Faculdade de Tecnologia de Americana
Curso de Processamento de dados

SEGURANÇA DA INFORMAÇÃO COM ÊNFASE EM CRIPTOGRAFIA E HARDWARE CRIPTOGRÁFICO

JOSÉ LOPES DA COSTA JUNIOR

Americana, SP
2010

Faculdade de Tecnologia de Americana
Curso de Processamento de dados

SEGURANÇA DA INFORMAÇÃO COM ÊNFASE EM CRIPTOGRAFIA E HARDWARE CRIPTOGRÁFICO

JOSÉ LOPES DA COSTA JUNIOR

lopes_lopes@uol.com.br

Monografia desenvolvida em cumprimento à exigência curricular do Curso de Processamento de Dados da FATEC-AM, sob orientação do Prof. Nelson Gonçalves Junior.

Área: Segurança da Informação

Americana, SP
2010

BANCA EXAMINADORA

Prof. Nelson Gonçalves Junior (Orientador)

Prof. Antonio Alfredo Lacerda

Prof. Irineu Ambrozano Filho

AGRADECIMENTOS

Primeiramente a Deus, por ter me concedido esta oportunidade.

Ao meu orientador Prof. Nelson Gonçalves Junior, que me guiou com suas dicas para a conclusão desta monografia.

A todos os mestres, especialistas e professores, que durante todo este período se dedicaram e transmitiram seus conhecimentos, contribuindo para meu aprendizado.

Aos meus amigos que junto comigo formaram a famosa JARM, “J” que representa meu nome José, “A” que representa Anderson, “R” que representa Rodrigo e “M” que representa Mário, juntos formamos um quarteto como os três mosqueteiros, inseparáveis e prontos para aprender e compreender todas as disciplinas para atingirmos nosso objetivo maior, a formatura.

DEDICATÓRIA

A minha amada esposa que sempre me incentivou e me apoiou.

RESUMO

O presente texto conceitua a importância da utilização de algoritmos e *hardwares* criptográficos na proteção dos dados e informações das empresas, com o crescente aumento da utilização de sistemas computacionais e transmissão de dados através de redes como internet é fundamental garantir a integridade das informações, entre os *hardwares* utilizados, os biométricos começam a se destacar mostrando uma tendência de utilização deste recurso para assegurar a identificação das pessoas, evitando desta maneira a falsificação ou adulteração dos dados.

Palavras Chave: Segurança, criptografia, biometria.

ABSTRACT

The present text conceptualizes the importance of using algorithms and encryption hardware to protect their data and corporate information, with the increasing use of computer systems and data transmission through networks like the Internet is vital to ensure integrity of information, among hardware used, biometric begin to highlight showing a tendency to use this resource to ensure the identification of individuals, thereby avoiding forgery or tampering of data.

Keywords: Security, encryption, biometrics.

SUMÁRIO

LISTA DE FIGURAS E DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AH	*Authentication Header*
CA	*Certification authorities*
CD	*Compact Disc*
CPU	Unidade Central de Processamento
DSA	*Digital Signature Algorithm*
DES	*Digital Encryption Standard*
DH	*Diffie-Hellman*
ECDH	*Elliptic Curve Diffie-Hellman*
E-CPF	Eletrônico – Cadastro Pessoa Física
ESP	*Encapsulating Security Payload*
IP	*Internet Protocol*
IPSEC	*Internet Protocol Security*
KEK	*Key Encryption Key*
MIME	*Multipurpose Internet Mail Extentions*
PBE	*Password-based encryption*
PGP	*Pretty Good Privacy*
PKC	*Public Key Certificate*

RSA *Rivest, Shamir, Adleman*

SET *Secure Electronic Transaction*

SHA *Secure Hash Algorithm*

S/MIME *Secure/Multipurpose Internet Mail Extentions*

SSL *Secure Sockets Layer*

USB *Univer salt Serial Bus*

INTRODUÇÃO

O **objetivo geral** foi passar uma noção da importância da utilização de sistemas de informação para assegurar a integridade das informações ou dados.

Como **objetivos específicos** foram transmitir o conceito de informação e segurança de sistemas de informação, mostrar a utilização da criptografia e *hardware* criptográficos que são utilizados para assegurar a integridade dos dados e identificação dos usuários.

O **método científico** utilizado foi o de pesquisa nas bibliografias citadas no capitulo sete.

O trabalho foi estruturado em sete capítulos, sendo que no primeiro se conceitua a segurança da informação, o segundo trata do sistema da informação e o terceiro conceituam a segurança do sistema da informação.

No quarto capitulo tratamos sobre a criptografia, que podemos considerar a essência da segurança dos sistemas de informação atualmente.

No quinto capitulo apresentamos alguns hardwares criptográficos que temos atualmente disponíveis no mercado, que garantem a integridade das informações.

Com base nas informações conseguidas a partir dos estudos realizados, o sexto capítulo traz às considerações finais e o sétimo as referências bibliográficas utilizadas.

1 CONCEITOS DE INFORMAÇÃO

Primeiramente precisamos entender o que é informação.

Independente do formato utilizado, a informação é um bem precioso para as pessoas e empresas.

Através da informação é que tomamos decisões importantes em nossa vida pessoal ou profissional.

As empresas possuem informações valiosas e necessitam proteger de seus concorrentes.

Podemos dizer que a informação é muito mais do que um grupo de dados.

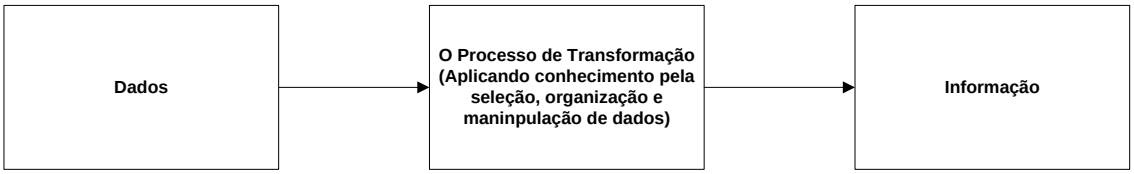
Os dados consistem em fatos não trabalhados, vários tipos de dados podem ser utilizados para representar fatos.

Os fatos tem que ser ordenados de uma forma significativa, para se tornarem informação.

A informação são os fatos organizados, adquirindo um valor adicional além do valor dos próprios fatos.

Para uma informação ser valiosa tem que ter as seguintes características:

Figura 1: O processo de transformação de dados em informação



Fonte: STAIR, R. M. /. REYNOLDS, G. W – Princípios de sistemas de informação - p. 05

Por esta razão, cada empresa define uma estrutura adequada para guardar com segurança suas informações, criando regulamentos com políticas, normas ou regras de segurança da informação.

Quando iniciamos nossa vida profissional dentro de uma empresa, está nos orienta sobre a importância de se manter em sigilo as informações de negócios, nos comunicando destas políticas.

Os autores STAIR, R. M., REYNOLDS, G. W. Princípios de Sistemas de Informação definem muito bem o significado de Segurança da Informação:

> “Segurança da Informação é um conjunto de orientações, normas, procedimentos, políticas com o único objetivo de proteger a informação das organizações.”

Quando falamos em proteger a informação, significa que devemos garantir a disponibilidade, integridade, confidencialidade, legalidade, auditabilidade e o não repudio de autoria.

Para poder garantir estes itens, geralmente à empresa solicita a seus colaboradores assinarem um Termo de Compromisso, onde é descrito as principais responsabilidades em relação à informação, a solicitação de renovação deste termo é feita anualmente.

2 SISTEMA DE INFORMAÇÃO

Os computadores desde a sua criação foram ganhando espaço em nossas vidas interferindo diretamente em nosso dia-a-dia.

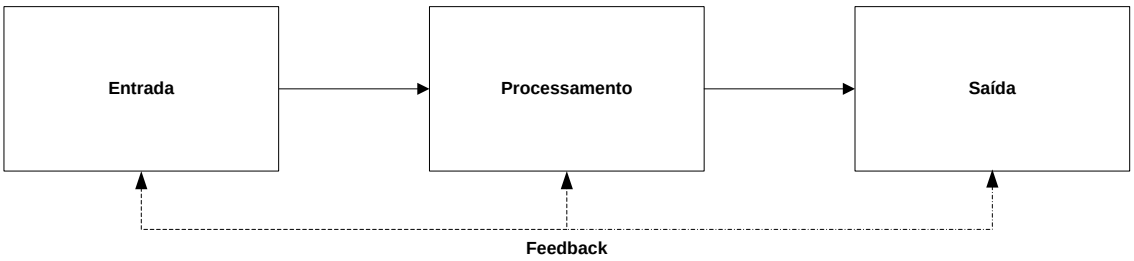
Os sistemas computadorizados, cada vez mais estão sendo utilizados para criar, armazenar e transferir informação, a cada dia que passa, deixamos de utilizar o papel para guardar as informações e utilizamos os meios digitais.

Estamos deixando de lado alguns conceitos antigos e utilizando cada vez mais as facilidades do universo da informática, instituições financeiras transferem diariamente milhões de Reais eletronicamente, fabricantes utilizam o sistema para solicitar suprimentos e distribuir mercadorias com mais rapidez, nós utilizamos os sistemas para guardar dados de nossa vida pessoal, como fotografias, documentos, dados do trabalho e para se comunicar com as pessoas.

Os autores STAIR, R. M. e REYNOLDS, G. W. conceituam no livro Princípios de Sistemas de Informação, p. 05:

> "Sistema de Informação é um conjunto de componentes inter relacionados que coletam (entrada), manipulam (processamento) e disseminam (saída) os dados e a informação e fornecem um mecanismo de *feedback* para atender um objetivo."

Figura 2: Os componentes de um sistema de informação



Fonte: STAIR, R. M. /. REYNOLDS, G. W – Princípios de sistemas de informação - p. 05

Entrada: Em um sistema de informação é a atividade de reunião, coleta de dados brutos.

A entrada pode ter vários formatos, e pode ser um processo manual ou automatizado.

Processamento: Em um sistema de informação, envolve a conversão e a transformação de dado em saídas úteis.

Saída: Em um sistema de informação envolve a produção de informação útil, geralmente em forma de documentos ou relatórios.

Também pode ser usada como entrada para outros sistemas ou dispositivos.

Feedback: Em um sistema de informação é a saída utilizada para promover as mudanças na entrada ou nas atividades de processamento.

O *feedback* também é importante para os tomadores de decisões.

3 A SEGURANÇA DE SISTEMAS DE INFORMAÇÃO

Os sistemas de informação em computador nos ajudam em nossas tarefas, mas eles são muito vulneráveis.

Abaixo podemos verificar as principais ameaças ao sistema de informação computadorizado.

Tabela 1: Ameaças ao sistema de informação computadorizado

Ameaças ao Sistema de Informação Computadorizado	
Ameaça	**Efeito**
Incêndio	O *hardware* do computador, arquivos e registro manuais podem ser destruídos.
Falha de energia elétrica	Todo o processamento do computador é suspenso; o *hardware* pode ser danificado e podem ocorrer "*Crashes*" ou interrupções das telecomunicações.
Mau funcionamento do *hardware*	Os dados não são processados com exatidão ou modo completo.
Erros de *software*	Os erros inadvertidamente introduzidos pelos usuários durante a transmissão, entrada, validação, processamento, distribuição, e outros pontos do ciclo de processamento da informação, destroem dados, prejudicam o processamento ou produzem saídas errôneas.
Crime por computador	O uso ilegal de *hardware*, *software* ou de dados resulta no roubo de dinheiro ou na destruição de dados ou serviços valiosos.
Mau uso do computador	Os sistemas de computador são usados com propósitos antiéticos.

Fonte: LAUDON, K. C. / LAUDON, J. P. – Sistemas de Informação - p. 262

O sistema de informação *online* e os sistemas baseados em redes de telecomunicações são mais vulneráveis porque interligam sistemas de informação em muitos locais diferentes.

As redes de dados sem fio são facilmente penetradas, visto que a transferência de dados utiliza dispositivos que são basicamente transmissores de rádio.

Um dos principais objetivos e desafios da segurança da informação são impedir o crime por computador.

Os crimes por computador podem variar desde uma brincadeira de adolescente até uma espionagem. O roubo monetário é a forma mais comum de crime por computador, mas também temos furto de serviços, informações, programas de computador, alteração de dados, danos ao *software*, etc.

Os *hackers* são um verdadeiro pesadelo a segurança do sistema de informação, pois usam a rede da internet para distribuir vírus de computadores, como por exemplo, os famosos “cavalo de tróia” que quando instalados se espalham rapidamente pelo sistema.

Para tentar combater este vírus, devemos tomar algumas medidas de segurança sugeridas pelos autores LAUDON, K. C. / LAUDON, J. P. – Sistemas de Informação – p. 264.

> "1. Fazer cópia de segurança (*backup*) logo que seja aberto um novo pacote de *software*, e armazenar as cópias em outro local.
>
> 2. Deixar em quarentena todo *software* novo ou arquivo de dados em um computador isolado, sempre o revisando cuidadosamente antes de sua instalação, principalmente se tiver sido obtido por meio de uma rede ou pela internet.
>
> 3. Restringir o acesso a programas e dados em termos de necessidade de uso.
>
> 4. Examinar regularmente todos os programas em busca de alteração de tamanho, visto que podem ter sinal de adulteração ou infiltração de vírus.
>
> 5. Ter muita atenção com programas "*shareware*" e "*freeware*", visto que são os principais pontos de entrada para vírus.
>
> 6. Instituir um plano para remoção imediata de todas as cópias de programas suspeitos e fazer *backup* dos dados relacionados.
>
> 7. Certificar-se de que todo *software* comprado esteja em sua embalagem original ou em invólucros selados."

A cada dia que passa, as empresas estão armazenando mais informações confidenciais nos computadores, informações que são muito valiosas aos concorrentes.

Com a crescente dependência em relação às redes e a Internet, temos três aspectos importantes da segurança, que exigem mais atenção:

1 – Garantir a segurança dos dados;

2 – Proteger os computadores e redes;

3 – Desenvolver os planos de recuperação dos desastres que afetam os sistemas de informação.

3.1 SEGURANÇA DE DADOS

Antigamente, quando falavamos em segurança de dados, nossa maior preocupação era não deixar nenhuma informação sobre as mesas do escritório, e todo final de dia guardavamos tudo em arquivos e trancavamos as portas com chave, garantindo assim, a integridade das informações.

Atualmente as informações são guardadas em computadores ou servidores das empresas.

Como podemos proteger os dados que mantemos em nossos sistemas?

Uma das formas de segurança de dados é a utilização de senhas, que concedem autorização as pessoas para acessarem um sistema de informação.

Uma senha pode ser exigida para a pessoa acessar um sistema, dados e arquivos.

Algumas empresas estão adotando a utilização de cartões de segurança em conjunto com as senhas para o usuário acessar as informações nos sistemas.

Com o crescente uso das telecomunicações e da internet, as empresas tiveram que pensar em uma maneira segura para manter estas informações, adotando um formato adicional de segurança, a criptografia de dados.

Com a criptografia, os dados são misturados em uma forma codificada antes da transmissão por uma rede de telecomunicações e depois decodificada no seu destino.

4 CRIPTOGRAFIA

Uma das principais razões para se utilizar a criptografia é garantir a integridade e confidencialidade das informações.

Criptografia é um termo que surgiu da fusão de duas palavras gregas “*kryptós*” e “*gráphein*”, que significam respectivamente “ocultos” e “escrever”.

A criptografia é usada para codificar dados de uma maneira que fiquem cifrados para que ninguém consiga acessar as informações, permitindo assim, que apenas o destinatário final descodifique e entenda a verdadeira mensagem.

Os autores BURNETT, S. e PAINE, S., Criptografia e Segurança, p. 08 nos fornece um bom exemplo de como isto acontece.

> “...suponha que seu material sigiloso se pareça com isto:
>
> *Do not believe that competion can match the new feature set, yet their support, services, and consulting offerings pose a serious threat to our salability. We must invest more money in our*
>
> Eis como os dados se parecem quando encriptados:
>
> G?SdJt:1/41Y18’1Y gmdcA#[< b:vR- o UGO>e’Q V ,< loj’utL0_”G ris6&igy §u&_a7AFT1=0_. . A’ ‘-R81- ykh . . . o2ii?itr0(trn)trv6R1i,,(04;_U6R’Q3/4V6 – A#Au&-9f >FemB06_c&&B1/28#uh&[G [gh_1>%=Gmdtn*’b81/4jwm1/4B-A_ -,1/4<”-iEj1t1bf=,AUH
>
> Mesmo que um invasor obtenha o conteúdo do arquivo, ele é ilegível. ”

Criptografia são algoritmos matemáticos utilizados para codificar as mensagens, sendo uma importante ferramenta para segurança de dados, entretanto não significa que a criptografia não pode ser quebrada.

Existem no mercado diversos algoritmos para utilizar na criptografia de dados, mas o mais utilizado é o da RSA (Rivest, Shamir, Adleman) que são as iniciais dos sobrenomes de seus criadores, Ron Rivest, Adi Shamir e Len Adleman, criado em 1977.

Esses algoritmos geram o que é chamado de chaves criptográficas, sendo uma chave pública e outra privada.

Um algoritmo é como se fosse uma receita de bolo, que você segue passo a passo como fazer, ou seja, ele contém uma lista de procedimentos que são executados em uma determinada ordem.

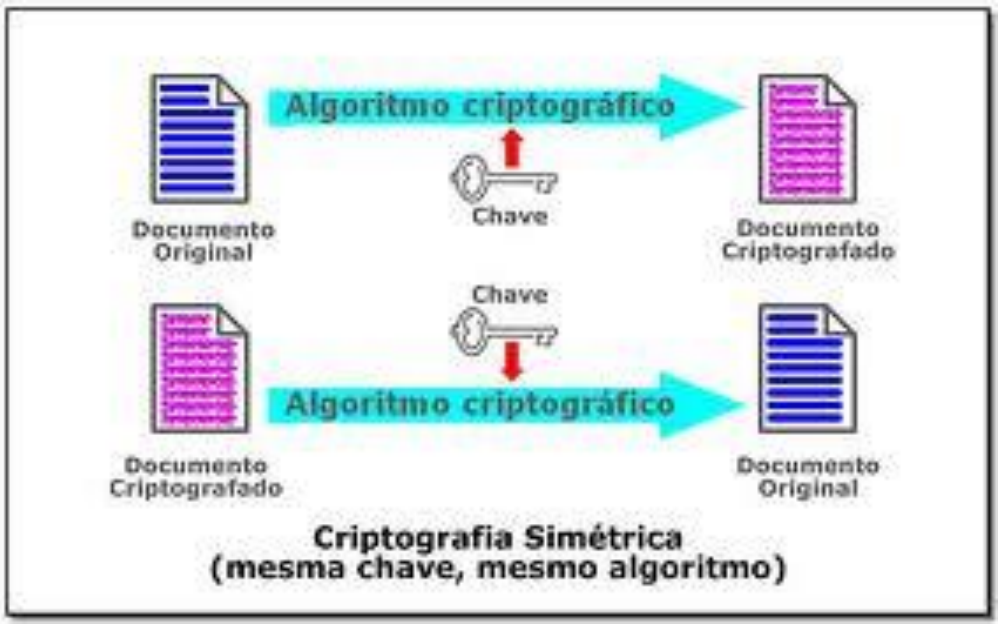
A palavra “chave” utilizada na criptografia refere-se ao fato de ser um número secreto escolhido para proteger os dados, funcionando como uma chave convencional que tranca a porta de nossa casa.

A utilização de chaves é necessária para impedir que invasores possam decifrar sua mensagem.

4.1 CHAVE SIMÉTRICA

Este é o primeiro tipo de criptografia, utiliza o mesmo algoritmo para converter as informações em *bits* aleatórios e para recuperação dos dados originais.

Figura 3: Criptografia Simétrica



Fonte: http://www.bpiropo.com.br/fpc20071203.htm. Acesso em 21 ago. 2010. 20h47.

Alguns invasores podem tentar descobrir está chave utilizando o método de ataque de força bruta que consiste em pegar seu texto criptografado e inserir no algoritmo de decriptografia junto com uma possível chave que vai testando uma a uma.

Este tipo de ataque pode levar muito tempo para ser decifrado, visto que quanto maior for o intervalo de uma chave, maior será o grau de dificuldade para localizar a correta.

Em média este algoritmo tem que testar no mínimo 50% para conseguir encontrar a chave correta.

Para testar suas chaves a RSA Laboratories propõem alguns desafios, oferecendo prêmio em dinheiro para a pessoa ou empresa que conseguir decifrar ou quebrar o código de uma mensagem em particular.

Os autores BURNETT, S. e PAINE, S., Criptografia e Segurança, p. 27, nos fornece alguns resultados destes desafios.

> "Alguns desafios foram testes do tempo de um ataque de força bruta. Em 1997, uma chave de 40 *bits* foi quebrada em três horas e uma chave de 48 *bits* durou 280 horas. Em 1999 a *Eletronic Frontier Foundation* encontrou uma chave de 56 *bits* em 24 horas. Em um dos casos, pouco mais de 50% do espaço de chave foi pesquisado antes de a chave ser encontrada. Em janeiro de 1997, foi publicado um desafio de 64 *bits*. Até dezembro de 2000, ele não tinha sido resolvido.
>
> Em todas essas situações, centenas ou até milhares de computadores operavam conjuntamente para quebrar as chaves. Na realidade, com o desafio de 56 *bits* de DES (*Digital Encryption Standard*) que a *Eletronic Frontier Foundation* quebrou em 24 horas, um dos computadores era um *cracker* especializado em DES."

A maioria das chaves utilizadas atualmente é do tamanho de 128 *bits*, as chaves mais longas indicam maior segurança.

Pelo exemplo citado acima podemos concluir que para quebrar uma chave de 128 *bits* a tecnologia e os invasores terão que avançar muito para diminuir os anos de vida útil desta chave.

A seguir temos uma tabela com os tempos para se quebrar uma chave utilizando um ataque de força bruta.

Tabela 2: Um cenário pior do que o pior das situações: quanto tempo um ataque de força bruta levaria quanto aos vários tamanhos de chaves

Bits	**1% do espaço da chave**	**50% do espaço da chave**
56	1 segundo	1 minuto
57	2 segundos	2 minutos
58	4 segundos	4 minutos
64	4,2 minutos	4,2 horas
72	17,9 horas	44,8 dias
80	190,9 dias	31,4 anos
90	535 anos	321 séculos
108	140.000 milênios	8 milhões de milênios
128	146 bilhões de milênios	8 trilhões de milênios

Fonte: BURNETT, Steve & PAINE, S. Criptografia e Segurança – O Guia Oficial RSA, p. 28

4.2 PROTEÇÃO DA CHAVE

Depois de gerada uma chave simétrica e encriptar os dados, precisamos proteger a chave, para isso, uma das técnicas utilizadas é a criptografia baseada em senha.

A chave que é utilizada para encriptar os dados é conhecida como chave de sessão, que é uma instancia da criptografia.

Para armazenar uma chave de sessão com segurança, necessitamos encriptá-la utilizando um algoritmo de chave simétrica.

Para ser feito isto há necessidade de se ter outra chave, conhecida como KEK (*Key encryption Key*), desta maneira a chave de sessão protege os dados armazenados e a KEK protege a chave de sessão.

Utilizando a criptografia baseada em senha, que é conhecida como PBE (*Password-based encryption*), não há necessidade de se armazenar a KEK, visto que quando necessitar de uma, podemos gerar e descartar após a utilização, quando formos decriptar o arquivo conseguimos gerar a mesma KEK.

As chaves criptográficas também podem ser armazenadas através da utilização de um dispositivo de *hardware*, como *tokens* e aceleradores de criptografia.

O *token* contém um *chip* com um processador, este *chip* funciona como um tipo de sistema operacional, mas com recursos limitados de entrada e saída.

O *token* nos dá uma segurança, pois por ser pequeno podemos levá-lo conosco para qualquer lugar, e evita que algum *hacker* possa conseguir os códigos.

Atualmente a maior parte das instituições financeiras já oferece está segurança aos clientes para garantir suas transações pela Internet.

Também temos os cartões inteligentes que contém um *chip* onde armazena uma senha para garantir a segurança das transações, as empresas de cartão de crédito estão substituindo seus cartões por este modelo.

Algumas empresas estão utilizando *tokens* criptográficos que são conectados através da porta USB (*Univer salt Serial Bus*) dos computadores, são mais rápidos e tem um bom espaço para armazenamento de senhas.

Os aceleradores de criptografia são baseados em *hardware*, com *chips* especializados que podem realizar operações criptográficas mais rápidas do que os microprocessadores em geral.

4.3 CHAVE PÚBLICA

A criptografia com chave simétrica mantém nossas informações seguras, mas para podermos compartilhar estas informações com outras pessoas necessitamos enviar a chave para a pessoa ter acesso.

Para enviar a chave de uma maneira segura, utilizamos a criptografia de chave pública.

Com a utilização de um PBE (*Password-based encryption*), a pessoa que detem a informação sigilosa, gera uma chave gravando em um CD ou em um *Token*, e entrega a pessoa que devera acessar suas informações, desta maneira cria-se uma segurança de que a chave não será descoberta por alguém não autorizado.

Entretanto este método não é muito eficaz quando necessitamos compartilhar esta chave com mais de uma pessoa, logisticamente nos traria algumas dificuldades.

Para resolver este problema, em 1970 pesquisadores criaram a criptografia de chave assimétrica, que possibilitou enviar as chaves de uma maneira segura.

Este processo utiliza duas chaves diferentes, mas relacionadas entre si, uma chave encripta a informação e a outra decripta, sendo que a chave que foi utilizada para encriptar não poderá ser utilizada para decriptar a informação, deverá obrigatoriamente utilizar contrapartida desta chave.

Apesar do algoritmo de chave pública poder ser quebrado, este tipo de chave é bastante eficiente, visto que o ataque de força bruta não é o ataque mais rápido, e até hoje ninguém foi capaz de desenvolver um algoritmo de chave pública que não tenha fraquezas.

A grande diferença de criptografia de chave simétrica e pública é que a simétrica opera os dados como *bits* e a pública como números.

Por tratar os dados como *bits* a chave simétrica executa o algoritmo passo a passo para encriptar e para decriptar simplesmente executa o processo invertendo os passos.

Já a chave pública como trata os dados como números, é uma função de via única, sendo a matemática fácil em uma direção, mas difícil na direção contraria.

Existem três algoritmos que são mais utilizados para resolver o problema de distribuição de chaves: RSA (*Rivest, Shamir, Adleman*), DH (*Diffie-Hellman*) e ECDH (*Elliptic Curve Diffie-Hellman*).

O algoritmo RSA encripta os dados, alimentando o algoritmo com um texto simples junto com uma chave pública, obteremos um texto cifrado.

O algoritmo DH, não gera uma chave simétrica e distribui com a tecnologia da chave pública, mas utiliza a tecnologia da chave pública para gerar uma chave simétrica. Este algoritmo não criptografa os dados, mas gera um segredo.

O algoritmo ECDH é uma curva elíptica, que para os criptógrafos caem em duas categorias principais chamadas de impar e par. Uma curva elíptica tem pontos, chamados de coordenadas x, y.

Entre os três algoritmos não podemos afirmar qual seja o melhor, o que temos que avaliar é a situação.

Para avaliar a situação temos que examinar a segurança, tamanho da chave, desempenho, tamanho de transmissão e interoperabilidade.

4.4 ASSINATURA DIGITAL

Em criptografia o ato de uma chave publica decriptar dados de maneira adequada, significa que estes dados devem ter sido encriptado com uma chave privada, esta técnica é chamada de assinatura digital.

Qualquer coisa que for encriptada com uma chave privada é reconhecida como uma assinatura digital.

Cada assinatura é única para os dados assinados e chaves utilizadas, se assinarmos duas mensagens utilizando a mesma chave, as assinaturas serão diferentes.

A assinatura digital é única, tornando a falsificação muito difícil, garantindo assim a autenticidade e integridade dos dados recebidos.

Por esta razão a cada dia as empresas estão utilizando mais este recurso que facilita a vida de vários executivos, pois podem sair em viagem e assinar seus contratos digitalmente através da comunicação via Internet.

Contratos ou acordos firmados através da assinatura digital já possui o mesmo valor jurídico que um assinado manualmente.

No Brasil a assinatura digital é conhecida como E-CPF, que é homologado e emitido por empresas autorizadas, tais como a Serasa.

4.5 CERTIFICADOS DE CHAVE PÚBLICA

Dentro de uma rede um método seguro de distribuição de chave pública para as partes envolvidas, é a utilização de certificados de chave pública, conhecidos como PKC (*Public Key Certificate*).

Atualmente temos vários certificados em utilização, como o *Pretty Good Privacy* (PGP) que é patenteado.

Os certificados mais populares são específicos de um aplicativo como certificados SET e o *Internet Protocol Security* (IPSec).

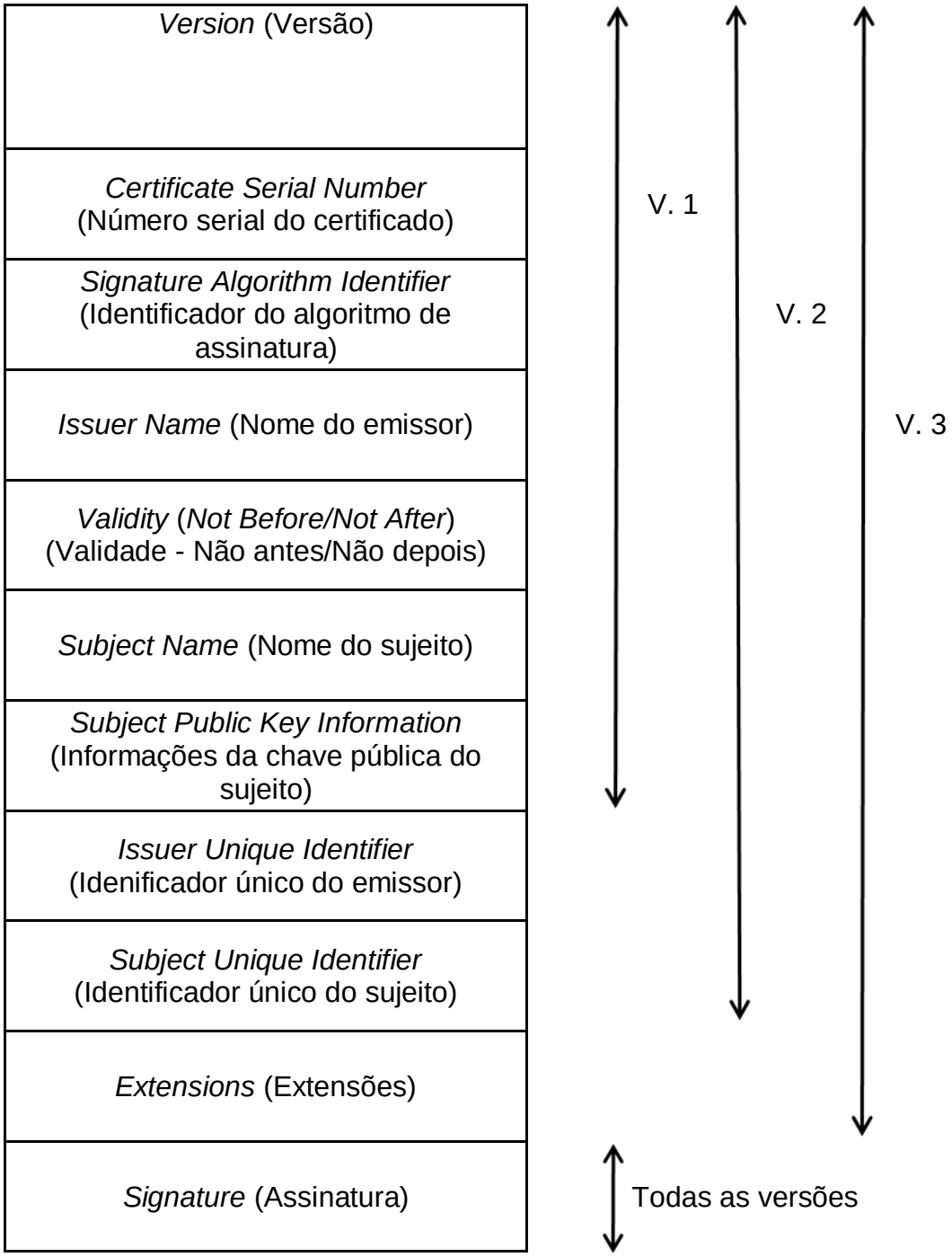
O formato de certificado mais aceito é o X.509 Versão 3 da *International Telecomunications Union*.

Os nomes das entidades tanto para o emissor quanto para o sujeito são únicos em um certificado de chave pública.

Existem as CA (*Certification authorities*) que fazem o fornecimento de certificados dando autenticidade a seus usuários finais.

Os certificados gerados são armazenados pelos seus usuários em suas máquinas locais.

Figura 4: Estrutura do Certificado X.509



Fonte: BURNETT, Steve & PAINE, S. Criptografia e Segurança – O Guia Oficial RSA, p. 147

4.6 PROTOCOLOS DE REDE E DE SEGURANÇA DE TRANSPORTE

Os protocolos de segurança têm um amplo serviço de criptografia e de autenticação, tornando seguro aplicativos, sistemas e redes.

Temos o IPSec (*Internet Protocol Security*) que utiliza uma estrutura de padrões abertos, assegurando uma comunicação privada e segura na rede de IP.

Desta maneira o IPSec garante a confidencialidade, integridade e autenticidade dos dados transmitidos, e também implementa criptografia e a autenticação na camada de rede.

Para proteger a confidencialidade, integridade e autenticidade dos pacotes de IP, o IPSec utiliza várias tecnologias de segurança.

Os serviços de segurança na camada de IP, são fornecidos pelo IPSec, que permite que um sistema possa selecionar os protocolos de segurança requeridos.

O IPSec é responsável em fornecer segurança na camada de IP, o que permite que os sistemas possam selecionar os protocolos de segurança requeridos, determinando qual algoritmo será utilizado no serviço e também qualquer chave criptográfica requerida para o fornecimento dos serviços de controle de acesso, integridade sem conexão, autenticação da origem dos dados, rejeição de pacotes repetitivos, criptografia e confidencialidade limitada do fluxo de tráfego.

Para o fornecimento destes serviços o IPSec necessita utilizar dois protocolos, conhecidos como *Authentication Header* (AH) e o *Encapsulating Security Payload* (ESP).

O AH é responsável por suportar o controle de acesso, a autenticação da origem de dados, a integridade sem conexão e a rejeição de ataques do tipo *replay*, utilizado por invasores para copiar um pacote e enviá-lo fora de sequencia para tentar confundir os nós de comunicação.

Também fornece os serviços de integridade de dados e de autenticação para os pacotes IP, garantindo a proteção contra ataques comuns montados contra redes abertas.

Como a tecnologia da assinatura digital é muito lenta o AH utiliza uma função de *hash* com chaves.

Apesar de tudo isso ele não garante a proteção de confidencialidade, permitindo a visualização dos dados conforme eles trafegam pela rede.

O ESP sozinho pode suportar confiabilidade, controle de acesso, confiabilidade limitada do fluxo de tráfego e também a rejeição de ataques do tipo *replay*.

Ele fornece os serviços de confiabilidade para os dados de IP enquanto eles trafegam por redes não-confiadas, podendo também fornecer o serviço de autenticação.

O *Secure Sockets Layer* (SSL) é o protocolo de Internet para a criptografia e autenticação com base em sessão, garantindo um canal seguro entre o cliente e o servidor.

Para evitar espionagem, adulteração ou falsificação de aplicativos cliente-servidor, o SSL fornece uma autenticação de servidor e outra opcional de cliente.

O SSL funciona na camada de transporte, e é totalmente independente dos protocolos de aplicativos utilizados.

4.7 PROTOCOLOS DE SEGURANÇA NA CAMADA DE APLICATIVO

Para manter a segurança do e-mail, utiliza-se a especificação conhecida como *Secure/Multipurpose Internet Mail Extentions* (S/MIME), que é baseado no padrão popular MIME.

Esse serviço de segurança são a autenticação, não-repúdio, integridade e a confidencialidade de mensagem.

Atualmente o S/MIMEv.3 é utilizado para aprimoramento de segurança do conteúdo de MIME, como dados tunelados, dados assinados em texto claro e dados assinados tunelados, e também proporciona suporte a vários algoritmos simétricos de criptografia de conteúdo.

Tabela 3: Algoritmos de segurança utilizados dentro do S/MIMEv.3

Algoritmo de resumo e de *hash*	Devem Suportar o MD5 e SHA-1
Algoritmos de assinatura digital	Agentes de envio e de recebimento devem suportar o DSA e RSA.
Algoritmos de chave de criptografia	Agentes de envio e de recebimento devem suportar *Diffie-Hellman* e também a criptografia RSA.
Algoritmo de criptografia de dados (chave de sessão)	Agentes de envio devem suportar uma chave RC2 de 40 bits, RC2 de 128 *bits* e o Triple DES. Agentes receptores precisam suportar o RC2 de 128 *bits* e o *Triple* DES, mas devem suportar o RC2/40.

Fonte: BURNETT, Steve & PAINE, S. Criptografia e Segurança – O Guia Oficial RSA, p. 210

O melhor algoritmo a ser utilizado sempre será o que tiver a maior chave, o que garantira a melhor segurança.

5 HARDWARE CRIPTOGRÁFICO

Os sistemas criptográficos têm um desempenho variável, sendo que alguns exigem muito do sistema do computador, para resolver está questão podemos utilizar um *hardware* criptográfico.

Atualmente encontramos no mercado diversos tipos de *hardware* criptográficos, tais como: Aceleradores criptográficos, *Tokens*, cartões de proximidade, cartões inteligentes, *JavaCards* e biometria.

5.1 ACELERADORES CRIPTOGRÁFICOS

Funcionam como um co-processador matemático, implementando no *hardware* um conjunto de funções que geralmente são tratados por um determinado *software*. Ele nos fornece dois benefícios, aumento de velocidade o que resulta no segundo beneficio que é a redução da carga de trabalho na CPU do sistema, permitindo desta maneira que a CPU possa ser utilizada por outros aplicativos de uma maneira mais eficiente.

Os aceleradores criptográficos tornaram-se populares devido a varias certificações associadas a eles.

Figura 5: Acelerador Luna

Fonte: BURNETT, Steve & PAINE, S. Criptografia e Segurança – O Guia Oficial RSA, p. 63

5.2 TOKENS CRIPTOGRÁFICOS

Os *tokens* de autenticação são muito importantes quando falamos de segurança de computador, pois fornecem um meio de autenticação e identificação de um usuário.

Os *tokens* mais avançados contem um microprocessador e memória semicondutora, suportando protocolos sofisticados de autenticação, garantindo um alto nível de segurança.

Existem vários modelos de *tokens* criptográficos.

Figura 6: Token criptográfico da Rainbow Technologies

Fonte: BURNETT, Steve & PAINE, S. Criptografia e Segurança – O Guia Oficial RSA, p. 232

Figura 7: Token criptográfico da Datakey

Fonte: BURNETT, Steve & PAINE, S. Criptografia e Segurança – O Guia Oficial RSA, p. 232

Outro modelo de *token* utilizado é o cartão de proximidade, que utilizam sinais de freqüência de rádio para fazer a autenticação do usuário.

Eles transmitem um sinal codificado quando estão dentro de um intervalo de uma leitora de proximidade.

Figura 8: Cartão e leitora de proximidade

Fonte: BURNETT, Steve & PAINE, S. Criptografia e Segurança – O Guia Oficial RSA, p. 233

Um dos *tokens* mais utilizados é conhecido como geradores de senha, por serem portátil e terem um alto nível de segurança. Ele fornece um código numérico aleatório de seis dígitos.

Figura 9: Token SecurID e SecurID no Palm OS

Fonte: BURNETT, Steve & PAINE, S. Criptografia e Segurança – O Guia Oficial RSA, p. 234

Os cartões conhecidos como inteligentes são um *token* do tamanho de um cartão de crédito com um *chip* embutido no circuito integrado, fornecendo a capacidade de memória e computacional. Este tipo é muito utilizado como um cartão de identificação para assegurar a identidade do portador, como cartão de crédito ou cartão bancário de débito.

Figura 10: Cartão inteligente da RSA Secutiry

Fonte: BURNETT, Steve & PAINE, S. Criptografia e Segurança – O Guia Oficial RSA , p. 236

Estes cartões podem ser conectados em uma variedade de dispositivos de leitora.

A maioria das instituições financeiras e de cartão de crédito já utiliza o cartão inteligente para evitar a clonagem.

O *JavaCard* é um *token* que opera com um cartão inteligente, existem outros tipos de *token* de Java, como o anel que contem um microprocessador de 8 *bits* chamado de *Crypto iButton*.

Figura 11: Anel Java

Fonte: BURNETT, Steve & PAINE, S. Criptografia e Segurança – O Guia Oficial RSA, p. 241

5.3 BIOMETRIA

A palavra biometria tem origem grega e significa *bio* = vida e *métron* = medida.

A biometria é a ciência utilizada para medir a característica física e comportamental do corpo humano, tais como impressão digital, retina, íris, impressão da palma da mão, estrutura fácil, voz.

Por está característica ser única de cada pessoa, a biometria está se tornando um excelente meio de autenticação com alto nível de segurança, visto que a senha passa a ser o próprio usuário.

A biometria funciona através de dois modos conhecidos como inscrição e verificação.

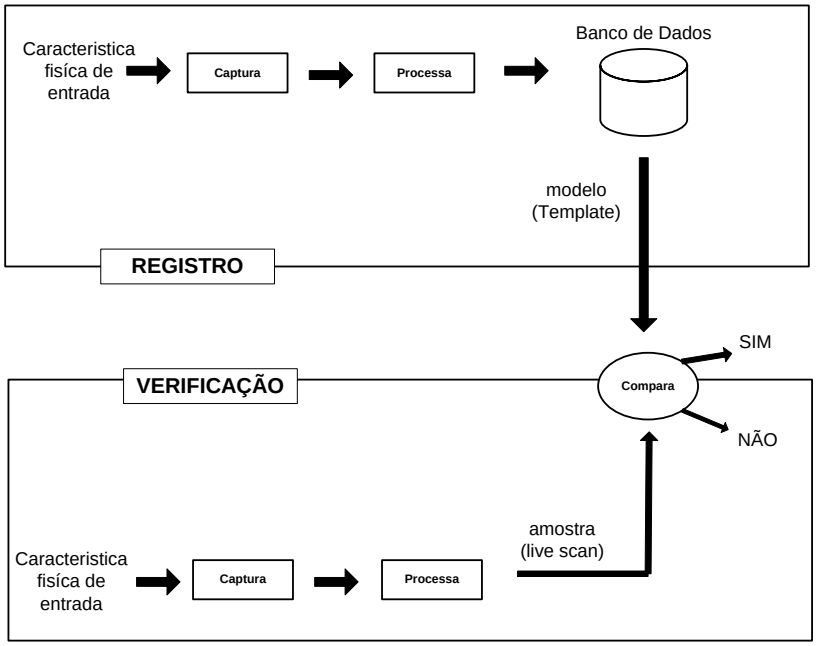
Todo usuário ao iniciar a utilização do recurso da biometria, deve ser inscrito em um sistema onde sua característica biológica ficará armazenada para futuro confronto de autenticação. A obtenção desta característica é feita através de um dispositivo de *hardware* conhecido como sensor.

Depois que o usuário já estiver inscrito, sua biometria será utilizada para verificar sua identidade e garantir a sua autenticidade.

O sensor efetua a leitura da característica biológica do usuário e efetua uma varredura no sistema para fazer a autenticação.

O sistema não guarda foto do rosto ou a impressão digital do usuário, mas sim o valor que representa a identidade biométrica, as características extraídas são convertidas em um padrão único e armazenadas como um dado numérico criptografado em um banco de dados.

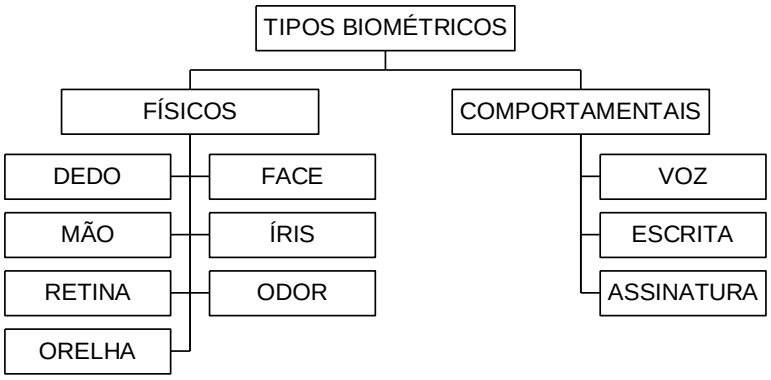
Figura 12: Modelo de registro e verificação biométrica



Fonte: PINHEIRO, J. M. Biometria nos Sistemas Computacionais – Você é a Senha, p. 55

O sistema de biometria é constituído pelos tipos físicos e comportamentais.

Figura 13: Elementos biométricos



Fonte: PINHEIRO, J. M. Biometria nos Sistemas Computacionais – Você é a Senha, p. 62

5.3.1 ELEMENTOS FÍSICOS

5.3.1.1 RECONHECIMENTO FACIAL

Está tecnologia trabalha com as medidas do rosto que nunca são alteradas, mesmo que a pessoa faça uma cirurgia plástica.

As medidas consideradas são a distância entre os olhos, entre a boca, entre nariz e olhos, entre olhos e queixo, boca e linha dos cabelos.

O seu funcionamento se dá através da captura da imagem com a utilização de uma câmera ou máquina fotográfica, em seguida um algoritmo faz a verificação dos pontos comuns, comparando com o registro existente no arquivo de banco de dados.

Apesar de um conjunto de imagens possibilitarem a identificação de uma pessoa, este método tem a desvantagem de oferecer pouca confiabilidade, exigir muito tempo para leitura e pesquisa da informação e um alto custo para ser implantado.

5.3.1.2 IMPRESSÃO DIGITAL

A impressão digital por ser uma característica única de cada pessoa, é considerada um dos tipos biométricos mais seguro.

O sistema funciona através da captura da imagem da impressão digital por meio óptico, que é processada digitalmente e comparada com o registro existente no banco de dados.

O sistema faz a identificação através das características datiloscópicas, que são as irregularidades das impressões digitais, chamadas de minúcias.

Figura 14: Minúcias encontradas na impressão digital

Fonte: PINHEIRO, J. M. Biometria nos Sistemas Computacionais – Você é a Senha, p. 64

Este sistema requer a utilização de um *scanner* com capacidade de capturar a impressão digital com um bom grau de precisão das minúcias, e também um *software* para tratar a imagem capturada e fazer o reconhecimento.

Este método também é conhecido como *Finger Scan*, oferece uma boa confiabilidade e tem baixo custo para implantação.

A única desvantagem é quando o dedo estiver sujo, desgastado, muito seco ou úmido, ou tiver com alguma deformidade como um corte ou calo, visto que poderão ocorrer erros no processo de comparação dos dados.

5.3.1.3 GEOMETRIA DA MÃO

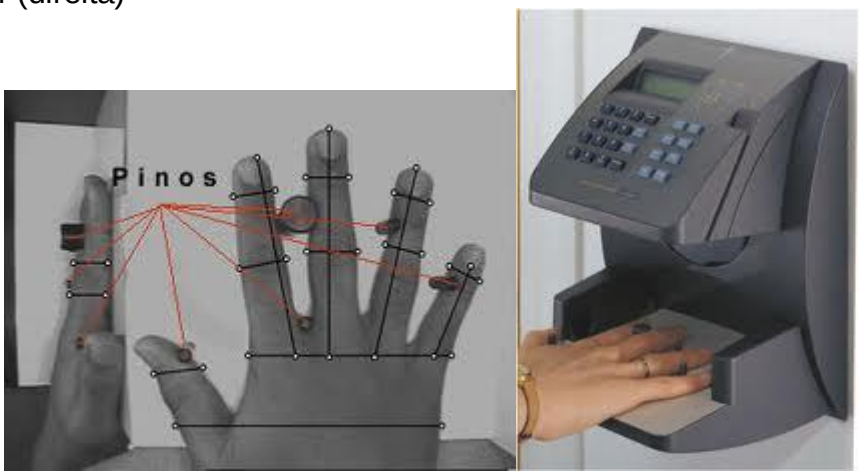
Este método utiliza um *scanner* para capturar as medidas das palmas das mãos, mãos e dedos, através de uma perspectiva tridimensional.

O *scanner* que efetua a leitura da geometria da mão possui guias parecidos com pinos para encaixar entre os dedos da pessoa, facilitando o reconhecimento do desenho da mão.

O sistema efetua o calculo das proporções entre os dedos e articulações da mão e efetua o registro no banco de dados.

É um sistema de baixo custo para ser implantado, mas não é muito confiável, visto que a presença de anéis no dedo da pessoa, ou o encaixe incorreto da mão no aparelho de leitura pode ocasionar problemas na identificação.

Figura 15: Medidas típicas da geometria da mão, imagem real (esquerda) e dispositivo leitor (direita)



Fonte: PINHEIRO, J. M. Biometria nos Sistemas Computacionais – Você é a Senha, p. 67

5.3.1.4 IDENTIFICAÇÃO PELA ÍRIS

A íris é a parte colorida do olho que se localiza em torno da pupila, contém 249 pontos de diferenciação que podem ser utilizados em um processo de reconhecimento de uma pessoa.

Em virtude das características da íris não se alterar pelo envelhecimento da pessoa, ela é considerada um identificador biométrico bastante estável, tornando-se mais preciso do que a identificação pela impressão digital ou pela face.

Mesmo que uma pessoa esteja utilizando lentes de contato ou óculos não muito escuros, não compromete o seu reconhecimento, o que traz mais segurança ao processo.

Este sistema tem alto desempenho no processo de verificação e identificação, podendo ultrapassar a marca de 100 mil registros por segundo.

A desvantagem deste processo, é que dependemos da colaboração do usuário para fazer a coleta dos dados da íris, por ser muito pequena e localizada atrás de uma superfície refletora e parcialmente oculta por pálpebras que piscam constantemente, dificultando o registro dos dados.

O processo é feito em três etapas, o da aquisição da imagem da íris, a aplicação de um algoritmo de extração e reconhecimento das características biométricas, e a extração das características que geram o *iriscode*.

Apesar de ser uma tecnologia excelente para reconhecimento, o seu desenvolvimento em larga escala está impedido por falta de base instalada.

5.3.1.5 IDENTIFICAÇÃO PELA RETINA

O método é semelhante ao reconhecimento pela íris.

A retina é a membrana interna do globo ocular, composta por vasos sanguíneos que desenham um padrão único e pessoal, permitindo o reconhecimento da pessoa, pelo tipo e características destes vasos, sendo considerado um dos métodos biométricos mais seguros.

Os dados da retina são adquiridos através de um exame “in loco”, convertidos em sinal analógico e transformados em sinal digital para ser armazenado no banco de dados do sistema biométrico.

A desvantagem deste sistema é que o método utilizado para leitura é difícil e incomodo, visto que exige que a pessoa olhe fixamente para um ponto de luz infravermelho, até que a câmera consiga focalizar e capturar os padrões, e também tem um alto custo para ser implantado.

5.3.2 ELEMENTOS COMPORTAMENTAIS

5.3.2.1 RECONHECIMENTO DE VOZ

Está tecnologia também é conhecida como *Speaker ID*, que analisa os padrões harmônicos, para isto é necessário um dispositivo para adquirir a característica biométrica, que pode ser um microfone ou telefone.

O sistema funciona com a captura e processamento digital ao áudio falado, utilizando um algoritmo especial, que faz o fracionamento do áudio em pequenos fonemas.

O sistema funciona com o armazenamento do som gravado pelo usuário, que pode ser utilizado palavras ou frases predefinidas para ser pronunciada.

O sistema analisa os padrões harmônicos e verifica a probabilidade de cada fonema para obter a identificação do usuário.

Este é um sistema simples e de fácil utilização, que pode resultar em redução de custos operacionais e aumento na segurança.

A desvantagem deste sistema é que os ruídos no ambiente, estado de saúde do usuário como gripe, estresse podem interferir na identificação.

5.3.2.2 RECONHECIMENTO PELA DINÂMICA DA DIGITAÇÃO

Está tecnologia é conhecida como *Keytrokes Dynamics*, geralmente utilizada para controle de acesso a equipamentos de uma rede de computadores.

Não é um sistema muito confiável, mas é de baixo custo para ser implantado, a autenticação do usuário é feita através de uma analise que se baseia na forma como foi digitado o nome e senha.

A vantagem deste sistema é que ele não necessita utilizar nenhum *hardware* adicional para seu funcionamento, basta ter o *software* para analise do ritmo da digitação para fazer a identificação do usuário.

5.3.2.3 RECONHECIMENTO DA ASSINATURA MANUSCRITA

A nossa assinatura manual é aceita por vários meios e é a maneira mais utilizada para confirmar a identificação pessoal.

Este método analisa a velocidade e a pressão exercida pela mão sobre a caneta e o papel no ato da assinatura, além disso, também procura armazenar as características mais constantes na assinatura.

Os sistemas existentes no mercado baseiam-se em dois tipos, dinâmicos e estáticos e utilizam uma caneta especial com uma prancheta digitalizadora para obter a assinatura e efetuar o armazenamento no banco de dados.

O sistema dinâmico de assinatura é conhecido como sistema *On-line*, que usa as características da escrita como a velocidade e aceleração.

Este método analisa o formato das letras, a pressão da caneta sobre o papel, a velocidade, e os pontos onde a caneta não toca no papel, garantindo uma alta taxa de acerto, entretanto este sistema biométrico tem um alto custo para implantação.

A desvantagem deste sistema é a necessidade de uma grande quantidade de amostra de assinatura dos usuários para serem cadastradas no banco de dados, além disso, muitos usuários alteram suas assinaturas com o decorrer do tempo, o que requer um recadastramento para atualizar o sistema.

O sistema estático é conhecido como Sistema *Off-line*, utiliza apenas a imagem da assinatura para obter as informações que alimentam o sistema, tendo uma taxa de acerto inferior ao sistema *On-line*.

A vantagem deste sistema é que há a preservação do processo da escrita, visto que não utiliza nenhum dispositivo eletrônico que possa interferir na assinatura.

6 CONSIDERAÇÕES FINAIS

Considerando os dados estudados nesta monografia, podemos concluir que com o crescente aumento da utilização da internet, computação em nuvens, banco de dados, Data Center, a segurança dos dados ou da informação é fundamental para as empresas.

As empresas estão cada vez mais investindo em *hardware* e *software* para garantir a integridade das informações para seus clientes.

Para atingir este objetivo, as empresas estão investindo pesado na instrução dos usuários para que eles aprendam utilizar os sistemas corretamente e armazenar as informações de uma maneira segura.

Com toda está preocupação, houve a necessidade das empresas especializadas em segurança da informação, desenvolver sistemas para assegurar as transações, desta maneira iniciou-se a utilização da criptografia nos sistemas de informação, através de algoritmos criptográficos, que foram introduzidos nas transações realizadas pelas empresas, seja para garantir o armazenamento das informações no banco de dados, ou para transmissão de informações por e-mail ou através do uso da internet.

Os *hardwares* criptográficos foram introduzidos para fornecer uma segurança adicional ao sistema, visto que podem assegurar a identificação do usuário.

Dentre eles, os mais utilizados são os *tokens*, principalmente pelas instituições financeiras que necessitam assegurar a seus clientes que suas transações não serão expostas aos *hackers*.

Além do *token*, a utilização de *hardwares* biométricos vem se afirmando como uma tendência para o mercado num futuro próximo, com destaque para a identificação através da impressão digital e reconhecimento facial.

A identificação através da impressão digital já está sendo incluída em alguns equipamentos de uso doméstico e comercial, como os *notebooks*, também foi

testada nas eleições realizada este ano no Brasil, para identificar os eleitores em algumas zonas eleitorais.

Muitas empresas estão aderindo à utilização do sistema de biometria com reconhecimento através da impressão digital, o que tem gerado uma economia com problemas de remissão de senhas para os usuários que esquecem ou bloqueiam seu acesso.

Seguindo está tendência, o reconhecimento facial está sendo estudado para ser utilizado como identificação das pessoas na próxima copa do mundo a ser realizada no Brasil.

Alguns veículos já estão sendo equipado para acionamento da partida somente após o reconhecimento do proprietário através da impressão digital ou o reconhecimento facial.

Empresas especializadas estão investindo nestes equipamentos que estão sendo chamados de dispositivos antifurto veicular biométrico.

Isto tudo somente vem confirmar a tendência do futuro, haverá um aumento na utilização dos sistemas de biometria para identificação das pessoas, seja para obterem acesso aos seus computadores pessoais ou sistemas no trabalho, para acionarem seus carros ou até mesmo abrirem a porta para entrar em suas casas, ao invés de utilizarem as chaves comuns existentes atualmente.

7 REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Citação:** NBR-10520/ago - 2002. Rio de Janeiro: ABNT, 2002.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Referências:** NBR-6023/ago. 2002. Rio de Janeiro: ABNT, 2002.

BURNETT, Steve & PAINE, S. **Criptografia e Segurança – O Guia Oficial RSA.** 6ª Edição**.** Rio de Janeiro: Editora Elsevier Editora Ltda., 2002.

FONTES, E. **Segurança da Informação – O usuário faz a diferença.** São Paulo: Editora Saraiva, 2006.

LAUDON, K. C., LAUDON, J. P. **Sistemas de Informação.** 4ª Edição. Rio de Janeiro: Etitora LTC, 1999. p.260-281.

PINHEIRO, J. M. **Biometria nos Sistemas Computacionais – Você é a Senha.** Rio de Janeiro: Editora Ciência Moderna Ltda., 2008.

STAIR, R. M., REYNOLDS, G. W. **Princípios de Sistemas de Informação.** 4ª Edição. Rio de Janeiro: Editora LTC, 2002. p. 2-29.