FAE
CENTRO UNIVERSITÁRIO

CRISTIAN FERNANDES DE SOUZA
RAFAEL DUARTE DE PAULA RIBAS

AVALIAÇÃO DOS SISTEMAS BIOMETRICOS E SUAS OPORTUNIDADES DE APLICAÇÃO

CURITIBA
2012

CRISTIAN FERNANDES DE SOUZA

RAFAEL DUARTE DE PAULA RIBAS

AVALIAÇÃO DOS SISTEMAS BIOMETRICOS E SUAS OPORTUNIDADES DE APLICAÇÃO

Trabalho acadêmico apresentado como requisito parcial para avaliação da disciplina de Pesquisa e Projeto de Curso de Pós Graduação para a Especialização *lato sensu* em Gestão da Tecnologia da Informação da FAE Centro Universitário.

Orientador : Prof. Dr. Luis Pedro Zambon

CURITIBA

Dezembro 2012

CRISTIAN FERNANDES DE SOUZA
RAFAEL DUARTE DE PAULA RIBAS

AVALIAÇÃO DOS SISTEMAS BIOMETRICOS E SUAS OPORTUNIDADES DE APLICAÇÃO

Este trabalho foi julgado adequado para obtenção do título *lato sensu* em Gestão da Tecnologia da Informação e aprovado na sua forma final pela Banca Examinadora, da FAE Centro Universitário.

Curitiba, 04 de dezembro de 2012.

BANCA EXAMINADORA

Prof. Dr. Luis Pedro Zambon
Orientador

_____

_____

Dedicamos este projeto de pesquisa aos nossos pais e esposas por nos darem força e apoio nos momentos difíceis deste longo caminho.

Agradecimentos

Queremos agradecer em primeiro lugar a Deus, pela força e coragem durante todo este projeto.

Ao Professor. Doutor. Luis Pedro Zambon pelo auxilio e contribuições ao trabalho e também por seu comprometimento.

Aos pais e esposas que com muito carinho e apoio, não mediram esforços para que chegássemos a esta etapa de nossas vidas.

RESUMO

RIBAS, Rafael Duarte de Paula, SOUZA, Cristian Fernandes de. **Avaliação dos sistemas biométricos e suas oportunidades de aplicação.** 71p. Trabalho de conclusão de curso (Gestão da Tecnologia da Informação) – FAE – Centro Universitário. Curitiba, 2012.

Com o crescente avanço de pesquisas e demandas por novas tecnologias de segurança da informação, é cada vez mais comum vermos empresas utilizando a segurança biométrica para proteger seus dados e acesso a locais restritos. Questões como segurança nacional, comércio eletrônico e acesso a áreas de segurança virtual ou física são alguns exemplos onde à identificação pessoal é vital. Os métodos convencionais de autenticação e segurança utilizados, nem sempre são seguros, pois podem facilmente ser roubados ou compartilhados. A adoção da tecnologia biométrica trata de proteger as empresas de fraudes e ameaças virtuais. Neste trabalho são apresentados os principais tipos de segurança biométrica, correlacionando com outros tipos de sistemas de segurança da informação. Com os estudos dos principais meios de segurança da informação utilizados, o principal objetivo foi identificar as melhores práticas da TI (Tecnologia da Informação) em sistemas de segurança da informação, correlacionando com a legislação que trata de auditoria voltada à segurança da informação em ti e a segurança biométrica aplicada ao case recente do sistema de votação brasileiro. o presente estudo tomou por base a avaliação dos dados fornecidos pelo TSE (Tribunal Superior Eleitoral) sobre a implantação e uso da tecnologia biométrica nas eleições de 2012. Como resultado do presente trabalho foi possível identificar as principais dificuldades do TSE na implantação do cadastramento eleitoral utilizando o sistema biométrico e também a adoção da biometria pelos eleitores. A partir da conclusão do trabalho, foram identificadas oportunidades de aplicações de sistemas biométricos em outros sistemas de autenticação e acesso a informação.

Palavras-chave: Biometria. Sistemas de Segurança da Informação. Eleições 2012. Aplicações biométricas. Segurança biométrica.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

AI – Adquirir e Implementar

ATM – Terminal de Atendimento Bancário

CERT – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança.

CNPJ – Cadastro Nacional de Pessoa Jurídica

COBIT – Control Objectives for Information and Related Technology

CPF – Cadastro de Pessoa Física

DDoS – Ataque de negação de serviço

DIRETRAN – Diretoria de Trânsito

DNA – Ácido Desoxirribonucleico

DS – Entregar e Suportar

FIEP – Federação das Indústrias do Estado do Paraná

ICP- Infraestrutura de Chaves Públicas

IEC – International Eletroteclimical Comission

ISO – International Organization for Standardization.

ITIL – Information Technology Infrastructure Library

ME – Monitorar e Avaliar

NBR - Norma Brasileira

NF-e – Nota Fiscal Eletrônica

NIC.BR – Núcleo de Informação e Coordenação do Ponto BR.

PDV – Ponto de Venda

PM – Project Management

PO – Planejar e Organizar

PR – Estado do Paraná

RSA – Algoritmo de Criptografia

SERPRO – Serviço Federal de Processamento de Dados

SOX – Sarbanes-Oxley

TI – Tecnologia da informação

TRE – Tribunal Regional Eleitoral

TSE – Tribunal Superior Eleitoral

UTI – Unidade de Tratamento Intensivo

VOIP – Voice Over Internet Protocol

SUMÁRIO

1 INTRODUÇÃO

Com a expansão diária do mundo da tecnologia, a autenticação e identificação pessoal para acesso a sistemas estão cada vez mais comuns em empresas de todo o mundo. Questões como segurança nacional, comércio eletrônico e acesso a áreas de segurança virtual ou física são alguns exemplos onde à identificação pessoal é vital. Senhas, cartões de identificação e de acesso, passaportes são algumas das medidas de segurança que vinham e continuam a ser utilizadas. Estes métodos são pouco seguros. Senhas, cartões de acesso e identificação podem ser roubados ou compartilhados. Este tipo de identificação não permite diferenciar entre um usuário autorizado e alguém que teve acesso por meios ilícitos.

A identificação biométrica usa de características próprias das pessoas para identificação, por meio da impressão digital, íris, voz ou assinatura oferecem meios de autenticação seguros e de confiança que podem ultrapassar os problemas conhecidos ganhando assim aceitação das empresas, governo e da população em geral.

Este trabalho tem por objetivo abordar e comparar as características dos sistemas de segurança biométrico com outros tipos de sistemas de segurança aplicáveis à segurança da informação, para identificar oportunidades de aplicação em sistemas de acesso. Aprofundando-se mais no assunto este trabalho irá apresentar um estudo com base em um caso real, utilizando dados fornecidos pelos TSE (Tribunal Superior Eleitoral) sobre o uso da biometria nas eleições de 2012.

1.1 PROBLEMA

Qual a relevância dos sistemas de segurança biométricos para garantir a segurança da informação?

1.2 HIPÓTESE

A hipótese de pesquisa foi definida como: O uso de sistemas biométricos

tende a garantir a segurança da informação com maior confiabilidade do que os sistemas tradicionais que não utilizam sistemas biométricos.

1.3 OBJETIVO

Comparar as características dos sistemas de segurança biométrico com outros tipos de sistemas de segurança aplicáveis à segurança da informação, para identificar oportunidades de aplicação em sistemas de acesso.

1.3.1 Objetivos Específicos

a) Levantar o estado da arte da tecnologia em relação aos sistemas de segurança da informação;
b) Levantar o estado da arte da tecnologia em relação aos sistemas de segurança biométricos;
c) Caracterizar os vários tipos de segurança da informação;
d) Analisar um estudo de caso que aplique a biometria;
e) Comparar as características dos sistemas de segurança biométricos com outros tipos de segurança aplicáveis à segurança da informação;
f) Identificar oportunidades de aplicação dos meios de segurança mais usados.

1.4 JUSTIFICATIVA

As empresas que desejam alcançar valor, inovação, eficiência e crescimento dependem da informação, sendo assim, seu sucesso depende em manter uma estrutura de TI segura e confiável. A segurança da informação é algo primordial nos dias de hoje, seja perante usuários comuns, empresas ou organizações em geral (PINHEIRO, 2008).

Tendo em ênfase essa perspectiva de tecnologia da informação segura, analisaremos no trabalho proposto se os sistemas de segurança mais disseminados atualmente, tais como, o uso de senhas ou tokens são os mais indicados, ou se a necessidade atual obrigará as empresas a usarem métodos de segurança mais

eficazes, como a biometria.

Para Vigliazzi (2006, p.2), “biometria, na segurança da informação, significa a verificação da identidade de um indivíduo através de uma característica única inerente a essa pessoa por meio de processos automatizados”.

O trabalho procurará analisar se o uso de sistemas biométricos é mais seguro que o uso de sistemas de segurança tradicionais. Alguns exemplos de sistemas biométricos são caligrafia, geometria das mãos, timbres de voz, estrutura da íris e das veias, como são fenótipos do ser humano não podem ser reproduzidos, perdidos ou esquecidos.

Segundo Tracy Wilson (2005) devem ser tomadas precauções com relação à biometria, que como qualquer outro sistema não é perfeito, ela por si só não faz milagres sendo necessária a intervenção do usuário e o uso de sistemas adicionais de segurança nas organizações.

Para analisar os sistemas de segurança com ênfase na biometria serão estudadas normas sobre o assunto, alguns meios em que a biometria é usada, e um estudo de caso prático do uso de sistemas de biométricos em urnas eletrônicas utilizadas pelo Superior Tribunal Eleitoral.

2. FUNDAMENTAÇÃO TEÓRICA

A segurança da informação é o meio pelo qual empresas, governos e pessoas tentam proteger informações importantes de intervenções alheias a seus interesses. Gestores e analistas de segurança da informação têm a responsabilidade de gerir os meios de segurança, pois a informação é o ativo mais valioso para uma organização, sendo assim, é necessário elaborar e garantir critérios que protejam as informações contra fraudes, roubos ou vazamentos de informação.

Para estabelecer informações sobre segurança da informação, foram consultados diversos documentos publicados por órgãos responsáveis por este assunto, assim como outros documentos, tais como:

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança, conhecida popularmente como CERT, é um órgão de âmbito internacional que no Brasil é controlado pelo Núcleo de Informação e Coordenação do Ponto BR, mantido pelo NIC.BR. O CERT é responsável por tratar incidentes de segurança em computadores que envolvam redes conectadas à Internet brasileira. (CERT, 2012).

Uma breve explicação sobre normas que tratam de segurança também são apresentadas no trabalho, norma bastante conhecida no meio acadêmico e em empresas no âmbito da tecnologia, é a ISO 27002:2007, que trata de práticas para a segurança da informação, com ênfase em princípios e diretrizes gerais.

Outro ponto importante para o trabalho é estabelecer a relação do guia de boas práticas do Control Objectives for Information and Related Technology conhecido como COBIT, na relação das práticas usadas no mercado.

Por fim também é abordada a Lei Sarbanes-Oxley conhecida como SOX, pois, mesmo não sendo uma lei voltada para TI é embasada em normas de auditoria, e pode ser adaptada pelos administradores às necessidades da empresa.

2.1 SEGURANÇA DA INFORMAÇÃO

Para conceituar o que é segurança da informação, primeiramente é preciso abordar o que é a informação. Segundo a norma NBR ISO IEC 17799:2005, a

informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida. Para Rezende e Abreu (2000), “a informação é o dado com uma interpretação lógica ou natural dada a ele por seu usuário”. Em ambas as definições, a informação é tratada como um dado que faz parte de transações, negociações ou apenas dizer que faz parte do conhecimento. Pode ainda ser definida como um conjunto de medidas de controle e políticas de segurança, tendo como objetivo a proteção das informações de clientes e empresas, controlando o risco ou alteração por pessoas não autorizadas.

Segundo Silva (2003, p.16), “a segurança da informação engloba um número elevado de regras, que podem estar sob a gestão de uma ou mais pessoas”.

Entre estas regras estão:

a) Segurança de redes;
b) Segurança física;
c) Segurança de computadores;
d) Segurança de pessoas;
e) Segurança de aplicações;
f) Criptografia;
g) Gestão de projetos;
h) Formação;
i) Conformidade.

Para tanto estas regras são seguidas por indivíduos de cada empresa, o que torna as mesmas sujeitas a falhas, caso não possuam em seus escopos de funcionalidades de segurança o controle de redundância da informação a ser protegida.

Entende-se então por informação todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa. Para tanto se estabeleceu na norma NBR ISO IEC 17799:2005 que a segurança da informação deve proteger a informação ou dado, de qualquer tipo de ameaça que possa comprometer os negócios de uma organização. Assim maximizando o retorno sobre os investimentos realizados e garantindo que as oportunidades de negócios não sofram nenhuma interferência devido a alguma falha na segurança da informação. A segurança da informação se refere à proteção existente sobre as informações de uma determinada empresa ou pessoa, isto é, aplica-se tanto às informações corporativas quanto às

pessoais. E ela pode estar guardada para uso restrito ou exposta ao público para consulta ou aquisição.

Baseado no conceito de informação, a segurança da informação pode ser obtida a partir da implantação de um grupo de normas e regras, incluindo políticas de segurança, procedimentos e adequação de estruturas organizacionais. As políticas de segurança servem para que uma organização possa ter maior controle sobre a utilização da infraestrutura tecnológica e também visa melhorar a produtividade através de um ambiente mais organizado. Os controles sobre o acesso e compartilhamento de informação precisam ser estabelecidos e monitorados, pois é necessário garantir a integridade dos negócios de uma organização.

A segurança da informação está relacionada diretamente também com a integridade e confidencialidade de dados, não estando limitada somente a proteção de dados eletrônicos, mas sim também abrange o acesso à proteção de informações e dados.

Quando se aborda a confidencialidade, quer se enfatizar que a informação ou dado somente poderá ser concedida ao proprietário ou aquelas entidades que foram previamente autorizadas.

Para o estabelecimento das Políticas de Segurança da informação nas empresas, devem-se levar em conta os riscos associados à falta de segurança, às permissões a serem dadas às informações ou dados e o custo de implantação de mecanismos de proteção aos dados e informações. Mecanismos estes que podem ser físicos ou lógicos, e que neste caso a biometria se enquadra em sistemas de controle de acesso lógico. Pois utilizam a lógica de identificação de características físicas únicas para verificação e validação do acesso às informações e dados.

Para Pinheiro (2008, p.8), “a segurança da informação pode ser comparada a uma corrente formada por quatro elos (infraestrutura, tecnologia, aplicações e pessoas). A força desta corrente será medida pelo elo mais fraco.” Ou seja, se nenhum destes elos for bem estruturado ou capacitado para seguir as políticas de segurança definidas pela empresa, a segurança da informação tende a ser violada.

A segurança da informação também está relacionada diretamente com a integridade e confidencialidade de dados, não estando limitada somente a proteção de dados eletrônicos, mas sim também abrange o acesso a proteção de informações e dados.

Atualmente quando se trabalha com o conceito de segurança da informação, deve-se seguir o padrão estabelecido pela norma NBR ISO/IEC 17799:2005. Ela estabelece que a segurança da informação tenha como objetivos principais a:

a) Confidencialidade;
b) Integridade;
c) Disponibilidade das informações.

Quando se aborda a confidencialidade, quer-se enfatizar que a informação ou dado somente poderá ser concedida ao proprietário ou aquelas entidades que foram previamente autorizadas. Na integridade dos dados, deve-se garantir que a manipulação dos mesmos mantenha todas as características do dado original, incluindo o ciclo de vida do dado: criação, manutenção e exclusão. Na disponibilidade, deve-se garantir que os dados estarão disponíveis para o proprietário e todos os colaboradores autorizados pelo mesmo (PINHEIRO, 2008).

Existem outros cinco objetivos básicos que também devem ser considerados para a proteção da informação (ISO 17799:2005):

a) A consistência dos dados que se deve certificar atua de acordo com a expectativa dos usuários;
b) O isolamento ou uso legítimo controla o acesso e garante que somente usuários autorizados utilizem os recursos do sistema;
c) A auditoria, que tem como fim proteger os sistemas contra erros e atos cometidos por usuários autorizados. Onde a identificação dos autores e ações realizadas no sistema deve ser gravada em arquivos de logs;
d) A confiabilidade das informações e dados garante que mesmo em condições adversas, o sistema atuará conforme o esperado;
e) E a legalidade das informações, que garante que as mesmas devem estar em conformidade com os preceitos da Política de Segurança em vigor.

Estes cinco objetivos complementam os objetivos definidos pela norma ISO 17799:2005 e são de extrema importância para que a segurança da informação passe a ser seguida de acordo com as políticas de segurança da informação definidas em cada empresa.

Para Laureano (2005, p.11), “as redes de computadores, e consequentemente a Internet mudaram as formas como se usam sistemas de

informação. As possibilidades e oportunidades de utilização são muito mais amplas que em sistemas fechados, assim como os riscos à privacidade e integridade da informação. Portanto, é muito importante que mecanismos de segurança de sistemas de informação sejam projetados de maneira a prevenir acessos não autorizados aos recursos e dados destes sistemas".

Segundo Alves (2010,p.13):

> A informação é o ativo mais valioso das organizações, ao mesmo tempo também passa a ser o mais visado e desejado por pessoas mal intencionadas com objetivo de vasculhar por curiosidade, furtar para obter informações sigilosas e valiosas, trazer danos seja por diversão, benefício próprio ou vingança ou descobrir segredos. Por essas razões, mais do que nunca, existe uma preocupação enorme com relação à segurança das informações nas organizações e até mesmo nos lares, pois ela representa a inteligência competitiva dos negócios (competitividade) e lucratividade. Desta forma existe a exposição a uma enorme variedade de ameaças e vulnerabilidades.

Infelizmente, ainda não é da cultura das empresas investirem no treinamento e na conscientização dos seus funcionários, tanto quanto seria necessário para criar o cenário de proteção almejado. Afinal, eles também fazem parte da segurança da informação, mas as empresas acabam deixando de lado outro aspecto tão importante quanto à tecnologia, que é o fator humano, que por sinal é o elo mais fraco da segurança da informação.

Quanto mais a tecnologia e os dispositivos de segurança evoluir, dificultando assim a exploração de vulnerabilidades, mais os invasores explorarão o fator humano. Há somente uma maneira de combater a questão do fator humano e isso deve ser feito através de treinamentos e conscientização dos funcionários.

> Empregados devem ser treinados e orientados sobre o que a informação precisa para estar protegida e como protegê-la. Porém uma empresa pode ter adquirido as melhores tecnologias de segurança que o dinheiro pode comprar, pode ter treinado seu pessoal tão bem que eles trancam todos os segredos antes de ir embora e pode ter contratado guardas para o prédio na melhor empresa de segurança que existe. Mesmo assim essa empresa ainda estará vulnerável. Os indivíduos podem seguir cada uma das melhores práticas de segurança recomendadas pelos especialistas, podem instalar cada produto de segurança recomendado e vigiar muito bem a configuração adequada do sistema e a aplicação das correções de segurança. Esses indivíduos ainda estarão completamente vulneráveis. (MITNICK, SIMON, 2003, p. 3).

Portanto, segurança da informação é um conjunto de práticas e atitudes

diversas que podem ser adaptadas de acordo com o tamanho ou interesse da empresa, para a proteção, sigilo dos dados importantes que não devem ser compartilhados com indivíduos alheios ao sistema.

2.2 TIPOS DE SEGURANÇA DA INFORMAÇÃO

Há diversas maneiras de proteger a informação dentro das empresas, tanto de funcionários internos quanto externos. Os principais meios são:

a) Senhas;
b) Cookies;
c) Criptografia;
d) Certificados digitais.

Cada tipo de segurança de informação possui suas particularidades e fraquezas frente a novos tipos de segurança de informação como a biometria. Estão definidas abaixo algumas características sobre cada tipo de segurança da informação.

2.2.1. Senhas

Segundo o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT. BR, 2012):

> Uma senha (*password*) na Internet, ou em qualquer sistema computacional, serve para autenticar o usuário, ou seja, é utilizada no processo de verificação da identidade do usuário, assegurando que este é realmente quem diz ser.

Segundo o CERT.BR, se alguma outra pessoas obtiver acesso a sua senha ela poderá realizar as seguintes ações:

a) Ler e enviar e-mails em seu nome;
b) Obter dados bancários, como número e senha do banco, cartões de crédito, débito, e até realizar operações financeiras em seu nome;
c) Se passar por você, efetuando ataques e invasões a outros computadores.

Portanto, a senha é de uso pessoal, e não deve ser compartilhada com ninguém, pois quando feito pode ocasionar um incidente de segurança da

informação.

2.2.2. Cookies

Segundo o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT. BR, 2012), “cookies podem ser definidas como informações armazenadas no browser de navegação, contendo pequenas informações sobre os sites visitados anteriormente”. Servem ainda para agilizar o acesso a determinado conteúdo, como por exemplo:

a) Armazenar senhas de sites recentemente visitados;
b) Manter sites de compras com informações sobre produtos vistos anteriormente.

2.2.3 Criptografia

Segundo França (2005, p.1), “a criptografia é a ciência que oculta o significado de uma mensagem e tem como ferramenta os recursos matemáticos para cifrar e decifrar mensagens”. Parte destas informações armazenadas em cookies podem ser objetos de códigos maliciosos, ou podem ser utilizados para realizar invasões em computadores de empresas com o objetivo de extrair informações privilegiadas.

As empresas fornecedoras de soluções de segurança da informação têm investido cada vez mais em produtos e serviços que facilitem o controle das informações e dados que transitam dentro das empresas e também quando são compartilhados entre empresas. A criptografia é um dos tipos de segurança da informação mais utilizados na atualidade. Segundo a definição da CERT. BR (CERT. BR, 2012), a criptografia é uma mensagem em código ou cifrada, que serve para autenticar a identidade de usuários, proteger a comunicação pessoal e profissional, além de transações bancárias e comerciais. Uma mensagem criptografada deve ser privada, somente quem enviou teve acesso ao conteúdo da mensagem tendo ainda a opção de ser assinada, para que o destinatário possa identificar a integridade do destinatário, ou se a mensagem teve alguma alteração. Na criptografia os dados ou informações acessadas dentro das empresas são verificados e possuem a garantia de que são seguros, verdadeiros e que não são manipuláveis. Para garantir sua

autenticidade a criptografia se baseia em chaves de autenticação que servem para decodificar os dados e informações a serem acessados.

A criptografia engloba tecnologias que podem mesclar palavras e imagens visando ocultar informações armazenadas ou transmitidas por algum meio de comunicação. O processo de criptografia consiste em pegar um texto e através de um algoritmo e uma senha deixar o texto inteligível. Os algoritmos não são secretos, pois o importante não é a utilização dele, mas sim como funciona e como utiliza a chave. O algoritmo será mais eficiente quando for menor o uso da chave e mais resistente a criptoanalise. A criptoanalise é o processo de descobrir qual é o conteúdo protegido sem o uso de nenhuma chave (PINHEIRO, 2008).

Para Pinheiro (2008,p.12), na criptografia "[…] há duas possibilidades: criptografia por chave secreta (ou criptografia simétrica) e criptografia de chave pública (ou chave assimétrica)". As chaves públicas (chave assimétrica) são as que todos têm acesso e são utilizadas para certificar documentos e transações. Já as chaves privadas (chave simétrica ou secreta) são as que somente as empresas possuem, e como o nome diz, são privadas e de acesso confidencial, pois caso sejam reveladas qualquer documento poderia ser acessado.

QUADRO 01 - Visão comparativa entre os tipos de chave pública e privada.

CRIPTOGRAFIA COM USO DE CHAVE PRIVADA	**CRIPTOGRAFIA COM USO DE CHAVE PÚBLICA**
Uso de um único algoritmo e uma chave privada	Uso de um único algoritmo e duas chaves públicas
Os usuários compartilham o algoritmo e a chave	Os usuários compartilham um par de chaves
Uso de uma chave privada	Apenas uma das chaves é privada
Impossível de decodificar a mensagem sem a chave privada	Impossível de decodificar a mensagem sem o uso das chaves
O algoritmo utilizado e as amostras da mensagem não são suficientes para revelar a chave privada	O algoritmo utilizado, as amostras da mensagem e a chave pública não são suficientes para revelar a chave privada.

FONTE: Adaptado pelos autores com base na proposta por Pinheiro (2008,p.12)

Podemos concluir pela comparação apresentada na tabela acima que o uso de chaves privadas na criptografia é muito mais seguro para a segurança da informação, do que o uso de chaves públicas.

2.2.4 Certificado Digital

Segundo a ICP-Brasil, outro tipo de segurança de informação que muito é utilizada atualmente e serve para certificar documentos, transações e até confirmar acesso a arquivos privados, é a certificação digital. Este tipo de segurança é emitido por um órgão ou instituição autorizada pelo governo local.

Para a CERT. BR (CERT. BR, 2012):

> O certificado digital é um arquivo eletrônico que contém dados de uma pessoa ou instituição, utilizados para comprovar sua identidade. Este arquivo pode estar armazenado em um computador ou em outra mídia, como um *token* ou *smart card*.

Alguns exemplos de certificados digitais utilizados na atualidade são o CNPJ, CPF e NF-e. Cada certificado possui informações, dados pessoais ou institucionais e estes dados garantem a validade dos certificados.

Algumas das principais informações encontradas em um certificado digital são:

a) Dados de identificação pessoal ou institucional (nome, razão social, CNPJ/CPF, número de identificação, cidade, estado, etc);
b) Nome da instituição certificadora;
c) Número de série e validade do certificado;
d) Para garantir a autenticidade do certificado, cada um conta com uma assinatura digital.

Constata-se, então que o uso da criptografia assim como o uso de certificados digitais é mais eficiente que somente o uso de senha e cookies para autenticação em sites, ou documentos. Visto que na criptografia e no certificado digital as informações estão protegidas por medidas de segurança que garantem que a segurança da informação não será violada, ao menos que a parte provedora da chave privada ou do certificado digital possua falha em suas políticas de segurança e que permitam o acesso a informações privilegiadas.

2.3 PROBLEMAS FREQUENTES DE SEGURANÇA DA INFORMAÇÃO

Para a CERT. BR (2012) um incidente de segurança é “qualquer evento adverso que será relacionado com a segurança de sistemas de computação ou redes de computadores”. Como exemplos podem ser citados:

a) Acessos não autorizados a sistemas e dados;
b) Ataque de negação de serviço (DDoS);
c) Uso e modificação dos sistemas sem autorização;
d) Desrespeito às políticas de segurança;
e) Desrespeito às políticas de uso aceitável pela empresa.

Os problemas mais frequentes de segurança da informação dentro das empresas têm sido observados pela comunidade de segurança da informação nos últimos anos e tem como principal resultado os ataques aos usuários finais de internet, sejam eles residenciais ou corporativos. Segundo uma pesquisa feita por Cristine Hoepers e Klaus Steding-Jessen (2005), normalmente estes ataques são atribuídos a diversos fatores, entre eles:

a) O acesso à banda larga para usuários domésticos se tornou comum nos últimos anos, desta forma os usuários ficam mais tempo conectados a internet. Além de não terem restrições em seus computadores, o que facilita o acesso a sites e downloads, que podem conter conteúdo considerado perigoso;
b) Com a expansão da internet, as empresas em geral aumentaram seus níveis de segurança em seus servidores, tornando ainda mais difícil os ataques a seus dados e informações. Porém muitos dos ataques ocorrem diretamente com os funcionários destas empresas.

Nesta pesquisa ficaram evidentes que os usuários sejam eles residenciais ou corporativos, podem ser vítima de ataques feitos pela internet principalmente pelas seguintes técnicas:

a) Através do uso da engenharia social. Onde o usuário é iludido a acreditar em alguma notícia. A notícia na verdade carrega no seu código fonte um arquivo ou link para que o usuário acesse ou faça o download. Feito este acesso ou download, um código malicioso pode efetuar ataques a outros computadores, utilizando a identidade daquele usuário.
b) Outra forma de ataque é através do uso de *worms* ou *bots* nas redes de computadores. Um worm ou bot podem ser definidos como códigos maliciosos que permitem que o invasor controle o computador do usuário remotamente. Assim desta forma, o invasor passa a ter controle total sobre o computador do usuário, quando este está infectado por qualquer uma destas formas de ataque (CERT,2012).

Estas situações correspondem a falhas de segurança dentro das empresas brasileiras. Segundo o SERPRO (Serviço Federal de Processamento de dados), há 10 anos, as empresas possuíam infraestruturas diferentes das infraestruturas atuais.

As empresas armazenavam as informações em seus servidores centrais, em seus mainframes, tornando as informações disponíveis em somente um local. Nesta época os usuários não tinham tanto acesso a informação e não manipulavam tanto a informação como nos dias atuais.

O conceito definido em relação ao assunto segurança foi aumentando e as empresas passaram a se preocupar com autenticação e senha de acesso, já que as informações passaram a ser transferidas para diversos computadores.

Com a ascensão e crescimento das empresas, o uso de redes corporativas começou a se intensificar e as redes começaram a se tornar mais estruturadas. Em vez de redes locais, as informações passaram a transitar em redes entre empresas locais e também entre empresas localizadas em outros países. Assim foi feita a integração da internet entre as empresas. Porém a grande preocupação com a integridade das informações, que agora passavam a ser compartilhadas também com outras corporações em transações comerciais, cresceu e tornou-se assunto prioritário nos escritórios de TI (SERPRO,2010).

Hoje, as empresas possuem muito mais infraestruturas e suas informações não estão mais centralizadas, agora são distribuídas de diversas formas (telefonia móvel, e-mail, intranet, telefonia VOIP, extranet, etc).

Para Sêmola (2000), “segurança não se faz com a simples aplicação de tecnologia”. A segurança deve ser feita com o uso inteligente da informação, ou seja, através do uso da tecnologia, as empresas sejam elas pequenas ou grandes devem definir suas políticas de segurança, pois as principais ameaças de falhas de segurança da informação estão dentro das próprias empresas, e são as pessoas que fazem com que dados empresariais ou informações confidenciais acabem sendo divulgadas ou tendo seus acessos liberados, por invasões ou até mesmo por crimes de coação aos funcionários destas empresas.

O objetivo das políticas é descrever o que fazer para proteger a informação.

Para a CERT. BR (CERT. BR, 2012),

> A política de segurança atribui direitos e responsabilidades às pessoas que lidam com os recursos computacionais de uma instituição e com as informações neles armazenados. Ela também define as atribuições de cada um em relação à segurança dos recursos com os quais trabalham. Uma política de segurança também deve prever o que pode ser feito na rede da instituição e o que será considerado inaceitável. Tudo o que descumprir a política de segurança pode ser considerado um incidente de segurança. Na política de segurança também são definidas as penalidades às quais estão sujeitos aqueles que não cumprirem a política. Antes que a política de

> segurança seja escrita, é necessário definir a informação a ser protegida. Uma política de segurança deve cobrir os seguintes aspectos: aspectos preliminares; política de senhas; direitos e responsabilidades dos usuários; direitos e responsabilidades do provedor dos recursos; e ações previstas em caso de violação da política.

Para que uma política de segurança seja utilizada de forma correta e que os usuários sigam tal política, é necessário informar aos usuários dos recursos computacionais a política da segurança da informação da empresa, informando seus direitos e responsabilidades.

Segundo o estudo *Relatório sobre ameaças à segurança na internet. Principais Conclusões*, realizado pela SYMANTEC em Abril de 2012,

> As atividades maliciosas originadas em computadores infectados no Brasil levaram o país para o topo da tabela como fonte de atividades maliciosas na América Latina em 2011 e para o quarto lugar em nível mundial.

Nesta pesquisa pôde-se concluir que as empresas têm enfrentado a cada ano mais ameaças virtuais e ataques a seus servidores de arquivos. A Symantec sugere que as empresas devem tomar algumas medidas de segurança para evitar que seus dados e informações sejam acessados por pessoas com interesse de roubo, compartilhamento e danos às empresas. Sendo que a principal recomendação é o uso de políticas de segurança que sejam eficazes e devidamente controladas.

Outra pesquisa nesta área, foi realizada pela CISCO em 2012 no Brasil, com ênfase em que, “tudo indica que o Brasil terá um crescimento anual de 53% na internet, já leva em conta as circunstâncias econômicas do País.”

Por tanto levando em conta o crescimento econômico no País, devemos observar que os ataques a instituições governamentais, bancárias e privadas tem tendência a aumentar, já que a difusão da informação entre as empresas e entre os próprios usuários tem tido seu crescimento gradualmente proporcional ao crescimento da internet no País. Se analisarmos a tabela abaixo, podemos ver que segundo a SYMANTEC (2012), o Brasil é o quarto colocado no ranking mundial de atividades maliciosas praticadas contra usuários, porém é o primeiro no ranking das Américas em atividades maliciosas.

FIGURA 01:Comparativo de atividades maliciosas por fontes

Atividade Maliciosa por Fontes: Ranking das Américas, 2011

País	Ranking regional 2011	Ranking mundial 2011	Ranking regional 2011 - Código Malicioso	Ranking regional 2011 – Spam Zombies	Ranking regional 2011 - Hosts de phishing	Ranking regional 2011 – Bots	Ranking regional 2011 – Ataques de Rede	Ranking regional 2011 – Ataques Web por País
Brasil	1	4	1	1	1	1	1	1
Estados Unidos	1	1	1	1	1	1	1	1
Argentina	2	22	5	2	3	2	2	4
Canadá	2	16	2	2	2	2	2	2
Colômbia	3	28	3	5	2	7	5	5
México	4	29	2	7	5	6	3	2
Chile	5	34	4	4	4	4	4	3
Perú	6	41	7	3	10	3	7	11
Venezuela	7	11	6	9	9	9	6	6
República Dominicana	8	54	9	6	25	5	9	15
Uruguai	9	61	20	8	15	13	8	9
Porto Rico	10	73	11	17	20	8	10	13

Fonte: Symantec *Países da América do Norte

FONTE : Symantec (2011)

Mais uma vez é possível observar que as políticas de segurança da informação utilizadas nas empresas, permitem que as informações sejam comprometidas através de ataques a seus usuários, roubo de dados de acesso, além de invasões a servidores de dados e etc. Podemos concluir que os principais problemas de segurança de informação são causados principalmente pelo uso indevido de dados na internet. Sendo que na internet todos estão conectados, e os dados podem ser muitas vezes compartilhados nesta rede para fins de negócios, ou para compartilhamento impróprio de conteúdo. Com a aplicação de políticas de segurança da informação, estes dados tendem a ser mais seguros e com restrição de acesso somente para usuários autorizados. Outro fator que contribui com o crescimento de ataques virtuais a servidores e computadores são os próprios usuários, que compartilham dados e informações na internet, que podem ser utilizados por pessoas com má intenção. Podemos concluir também que pelo compartilhamento excessivo de informações na rede mundial de computadores, os ataques e controle de computadores remotos, tendem a crescer nos próximos anos. Por tanto devemos proteger ao máximo as informações que consideramos confidenciais, com o uso de técnicas de segurança, como a biometria por exemplo.

2.4 BIOMETRIA

A Biometria é um ramo da ciência que busca mensurar os seres vivos. Seu significado vem do grego Bio = vida e metria = medida, ou seja, biometria é a medida da vida.

> Segundo Douglas Vigliazzi “a biometria na segurança da informação, significa a verificação da identidade de um indivíduo através de uma característica única inerente a essa pessoa por meio de um processo automatizado”.

Como a biometria é um apanhado de características únicas de cada indivíduo, sua própria anatomia será usada para identificar se a pessoa é mesmo quem diz ser.

A utilização da biometria no controle de acesso permite que um indivíduo possa ser autenticado com alguma característica inerente a si próprio, mesmo que esqueça seu crachá ou senha de acesso. Para utilizar sistemas automatizados de identificação biométrica, é necessário trabalhar com sistemas de inteligência artificial ou redes neurais artificiais.

A biometria está ligada diretamente à segurança da informação, pois os sistemas biométricos utilizados nas empresas restringem o acesso à informação ou a áreas distintas, que são restritas somente a pessoas previamente autorizadas. Para tanto se deve entender primeiramente o que é a segurança da informação e como ela afeta diretamente a escolha e o uso de sistemas biométricos.

> Do ponto de vista da segurança dos sistemas computacionais, a biometria permite a verificação da identidade de uma pessoa através de uma característica única, inerente a ela. Essa característica pode ser fisiológica, também conhecida como “característica estática”, representada por traços fisiológicos, originários do tempo (impressão digital ou características faciais, por exemplo) ou uma característica comportamental, também conhecida como dinâmica aprendida ou desenvolvida ao longo da utilização constante, e que pode variar fortemente ao longo do tempo. Além disso, pode ser facilmente alterada pela vontade ou estado do usuário (assinatura manuscrita ou uma amostra de voz, por exemplo). Cada pessoa é única, se analisada com suficiente detalhamento. É praticamente impossível que pessoas diferentes tenham a mesma e idêntica representação biométrica em qualquer sistema com um limiar de precisão razoável. Contudo, ao lidar com tecnologias de autenticação, encontram-se limites na extração de características, resolução das imagens, na capacidade de armazenamento e na habilidade de comparação entre dados extraídos. Na verdade, um sistema biométrico não grava a foto do rosto ou da impressão digital, por exemplo, mas o valor que representa a identidade biométrica do indivíduo.

(PINHEIRO, JOSÉ MAURICIO, 2008, p.38).

Segundo a definição de Pinheiro (2008), o sistema biométrico não realiza a gravação de dados fisiológicos ou comportamentais dos indivíduos, mas sua principal função é comparar os dados lidos com os dados que estão armazenados dentro da base de dados do sistema que foi desenvolvido. Para que o sistema possa reconhecer os traços fisiológicos ou comportamentais de uma pessoa, a autenticação biométrica deve realizar duas fases: registro no sistema e reconhecimento da característica biométrica.

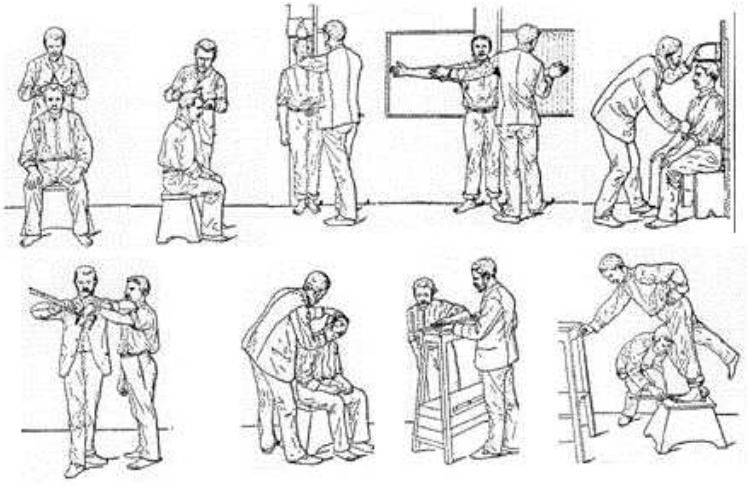
Para Pinheiro (2008) é necessário primeiramente que todos os usuários sejam cadastrados através de um dispositivo de entrada de dados, para conseguir armazenar os dados necessários visando à autenticação do indivíduo. Objetos como escâner, microfone, leitor ótico ou outro meio eletrônico, são meio utilizados para colher essa representação digital.

Depois de cadastrado, o indivíduo que irá fornecer uma amostra de sua característica biométrica, a qual será usada pelo sistema para gerar um modelo biométrico, essa amostra é convertida em algoritmo matemático que será criptografado. Quando o usuário necessitar ter acesso ao sistema, uma verificação será realizada e será comparada com o modelo biométrico armazenado no banco de dados.

De um modo não sofisticado, a biometria já existe há séculos. Partes de nossos corpos e aspectos de nosso comportamento têm sido usadas no decorrer da história como um modo de identificação. Os estudos das imagens digitais datam da antiguidade da China; o ser humano lembra e identifica uma pessoa pelo seu rosto ou pelo som de sua voz; e uma assinatura é o método estabelecido para autenticação em bancos, para contratos legais e em muitas outras ocasiões.

De fato o primeiro método de identificação biométrica aprovado na sociedade, foi inventado por um francês chamado Alphonse Bertillon em 1879, e foi batizado de “Bertillonage”. Seu método baseava-se nas medidas de várias partes do nosso corpo. Para esta época, o método utilizado era muito eficaz e rigoroso. Segundo Moraes (2006), os “traços usados para identificar pontos de medição na face, como tamanho do nariz, queixo, narinas, queixo, bochechas”, conforme podemos observar na figura abaixo.

FIGURA 02: Método de Bertillon:



FONTE: Pinheiro (2008 p.41)

Porém segundo Pinheiro (2008) o cientista Francis Galton aprimorou o método de Bertillon e hoje é considerado um dos fundadores da biometria. Galton utilizava em sua pesquisa habilidades e disposições mentais, a qual incluía estudos de gêmeos idênticos. Esta pesquisa foi pioneira em demonstrar que vários traços são genéticos. A paixão de Galton pela medição permitiu que ele abrisse o Laboratório de Antropométrica na Exibição Internacional de Saúde em 1884, onde ele coletou estatísticas de milhares de pessoas. Em 1892, Galton inventou o primeiro sistema moderno de impressão digital. No trabalho de pesquisa executado por Galton, ele provou cientificamente que as impressões digitais não mudam no curso da vida de um indivíduo e que nenhuma digital é igual à outra, mesmo em caso de irmãos gêmeos, as digitais são diferentes.

É por este motivo que a biometria está sendo utilizada para tentar suprir as falhas de segurança existentes nos estabelecimentos, porque com o uso de métodos de segurança mais apurados, ou ainda o conjunto deles, as informações tem mais chance de serem protegidas.

2.5 TIPOS DE SISTEMA DE AUTENTICAÇÃO BIOMÉTRICOS

Os tipos de tecnologias biométricas podem ser explorados através das características físicas dos indivíduos, utilizando diferentes técnicas para reconhecê-los (ARAÚJO, 2007).

As tecnologias biométricas exploram as características físicas dos indivíduos utilizando-se de diferentes técnicas que objetivam reconhecê-los. Abaixo apresentamos apenas oito técnicas, seis físicas:

a) Geometria da mão;
b) Impressão digital;
c) Reconhecimento de retina;
d) Reconhecimento da íris;
e) Reconhecimento facial.

E três características comportamentais:

a) Voz;
b) Dinâmica da digitação;
c) Reconhecimento de assinatura.

2.5.1 Reconhecimento pela geometria da mão

Para o reconhecimento da geometria da mão normalmente são utilizadas técnicas que resultam de análises das características da mão, tais como:

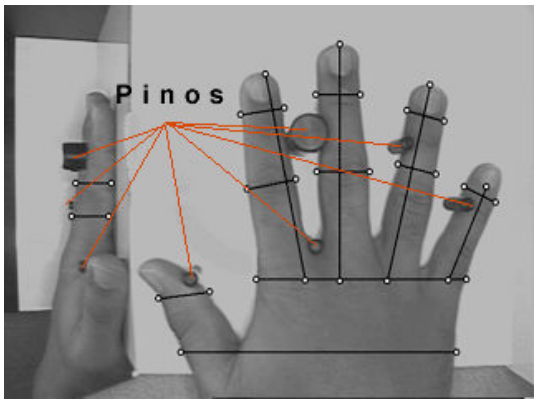
a) O formato;
b) O comprimento dos dedos;
c) As linhas que compõem a palma da mão.

As características da mão são únicas para cada indivíduo. Porém segundo Thian (2001), devido ao grande número de registros que a geometria da mão possui quando comparada com outros tipos de biometria, não temos muitos dados de registros que possam ser utilizados para distinguir um indivíduo de outro. Portanto, o reconhecimento da geometria da mão pode falhar caso as características da mão sejam semelhantes.

Na figura abaixo podemos notar como é realizada a leitura da geometria da

mão, através das digitais. Esta leitura relaciona além das digitais lidas pelo sensor biométrico, também as linhas de expressão que temos nas mãos. Desta forma é possível identificar cada indivíduo comparando a leitura com as informações já armazenadas no banco de dados.

FIGURA 03: Pontos característicos utilizados na geometria da mão



FONTE: Pinheiro (2008 p.67)

2.5.2 Impressão Digital

A impressão digital é o método de biometria mais utilizado no mundo todo, além de ser barata também é segura. (SANTOS 2007; PINHEIRO, 2008; BOLZANI, 2004).

O reconhecimento por impressão digital também é conhecido como *Finger Scan*, além de ser um método de autenticação rápido, é confiável e de baixo custo de implantação. Para realizar o reconhecimento da impressão digital é necessário um *hardware* do tipo escâner para capturar os traços que definem as impressões nos dedos. Após o mapeamento destes traços o processo de leitura e comparação é realizado diretamente com a conexão com um banco de dados, onde anteriormente a impressão digital do indivíduo foi armazenada (PINHEIRO 2008).

Segundo Canedo (2012) os povos Assírios, Babilônios, Japoneses e Chineses, já usavam de fatores biométricos como a impressão digital para identificar comerciantes com quem se relacionavam, além disso, alguns artesãos usavam desse recurso como marca registrada de seus produtos.

Na atualidade os leitores biométricos que reconhecem a impressão digital, são muito utilizados para acesso a sistemas, pontos eletrônicos, e autenticação de usuários. Conforme podemos observar na figura abaixo, um leitor de reconhecimento por impressão digital é muito simples.

FIGURA 04: Leitor biométrico de identificação por impressão digital

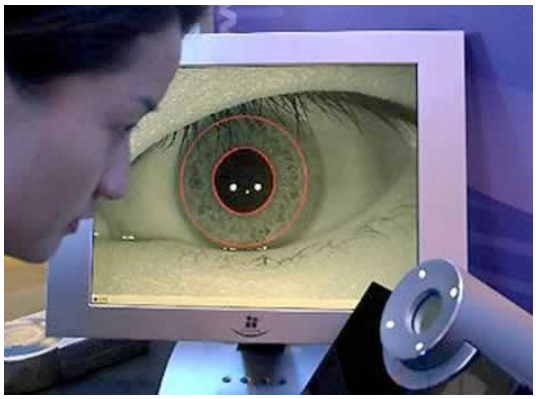
FONTE: http://www.acessoeponto.mixlog.com.br

2.5.3 Reconhecimento da retina

O reconhecimento da retina é baseado na análise das camadas dos vasos sanguíneos situados na parte de trás do olho. Com dispositivos ópticos, por meio do uso de um feixe de luz de baixa intensidade, é feito o reconhecimento dos padrões dos vasos sanguíneos (LIU,2001).

Este tipo de tecnologia pode atingir altos níveis de precisão, para isso é essencial que o indivíduo que irá ser identificado foque o olho em um ponto fixo do leitor para que a leitura seja mais correta. Conforme podemos observar abaixo, este método não é nada conveniente para os usuários que usam óculos ou tenham receio de um contato mais próximo com o leitor.

FIGURA 05: Leitor biométrico de reconhecimento da retina:



FONTE: http://www.fraudes.org

Um dos principais fatores para que o uso deste tipo de reconhecimento biométrico não seja muito aplicado nas empresas, é o fato de ter alto custo de aquisição, fator este determinante para implantação da tecnologia.

2.5.4 Reconhecimento da Iris

Conforme explicado no tópico anterior o olho humano também pode ser usado como método de identificação do ser humano. Além da identificação pela retina, também é possível realizar o reconhecimento de indivíduos através da íris, pois não sofre influência com a idade da pessoa, fator esse que pode ocorrer com as impressões digitais, por essa razão, é considerado um método com alto grau de confiabilidade. Segundo Pinheiro (2008), “O reconhecimento da íris é mais preciso que o da face e da impressão digital”, além disso, para Vigliazzi (2006), como a íris está protegida pela córnea, a probabilidade de danos são mínimos. O que torna o processo de reconhecimento menos invasivo ao indivíduo.

Para o reconhecimento da íris, são utilizadas algumas características que primeiramente são cadastradas no sistema, para que nos próximos processos de reconhecimentos possam ser comparados. Entre estas características estão: as criptas, a pigmentação, os radiais, a área da pupila, a área ciliar e o anel limite entre a íris e a córnea. Abaixo podemos verificar um exemplo do reconhecimento biométrico por íris.

FIGURA 06: Características da Iris utilizadas na biometria

FONTE: http://www.aenfermagem.com.br

2.5.5 Reconhecimento facial

O reconhecimento facial faz a análise do rosto das pessoas, segundo Pinheiro (2008), esse sistema usa como referência características do ser humano que nunca mudam, como as medidas do rosto, distância entre os olhos, distância entre boca, nariz e olhos, queixo, boca e linha dos cabelos, mesmo depois da realização de cirurgias plásticas estas características permanecem. Segundo Canedo (2012) no Egito, pessoas eram identificadas pela altura e cor dos olhos.

Atualmente muitas aplicações utilizam o reconhecimento facial para identificar seus usuários. Podemos ter o uso desde acesso a locais restritos, ou cadastro de clientes, até em televisões. Abaixo apresentamos um exemplo de reconhecimento facial, onde são utilizadas as medidas e distâncias entre os olhos, nariz e boca.

FIGURA 07: Reconhecimento facial pelo uso de características e medidas

FONTE: http://tutorial-info-dica.blogspot.com.br

2.5.6 Reconhecimento da voz

O reconhecimento de voz utiliza diferentes técnicas para reconhecer a voz humana. Uma das principais técnicas utilizadas é o reconhecimento de silabas e transformação destas em palavras. Esta técnica é muito utilizada por softwares de atendimento eletrônico, pois torna o atendimento muito mais customizado para o cliente.

O reconhecimento pela voz, também é conhecido como Speaker ID, e é uma tecnologia que analisa os padrões harmônicos e não apenas reproduções de sequências predefinidas de voz (PINHEIRO,2008).

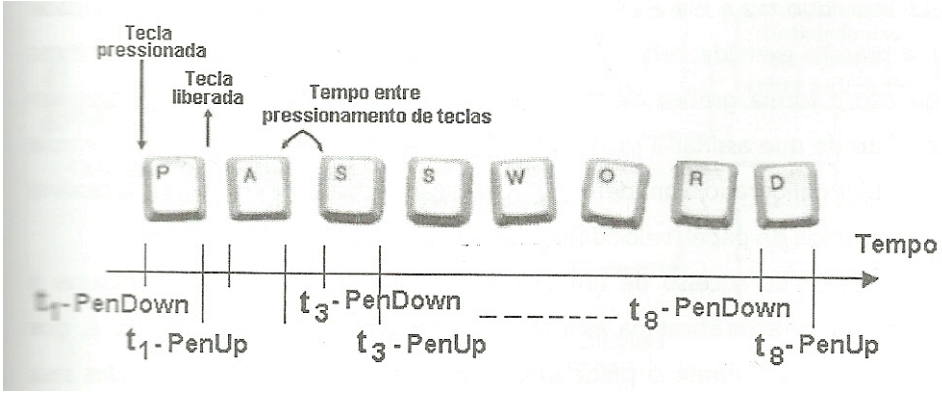
Uma das principais vantagens desta tecnologia por reconhecimento de voz é a usabilidade deste sistema, já que o usuário não precisa interagir fisicamente com o sistema, precisa apenar pronunciar comandos que sejam aceitos pelo programa.

A principal desvantagem do reconhecimento de voz é o reconhecimento de certos regionalismos e gírias pronunciadas pelos usuários, outra desvantagem é a separação do ruído acústico e interpretação de sílabas no meio deste ambiente.

2.5.7 Reconhecimento da dinâmica de digitação

Segundo Costa (2005) o reconhecimento da dinâmica de digitação utiliza uma técnica que analisa o tempo geral e o intervalo de digitação. Para o reconhecimento da dinâmica de digitação, é utilizado o monitoramento dos padrões comportamentais do indivíduo, por meio do padrão utilizado para digitar palavras, frases e/ou textos completos para acesso à informação.

FIGURA 08: Funcionamento da dinâmica da digitação



FONTE: Pinheiro (2008 p.77)

Por via de regra, o sistema que utilize o reconhecimento da dinâmica de digitação, inicialmente deve requerer que o usuário em seu primeiro acesso, digite uma mesma frase determinadas vezes, para reconhecer o padrão que será identificado nos próximos acessos.

A grande desvantagem deste tipo de sistema biométrico é que o indivíduo pode estar com seu estado comportamental alterado e pode resultar em modelos não reconhecidos pelo sistema.

Para Pinheiro (2008), as características de digitação são únicas para cada indivíduo, e “essas características dificilmente podem ser imitadas por um usuário ilegítimo e, mesmo o conhecimento da senha da pessoa pela qual se tenta passar, dificilmente obterá permissão de acesso”.

2.5.8 Reconhecimento da assinatura manuscrita

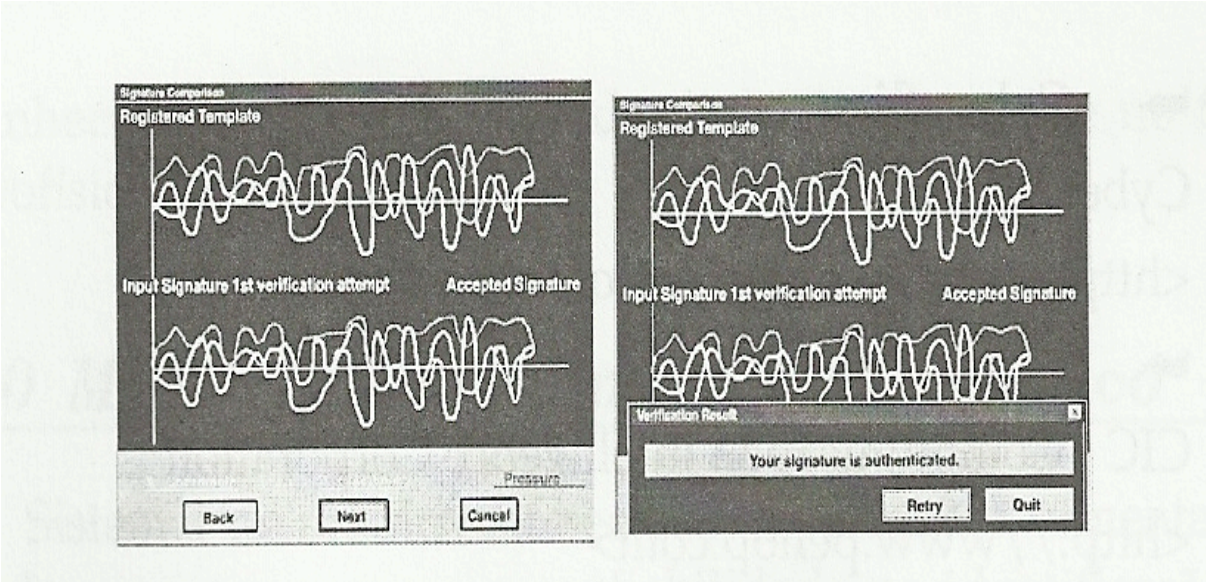
O reconhecimento da assinatura manuscrita surgiu devido o aumento das exigências por segurança da informação, e o reconhecimento da assinatura manuscrita passou a ser um sistema fundamental para a identificação de usuários e para autenticação de operações. Basicamente o reconhecimento da assinatura

verifica o padrão da assinatura e certas características que correspondam à assinatura armazenada em banco de dados. As características podem ser o traçado da assinatura, a pressão exercida na assinatura e a velocidade da mesma. Para Pinheiro (2008), o reconhecimento da assinatura manuscrita é um método de autenticação pessoal baseado em uma biometria comportamental que analisa a maneira como um indivíduo faz a sua assinatura.

Apesar de este sistema ser extremamente seguro, até contra especialistas em falsificação de assinaturas, o padrão de assinatura de um ser humano pode mudar com o tempo, ou de acordo com o comportamento do indivíduo. Além de que em certas circunstâncias de saúde alguns usuários não podem utilizar este tipo de sistema, por serem incapazes de reproduzir sempre o mesmo padrão de assinatura.

Segundo Vigliazzi (2006), existem alguns outros fatores que podem influenciar no reconhecimento de uma assinatura, pois “[…] as assinaturas podem variar suas características de acordo com o ambiente, papel, caneta”. A seguir podemos visualizar um sistema de comparação de assinaturas manuscritas.

FIGURA 09: Funcionamento da assinatura manuscrita



FONTE: Vigliazzi (2006 p.65)

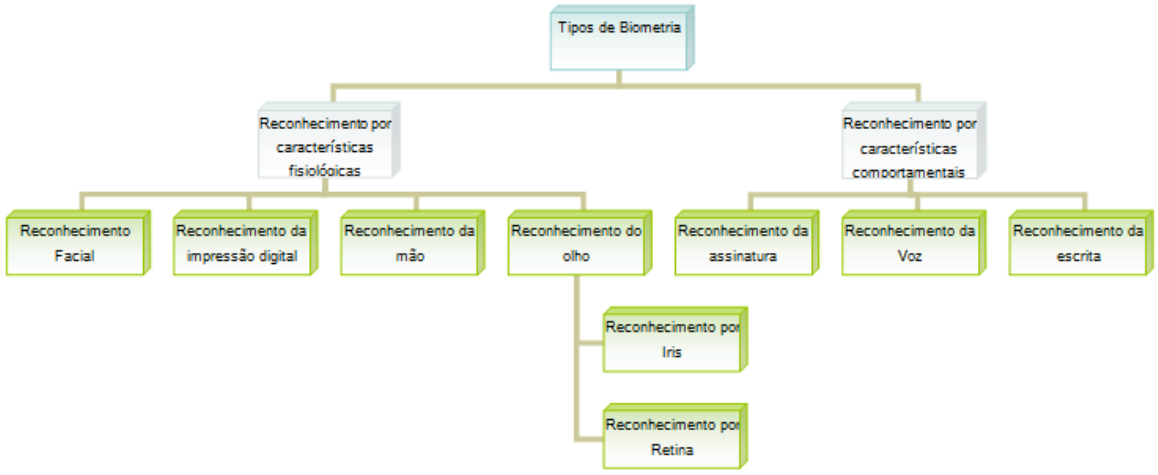
2.5.9 Considerações sobre os tipos biométricos

Os diferentes tipos de tecnologia biométrica têm aplicações específicas para cada caso de uso. O que se pode observar é que cada tecnologia possui sua particularidade de infraestrutura a ser disponibilizada, o custo de aquisição e se o

método escolhido é invasivo ou não. Dentro dos tipos de tecnologia biométrica podemos citar que as que possuem o pior desempenho em relação ao combate a fraude. Destas são as tecnologias biométricas comportamentais, como a biométrica pelo reconhecimento da voz, reconhecimento da assinatura e o reconhecimento pela dinâmica de digitação.

Devemos considerar que não há um método melhor que outro, e sim que a escolha de um tipo de segurança biométrica varia de acordo com a necessidade da empresa.

FIGURA 10 – Tipos de Biometria



Fonte: Os autores (2012)

2.6 IMPLICAÇÕES LEGAIS E PADRÕES DE QUALIDADE EXIGIDOS PARA O TEMA

2.6.1 Iso 17799:2005

A ISO 17799:2005 de acordo com a própria lei, é uma norma brasileira que cuida de técnicas de referência em segurança da informação, foi elaborada no Comitê Brasileiro de Computadores e Processamento de Dados e pela Comissão de Estudo de Segurança Física em Instalações de Informática. A partir de 2007 foi rebatizada com a nova nomenclatura de numeração de normas, passando a ser ISO 27002:2007, porém tratam do mesmo assunto sem grandes modificações.

Essa norma visa a estabelecer critérios, ideias e sugestões que podem ser

seguidas pelas organizações quando colocamos em pauta o quesito segurança da informação. A norma ISO 27002:2007define segurança da informação como a maneira de proteger a informação de ameaças, garantir a continuidade dos negócios, minimizar os riscos e maximizar retorno sobre investimentos e oportunidades, pois a informação como qualquer outro ativo da organização é importante para o negócio e deve ser protegida de maneira adequada.

A norma ISO 27002:2007 coloca como base três requisitos que devem ser estudados quando analisamos a segurança da informação nas organizações. Analisar os objetivos e estratégias da organização e com isso avaliar riscos, vulnerabilidades, e ameaças ao negócio.

Outro ponto importante analisado na norma é a recomendação de verificar as legislações, estatutos e contratos com que a empresa está relacionada buscando os melhores meios de segurança atrelados aos objetivos do negócio. Além disso, a empresa deve analisar princípios, objetivos e requisitos do negócio, visando a relação com as operações da entidade.

Depois desse exame preliminar deverão se analisados os requisitos de segurança da Informação, e por meio da analise de riscos, os gastos serão norteados de acordo com o nível de segurança adequado ao negócio, ou seja, os custos de investimento vão variar com o nível de segurança e com as necessidades da empresa.

Compreende-se nesse ponto de acordo com a norma ISO 27002:2007que os requisitos de segurança são relacionados diretamente com a análise de riscos da empresa, cujos resultados dessa análise poderão ser utilizados para estabelecer prioridades para minimizar os riscos de segurança da informação. Depois de verificados os requisitos e analisados os riscos deve-se estudar os controles que devem ser estabelecidos para que os riscos sejam diminuídos a um nível aceitável. Os controles ou conjunto de controles podem der estabelecidos com base nesta norma, sempre de acordo com as necessidades encontradas nas analises anteriores e em conformidade com as necessidades da empresa. As escolhas dos controles adequados estão relacionadas diretamente com as decisões da organização com base nos seus riscos aceitos, e ainda em regulamentos nacionais e internacionais, a que organização esteja sujeita.

Percebe-se segundo a norma ISO 27002:2007 que os principais pontos a serem estabelecidos no início do estudo da viabilidade de segurança da informação

são três:

a) Requisitos de segurança da informação;
b) Riscos da segurança da informação;
c) Controles que serão utilizados.

Com analise preliminar da norma podemos concluir que quem escolhe o tipo de segurança que deverá ser utilizado é a própria empresa, pois da análise dos pontos internos é que poderão ser estabelecidos requisitos para as suas necessidades, que a partir da escolha dos controles adequados partiram para a implantação do grau de segurança da informação que realmente necessita.

A norma trata de 11 aspectos principais que serão analisados com ênfase na segurança da informação, a título de ilustração, serão colocados os principais objetivos desses tópicos constantes na norma. O objetivo geral da norma ISO 27002:2007, é de ser um guia prático de segurança da informação da organização e gestão da segurança, estabelece ainda diretrizes e princípios para iniciar, programar, manter e melhorar a gestão de segurança da informação em uma organização.

Abaixo são citados 11 aspectos que constam na norma ISO 27002:2007 necessários para avaliar o grau de segurança em uma empresa:

1) Política de Segurança da Informação
2) Organizando a Segurança da Informação
3) Gestão de Ativos
4) Segurança em Recursos Humanos
5) Segurança Física e do Ambiente
6) Gerenciamento das Operações e Comunicações
7) Controle de Acesso
8) Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação
9) Gestão de Incidentes de Segurança da Informação
10) Gestão da Continuidade do Negócio
11) Conformidade

2.6.2 Sox

Quando se trata de outras práticas de gestão como o Control Objectives for Information and Related Technology conhecido popularmente como Cobit ou ainda a

norma sobre ou ainda a Lei Sarbanes Oxley chamada de SOX, é uma norma voltada para a auditoria financeira das empresas, mas, com o devido cuidado pode ser adaptada e usada em pela TI em benefício desta. Esses assuntos colocam em pauta meios relacionados a boas práticas sobre diversos processos sobre segurança da informação, ou riscos oferecidos por meios adversos à segurança os quais podem ser prejudiciais as instituições como um todo.

A lei Sarbanes-Oxley conhecida como SOX segundo Fagundes (2012) foi criada nos Estados Unidos com o intuito de estabelecer normas para o controle financeiro de empresas de capital aberto que possuam ações na bolsa de Nova York. Ela foi criada com o intuito de analisar o capital das empresas e punir seus administradores por fraudes e afins, em resumo, é uma lei de proteção a acionista e pessoas que tem ligação com empresas de capital aberto ao redor do mundo. A necessidade da adequação com a norma se faz necessária, pois, pode acarretar problemas legais ou até publicidade negativa a empresa.

A SOX é um conjunto de normas de auditoria que passaram a ser utilizadas nas empresas visando o bem estar do sistema financeiro da companhia, mas no decorrer do processo de adaptação começaram a ser também de certa forma exigidas pela área de tecnologia das empresas, pois com a utilização de novos sistemas e tecnologias as finanças das empresas passaram a ser controladas de maneira eficaz quando fazem parte dos sistemas informatizados. (Lathi 2006; Peterson 2006).

De uma maneira geral as empresas tiveram que se adaptar aos novos sistemas de auditoria e desta maneira buscaram submeter os seus sistemas de tecnologia aos conceitos sugeridos, porém a ênfase dada na TI não foi obrigatória, mas sem dúvida surgiu do consenso das empresas, visando assim, atender novas necessidades do mercado, como maior controle e transparência de suas contas.

Outra característica importante é que as empresas resolveram utilizar do SOX em suas áreas de tecnologia para ter pontos positivos no mercado, ou seja, para demonstrar que mudanças estão ocorrendo e que a empresa é adepta de novas tecnologias.

Como a SOX é apenas um conjunto de normas não faz menção a como seria possível adaptar os critérios de auditoria as áreas de tecnologia, segundo Lathi; Peterson (2006) não existe menção na norma principalmente na Seção 404, por essa razão podem ser utilizadas algumas das ferramentas de gestão existentes

no mercado como ITIL, Six Sigma ou COBIT, porém a maioria dos auditores e profissionais da área indicam o uso do COBIT, conjunto de boas práticas que se pode ser adaptado ao tamanho da empresa, e as suas necessidades.

2.6.3 Cobit

O COBIT é uma ferramenta de gestão que auxilia no gerenciamento e controle das iniciativas, ou adaptações das áreas de TI nas empresas, é um guia para a gestão de Tecnologia da Informação.

O COBIT é um conjunto de boas práticas em TI, e representa o consenso de especialistas na implantação e manutenção dos setores de tecnologia de uma empresa. É uma ferramenta focada mais nos controles e menos na execução, visando à busca de otimização dos investimentos em TI, além de assegurar a entrega dos serviços e prover métricas para analisar quando ocorrem problemas. (COBIT 2007)

Sendo muito difundida nos meios de gestão das empresas ao redor do mundo, pode ser implantada em qualquer tipo de companhia, pois, como sendo um apanhado de boas práticas de gestão, não precisa ser implantada em sua totalidade, mas apenas ao que a empresa necessita. (Lathi 2006; Peterson 2006).

O modelo de gestão COBIT é dividido em 4 domínios, esses domínios em 34 processos de execução. Segundo Lathi (2006); Peterson (2006):

Os quatro domínios são:

a) Planejamento e organização
b) Aquisição e implementação
c) Distribuição e suporte
d) Monitoração e avaliação

Além disso, o modelo COBIT agrega valor para a instituição, pois busca:

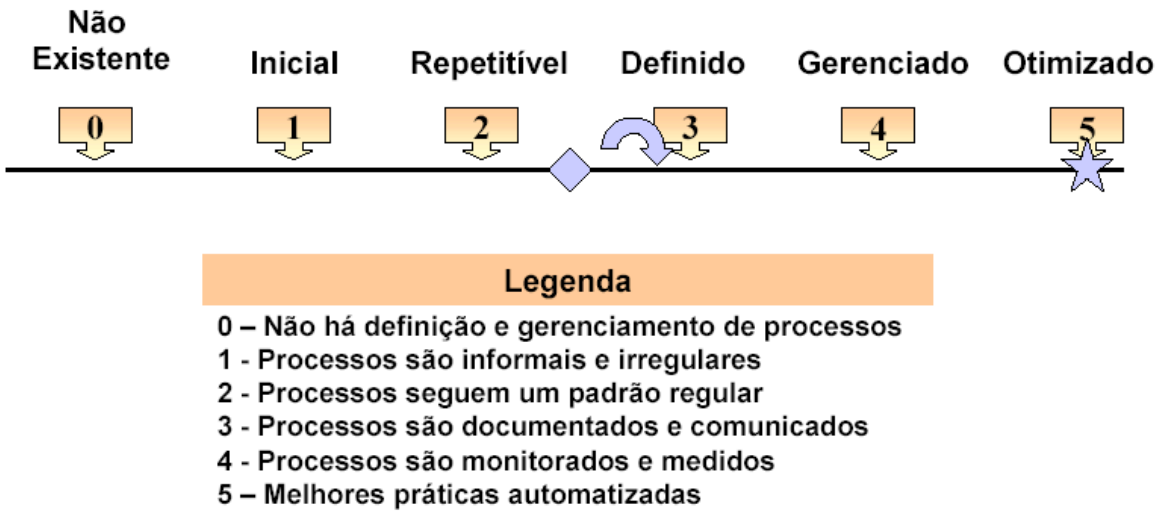
a) Fazer uma ligação com os requisitos de negócios.
b) Organizar as atividades de TI em um modelo de processos geralmente aceitos.
c) Identifica os mais importantes recursos de TI a serem utilizados.
d) Define os objetivos de controle gerenciais a serem considerados.

Outro ponto que merece destaque é que além da percepção do enquadramento da empresa nos moldes hoje aceitos o COBIT pode ser usado para

fazer uma análise detalhada da empresa do que será necessário adequar aos requisitos da ferramenta, são os níveis de maturidade pregados pelo COBIT.

Segundo o próprio COBIT(2007), a analise dos processos tendo como base os modelos de maturidade do COBIT é uma ferramenta crucial na implantação da governança de TI. Depois de identificados os processos e controles críticos de TI, o modelo de maturidade pode identificar em que patamar estão os atributos de TI da empresa em capacidade o que poderão demonstração para os executivos. Desta maneira serão desenvolvidos meios para elevar os processos aos níveis de capacitação desejados pela organização.

FIGURA 11 – Modelo de maturidade do COBIT



Fonte: http://www.mundopm.com.br

2.6.4 Relação Cobit e Sox

Quando uma empresa resolve entrar em conformidade com a SOX procedimentos informais não poderão ser mais aceitos, gerando a necessidade de documentação sobre os controles que serão implantados. Para Lathi (2006); Petersos (2006, p.42) os controles devem incluir: Revisão periódica da eficácia dos controles;

a) Controles de segurança externa;
b) Controles de gerenciamento de alteração de segurança externa;
c) Segurança de arquivos e pastas;
d) Controle de acesso a dados financeiros sigilosos em sistemas que não forem os de produção;

e) Teste de processo e backup e restauração;
f) Controle de acesso físico;
g) Resposta rápida ao encerramento de contratos e desligamentos de funcionários;
h) Processo de divulgação, investigação e resolução de problemas de segurança;
i) Política de retenção de dados.

Desta maneira, COBIT é usado muitas vezes em conjunto com a SOX, pois, através de seus fundamentos podem ser encontradas maneiras para adaptar o que a lei sobre auditoria contábil exige e os pontos de gestão que a empresa necessita, isso porque, a seção 404 da SOX não explica explicitamente como fazer à adaptação a norma de auditoria SOX às necessidades de TI da empresa, e como o COBIT tem mais de 300 objetivos genéricos que podem ser usados para qualquer tipo de empresa é a escolha mais comuns entre as organizações. (Lathi 2006; Peterson 2006).

Para finalizar, as principais áreas da auditoria de TI com ênfase na SOX são a segurança da informação, a alteração de programas e o backup e recuperação de dados, pontos estes que podem ser direcionados com a ajuda das ferramentas do COBIT.

2.7 CONCLUSÕES DO CAPÍTULO

Neste capítulo foi apresentada a fundamentação teórica com ênfase em elementos sobre segurança da informação, buscando assim esclarecer alguns pontos necessários de conhecimento antes de chegar ao ponto principal do trabalho que é o uso da biometria em sistemas de acesso.

Foram apresentados pontos sobre segurança da informação buscando situar o leitor nos conceitos hoje aceitos nas normas e costumes do mundo todo, alguns exemplos do uso da biometria no cotidiano, além de algumas leis, normas e ferramentas de gestão.

Com o intuito de comparação para com os meios biométricos e o sistema de impressão digital usado pelo TSE nas eleições de 2012, será utilizado como base de comparação a SOX, a norma ISO 27002:2007 e o COBIT 4.1, em setembro de 2012

foi lançada a nova versão do COBIT a versão 5, mas como o TSE vem se preparando para essa nova modalidade de urnas nas eleições há bastante tempo é julgamos prudente analisar o estudo de caso com ênfase das ferramentas do COBIT vigentes na época, ou seja, a versão 4.1 e não a versão 5.

3. METODOLOGIA DE PESQUISA

A metodologia de pesquisa tem por objetivo organizar o desenvolvimento do estudo, por meio de instrumentos de pesquisa, coleta e análise de dados, transformando em realidade o objetivo da pesquisa.

Para isso usa-se o tipo de pesquisa chamado de exploratória que segundo Gil (2002), tem por objetivo explorar a realidade, sendo assim, os procedimentos de pesquisas bibliográficas e documentais são os mais indicados.

Desta forma com este os componentes desta pesquisa serão apresentados resumidamente no quadro 01 e descritos na sequência do projeto.

QUADRO 02 – PROTOCOLO DE PESQUISA

Objetivos específicos	Procedimentos de pesquisa	Fonte de coleta de dados	Fundamentação
a) Levantar o estado da arte em relação aos sistemas de segurança da informação;	Pesquisa bibliográfica	Livros técnicos, artigos e sites especializados.	Livros e materiais especializados
b) Levantar o estado da arte em relação aos sistemas de segurança biométricos;	Pesquisa bibliográfica	Livros técnicos, artigos e sites especializados.	Livros e materiais especializados
c) Caracterizar os tipos vários de segurança da informação;	Pesquisa bibliográfica	Livros técnicos, artigos e sites especializados.	Livros e materiais especializados
d) Pesquisar estudos de caso que apliquem a biometria;	Pesquisa de levantamento	Livros técnicos, artigos e sites especializados.	Estudo de caso com materiais do TSE
e) Identificar oportunidades de aplicação dos meios de segurança mais usados;	Pesquisa de levantamento	Livros técnicos, artigos, sites e órgãos especializados.	Estudo de caso com materiais do TSE
f) Comparar as características dos sistemas de segurança biométricos com outros tipos de segurança aplicáveis à segurança da informação	Pesquisa bibliográfica, documental e levantamento	Livros técnicos, artigos, sites e órgãos especializados	Livros e materiais especializados e órgãos especializados no assunto

FONTE: Os autores (2012)

3.1 PROCEDIMENTOS DE PESQUISA

Em cada objetivo do projeto, serão utilizados procedimentos de pesquisa do tipo bibliográfica e documental dos assuntos recentes relacionados com o uso da biometria nos meios de segurança da informação.

Para Severino (2007), a pesquisa bibliográfica se realiza por registros disponíveis, pesquisas anteriores, em documentos impressos, livros, artigos, teses.

A pesquisa tem o objetivo de tornar o problema mais explícito, proporcionando maiores informações sobre o assunto a ser investigado, o aprimoramento de ideias e a descoberta de intuições são o foco principal desse tipo de pesquisa.

Há diferentes propósitos na utilização dessa modalidade de pesquisa, descrever a situação do contexto em que está sendo feita determinada investigação, desenvolver teorias e explicar as variáveis causais de determinados fenômenos em situações muito complexas que não possibilitem a utilização de levantamentos e experimentos.

Este trabalho de pesquisa científica se caracterizará como pesquisa bibliográfica e documental, pois será desenvolvido com base em livros, artigos e arquivos públicos relacionados ao tema da pesquisa.

Quanto à classificação das fontes de referência, os materiais utilizados, em geral, serão livros, publicações periódicas, documentos oficiais e jurídicos, além de consultas a websites na internet, todos de referência informativa, os quais contêm informações buscadas para elaboração da pesquisa.

A principal vantagem da pesquisa bibliográfica reside no fato de permitir ao investigador a cobertura de uma gama de fenômenos muito mais ampla do que aquela que poderia pesquisar diretamente. Essa vantagem torna-se particularmente importante quando o problema de pesquisa requer dados muito dispersos pelo espaço (GIL 2002).

Segundo Rampazzo (2004),

> “a pesquisa é chamada de documental porque os documentos de fonte primária, a saber, os dados primários provenientes de órgãos que realizaram as observações. Esses dados primários podem ser encontrados em arquivos, fontes estatísticas e fontes não escritas”.

3.2 INSTRUMENTOS E TÉCNICAS DE COLETA DE DADOS

Serão utilizados como instrumentos e técnicas de estudos sobre tecnologia da informação, visando atender objetivos específicos, através do uso de pesquisa bibliográfica, documental, observações estruturadas e estudo de caso.

Conforme mencionado no tópico anterior à pesquisa bibliográfica e documental será realizada através do acesso a livros, registros, reportagens, debates e outros meios de informação.

Para Fonseca (2002):

> A observação estruturada pode ser usada como técnica científica, no sentido em que podem ser previstos para realizá-la procedimentos, condições e normas que garantam a sua eficácia dando a seus resultados valor de controle.

Porém para Malhotra (2004) nas observações estruturadas são utilizadas: “Técnicas de observação em que o pesquisador define claramente os comportamentos a serem observados e os métodos pelos quais serão medidos.”

Para as pesquisas sobre o campo de ação dos sistemas biométricos serão usadas de informações sobre a evolução do uso de sistemas biométricos no tribunal superior eleitoral brasileiro, no uso de urnas eletrônicas com identificação biométrica por digitais visando à segurança da informação. Serão usados ainda dados de pesquisas documentais de arquivos públicos sobre o uso da biometria em sistemas de segurança da informação. Como base de fundamentação foram usadas ferramentas de gestão visando estabelecer formas confiáveis de estabelecer parâmetros sobre o uso da segurança nos sistemas de informação e desta maneira de conseguir dados mais fidedignos sobre biometria.

3.3 PROTOCOLO DE PESQUISA

Para definir os patamares de inicio do estudo sobre a biometria foram verificados os principais pontos sobre segurança da informação vigentes no mercado, buscando ilustrar de uma maneira geral como funciona a busca pela proteção das informações relevantes dos interesses das pessoas e empresas.

Desta maneira a busca de informações fidedignas foi importante, normas como a ISO 27002:2007, COBIT, SOX e órgãos especializados no assunto como a

CERT foram consultados. Para a composição final do trabalho com ênfase em fatores biométricos foram consultados artigos sobre o TSE.

3.4 ROTEIRO METOLÓGICO DA PESQUISA

As atividades previstas para execução durante o processo de pesquisa foram estruturadas de acordo com a sequência de etapas apresentadas abaixo:

1. Verificação dos meios de segurança da informação mais difundidos no mercado;
2. Identificação e apresentação das ferramentas biométricas de segurança da informação mais difundidas no mercado;
3. Identificação das forças e fraquezas dos meios biométricos propostos na pesquisa;
4. Analise da ISO 27002:2007 e das ferramentas de COBIT e SOX na sua contribuição na segurança da informação.
5. Identificação das estratégias usadas pelo TSE na utilização de urnas com leitor biométrico de digital.

Por meio da execução das atividades previstas no roteiro acima, pretende-se cumprir as exigências deste projeto e com isso atingir os objetivos específico e geral.

Na etapa 01 procurar-se-á estabelecer relação com os meios de segurança da informação existentes e sua usabilidade.

Na etapa 02 será baseada em uma compilação sobre os meios biométricos e seus usos em conjunto.

Na etapa 03 serão relacionados os dados coletados do TSE com os principais meios de gestão existentes no mercado.

Na etapa 04 se dará a apresentação de novas oportunidades de uso dos sistemas biométricos em empresas brasileiras.

Na etapa 05 será realizado o cruzamento e análise das informações obtidas nas etapas anteriores, possibilitando a identificação da existência ou não de estratégias para atender ao objetivo proposto neste projeto.

4. ANÁLISE DE RESULTADOS

4.1 ANÁLISE DA EVOLUÇÃO DO TRIBUNAL SUPERIOR ELEITORAL COM RELAÇÃO ÀS URNAS ELETRONICAS DE VOTAÇÃO

O processo de informatização do TSE começou em 1986, com o recadastramento de boa parte da população brasileira, porém somente em 1994 é que o processo foi efetivamente concluído e o resultado das eleições foi feito pelo computador central do TSE.

O uso de novas tecnologias contra fraudes em eleições pelo TSE começou em 1996, com a utilização de urnas eletrônicas para votação, apuração e conferência das eleições, garantindo maior sigilo e mitigando fraudes decorrentes do processo manual da conferência de votos. (ANJOS; 2010).

Como a cultura dos políticos brasileiros a efetiva manipulação do eleitorado continua a ser forte, meios de segurança visando pelo menos a certeza de que os votos não sejam manipulados durante e depois das eleições, devem ser cada vez mais utilizados.

O uso de sistemas biométricos nas urnas eletrônicas marca da data de 2008, ano em que foram usadas pela primeira vez nas eleições municipais em apenas três cidades brasileiras. Em 2010, como teste 23 estados totalizando 60 municípios usaram urnas biométricas nas eleições. Neste mesmo ano, visando aumentar a segurança dos sistemas, o TSE começou o recadastramento dos eleitores, visando à implantação de sistemas biométricos de leitura das digitais da mão, sistema esse que em 2012 foi usado em cidades como: Aracaju (Sergipe), Curitiba (Paraná), Goiânia (Goiás), Maceió (Alagoas) e de Porto Velho (Rondônia).

> “Os eleitores de 299 cidades foram convocados para cadastrar sua impressão digital e fotografia, além de atualizar os dados. Em Curitiba, o recadastramento reduziu de 1,31 milhão para 1,17 milhão o total de eleitores da cidade”. Agência Brasil (2012).

O projeto inovador atraiu a atenção de vários países ao redor do mundo, o Brasil assinou acordos de cooperação técnica, com a Argentina, Paraguai, México, Equador e República Dominicana. Para o secretário a identificação

biométrica por impressão digital vai garantir a lisura do processo de votação por se tratar de um processo mais ágil e seguro.

Para esse processo o Brasil terá que investir cerca de 485 milhões de reais em oito anos, porém para assegurar a vantagem desse novo sistema e garantir a eficiência do novo sistema, o TSE procurou ajuda através de pareceres de peritos da polícia federal. Além disso, para garantir que os dados de impressões digitais não sejam usados para fins diversos dos de votação, os dados coletados no recadastramento são enviados para o banco de dados da policia federal e depois de processados são armazenados no TSE. (TRE-PR 2012).

O funcionamento do sistema segue da seguinte forma:

a) O eleitor não pode votar em qualquer lugar do país;
b) Os dados do eleitor só estarão disponíveis na sessão na qual ele foi cadastrado;
c) Ainda há a necessidade de justificação do voto no caso do eleitor estiver fora da cidade;
d) A urna será bloqueada e desbloqueada a cada voto;
e) O mesário fara a conferência para verificar se a pessoa que irá votar é a mesma que está cadastrada, analisando o número do título e a foto armazenada no sistema;
f) No caso de não reconhecimento da digital o mesário poderá liberar a urna para votação por meio da conferência de dados e título do eleitor;
g) No caso de impressão digital diferente do cadastro será aberta investigação e o eleitor poderá perder o seu título;

Os primeiros testes com urnas datam do ano de 2008, porém o recadastramento dos eleitores começou um antes. O TSE procurou cidades onde a influência climática e a distância facilita-se a utilização da biometria por digitais e a distancia não atrapalha o transporte e montagem da estrutura necessária à coleta de dados.

Outro ponto interessante é que o TSE fez parcerias buscando estabelecer critérios diversos de confiabilidade nos novos sistemas biométricos em implantação, segunda a revista TRE-Paraná (2012) usaram de tecnologias da empresa francesa Lafis, a qual já era usada pela polícia federal para leitura biométrica, e também adaptaram o software fornecido pela mesma empresa para armazenamento de dados cadastrais dos indivíduos.

Essa nova implantação para o uso de urnas biométricas ocorreu primeiramente em locais onde o recadastramento obrigatório de leitores foi obrigatório, visando unir as necessidades às novas mudanças, pois, em várias cidades foram usadas às urnas biométricas para testar o seu funcionariam na prática.

A título de informação não é só com o bom andamento das eleições que o TSE se preocupou, mas também com a segurança dos meios de fabricação e divulgação de como foram construídas e de como funcionarias as urnas eletrônicas com sensor biométrico.

> O acesso à fábrica é controlado por um rigoroso sistema de segurança. “A finalidade é evitar o vazamento de informações sigilosas”, diz o diretor da Diebold Procomp, Lucas Costa. Representantes do TSE acompanham de perto todo o processo de confecção das urnas e o acesso à fábrica. As urnas são supervisionadas pelos agentes de Brasília antes mesmo de ficarem prontas. O passo seguinte, antes de serem aprovadas, é deixar o equipamento “votando” por oito horas seguidas. É muito complicado para nós deixarmos alguém entrar sem a autorização do TSE. (Revista TRE Paraná 2012)

Umas das cidades na qual foi estabelecido esse projeto foi Curitiba no Paraná, onde no ano de 2011 quase toda a população foi recadastrada na justiça eleitoral, fato esse que possibilitou a usabilidade de urnas eletrônicas com leitores biométricos nessa região nas eleições de 2012.

Para estes feitos o TSE buscou ajuda de outros órgãos do estado do Paraná como o DIRETRAN, departamento de trânsito curitibano, para ajudar na locomoção da população nos maiores centros de recadastramento instalados, além da Fiep Federação das Indústrias do Estado do Paraná e da Associação Comercial do Paraná que prestaram auxílio ao TRE/PR, auxiliando na divulgação.

O TSE usou de algumas táticas para fazer com que as pessoas não deixassem de comparecer aos centros de recadastramentos, usou de diversos instrumentos, como: a criação de uma marca com a representação de um polegar para com a imagem demonstrar o que seria essa tal de biometria, além de propagandas na televisão, rádio, uso de folders e propagandas diversas sobre a necessidade do recadastramento para que a eleição de 2012 pudesse ser um marco no uso da biometria como segurança da informação nas eleições.

No inicio usaram propagandas convidativas, até histórias em quadrinhos foram feitas para convencer o eleitor, porém com o prazo se extinguindo o governo passou a usar de propagandas mais severas usando do poder de coerção do estado

informando, que quem não fizesse o recadastramento teria o título de eleitor cancelado.

FIGURA 12: Propaganda para cadastramento biométrico em Curitiba-PR

FONTE: http://www.tre-pr.jus.br

Com a primeira etapa cumprida, o TSE tem como objetivo cadastrar todos os eleitores até 2018, para que as eleições possam utilizar 100% de urnas biométricas em todo o território brasileiro.

QUADRO 03 - Comparativo entre as eleições nacionais de 2008, 2010 e 2012

ELEIÇÃO	Eleitorado	Quantidade de municípios	Zonas Eleitorais	Urnas eletrônicas	Força de trabalho no TSE	
2008 (municipal)	130.472.076	5.564	3.011	455.971	1.446	
2010 (estadual)	135.804.433	5.676	3.025	463.707	1.574	
2012 (municipal)	138.544.348	5.568	3.011	501.923	1.766	
CANDIDATOS	**Candidaturas por eleição**	**Candidaturas por eleição**	TOTAL	**Candidatos por vaga**	**Candidatos por vaga**	TOTAL
	Prefeito	**Vereador**		**Prefeito**	**Vereador**	
2008	15.141	330.630	345.771	5.563	51.992	7.555
2012	15.652	449.751	480.570	5.568	57.422	2.996

URNAS BIOMÉTRICAS	**Quantidade de eleitores**	**Quantidade de municípios**	**Quantidade de Estados**
2008	40.728	3	3
2010	1.136.140	60	23
2012	7.779.792	299	24

FONTE: http://www.tse.jus.br

No quadro acima foi estabelecido o número do eleitorados com relação ao ano e o tipo de eleição. Nesta perspectiva verifica-se que a quantidade de eleitores que estão usando a urna biométrica foi bem menor que a quantidade total de seções eleitorais espalhadas pelos diversos municípios de todo o Brasil Porém percebe-se

que a relação da quantidade de estados usando as novas urnas se relacionados com os municípios tiveram um crescimento muito grande, pode-se afirmar que o número de cidades que passaram a usar urnas biométricas praticamente cresceu em cinco vezes das eleições de 2010 para as de 2012, o que aumenta a diversidade no teste sugerido das urnas. Percebe-se que o projeto almejado para 2018 com a utilização do sistema de leitura de impressão digital em todos os municípios pode se concretizar.

Nesta perspectiva a busca de sistemas mais seguros merece confiança da população, votos comprados e manipulação de urnas se tornarão mais difíceis de serem realizados.

Como ilustração segue a ordem de autenticação nas urnas biométricas, que segundo Anjos (2010) segue cinco passos:

a) O primeiro passo é que para Assinatura digital, que é usado um algoritmo exclusivo de conhecimento apenas pelo TSE.
b) No segundo passo a urna verifica a assinatura dos programas e em caso de não conformidade não funciona.
c) No terceiro passo é usada a criptografia digital que é um mecanismo de segurança que deixa os dados embaralhados, tornando-os inacessíveis a pessoas não autorizadas.
d) No quarto passo é emitido o boletim da urna que é criptografado de forma segmentada, assinado digitalmente e então transmitido.
e) No quinto passo depois que os dados são recebidos pelo TSE são decriptografados, isto é, os dados anteriormente criptografados são recuperados, desembaralhados.

Resumidamente os passos para o boletim de uma urna são:

> a) validação da compatibilidade da chave pública de assinatura digital do boletim de urna com a chave privada do totalizador; b) decriptografia do boletim de urna de forma segmentada; c) leitura do boletim de urna decriptografado; d) armazenamento do boletim de urna criptografado e decriptografado. Anjos (2010).

Além da segurança o uso de sistemas biométricos agiliza o sistema, pois os dados coletados de autenticação normalmente são bem mais rápidos do que no uso de métodos tradicionais menos seguros, tornando as votações mais fáceis e menos maçantes.

4.2 RELAÇÃO ENTRE O SISTEMA BIOMÉTRICO DO TSE, SOX E COBIT

O TSE como órgão do governo, e visando o bem estar da sociedade deve estar de acordo com as Leis vigentes, em termos de comparação quadro nº 4 tenta demonstrar esse viés, onde são mostrados pontos de inter-relação entre algumas normas usadas pelas empresas em geral principalmente na área de tecnologia.

Como mencionado na fundamentação à norma Sarbanes Oxley é uma lei voltada para auditoria das empresas com ênfase principal em regulamentar os setores financeiros das instituições, porém o que está acontecendo hoje no mercado é a informatização dos sistemas, ou seja, a empresa que não tem um setor de tecnologia tem que criá-lo buscado excelência em gestão administrativa.

Para fazer uso da ferramenta que necessita não há um manual pronto como uma receita prática do que deve ser implantado na empresa para que ela passe a funcionar conforme as normas ou ainda práticas de gestão mais aceitas no mercado, isso será feito com um estudo preliminar do que a instituição normalmente necessita ou está apta a aceitar dentro de sua administração.

Nessa perspectiva muitos auditores, administradores e outros estão usando para se correlacionarem com as normas da SOX, o manual de boas práticas chamado COBIT que vai demonstrar através de vários processos como adequar a empresa às ferramentas de gestão atuais, pois seus objetivos de controle estão em conformidade com a SOX.

QUADRO 04 - Objetivos de controle COBIT que se enquadram na SOX e que podem ser usadas na implementação da norma na empresa.

SEGURANÇA	**GERENCIAMENTO DE ALTERAÇÕES**
Procedimento de prevenção contra vírus	Gerenciamento de alterações em aplicativos
Procedimento de controle de acesso baseado em crachá	Gerenciamento de alterações em banco de dados
Procedimento para monitoração de acesso físico do usuário	Gerenciamento de alterações no sistema operacional e em hardware
Controles ambientais	Procedimento de gerenciamento de alterações e projeto de rede
Procedimento para a concessão de acesso ao centro de dados	Procedimento de gerenciamento de alterações em firewall
Procedimento de conectividade de rede remota	
MONITORAÇÃO	**ACESSO LÓGICO**
Monitoração do desempenho e capacidade do servidor	Procedimento para a manutenção do acesso de usuários a aplicativos
Procedimento de monitoração de disponibilidade da rede	Procedimentos de controles de senhas para autenticação no sistema
Procedimentos de backup/restauração	Controle de segurança de aplicativos e bancos de dados
Procedimentos de backup	Controles de administração de senhas de aplicativos
Procedimentos de backups de nós da rede	Procedimentos para concessão de acesso a controles de segurança do sistema operacional para sistema de arquivos/servidores
Controles de monitoração da segurança da rede	

FONTE: Lathi ; Peterson (2006)

Analisando o quadro acima depois de visualizar as características da implantação das urnas eletrônicas com ênfase em biometria feitas pelo TSE, pode-se verificar que estão de acordo com as sugestões do COBIT com ênfase na Sox divulgadas por Lathi; Peterson(2006), pois foram verificados os principais pontos sugeridos, como:

a) Segurança, quando da confecção das urnas eletrônicas por pessoal especializado e autorizado.
b) Gerenciamento de alterações, que só poderiam ser feitos por membros autorizados de dentro da própria estrutura do TSE.
c) Monitoração, pois, todo o processo foi analisado desde a montagem das urnas, locais escolhidos para testes, cadastramentos dos eleitores, treinamento dos funcionários, uso das urnas e termino da votação com ênfase na contagem de votos e armazenamento sigiloso das informações.
d) Acesso lógico, só os usuários autenticados pelo sistema poderiam ter acesso aos meios.

Desta maneira percebe-se que o TSE seguiu alguns dos passos que podem ser julgados necessários à segurança das informações. E com base nas normas seguidas obteve o sucesso na implantação de seus projetos pilotos e efetivação das primeiras eleições com uso de urnas biométricas.

4.3 RELAÇÃO ENTRE O SISTEMA BIOMÉTRICO DO TSE E ISO 27002:2007

A ISO 27002:2007 diferencia-se da norma SOX, pois foi estabelecida como uma norma inteiramente relacionada com a área de Tecnologia. Em sua essência define meios para estabelecer as oportunidades de implantação de sistemas como um todo.

Essa norma é focada principalmente na análise do que a corporação necessita, dando ênfase aos estudos dos riscos que a empresa possui no mercado e quais devem ser aceitas, buscando assim estabelecer os critérios de segurança necessários que a empresa deve aplicar. Essa constatação se dará com o auxilio dos próprios interessados ou se houver necessidades peritos poderão ajudar no processo.

Essa norma busca minimizar os riscos e maximizar o retorno sobre os

investimentos.

Percebe-se então que o TSE também está adequado com a ISO 27002:2007, pois, seguiu os quesitos de:

a) Requisitos de segurança da informação;
b) Riscos da segurança da informação;
c) Controles que serão utilizados.

O TSE tomou as precauções necessárias na implantação dos sistemas, pois procurou desde o início da operação equacionar os riscos e oportunidades, fazendo todos os testes necessários antes de partir para a implantação do projeto como um todo, percebe-se que a grosso modo a estrutura de implantação pela qual o TSE optou está tendo uma boa aceitação.

Desta maneira o projeto sobre biometria estabelecido pelo TSE para segue os parâmetros da legislação vigente.

O quadro abaixo visa demonstrar em poucos passos quais são as necessidades envolvidas na análise estabelecida pela ISO 27002:2007

QUADRO 05 – Análise de passos da ISO 27002:2007

1	Política de Segurança da Informação	• Visa promover orientação de acordo com os requisitos do negócio e com base nas leis e regulamentos, com orientação e apoio da direção na determinação da segurança da informação.
2	Organizando a Segurança da Informação	• Quando relacionada à infraestrutura interna da empresa o objetivo é o de gerenciar a segurança da informação. • Com relação às partes externas o objetivo principal é o de manter a segurança de dados acessados por agentes externos a empresa.
3	Gestão de Ativos	• Se relacionados com a responsabilidade, os ativos da empresa devem ser resguardados e protegidos por um controle interno eficaz. • Com relação à classificação da informação dos ativos, esses devem receber um nível adequado de proteção de acordo com a sua importância.
4	Segurança em Recursos Humanos	• Antes da contratação de indivíduos deve-se assegurar que os funcionários tenham papéis bem definidos na organização visando mitigar roubos, fraudes e mal uso de recursos. • Durante a contração os funcionários devem estar conscientes de suas responsabilidades visando apoiar as políticas de segurança utilizadas; • No encerramento da contratação deve-se assegurar que o funcionário não tenha mais acesso aos sistemas da empresa e que devolva os equipamentos utilizados na sua rotina de trabalho
5	Segurança Física e do Ambiente	• Nas áreas que necessitam de alto nível de segurança o acesso de indivíduos estranhos ao ambiente de trabalho deve ser evitado. • Os equipamentos devem ser mantidos seguros de intervenção por pessoal não autorizado, deve haver a prevenção de interrupção de alguma atividade por dano a algum equipamento, tais como ameaças físicas ou com relação ao meio ambiente.
6	Gerenciamento das Operações e Comunicações	• Garantir que os recursos de processamento da informação sejam operados de maneira segura e correta. • Os serviços de terceiros devem ser gerenciados, deve ainda ser implementado um nível de segurança de acordo com as necessidades de entrega de serviço. • Os sistemas devem ser planejados e aceitos visando diminuir os riscos a falhas. • Dispositivos móveis não autorizados e introdução de códigos maliciosos devem ser evitados, visando proteger a integridade da informação e dos softwares utilizados. • Cópias de segurança devem ser mantidas para recuperação de arquivos perdidos, visando manter a integridade e disponibilidade da informação. • Visando garantir que as informações na rede trafeguem de maneira segura, deve ser feito um bom gerenciamento de redes, visando proteção e segurança das próprias redes e da estrutura de suporte. • Mídias móveis devem ser controladas, prevenindo divulgação, destruição ou interrupção de informações essenciais aos negócios da companhia. • A troca de informações e softwares em ambiente interno e externo deve ser feito de maneira segura.

		• Serviços de comércio eletrônico e transações online podem ser utilizados, desde que com garantia de execução segura. • Deve ser feito o monitoramento dos sistemas e eventos de segurança da informação devem ser registrados além dos logs de registro de operadores e falhas.
7	Controle de Acesso	• Recomenda-se que os controles de acesso e os processos do negócio devem ser relacionados com as necessidades do negócio e com ênfase na segurança da informação. • Deve ser estabelecido um sistema de gerenciamento de acesso ao usuário, assegurando acesso autorizado e prevenindo o não autorizado. • Devem-se treinar os usuários com ênfase na responsabilidade nos sistemas de acesso, para evitar acesso não autorizado ou roubo de informações. • Os serviços relacionados à rede interna da organização devem ser controlados prevenindo o acesso não autorizado, além disso, o uso de interface apropriada e mecanismos de autenticação são necessários. • O controle de acesso aos sistemas operacionais da empresa deve ser restrito, e devem ser tomados alguns cuidados: autenticação dos usuários, os registros de tentativas de autenticação nos sistemas, avisos de segurança violada e tempo de conexão restrito por usuário. • O acesso à informação deve ser restrito e liberado apenas para usuários autorizados. • Quando usados dispositivos móveis a proteção deve ser proporcional aos riscos.
8	Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação.	• Garantir que a segurança é parte integrante do sistema. • As aplicações devem ser processadas de maneira correta para evitar erros, perdas ou modificações não autorizadas. • Controles criptográficos devem ser estabelecidos buscando proteger os meios como confidencialidade, autenticidade e integridade. • Arquivos de sistema e códigos fonte devem ser preservados visando garantir a segurança. • Processos de suporte e desenvolvimento devem ser estritamente controlados. • Riscos de vulnerabilidades devem ser rejeitados.
9	Gestão de Incidentes de Segurança da Informação	• Assegurar que meios frágeis de segurança sejam comunicados permitindo ação corretiva em tempo. • Melhorias contínuas de gestão de incidentes devem ser estabelecidas visando assegurar efetividade.
10	Gestão da Continuidade do Negócio	• Os negócios da empresa devem ser contínuos no tempo, para isso falhas devem ser mitigadas, visando minimizar os impactos na organização e controles para diminuir riscos podem ser usados se necessário.
11	Conformidade	• A segurança da informação deve estar submetida a regulamentos, leis ou obrigações contratuais as quais a empresa é submetida. • A segurança da informação deve ser avaliada periodicamente visando analisar se estão em conformidade com as políticas e normas da organização. • Em caso de auditoria as informações dos sistemas devem ser protegidas.

FONTE: Norma ISO 27002: 2007

4.4 RELAÇÔES ENTRE TSE, SOX,COBIT E ISO 27002:2007

Abaixo o quadro relaciona os quatro domínios do COBIT com os 34 processos de negócio em TI, sua relação com o SOX, ISO 27002:2007 e aplicação ao TSE na segurança das urnas biométricas:

QUADRO 06 – Relação entre COBIT, SOX, ISSO 27002:2007 e o TSE

COBIT	SOX	ISO 27002	TSE
PLANEJAR E ORGANIZAR			
PO1 Definir um Plano Estratégico de TI	Aplicação Necessária	Não se aplica	Pode ser aplicado
PO2 Definir a Arquitetura das Informações	Aplicável	X	Se aplica
PO3 Determinar a Direção Tecnológica	Aplicação não necessária	X	Se aplica
PO4 Definir os Processos, a Organização e os Relacionamentos de TI.	Aplicável	X	Se aplica
PO5 Gerenciar o Investimento de TI	Aplicação não necessária	Não se aplica	Se aplica
PO6 Comunicar as Diretrizes e Expectativas da Diretoria	Aplicação necessária	X	Se aplica
PO7 Gerenciar os Recursos Humanos de TI	Aplicável	X	Pode ser aplicado
PO8 Gerenciar a Qualidade	Aplicação necessária	X	Se aplica
PO9 Avaliar e Gerenciar os Riscos de TI	Aplicável	X	Se aplica
PO10 Gerenciar Projetos	Aplicação necessária	Não se aplica	Pode ser aplicado

COBIT	SOX	ISO27002	TSE
Adquirir e Implementar			
AI1 Identificar Soluções Automatizadas	Aplicável	X	Se aplica
AI2 Adquirir e fazer manutenção de Software de Aplicativo	Aplicável	X	Se aplica
AI3 Adquirir e Manter Infraestrutura de Tecnologia	Aplicação necessária	X	Se aplica
AI4 Habilitar Operação e Uso	Aplicável	X	Se aplica
AI5 Adquirir Recursos de TI	Aplicável	X	Pode ser aplicado
AI6 Gerenciar Mudanças	Aplicação necessária	X	Se aplica
AI7 Instalar e Homologar Soluções e Mudanças	Aplicação não necessária	X	Pode ser aplicado
COBIT	**SOX**	**ISO27002**	**TSE**
Entregar e Suportar			
DS1 Definir e Gerenciar Níveis de Serviços	Aplicável	X	Se aplica
DS2 Gerenciar Serviços Terceirizados	Aplicação necessária	X	Pode ser aplicado
DS3 Gerenciar o Desempenho e a Capacidade	Aplicação necessária	X	Se aplica
DS4 Assegurar a Continuidade dos Serviços	Aplicação necessária	X	Se aplica
DS5 Assegurar a Segurança dos Sistemas	Aplicação necessária	X	Se aplica
DS6 Identificar e Alocar Custos	Não se aplica	Não se aplica	Pode ser aplicado
DS7 Educar e Treinar os Usuários	Não se aplica	X	Se aplica
DS8 Gerenciar a Central de Serviço e os Incidentes	Aplicação necessária	X	Se aplica
DS9 Gerenciar a Configuração	Aplicável	X	Se aplica
DS10 Gerenciar Problemas e incidentes	Aplicação necessária	X	Se aplica
DS11 Gerenciar os Dados	Aplicação necessária	X	Se aplica
DS12 Gerenciar o Ambiente Físico	Aplicação necessária	X	Se aplica
DS13 Gerenciar as Operações	Aplicável	X	Se aplica
COBIT	**SOX**	**ISO27002**	**TSE**
Monitorar e Avaliar			
ME1 Monitorar e Avaliar o Desempenho de TI	Aplicação necessária	X	Se aplica
ME2 Monitorar e Avaliar os Controles Internos	Aplicável	X	Se aplica
ME3 Assegurar a Conformidade Com Requisitos Externos	Aplicável	Não se aplica	Se aplica
ME4 Prover Governança de TI	Não se aplica	Não se aplica	Se aplica

FONTE: Adaptação do COBIT 4.1 e sugestões de Lathi; Peterson(2006)

O quadro acima é uma adaptação dos requisitos sugeridos pelo COBIT4.1 para qualquer empresa, porém como exigência da norma Sarbanes-Oxley com relação a exigências de auditoria para empresas como um todo, Lathi; Peterson(2006) sugerem algumas relações entre a norma e as boas práticas do COBIT, para isso foi então colocada no quadro níveis de aplicação sugerida por esses autores e uma relação com o TSE sugerida pelo trabalho proposto com ênfase na biometria dos sistemas.

Na análise do quadro acima se percebe que todos os pontos do COBIT podem ser aplicados ao TSE, porém muitas vezes como sendo um órgão governamental algumas exigências não serão vistas pelo próprio órgão, sendo então, que alguns pontos do manual de boas práticas poderão não ser aplicados ou não serão necessários.

Percebe-se ainda que alguns pontos da SOX também não precisam ser aplicados, mas alguns deles dizem respeito a custos e a norma fala em controle de finanças nada mais lógico do que a aplicação ser obrigatória, Aqui pode ser feita uma ressalva, por que os pontos aqui relacionados tem muito mais ênfase com o

setor de tecnologia da empresa do que qualquer outro, por isso, alguns processos não são necessários.

Outro ponto interessante é a relação com a ISO 27002:2007, como ela estabelece normas a serem seguidas e sempre de acordo com os riscos da empresa muitos pontos só serão aplicados se realmente forem necessários.

Uma observação interessante é a relação entre alguns pontos do COBIT que não são necessários na aplicação da norma SOX, que também não serão aplicados na ISO 27002:2007, ou seja, a relação entre elas pode ser parecida.

4.5 OPORTUNIDADES DE APLICAÇÃO

4.5.6 Tabela de oportunidades

Visando a segurança da informação, podemos definir que atualmente existem várias oportunidades de aplicação da biometria para proteger dados, informações e até mesmo controlar acesso de pessoas. Abaixo identificamos algumas oportunidades e detalhamos como as mesmas podem ser aplicadas.

QUADRO 07 – Oportunidades de aplicação da tecnologia biométrica

OPORTUNIDADE	DESCRIÇÃO
Identificação criminal	Identificação de vítimas, suspeitos ou qualquer individuo passível a aplicação da lei. O principal objetivo do uso da tecnologia biométrica para identificação criminal é identificar um indivíduo em um processo criminal.
Instituições financeiras	Pode ser utilizada a tecnologia biométrica em terminais bancários (ATM), acesso a bancos e Pontos de Venda (PDV). O uso da biometria nestas aplicações pode substituir o uso de senhas e smart cards.
E-commerce	O sistema biométrico pode ser utilizado para complementar à autenticação de usuários nos sistemas e efetuar transações financeiras. O uso da biometria nestes casos pode servir para a substituição do uso de senhas.
Sistemas de Informação	A aplicação de sistemas biométricos neste caso serve basicamente para controlar o acesso a sistemas. A biometria é utilizada para o acesso a computadores pessoais e acesso a rede.
Edifícios inteligentes	Pode ser utilizado para a identificação de indivíduos que entram e saem de edifícios ou de áreas restritas.
Sistemas de benefícios	Pode ser aplicado para o uso em retirada de aposentadorias, vale-transporte, vale alimentação, votação, imigração e serviços governamentais eletrônicos.
Sistema Penitenciário	Uso para controle de entrada e saída de indivíduos em prisões. Assim como pode também ser utilizado para a captura de criminosos.
Instituições de Ensino	Controle de acesso e identificação de professores, alunos e funcionários, a áreas como biblioteca, direção, refeitório, ginásio, etc.
Sistemas Militares	Uso para controlar o acesso a áreas restritas como bases militares, sistemas de defesa, etc.
Hospitais e Centros cirúrgicos	Controle de acesso a UTI, centro cirúrgico e a áreas restritas dentro de hospitais.

Fonte: Os autores (2012)

O que podemos notar nas oportunidades da tabela acima, é que em sua maioria procura-se proteger o uso de sistemas, acesso a locais restritos e também acesso a informações confidenciais. Para cada tipo de oportunidade, pode-se utilizar um ou mais meios de segurança biométrica. Sejam eles de identificação única, como o reconhecimento da digital apenas, ou também de forma combinada, como o reconhecimento facial e o reconhecimento da assinatura.

Conforme já dito em capítulos anteriores, a escolha pela melhor tecnologia biométrica depende totalmente da empresa e das decisões que forem tomadas para proteger e garantir a segurança da informação.

4.6 TENDÊNCIAS DA BIOMETRIA PARA O FUTURO

Assim como outras tecnologias, a biometria é uma ciência que tende a evoluir com o longo dos anos. Novas técnicas e novas tecnologias serão pesquisadas e desenvolvidas para aprimorar as técnicas existentes, como o reconhecimento da voz, e até obsoletar técnicas que não sejam mais tão eficientes.

Segundo um estudo realizado por Mark Nixon da Universidade de Southampton, na Inglaterra (2012), “acredita-se que o formato da orelha e os passos das pessoas são tão únicos quanto às impressões digitais e ainda mais difíceis de serem copiados”.

Também há indícios de que a tecnologia biométrica a ser utilizada no futuro, seja o uso do odor e do DNA das pessoas (IDGNow,2009). Segundo Bastos(2008), o futuro da biometria também poderá ser utilizado com o uso da medição das ondas cerebrais de cada indivíduo. Já que existe um padrão na emissão das ondas cerebrais, e elas se manifestam sempre mantém em um mesmo ritmo e padrão para cada pessoa.

O que podemos concluir sobre o futuro da biometria, é que cada vez mais as tecnologias serão aprimoradas para utilizarem propriedades fisiológicas de cada indivíduo. Já que o uso de tais particularidades tende a ser muito mais eficientes e seguras que o uso de características comportamentais.

4.7 RELAÇÃO DE APLICABILIDADE EM BIOMETRIA

Conforme o capítulo 2 da fundamentação teórica existem vários tipos de sistemas de segurança da informação. Dentre elas umas mais seguras e outras mais frágeis e passíveis de quebra do sigilo de dados. O uso de um único tipo de segurança da informação não garante que os acessos a locais restritos ou dados serão protegidos. Para tanto se recomenda o uso de técnicas de segurança da informação combinadas com o uso de sistemas biométricos. Vale a pena lembrar que existem sistemas biométricos que também não podem ser considerados 100% seguros. Segundo Vigliazzi(2006), Pinheiro(2008), quanto maior o nível de segurança, menor será a probabilidade de fraude. Detalhamos no quadro a seguir algumas oportunidades de aplicação, onde o uso da segurança da informação é

utilizado de forma única, de forma combinada 2 a 2 e de forma combinada 3 a 3.

Para uma análise mais adequada, foram criadas as colunas “Custo” e “Risco”, com base na fundamentação teórica, onde se procurou qualificar o nível de segurança a partir do risco que o tipo de técnica está sujeita à quebra da confiabilidade. E o custo em relação a sua aplicabilidade.

QUADRO 08 – Tipos combinados de técnicas de segurança da informação

	Oportunidades de aplicação	**Tipo de Técnica**	**Custo**	**Risco**
Sistemas Únicos	Acesso a um banco de dados	Senha	Baixo	Alto
	Troca de arquivos entre governos	Criptografia	Baixo	Médio
	Acesso a dados cadastrais	Certificado Digital	Baixo	Médio
	Autenticação de transações financeiras	Biometria das Veias	Alto	Baixo
	Autenticação em sistemas de CRM	Biometria da Voz	Médio	Alto
	Autenticação em sistema de votação	Biometria da Digital	Baixo	Médio
	Controle de Imigração	Biometria da Face	Baixo	Médio
Sistemas Combinados 2 a 2	Acesso a um banco de dados	Senha + Token (RSA)	Baixo	Médio
	Troca de arquivos entre governos	Criptografia + Certificado Digital	Baixo	Baixo
	Acesso a dados cadastrais	Certificado Digital+ Biometria da Iris	Alto	Baixo
	Autenticação de transações financeiras	Biometria das Veias + Token (RSA)	Alto	Baixo
	Autenticação em sistemas de CRM	Biometria da Voz + Senha	Médio	Alto
	Autenticação em sistema de votação	Biometria da Digital + Assinatura	Baixo	Médio
	Controle de Imigração	Biometria Facial + Biometria da Digital	Baixo	Médio
Sistemas Combinados 3 a 3	Acesso a um banco de dados	Biometria da Digital+Senha+Token(RSA)	Baixo	Baixo
	Troca de arquivos entre governos	Criptografia + Certificado Digital + Biometria da Digital	Médio	Baixo
	Acesso a dados cadastrais	Certificado Digital+Biometria da Iris+Biometria da Digital	Alto	Baixo
	Autenticação de transações financeiras	Biometria das Veias+Token(RSA)+Assinatura	Alto	Baixo
	Autenticação em sistemas de CRM	Biometria da Voz+Senha+Biometria da digital	Médio	Alto
	Autenticação em sistema de votação	Biometria da Digital+Assinatura+Biometria facial	Baixo	Médio
	Controle de Imigração	Biometria facial + Biometria da Digital+Biometria da Iris	Médio	Baixo

FONTE: Os autores(2012)

Analisando o quadro comparativo de aplicabilidade de tipos de segurança da informação com tipos biométricos combinados é possível concluir que:

a) as aplicações que utilizam somente um tipo de segurança, ou utilizam somente tipos de segurança da informação tradicionais estão mais suscetíveis a riscos de falhas e vazamento de informações do que

sistemas que utilizam a combinação de 2 ou mais meios de segurança.

b) o uso de sistemas biométricos, tais como o reconhecimento da íris e o reconhecimento das veias são mais seguros e menos passíveis a falhas de segurança do que os meios considerados tradicionais como senhas e cartões de acesso.

Conclui-se então que o uso de sistemas biométricos são mais seguro e oferecem menos riscos do que somente o uso de sistemas tradicionais de segurança da informação como, por exemplo, as senhas e crachás.

5. CONSIDERAÇÕES FINAIS

No presente trabalho foram estudadas as tecnologias biométricas, suas aplicações e analise do caso de uso da biometria no tribunal superior eleitoral. Com este estudo foi possível verificar oportunidades e aplicações da biometria e sua relação com métodos de segurança existentes no mercado.

No capítulo 1 foram apresentados, o problema, a hipótese, os objetivos e a justificativa para o trabalho proposto.

No capítulo 2 foi apresentada a fundamentação teórica englobando temas sobre segurança da informação visando mostrar ao leitor atributos para compreender os conceitos de segurança da informação, problemas relacionados, conceito de biometria, e relação da biometria com os padrões legais geralmente aceitos.

No capítulo 3 foi relacionada à metodologia apresentada para os procedimentos de pesquisa dos dados coletados e do roteiro de trabalho estabelecido.

No capítulo 4 foram apresentadas as relações da utilidade da biometria no estudo de caso do TSE, além da relação dessa aplicação com práticas de auditoria em segurança da informação, tais como COBIT, ISO e SOX, utilizados no mercado, e se podem transformar-se em oportunidades de aplicação e algumas tendências para o futuro.

A problemática requerida para o estudo foi respondida, concluindo que os meios biométricos são realmente mais seguros que os sistemas de segurança tradicionais amplamente utilizados, como senhas, cartões, cookies, criptografia e certificados digitais. Pois possibilitam o uso de alguma característica física do individuo o que é impossível de ser copiada.

A hipótese para o trabalho também foi considerada verdadeira, pois o uso de sistema se segurança biométricos realmente garantem informações com maior confiabilidade se comparados com os sistemas tradicionais que não utilizam estes meios para autenticar e proteger a informação.

Com ênfase no objetivo específico foram comparadas características dos sistemas biométricos e identificadas oportunidades de aplicação nos sistemas de acesso, informações essas citadas no capítulo 4.

Dados os objetivos específicos foi levantado o estado da arte dos sistemas de segurança da informação e dos sistemas biométricos, além de caracterizar os vários tipos de segurança da informação existentes no mercado, analisando estudos de onde os sistemas podem ser aplicados. Na análise foram identificadas oportunidades de aplicação dos meios de segurança mais usuais.

Como a preocupação das pessoas, empresas e entidades com relação à segurança é um fator cada vez mais crescente, a procura por meios mais seguros é muito grande, desta maneira os meios de segurança biométricos podem ser uma boa alternativa.

A biometria utiliza características únicas do ser humano como a palma da mão, as digitais, a íris ou até mesmo a voz, portanto a chance de serem duplicados é quase mínima.

Como prova disso, segundo dados do Superior Tribunal Eleitoral, a implantação de urnas eletrônicas com ênfase na biometria já é uma realidade, a identificação do eleitor e a contagem dos votos são feitas com mais segurança e agilidade.

O uso da biometria em sistemas de acesso é a alternativa para os meios atuais de segurança pouco seguros, porém, vai depender muito do tipo do estabelecimento e do tipo de segurança que são necessários, quem vai decidir quais os meios de segurança que mais serão mais interessantes é a própria empresa.

Quando necessário um sistema mais seguro que o habitual, pode ser usada ainda da combinação de meios de segurança biométricos com outros meios não biométricos, buscando dificultar a entrada de um agente não autorizado às informações protegidas.

Conclui-se que meios de acesso com ênfase na biometria serão cada vez mais utilizados pelas empresas, pois são mais seguros e podem ser até mais rápidos para fornecer acesso a locais e informações pela praticidade do usuário, cujas suas características pessoais sempre estarão presentes junto consigo.

5.1 CONTRIBUIÇÕES PARA OS AUTORES

Baseado na fundamentação teórica deste trabalho e o estudo realizado sobre a implantação da tecnologia biométrica no sistema de votação brasileiro foi

possível aprofundar o conhecimento sobre os tipos de segurança da informação mais usuais e também sobre os tipos de segurança biométricos existentes. Muitas destas fundamentações e informações que foram abordadas e trabalhadas neste trabalho, não eram de fato conhecidas em profundidade pelos autores.

5.2 CONTRIBUIÇÕES PARA AS EMPRESAS

A tendência é que a aplicabilidade de sistemas biométricos em empresas ou órgãos governamentais aumente com o longo dos anos. Pois a busca por novas tecnologias e uso de meios de segurança da informação combinados deve se tornar um padrão de melhores práticas de tecnologia da informação em âmbito mundial.

Pela análise do uso da tecnologia biométrica no Tribunal Superior Eleitoral (TSE) que visa melhorar o sistema de votação das eleições brasileiras, pode-se verificar que com o uso da biometria, a chance de fraude nas eleições é quase nula, visto que o uso de tal tecnologia oferece maior segurança no reconhecimento do eleitor e aumenta a confiabilidade de que não haverá votos realizados por eleitores faltantes ou não existentes.

Desta forma o uso de sistemas de segurança da informação mais seguros pode deixar de ser apenas um luxo ou uma prática incomum, e pode passar a ser necessário para preservar o maior patrimônio das empresas, que é a informação.

5.3 CONTRIBUIÇÕES PARA A ACADEMIA

Através das fundamentações e estudo de caso abordado neste trabalho, a academia pode se basear em informações e conclusões que os autores realizaram. Tais informações podem ser utilizadas em outros trabalhos e também como base para fundamentação de pesquisas a serem realizadas.

O principal fator de contribuição para a academia foi o levantamento de dados a partir da pesquisa realizada com base no projeto de implantação do sistema biométrico no Tribunal Superior Eleitoral (TSE). Tais dados refletem em todo o processo de implantação do sistema biométrico e também se as melhores práticas de tecnologia da informação foram bem aplicadas.

5.4 SUGESTÕES PARA TRABALHOS FUTUROS

O assunto desenvolvido neste relatório de pesquisa dá margem a outras pesquisas relacionadas ao uso da tecnologia biométrica para autenticação e controle de acesso. Algumas sugestões de trabalhos futuros são pertinentes de serem mencionadas:

- Estudar sobre a possibilidade do uso de sistemas biométricos em outros segmentos governamentais como: Previdência, Serviço Único de Saúde, Planos de Auxilio a População (Bolsa família, Auxilio Gás, Luz Fraterna, etc), entre outros.

- Estudar e pesquisar sobre novas técnicas não invasivas para reconhecimento biométrico.

- Propor um sistema de padronização de reconhecimento biométrico com maior segurança para órgãos governamentais.

REFERÊNCIAS

ALVES, Cássio Bastos. **Segurança da Informação vs Engenharia Social -** Como se proteger para não ser mais uma vítima. Disponível em: <http://www.administradores.com.br/_resources/files/_modules/academics/academics_3635_20101207234707794d.pdf>. Acesso em: 24 Nov. 2012

ANJOS, Wilson Pedro dos. **Urnas Eletrônica E Biométrica: Sucesso E Confiabilidade.** Disponível em: <http://www.justicaeleitoral.jus.br/arquivos/tre-ms-artigo-sobre-as-urnas-eletronica-e-biometrica> Acesso em 30 Ago. 2012

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 17799: tecnologia da informação: técnicas de segurança - **Código de prática para a gestão da segurança da informação.** Rio de Janeiro, 2001. 56 p. Disponível em: <www.procedimentosemti.com.br/downloads/NBR17799.pdf> Acesso em: 25 Mai. 2012

BASTOS, Bruno Miguel Quintela. ***Autenticação* Biométrica *Através da Actividade.* Cerebral**. Disponível em: <http://ria.ua.pt/bitstream/10773/1971/1/2009000472.pdf> Acesso em: 20 Nov. 2012.

BRASIL, Agência. **TSE testa urna biométrica em 117 cidades** Disponível em: http://computerworld.uol.com.br/tecnologia/2012/08/13/tse-testa-urna-biometrica-para-eleicoes-de-outubro-em-117-cidades/ . Acesso em 05 Nov 2012

CANEDO, José Alberto **História da Biometria.** Disponível em: <http://www.forumbiometria.com/fundamentos-de-biometria/118-historia-da-biometria.html> Acesso em: 12 Ago. 2012.

CERT.BR, Centro de Estudos, Resposta e Tratamentos de Incidentes de Segurança no Brasil, **Cartilha de Segurança para Internet** Disponível em

<http://cartilha.cert.br> , Acesso em: 01 Jun. 2012.

CISCO . **Crescimento da internet no País será maior que a média mundial**. Disponível em: <http://tecnologia.terra.com.br/noticias/0,,OI5807139-EI12884,00> Acesso em: 01 Jun. 2012.

COBIT, 4.1. Frameword for IT Governance and Control. Disponível em: <http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx>. Acesso em: 15 Jun. 2012.

COSTA, Carlos Roberto do Nascimento. **Autenticação Biométrica via Teclado Numérico Baseada na Dinâmica da Digitação:** Experimentos e Resultados. Disponível em: <http://www.bibliotecadigital.unicamp.br/document/?code=vtls000380243> Acesso em: 12 Mai. 2012

DIONNE, Jean; LAVILLE, Christian; Adaptação SIMAN, Lara Mara; ***A Construção Do Saber:*** Manual da Metodologia da pesquisa em ciências humanas. 1º ed. Minas Gerais: Artmed, 1999.

ELEITORAL,Tribunal Superior***. Justiça Eleitoral Realiza Maior Eleição Informatizada do Mundo em 2012.*** Disponível em: <http://www.tse.jus.br/noticias-tse/2012/Outubro/justica-eleitoral-brasileira-realiza-a-maior-eleicao-do-mundo-em-2012/?searchterm=falhas%20nas%20urnas%202012> Acesso em: 04 Nov. 2012

FONSECA, José Saraiva da. **Metodologia da Pesquisa Científica** Disponível em:< http://books.google.com.br/books?id=oB5x2SChpSEC&printsec=frontcover&hl=pt-BR&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false> Acesso em: 25 Set. 2012

FRANÇA, Waldizar Borges de Araújo. **CRIPTOGRAFIA**. Disponível em: <http://www.ucb.br/sites/100/103/TCC/22005/WaldizarBorgesdeAraujoFranco.pdf> Acesso em: 24 Nov. 2012

GIL, Antônio C. ***Como elaborar projetos de pesquisa***. 4 ed. São Paulo: Atlas,

2009.

HOEPERS, Cristine; STEDING-JESSEN, Klaus. **O cenário da segurança da informação no Brasil.** Disponível em: <http://www.cgi.br/publicacoes/index.htm> Acesso em: 11 Mai. 2012

IDGNOW. **Futuro da biometria conta com reconhecimento por odor e calor humano** Disponível em: <http://idgnow.uol.com.br/seguranca/2006/08/30/idgnoticia.2006-08-29.9472410830/#&panel2-1> Acesso em 25 Nov. 2012

LAUREANO, Marcos Aurelio Pchek. **Gestão da Segurança da Informação**. Disponível em:< http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf>. Acesso em 25 Ago. 2012

LIU, Simon.;SILVERMAN, Mark. **A Practical Guide to Biometric Security Technology**. Disponível em: < ftp://yosemite.ee.ethz.ch/pub/lehre/inteco/SS02/material/00899930.pdf> Acesso em: 05 Jun. 2012

MALHOTRA, Naresh K. **Pesquisa de Marketing, Uma orientação aplicada.** ARTMED Editora, São Paulo, 2004.

MARCELO, Antonio; PEREIRA, Marcos. ***A Arte de Hackear Pessoas***. Rio de Janeiro: Brasport, 2005.

MITNICK, Kevin D.; SIMON, William L. ***A arte de enganar: Ataques de Hackers***: Controlando o Fator Humano na Segurança da Informação. São Paulo: Pearson Education, 2003.

MORAES, Alexandre Fernandes de. **Método para avaliação da tecnologia Biométrica na segurança de aeroportos.** Disponível em: <http://www.pcs.usp.br/~gas/v2/images/Publications/dissertacao_alexandremoraes.pdf> Acesso em: 05 Ago. 2012

NIXON, Mark. **Biometria poderá utilizar análise de passos e orelhas no futuro**. Disponível em: < http://www.estadao.com.br/noticias/vidae,biometria-podera-utilizar-analise-de-passos-e-orelhas-no-futuro,963521,0.htm> Acesso em: 23 Nov. 2012

PINHEIRO, José Maurício. ***Biometria nos Sistemas Computacionais*** - Você é a Senha. Rio de Janeiro: Ciência Moderna Ltda, 2008.

RAMPAZZO, Lino. ***Metodologia Cientifica:*** para alunos dos cursos de graduação e pós-graduação. 2º ed. São Paulo: Loyola, 2004.

REZENDE, Denis Alcides; ABREU, Aline França. **Tecnologia da Informação Aplicada a Sistemas de Informação Empresariais**. Editora Atlas. São Paulo,2000.

_____, Denis Alcides. ***Planejamento de Sistemas de Informação e Informática***. 4º ed. São Paulo: Atlas, 2011.

SANTOS, Antônio Raimundo. ***Metodologia Científica:*** A construção do conhecimento. São Paulo: DP&A,1999.

SANTOS, Rildo Ribeiro. ***Maturidade de TI utilizando o COBIT.*** Disponível em: < http://www.google.com.br/url?sa=t&rct=j&q=&esrc=s&source=web&cd=7&ved=0CGMQFjAG&url=http%3A%2F%2Fwww.mundopm.com.br%2Feventos%2Fgov%2Fapresentacoes%2FSpecialDAY_Maturidade_TI_COBIT_Rildo.ppt&ei=AOK8Ulj-EoS49QTIn4CYBw&usg=AFQjCNHRjRmYOQzqtg1_wyQd7bzTjHSitQ> Acesso em: 12 Nov. 2012.

SELNER, Claudiomir. **Análise de requisitos para sistemas de informações, utilizando as ferramentas da qualidade e processos de software** Florianópolis 1999 (trabalho de conclusão de curso) Universidade Federal de Santa Catarina programa de pós-graduação em Engenharia de Produção. Disponível em: <http://www.eps.ufsc.br/disserta99/selner/>. Acesso em: 29 Mai. 2012.

SÊMOLA, Marcos. **Segurança: muito mais do que tecnologia**. Disponível em:

<http://www.semola.com.br/disco/Coluna_IDGNow_18.pdf> Acesso em: 25 Nov. 2012

SERPRO. **Governo quer triplicar o acesso à banda larga em 4 anos**. Disponível em:<https://www.serpro.gov.br/noticias/governo-quer-triplicar-o-acesso-a-banda-larga-em-4-anos/?searchterm=h%C3%A1%2010%20anos> Acesso em: 01 Jun. 2012

SEVERINO, Antônio J. ***Metodologia do trabalho científico****.* 23 ed. São Paulo: Cortez, 2007. 304 p.

SILVA, Pedro Tavares; TORRES, Catarina Botelho; CARVALHO, Hugo. **Segurança dos Sistemas de Informação**. Edições Centro Atlântico, 2003.

STALLINGS, William. ***Arquitetura e Organização de Computadores:*** *Projeto para o Desempenho.* 5ª ed. São Paulo: Prentice Hall, 2002. 786 p.

SYMANTEC. **RELATÓRIO de Ameaças à Segurança na Internet - Vol. XVII**. Disponível em: <http://www.symantec.com/content/pt/br/enterprise/threatreport/LAM-ISTR17-pt.pdf > Acesso em: 25 Nov. 2012.

THIAN, Norman Poh Hoon. **Biometric Authentication System**, Disponível em: <http://hydria.u-strasbg.fr/~norman/BAS/publications.htm> Acesso em: 05 Jun. 2012

TURMAN Efrain;McLEAN ,Ephraim;WETHERBE James**, Tecnologia da informação para gestão**: Transformando os negócios da economia digital. Porto Alegre 2002.Bookman.Disponível em: <http://books.google.com.br/books?id=d5ekddxquNYC&printsec=frontcover#v=onepage&q&f=false >. Acesso em: 17 Mai. 2012.

VIGLIAZZI, Douglas. ***Biometria Medidas de segurança***. 2ª Ed, 2006.

WILSON, Tracy. **Como funciona a biometria** traduzido por HowStuffWorks Brasil. Disponível em: <http://informatica.hsw.uol.com.br/biometria.htm> Acesso em: 11 Mai 2012.