida Antônio de Costa, no bairro de Costa, próximo ao centro de Morro da Fumaça. Funciona nos turnos matutino e vespertino, atendendo a 58 alunos na educação infantil, 170 alunos de 1ª a 4ª séries e 192 de 5ª a 8ª séries, num total de 420 estudantes.

Hoje, em suas dependências, funciona uma escola profissionalizante, denominada de Escola Profissional Municipal Idalina Machado de Freitas, e que oferece

à comunidade em geral cursos de informática, de pintura em tecido e em tela, de crochê e ponto cruz e de costura industrial.

Utilizando-se ainda do espaço gratuito oferecido pela escola, nos períodos noturnos ocorrem, conforme horários estabelecidos, as atividades do Clube de Mães, as aulas de música, de Secretariado Executivo e de Técnico em Eletrotécnica, em convênio firmado com a SATC.

Independente das dependências utilizadas para os cursos profissionalizantes, a escola apresenta uma estrutura composta por 11 salas de aula, 6 banheiros coletivos, 1 biblioteca junto à sala de professores e de vídeo, 1 almoxarifado junto à sala de educação física, 1 cozinha, além de um amplo espaço físico destinado à prática de atividades esportivas e de recreação. Atualmente, conta com 32 funcionários capacitados, entre serventes, professores, secretária e diretor. Este ano a escola está sendo administrada pelo Sr. Marcos Silveira de Jesus.

Segundo Marcos, além do estudo em período regular, a escola oferece aulas de reforço escolar em períodos opostos ao que os alunos estudam, podendo ser atendidos individualmente ou em pequenos grupos. O objetivo dessas aulas é acelerar o processo ensino-aprendizagem de forma que todos possam ter rendimento satisfatório na aquisição e construção do conhecimento.

Atualmente para o gerenciamento das informações, tais como: cadastro da unidade escolar, dados cadastrais do aluno, manutenção dos dados (avaliações, freqüências, entre outros), consultas, relatórios, históricos e extrações de informações para enviar ao governo é utilizado o sistema SERIE Escola (Sistema Estadual de Registro e Informações Escolares).

O Sistema SERIE Escola, foi criado pelo CIASC, o qual desenvolve sistemas informatizados para a Secretaria Estadual da Educação e Cultura. Sendo assim,

é um sistema disponibilizado gratuitamente e adotado por muitos municípios catarinenses. E a cada atualização de versão, o governo disponibiliza um treinamento com as pessoas responsáveis por administrar o sistema (secretarias e diretores).

Porém todo envio de notas, fechamento de médias e controle de freqüências, são preenchidos de forma manual e entregue à secretaria, onde posteriormente serão repassadas ao sistema.

Além disso, de forma ultrapassada, as informações referentes a histórico escolar, boletins, diários de classe e freqüência são entregues de forma impressa aos responsáveis.

5.2 SERIE

Para o desenvolvimento do protótipo SMAAE, foi realizada uma analise do sistema atual utilizado pela Escola Municipal Pietro Maccari. Sendo assim, foi possível encontrar as deficiências do mesmo e coletar informações importantes com a finalidade de criar um protótipo que suprisse as necessidades da escola.

O Sistema Estadual de Registro e Informações Escolares (SERIE) é o sistema atualmente utilizado pela Escola Municipal Pietro Maccari para o gerenciamento das informações da instituição. Segundo Marcos (o atual diretor da escola), o mesmo também é adotado por muitas escolas municipais da região, pois possui a vantagem de ser fornecido gratuitamente pelo Governo Federal.

Esse sistema, basicamente é utilizado para cadastro da unidade escolar, dados cadastrais do aluno e manutenção dos dados (avaliação e freqüência). Também são gerados relatórios para a conferência e históricos para serem entregues aos alunos ou aos pais (em caso de alunos menores de idade).

Porem, como foi citado anteriormente, as informações relativas ao fechamento de médias e o controle de freqüência, ainda são preenchidas de forma manual e entregue a secretaria onde são repassadas ao sistema pela secretária ou pelo próprio diretor da escola. E as informações referentes a histórico escolar, boletins, diários de classe e freqüência são entregues de forma impressa aos responsáveis.

Além disso, o SERIE é um sistema Cliente/Servidor, ou seja, não é um sistema disponível via web e somente quem tem acesso a inserir ou consultar informações é o próprio diretor da escola ou a sua secretária.

Nesse caso, o sistema terá como usuário apenas o Administrador do sistema, ou seja, uma única pessoa que tem acesso a todos os módulos do sistema.

Todas as informações, para serem transportadas devem passar por um processo de exportação. Onde é gerado um arquivo em formato txt e gravado em disquetes ou outros meios magnéticos.

Para a solução desses problemas, desencadeou-se a proposta do desenvolvimento do protótipo SMAAE. O que diferencia o SMAAE do sistema atual, é que esse pretende ser mais prático e intuitivo. Além disso, o SMAAE é um protótipo de sistema que pode ser acessado via web, onde as informações são atualizadas por uma comunicação de certa forma segura entre cliente e servidor pela Internet.

5.3 SMAAE

Esse trabalho poderia ter sido implementado em vários outros tipos de softwares, pois se tratando da aplicação na área de segurança de informações, seria interessante, senão até mais adequado aplicar essas técnicas em sistemas voltados a área financeira, militar ou outros tipos de sistemas, onde é exigido o máximo de sigilo.

Mas a escolha em desenvolver um protótipo para essa aplicação, foi influenciada pelo fato de que já havia um projeto de estudo sendo desenvolvido sobre esse tipo de sistema. Sendo assim, tem-se um domínio sobre o cenário a ser pesquisado.

Além disso, para que a aplicação da segurança se torne mais eficaz é necessário, que se possua um profundo conhecimento sobre o sistema, identificando os pontos fracos para que se possa prevenir contra ataques de intrusos, principalmente em sistemas via web, onde os dados circulam na grande rede.

O SMAAE é um protótipo via web que tem por objetivo suprir as necessidades encontradas no sistema SERIE Escola (Sistema atualmente utilizado pela Escola Municipal Pietro Maccari).

Além disso, tem-se a vantagem de disponibilizar essas informações de forma digital a todos os envolvidos no processo e classificá-las para cada tipo de usuário, bem como: professores, alunos e o próprio administrador que nesse caso pode ser a secretária ou o diretor da escola.

Esse protótipo, por ser via web tem a vantagem de poder ser acessado de qualquer lugar, sendo necessário apenas possuir um computador com Internet e um navegador instalado. Além disso, é um sistema simples de utilizar se tornando bastante intuitivo.

O SMAAE possui três níveis de acesso, um para cada tipo de usuário, ou seja, esse protótipo possui três classes ou tipos diferentes de usuários, que são: Administrador, Professor e o Aluno. Para possibilitar a separação dos níveis de acesso, foi criada no banco de dados uma tabela chamada de tb_usuários, que possui a seguinte estrutura:

Tabela 1. Níveis de acesso.

Usuário	Nível	Senha
Admin	1	123
Professor	2	123
Aluno	3	123

No nível 1 Admin. Esse tipo de usuário é a pessoa que possui acesso total ao sistema, cadastros de professores e alunos, cadastro de disciplinas, atualização dos diários de classe, matriculas, entre outros. É a pessoa responsável por toda à parte de cadastro, manutenção ou alteração de informações no sistema. Esse acesso geralmente é fornecido ao(s) funcionários da Secretaria da Escola, bem como o próprio Diretor.

No nível 2 Professor. Esse tipo de usuário é a pessoa que tem acesso somente ao Diário de Classe e Diário de Freqüência das disciplinas e turmas que ele leciona, podendo fazer somente inclusões de dados.

No nível 3 Aluno. Esse tipo de usuário terá o acesso restrito apenas para consultas ao boletim e Histórico Escolar. Sendo assim, somente poderá visualizar as informações pertinentes a ele.

Essa estrutura, como foi mencionada nos capítulos anteriores, faz parte dos vários tipos de mecanismos utilizados para proporcionar segurança em sistemas, pois conforme o nível em que se encontra, o usuário só poderá ter acesso a determinados tipos de informações.

5.4 MODELAGEM DE DADOS E PROCESSOS

A modelagem do protótipo tem por objetivo explicar o funcionamento dos processos, bem como mostrar o fluxo de dados. Uma notação para modelagem de sistemas é a UML (*Unified Modeling Language*), Linguagem de Modelagem Unificada, sendo utilizada em estudos de caso (LARMAN, 2000). Entre os mais conhecidos e utilizados o diagrama de casos de uso.

5.4.1 Casos de uso

Os diagramas de caso de uso identificam todas as fases e situações, sendo um documento narrativo que descreve a seqüência de eventos que os três tipos de usuários (agentes externos) que utilizam o sistema executarão para completar um determinado processo, tornando-se uma excelente técnica para melhorar a compreensão dos requisitos do protótipo.

O protótipo SMAAE é composto por três diagramas de caso de uso, todos relacionados ao acesso dos usuários ao sistema. O objetivo é ilustrar o momento em que aceitam o certificado, mostrando também a diferença entre os itens do sistema que cada um tem acesso.

5.4.1.1 *Diagrama de caso de uso - Acesso do administrador*

Esse diagrama de caso de uso ilustra os procedimentos que o ator (administrador do sistema) deve seguir para ter acesso aos itens do sistema.

Caso de uso: Acesso do administrador.

Ator: Administrador.

Tipo: Primário e essencial.

Finalidade: Ter acesso aos cadastros gerais do protótipo.

Visão Geral: O usuário administrador, ao aceitar o certificado digital vai ter acesso total ao sistema. E toda a parte cadastral, movimentação de alunos e professores ficará sob sua responsabilidade.

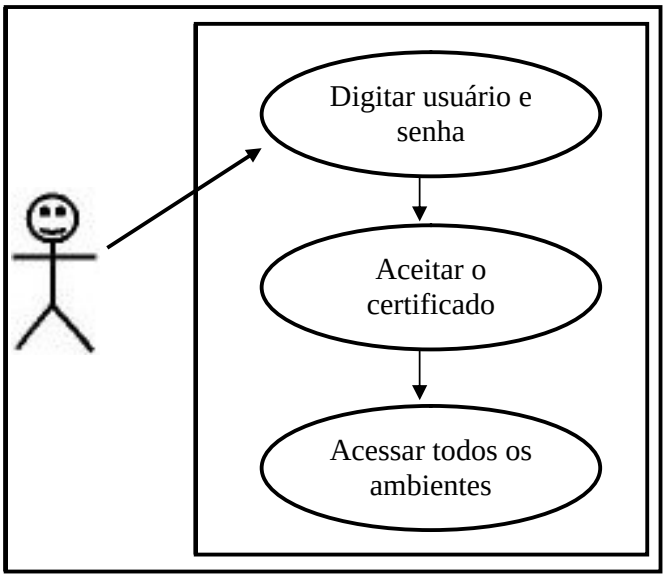

Figura 12. Caso do uso Acesso do administrador

5.4.1.2 *Diagrama de caso de uso - Acesso do professor*

Esse diagrama de caso de uso ilustra os procedimentos que o professor deve seguir para ter acesso ao diário de classe e diário de freqüência.

Caso de uso: Acesso do professor.

Ator: Professor.

Tipo: Primário e essencial.

Finalidade: Ter acesso ao diário de classe e diário de freqüência.

Visão Geral: O usuário professor, ao aceitar o certificado digital vai ter acesso somente ao diário de classe e diário de freqüência do sistema. Podendo apenas fazer a inclusão de notas e o controle de freqüências das disciplinas que leciona.

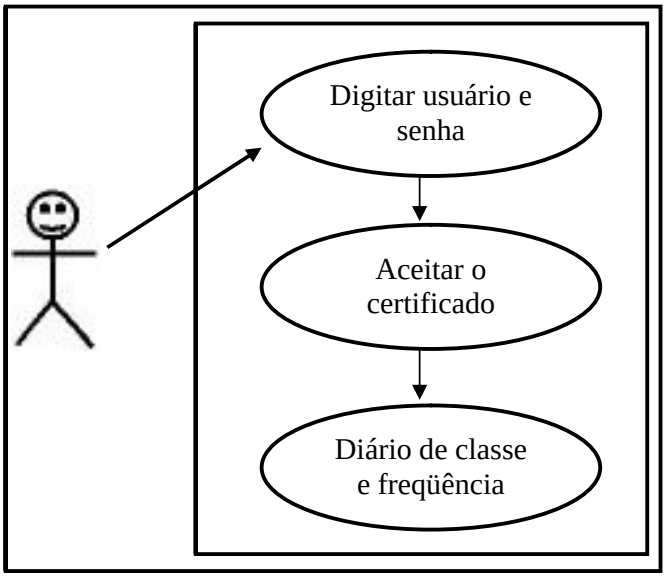

Figura 13. Caso de uso Acesso do professor

5.4.1.3 *Diagrama de caso de uso - Acesso do aluno*

Esse diagrama de caso de uso ilustra os procedimentos que o aluno deve seguir para ter acesso ao boletim e histórico escolar.

Caso de uso: Acesso do aluno.

Ator: Aluno.

Tipo: Primário e essencial.

Finalidade: Ter acesso ao boletim e histórico escolar.

Visão Geral: O usuário aluno, ao aceitar o certificado digital vai ter acesso somente ao boletim e ao histórico escolar do sistema. Podendo apenas consultar as informações pertinentes a ele, como: notas e o seu histórico escolar.

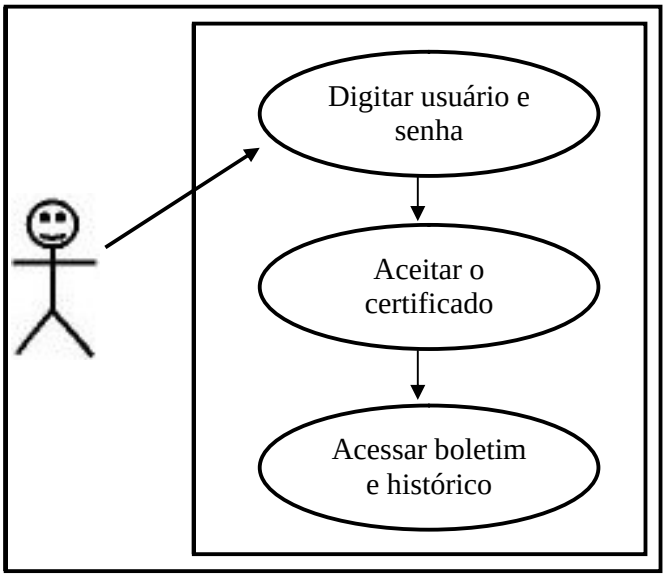

Figura 14. Caso de uso Acesso do aluno

Pode-se observar, que todas as três classes de usuários, são necessariamente obrigadas a aceitar o certificado digital para obter acesso ao sistema. Essa é uma forma do servidor autenticar o usuário para receber dados que serão criptografados enquanto estiverem trafegando na rede.

Também pode-se observar que existe diferença entre os módulos que cada usuário tem acesso. Isso funciona por meio da implementação de níveis de acesso, onde cada usuário terá a sua disposição, somente informações de seu interesse.

5.5 ACESSANDO O SMAAE ATRAVÉS DE UM PROTOCOLO SEGURO

Em uma aplicação real, o primeiro passo seria digitar o site onde o sistema está hospedado em um servidor autorizado. Para isso, o ideal seria utilizar um domínio para que o acesso seja de forma on-line com um servidor e que o mesmo deverá permanecer ligado. Nesse caso, como se trata de uma demonstração, a aplicação é acessada do próprio servidor, onde o intuito é mostrar à segurança sendo aplicada no protótipo desenvolvido.

O primeiro passo para acessar é digitar na barra de endereço do Internet Explorer (ou qualquer outro navegador) o seguinte endereço: http://localhost/.

Nesse momento aparece a tela principal do sistema, onde existem as três diferentes classes de usuários existentes nesse protótipo: Admin, Professor e Aluno. Figura.12.

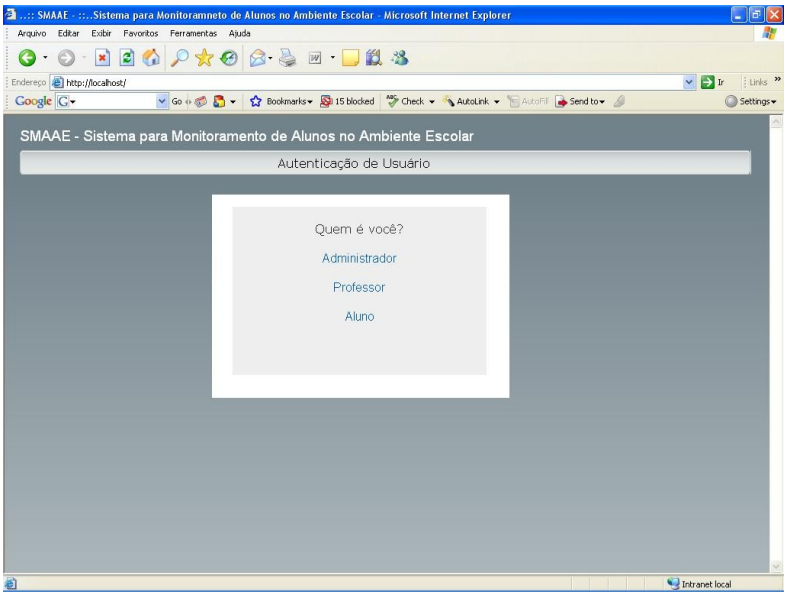

Figura 15. Indicando a classe do usuário

Nesse momento é necessário indicar qual o tipo de usuário deseja se conectar. Após escolher a opção que lhe atribui, surge então a tela de login, onde o usuário deve digitar o seu nome e a senha fornecida pelo admin.

O próximo passo é confirmar então se o usuário é quem ele diz ser após a confirmação dos dados. (Admin, Professor e Aluno) e posteriormente a senha correspondente (nesse caso, apenas para ilustrar foi utilizada a mesma senha ‘123’ para o acesso de ambos). Figura. 13:

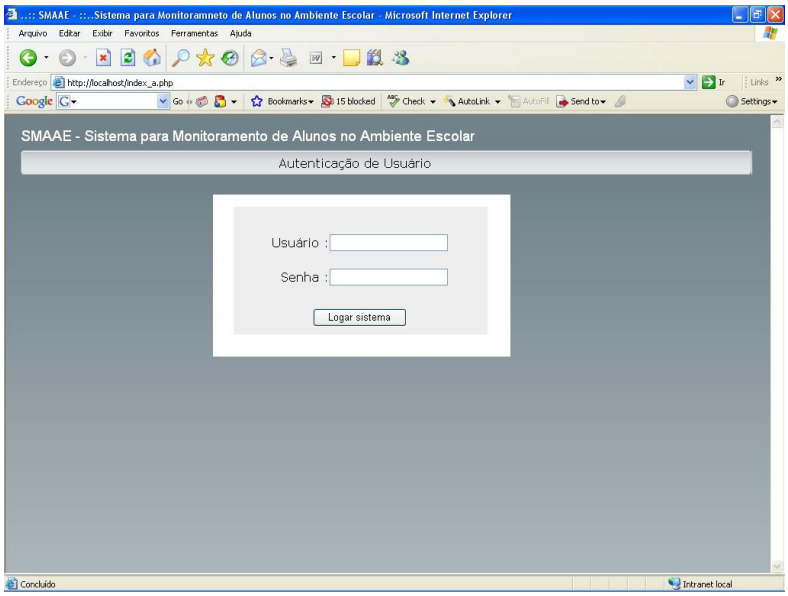

Figura 16. Efetuando login.

Após confirmar os dados de usuário, pode-se observar que aparece uma tela indicando que essa página estará utilizando um certificado digital e que toda a transmissão entre o usuário e servidor será feita de forma criptografada, ou seja, não podem ser vistas e nem alteradas durante a transmissão.

Porém, a mensagem de aviso que aparece, também indica que essa página comporta um certificado que não foi oficialmente distribuído por uma Autoridade Certificadora, portanto o mesmo não é um certificado oficial.

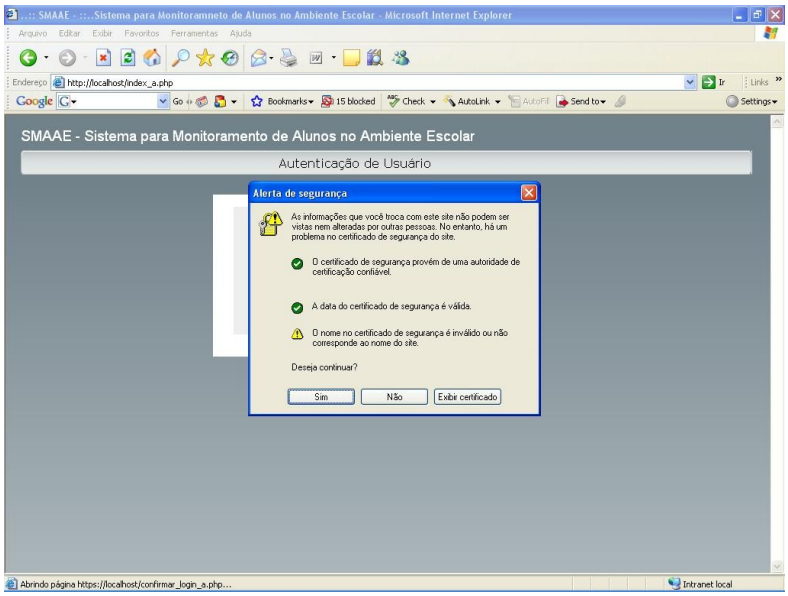

Figura 17. Aceitando o certificado digital

Isso é evidente pelo fato de que esse certificado foi gerado apenas para demonstrações de sua aplicação, sendo o intuito somente demonstrar a importância de se possuir um certificado digital.

A parte mais importante de todo esse processo é que a partir do momento em que é aceito o certificado, a URL deixa de mostrar o protocolo http e passa a rodar o protocolo https. Ou seja, deixou de ser um protocolo comum e passou a ser um protocolo seguro. Figura. 15:

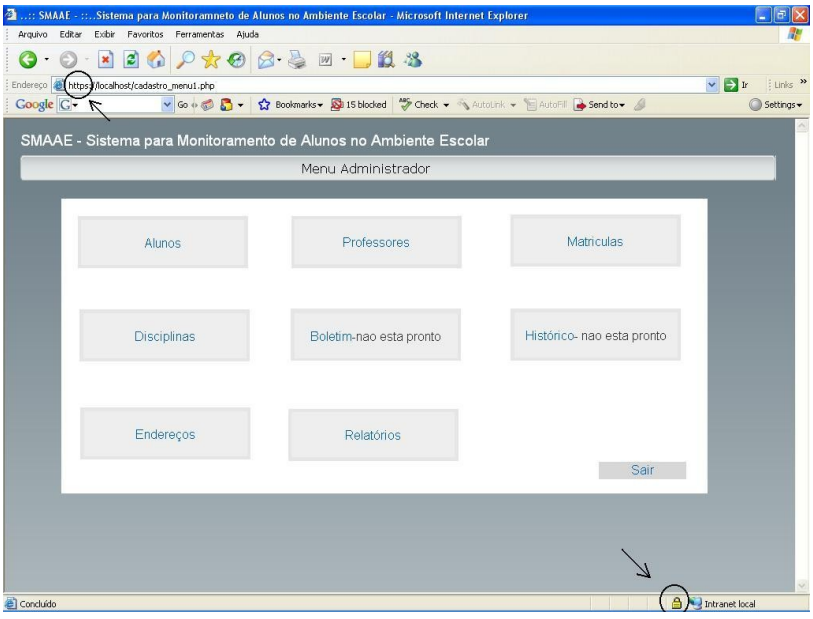

Figura 18. Site protegido pelo protocolo https

Outro símbolo que caracteriza um site seguro é o desenho de um cadeado que se encontra na parte inferior direita da tela.

Isso significa que a partir desse momento, toda e qualquer movimentação feita no sistema, passará por um canal seguro. Ou seja, caso um intruso consiga interceptar a comunicação entre as partes (cliente e servidor), não conseguirá ler a informação existente, pois os dados estarão criptografados e para isso teria que possuir a chave privada que se encontra no servidor.

O algoritmo criptográfico que executa esse processo é o RSA, que nesse certificado por exemplo, esta executando com uma chave de tamanho 1024 bits. Ele embaralha as informações que são passadas do usuário para o protótipo que está localizado no servidor.

Tudo isso é possível por meio do SSL (*Security Socket Layer*), uma camada de sockets de segurança, que conforme mencionado nos capítulos anteriores, foi projetado para fornecer criptografia de dados e autenticação entre cliente e um servidor WEB.

O SSL está localizado entre a camada de transporte e a camada de aplicação. Ele começa com uma fase de apresentação, que autentica o servidor ao cliente através de um certificado e suas respectivas chaves. O Cliente também pode ser autenticado junto ao servidor com a mesma técnica. Ou seja, para que o usuário consiga ter acesso ao site, deve primeiro aceitar o certificado que aparecerá após a tela de login.

Após a apresentação, então inicia-se a transmissão dos dados de forma criptografada, usando chaves de sessão negociadas durante a apresentação.

Para suportar o SSL, foi utilizado nesse trabalho o servidor Apache2, que vem em conjunto com o PHP (para desenvolvimento de softwares via web) e o MySQL (banco de dados).

São ferramentas gratuitas e disponíveis na Internet, destinadas ao desenvolvimento de aplicativos para web. Esse programa pode ser encontrado no site www.apache2triad.net e sua instalação é simples de ser realizada, bastando apenas fazer o download do arquivo e seguir os passos do próprio arquivo de instalação. Após a instalação do Apache2triad é gerada uma pasta dentro da raiz (C:\) do computador C:\Apache2triad.

O único detalhe que deve-se prestar muita atenção é que o monitor do servidor apache2 deve ser iniciado com suporte a SSL, porque por default ele sempre inicia como um servidor de páginas normal.

Essa informação será repassada com maior ênfase no item **5.4.1**, que mostra como é gerado o certificado digital. Mesmo porque, o SSL apenas funcionará se a chave e o certificado já tiverem sido criados e configurados corretamente. Portanto faz-se necessário uma demonstração do mesmo.

5.5.1 Gerando um certificado digital

A geração do certificado é muito importante, pois é por meio dele que a autenticação é solicitada e executada antes e durante a transmissão de dados. Agora, já considerando que as ferramentas já estão corretamente instaladas, deve-se executar os seguintes passos para a geração do certificado:

a) abrir o prompt de comando (dos) e apontar até o diretório \bin, ex: C:\Apache2triad\opssl\bin\.

b) executar o comando openssl req –config openssl.cnf –new –out meu-servidor.csr.

Figura. 19 Gerando a chave e o certificado

c) Observar que está sendo criada uma chave privada de 1024 bits utilizando a criptografia RSA. Para isso deve-se digitar a frase secreta:

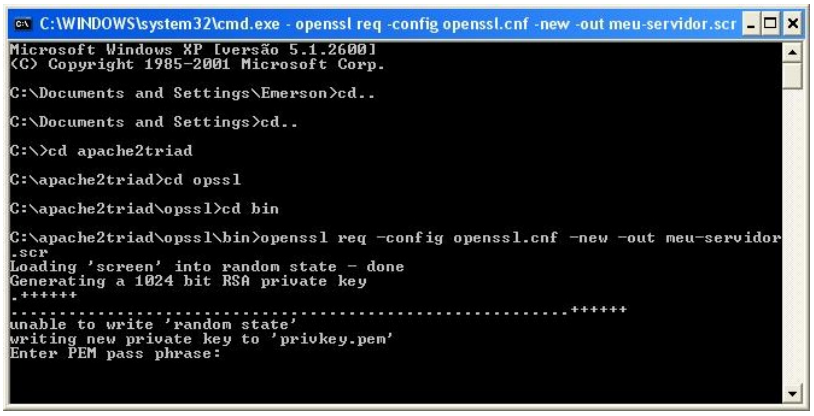

Figura 20. Cadastrando a chave secreta

Nesse momento é necessário o cadastramento das informações referentes ao certificado. Segue abaixo um exemplo de cadastro já preenchido.

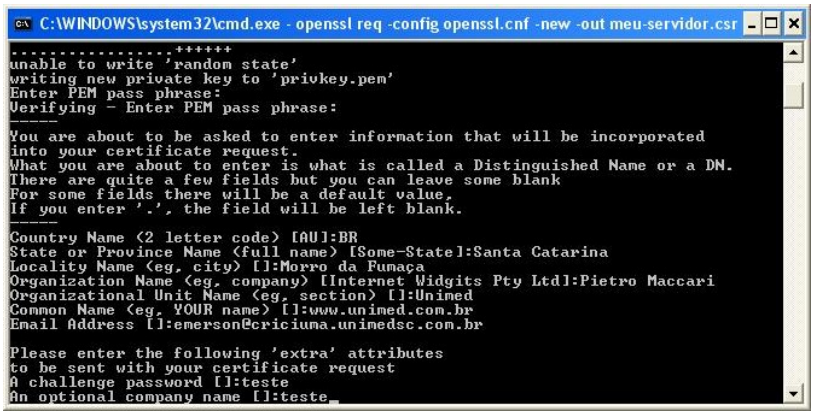

Figura. 21 Registrando o certificado.

Como pode-se observar, ao final do cadastro, é requisitada uma senha para o certificado, sendo que esse deve ser confidencial. E também será usada para a conexão do banco com o protótipo. Nesse caso a senha digitada foi “teste”.

O sistema nesse instante gera a chave (privkey.pem) e o certificado (meu-servidor.csr). Pode-se alterar esse nome “meu-servidor” para o nome do servidor que esta sendo utilizado.

É importante ressaltar também que no Commom name, deve ser informado o domínio exato ao qual o certificado pertence. Caso contrário, os navegadores emitem um alerta se esse domínio não for verdadeiro, assim como acontece no protótipo SMAAE.

d) Executar o comando openssl rsa –in privkey.pem –out my-server.key. Esse comando exclui a frase secreta da chave, impossibilitando o acesso de intrusos que podem utilizá-la para ataques. Nesse instante será solicitada novamente a digitação da frase secreta.

e) Executar o comando openssl x509 –in meu-servidor.csr –out my-server.cert –req –signkey my-server.key –days 365. Esse comando cria um certificado assinado, que pode ser utilizado até o momento em que se desejar adquirir um certificado original de uma autoridade certificadora. Esse exemplo, mostra um certificado que expira em um ano, ou seja, 365 dias. Esse período pode ser alterado com valor desejado após o parâmetro –days.

Na geração do certificado são criados dois arquivos: a chave (my-server.key) e o certificado propriamente dito (my-server.cert).

f) O último passo, é editar o arquivo ssl.conf que se encontra dentro da pasta de configurações do apache: c:\apache2triad\conf\, referenciando

os arquivos my-server.key e my-server.cert. Para fazer isso, edita-se as linhas do arquivo ssl.conf nas linhas iniciadas com os nomes SSLCertificateKeyFile e SSLCertificateFile respectivamente, indicando o caminho correto onde se encontram esses arquivos.

Agora para fazer o teste e verificar se o SSL está funcionando corretamente deve-se iniciar o monitor do apache em: Iniciar\ Apache2triad\ ApacheMonitor Apache2triad Apache2 Service with SSL. Caso já esteja iniciado o Apache2triad Apache2 Service, deve-se parar esse serviço e iniciar o Apache2triad Apache2 Service with SSL.

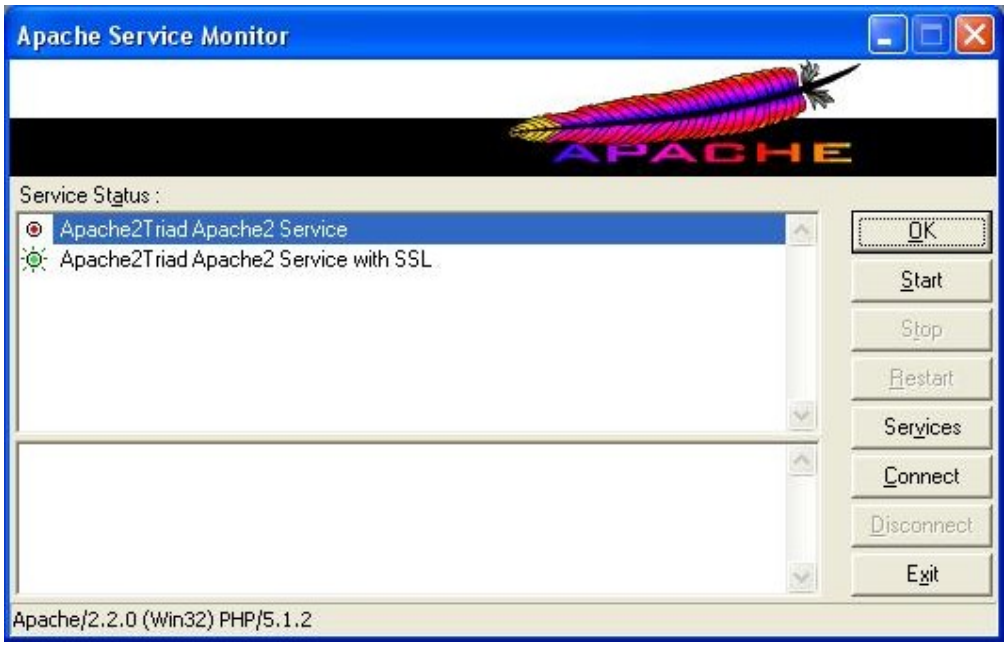

Figura. 22 Iniciando o apache2

Nesse momento, o SSL já esta funcionando. Portanto, a partir desse instante, sempre que o usuário abrir o navegar e tentar acessar o protótipo, o sistema vai solicitar que o certificado seja aceito pelo usuário, a fim de proporcionar um canal seguro para as informações.

Finalizando então o trabalho proposto, pode-se afirmar que tem-se um protótipo fácil de utilizar, auxiliando os professores e administradores de uma escola e

que implementa alguns mecanismos de segurança para que o tráfego de informações na rede seja feita de forma confiável.

6 CONCLUSÃO

Em geral, as instituições de ensino fundamental, médio ou superior lidam com vários tipos de informações, desde o cadastro de alunos e professores, matrículas, boletins, diários de classe e freqüência até o histórico escolar dos alunos.

O trabalho desenvolvido procurou criar um protótipo via web com uma proteção mínima, para a manipulação das informações de uma instituição de ensino. Para isso foram utilizados mecanismos de segurança apresentados no decorrer do trabalho, proporcionando integridade e confidencialidade aos dados que trafegam na rede.

Essas informações, primeiramente são analisadas e classificadas de acordo com sua importância dentro da instituição. Após sua classificação, são estabelecidos os mecanismos de proteção dessas informações, nesse caso os mecanismos de proteção utilizados foram: o controle de níveis de acesso e os protocolos seguros (HTTPS), que utilizam os certificados digitais para garantir um canal de comunicação seguro entre o usuário e o servidor.

Dentre as várias técnicas de segurança das informações, a criptografia é considerada um dos melhores mecanismos de proteção, tendo em vista que ela garante a integridade e confiabilidade dos dados e informações, de forma que foi um dos mecanismos mais estudados nesse trabalho.

Foram apresentados os tipos de algoritmos criptográficos mais conhecidos, bem como o tamanho das chaves que cada um suporta.

O protótipo utilizado para a implementação do trabalho, apesar de ser de pequeno porte, serviu para ilustrar que a segurança voltada a aplicativos via *web* é uma

grande vantagem, principalmente quando os dados que se deseja proteger são de grande importância para o contínuo funcionamento da instituição.

Outra vantagem está relacionada com a agilidade e facilidade na manipulação do sistema, que possuindo uma interface amigável, provavelmente tende a auxiliar os usuários na sua utilização.

O foco principal do trabalho então, não foi tão somente o protótipo, mas também os métodos de proteção aplicados a ele com o objetivo de proteger às informações.

A princípio, o intuito era colocar em funcionamento, mais alguns tipos de mecanismos de proteção, tais como: Assinatura Digital e Criptografia aplicada aos dados que ficam armazenados no banco de dados. Mas devido a restrições de tempo existente não pode ser concretizado, sendo que até algumas rotinas do protótipo não puderam ser totalmente concluídas, ficando disponível para trabalhos futuros.

Ao fim desse trabalho, pode-se concluir que os protocolos seguros, podem fornecer um alto nível de segurança a um sistema via web e que os conceitos e técnicas pesquisados e apresentados, podem ser aplicados a vários tipos de organizações, proporcionando também uma contribuição científica conforme o esperado.

Outro fator positivo após a finalização desse trabalho, foi o aprendizado adquirido, onde foram absorvidos vários conceitos e técnicas de segurança de informação e redes de computadores, além de conhecer e se familiarizar com as ferramentas de desenvolvimento para web. Apesar das dificuldades encontradas, o desenvolvimento desse trabalho gerou um crescimento pessoal satisfatório.

E por último, pode-se concluir que a informação é um dos bens mais importantes de uma instituição e que deve ser protegida, garantindo o bom andamento da mesma. Sendo assim, é importante elaborar de uma boa política de segurança que

indique quais informações devem ser protegidas bem como os mecanismos mais adequados para fazê-lo, levando-se em conta o custo x benefício.

REFERÊNCIAS

BORGES. R. P. **Segurança de informações médicas em prontuário eletrônico utilizando assinatura digital**. 2004. Trabalho de conclusão do curso apresentado para a obtenção do Grau de Bacharel em Ciência da Computação da Universidade do Extremo Sul Catarinense, Criciúma, 2004.

CARUSO, Carlos A. A.; STEFFEN, Flávio Deny. **Segurança em informática e de informações**. 2.ed. São Paulo: SENAC/SP, 1999.

CARVALHO, Daniel Balparda de. **Criptografia**: métodos e algoritmos. 2.ed Rio de Janeiro: Book Express, 2001.

COLOMBO. Fabrizio. **Reserva de matricula on-line.** 2001. Trabalho de conclusão do curso apresentado para a obtenção do Grau de Bacharel em Ciência da Computação da Universidade do Extremo Sul Catarinense, Criciúma, 2001.

DEMÉTRIO, Rinaldo. **Internet**. São Paulo: Érica, 2001.

DIAS, Cláudia. Segurança e auditoria da tecnologia da informação. Rio de Janeiro: Axcel Books do Brasil, 2000.

FELDHAUS. F. W. Segurança de dados digitais utilizando esteganografia. 2004. Trabalho de conclusão do curso apresentado para a obtenção do Grau de Bacharel em Ciência da Computação da Universidade do Extremo Sul Catarinense, Criciúma, 2004.

FERREIRA. A. B. H. **Novo dicionário da língua portuguesa**: 2ª edição revista e ampliada. Rio de Janeiro: Nova Fronteira S.A., 1986.

GIL, Antonio de Loureiro. **Segurança em informática**: ambientes mainframe e de microinformática segurança empresarial e patrimonial 200 questões sobre segurança. 2 ed. São Paulo: Atlas, 1998.

GRIZZO, Erico. **Internet**: o que é. o que oferece, como conectar-se. São Paulo: Ática, 2002.

KUROSE, J. F.; ROSS, K. W. **Redes de computadores e a internet**: uma abordagem top-down. São Paulo: Pearson Addison Wesley, 2006.

LARMAN, Craig. **Utilizando UML e padrões**: uma introdução à análise e ao projeto Orientados a Objetos. Porto Alegre: Bookman, 2000.

MARTINI, Renato. **Criptografia e cidadania digital**. Rio de Janeiro: Ciência Moderna, 2001.

NORTHCUTT, Stephen (...[et al.]). **Desvendando** : segurança em redes. Rio de Janeiro: Campus, 2002.

PETERSON, L. L.; DAVIE, B. S. **Redes de computadores**: uma abordagem de sistemas. Rio de Janeiro: Elsevier, 2004.

TERSARIOL. Alpheu. **Minidicionário brasileiro**. Rio Grande do Sul: Edelbra, 1996.