

UNIVERSIDADE PAULISTA
RAPHAEL TREVIZAM FERMINO DE OLIVEIRA

TECNOLOGIA DA INFORMAÇÃO:
Estudo da criptografia para projetar uma nova infraestrutura de
chave pública destinada à geração de identidade eletrônica

RIO DAS PEDRAS
2010

RAPHAEL TREVIZAM FERMINO DE OLIVEIRA

TECNOLOGIA DA INFORMAÇÃO:

Estudo da criptografia para projetar uma nova infraestrutura de chave pública destinada à geração de identidade eletrônica

Trabalho de desenvolvimento e aplicação dos conhecimentos adquiridos nas disciplinas de Modelagem de Sistemas de Informação, Gestão Estratégica de Recursos Humanos, Segurança da Informação e Planejamento Estratégico de Tecnologia da Informação, realizado com base em uma solicitação fictícia da Prefeitura Municipal de Curitiba, Paraná, e apresentado à Universidade Paulista (UNIP), com a finalidade de Projeto Integrado Multidisciplinar (PIM VI).

Orientador: Prof. Luiz Antônio de Lima

RIO DAS PEDRAS
2010

Oliveira, Raphael Trevizam Fermino de, 1983

Tecnologia da Informação: Estudo da criptografia para projetar uma nova infraestrutura de chave pública destinada à geração de identidade eletrônica / Raphael Trevizam Fermino de Oliveira. - 2010.

36 f. ; 29,7 cm

Orientador: Luiz Antônio de Lima.

Projeto Integrado Multidisciplinar VI – Universidade Paulista, Pólo de Rio das Pedras, Gestão de Tecnologia da Informação, 2009.

1. Modelagem de Sistemas de Informação. 2. Gestão Estratégica de Recursos Humanos. 3. Segurança da Informação. 4. Planejamento Estratégico de Tecnologia da Informação. I. Lima, Luiz Antônio. II. Universidade Paulista, Pólo de Rio das Pedras. Gestão de Tecnologia da Informação. III. Tecnologia da Informação.

RESUMO

Os procedimentos para se embalar informações confidenciais e altamente sigilosas, tornando-as ilegíveis a olho nu ou irreconhecíveis a estranhos, a fim de transportá-las publicamente com fidúcia, são estudados há séculos por renomadas sociedades, como a Francomaçonomia. A criptografia é o recurso mais utilizado. Ela é explorada pela ciência denominada de criptologia, um ramo da matemática que se divide em dois grandes campos: criptografia e criptoanálise. Seus pesquisadores são criptógrafos, criptólogos e criptoanalistas. A informática emprestou e acrisolou os métodos antigos, fazendo uso de algoritmos complexos. O resultado desse casamento resolveu um dos maiores problemas da atualidade, proporcionando tranquilidade às transações comerciais e de lazer online, com a criação de certificados e assinaturas digitais, através das quais é impossível repudiar ou deixar de assumir uma ação praticada no mundo cibernético. Mesmo com tanta robustez e solidez, isoladamente, as tecnologias são incapazes de asseverar a segurança dos sistemas. Faz-se necessário descrever e definir políticas específicas, envolvendo a cultura dos atores. Não apenas os ambientes virtuais necessitam de proteção, mas também os ambientes físicos. Vários critérios e normas devem ser considerados. Assim sendo e observados, fundamentados e conceituados os temas aludidos acima, esse trabalho objetivou-se em apresentar o projeto básico de uma nova Infraestrutura de Chave Pública consentâneo com a legislação vigente, principalmente em harmonia com a lei 8.666, de 21 de junho de 1993, conforme solicitação da Prefeitura Municipal de Curitiba, Paraná, para a geração de identidade eletrônica aos cidadãos curitibanos, apontando de forma argumentada e explícita as melhores soluções e venábulo. Embasado nas teorias e conhecimentos assimilados, ao final o leitor consegue vislumbrar o funcionamento dos serviços propostos.

Palavras-chave: Criptografia; criptoanálise, criptologia; criptógrafos; criptólogos; criptoanalistas; algoritmos; certificados e assinaturas digitais; infraestrutura de chave pública; identidade eletrônica

ABSTRACT

The procedures for hiding sensitive information, making them unreadable to the naked eye or unrecognizable to outsiders in order to transport them publicly with fiduciary, are studied for centuries by renowned companies such as Freemasonry. Encryption is the most used resource. It is operated by the so-called science of cryptology, a branch of mathematics that is divided into two main fields: cryptography and cryptanalysis. Its researchers are cryptographers, cryptology and cryptanalysis. Computing lent and purifies the old methods, using complex algorithms. The result of this marriage has solved a major problem today, offering tranquility in business transactions and entertainment online, with the creation of digital signatures and certificates, through which it is impossible to reject or fail to take an action committed in the cyber world. Even with such strength and solidity, in isolation, the technologies are incapable of guaranteeing the security of systems. It is necessary to describe and define specific policies, involving the culture of the actors. Not just virtual environments need protection, but also the physical environments. Several criteria and standards should be considered. That said and observed, reasoned and respected the issues alluded to above, this work is aimed to present the basic design of a new Public Key Infrastructure in line with current legislation, especially in harmony with Law 8666 of June 21, 1993, as requested by the Prefeitura Municipal de Curitiba, Paraná, to the generation of electronic identity for citizens curitibanos, explaining the best solutions and resources. Grounded in the theories and knowledge assimilated in the end the reader can envision the operation of the proposed services.

Keywords: cryptography, cryptanalysis, cryptology; cryptographers; cryptologists; cryptanalysts, algorithms, certificates and digital signatures, public key infrastructure, electronic identity

SUMÁRIO

1. INTRODUÇÃO.....	6
2. DESENVOLVIMENTO	8
2.1. Chaves e Algoritmos	11
2.2. Certificação e Assinatura Digital.....	14
2.3. Segurança da Informação.....	16
2.4. Reformulação do Modelo de Identidade Individual do Cidadão.....	21
2.5. Banco de Dados	21
2.6. Nova Infraestrutura de Chave Pública - ICP	23
2.7. Política de Segurança	25
2.8. Processo de Substituição de Identidade.....	26
2.9. Recrutamento, Contratação e Plano de Treinamento	28
2.9.1. Modelo Sugestivo de Cargo.....	29
2.9.2. Treinamento.....	30
2.10. Legislação	32
3. CONCLUSÃO	34
REFERÊNCIAS BIBLIOGRÁFICAS	36

1. INTRODUÇÃO

A Prefeitura Municipal de Curitiba, Paraná, de maneira audaciosa e inusitada, pretende adotar o documento de identidade eletrônico aos cidadãos curitibanos.

Essa iniciativa tem como principais metas o recadastramento das pessoas, a agilização dos processos de identificação e a concessão de acesso a diversos serviços eletrônicos.

Para isso, ela solicitou o desenvolvimento de um projeto básico de implantação de Autoridade Certificadora (AC) reconhecida pelo ICP-Brasil (Autoridade Suprema para a Aprovação de AC).

Vários componentes serão necessários à formação da nova estrutura, tais como servidores, programas, banco de dados, método de substituição do documento de papel pelo eletrônico, recrutamento e contratação de pessoal e plano de treinamento.

Assim sendo, o objetivo deste trabalho é desenvolver um estudo dos procedimentos para se embalar e proteger informações sigilosas, identificando e analisando as vantagens e desvantagens dos recursos mínimos necessários, a fim de fundamentar as escolhas.

Portanto, buscar entender o que é criptografia, examinando seus ramos, modelos de algoritmos, chaves, certificados e assinaturas digitais.

Também descrever a importância da confiança da informação, especificando como deve ser realizada a segurança virtual e física, citando fatos reais, com o objetivo de exemplificar a gravidade de falhas neste aspecto e salientar a relevância de uma boa política tratando o tema, no sentido de educar corretamente os colaboradores e garantir sucesso total.

Dentro do contexto do parágrafo anterior, com relação ao local onde serão hospedados os servidores, decidir entre instalá-los no prédio da prefeitura ou em um datacenter.

Sobre o novo banco de dados, especificar a linguagem e o modelo a ser adotado, incluindo um breve diagrama da estrutura do sistema.

A respeito da nova Infraestrutura de Chave Pública – ICP, apresentar o seu funcionamento através de um esquema e sugerir um método de substituição da identidade de papel pela eletrônica.

Ainda, determinar os critérios necessários e imprescindíveis à formação da nova equipe bem como um plano de treinamento.

Por fim, argumentar sobre a lei 8.666, de 21 de junho de 1993. Ela servirá de base para as licitações.

2. DESENVOLVIMENTO

A melhor maneira para se evitar o acesso a informações confidenciais e sigilosas, por pessoas não outorgadas, é uma questão discutida há vários séculos.

A Francomaçonomia e a Antiga e Mística *Ordem Rosae Crucis* ou Ordem Rosa-cruz, sociedades por onde passaram cientistas ilustres como *John Dee, Elias Ashmole, Robert Fludd, Paracelso, Bacon, Descartes, Pascal, Spinoza, Newton e Leibniz*, servem de modelo e referência.

Alguns conhecimentos estudados apenas pelas mentes mais brilhantes do mundo, baseados em verdades herméticas, que precisavam ser ocultados dos homens comuns, foram escondidos por muitas gerações, outros permanecem protegidos, ou seja, sem revelação.

O sucedido com Galileu Galilei ilustra bem a relevância de se proteger informações. Também mostra as consequências ao deixá-las cair em mãos erradas, em circunstâncias inoportunas.

Astrônomo, matemático e médico, Nicolau Copérnico, através da Teoria do Modelo Heliocêntrico, afirmou que a Terra girava em torno do seu próprio eixo uma vez por dia – o denominado efeito de rotação – e ao redor do Sol uma vez ao ano – o chamado efeito de translação.

Embora essa teoria ferisse o dogma da Igreja Católica, a mesma não havia condenado e aparentemente não condenaria a Teoria de Copérnico como herética.

Sendo fortemente motivado pelo papa Urbano VIII a prosseguir com seus estudos e a escrever um livro a respeito do assunto, Galileu Galilei confirmou o estudo de Copérnico, em sua obra *Dialogo di Galileo Galilei sopra i due Massimi Sistemi del Mondo Tolemaico e Copernicano* (Diálogo sobre os dois principais sistemas do mundo). Entretanto o papa ficou insatisfeito com o desenrolar da história, submetendo Galilei a um julgamento onde ele foi sentenciado à prisão por tempo indeterminado, além de ser compelido a revogar publicamente sua opinião sobre o tema.

Concisamente, esta história demonstra as consequências oriundas do vazamento ou falsa interpretação de uma mensagem. O estrago pode ser catastrófico, com proporções incomensuráveis.

Contudo, seria realmente possível ocultar uma informação, mesmo

transportando-a em meios públicos, garantindo assim a sua integridade?

Quem pode responder a esta indagação é a ciência nomeada de criptologia, um ramo da matemática.

Explorada pelos criptógrafos, criptólogos e criptoanalistas, essa ciência se divide em dois grandes campos, a saber: criptografia e criptoanálise.

Enquanto a criptografia visa aperfeiçoar os métodos de esconder a mensagem genuína e encaminhá-la com segurança ao destinatário, a criptoanálise busca interceptar e decifrá-la antes de ela atingir seu destino.

Outro recurso conhecido é a esteganografia. Ao invés de embalar a mensagem, ele apenas embaralha os caracteres, tornando-os ininteligíveis, portanto, fazendo-os perder totalmente o sentido a olho nu.

De forma análoga à esteganografia, a maçonaria criou um alfabeto usando da simbologia, onde convertia as letras triviais em símbolos ou *symbolon*. Dessa forma dificultava a interpretação aos leigos. Atualmente o esquema é frívolo e chega a ser infantil, como definiu Brown (2009).

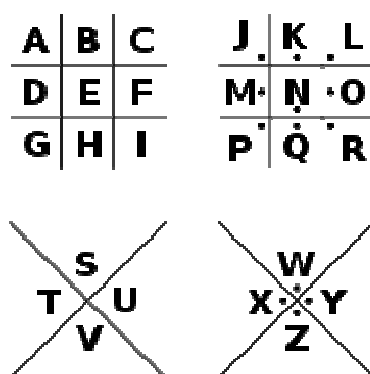


Figura 1 – Esquema ou Cifra Maçônica¹

Os espaços onde são recepcionadas as letras do alfabeto latino ou alfabeto romano se transformam em símbolos, como os da mensagem abaixo:

Figura 2 – Exemplo de Frase Cifrada com o Esquema Maçônico²

Assim sendo, apenas os detentores e conhecedores do esquema ou “chave”

¹ Fonte: <http://pt.wikipedia.org/wiki/Cifra_ma%C3%A7%C3%B3nica>

² Fonte: <http://pt.wikipedia.org/wiki/Cifra_ma%C3%A7%C3%B3nica>

conseguiam decifrar a mensagem.

Embora o diagrama tenha sido desvelado e seja de fácil compreensão, para dificultar a tradução, alguns conceitos ou fundamentos matemáticos eram usados com o intuito de bagunçar a ordenação dos símbolos, como o quadrado de Dürer. A desordem e reorganização geradas eram chamadas de alquimia ou fenômenos alquímicos. Contudo, antigamente as mensagens maçônicas eram invisíveis.

Partindo para uma visão contemporânea, dificultar a captura e o entendimento da informação por terceiros é uma tarefa estritamente imprescindível.

De acordo com a Intel Corporation (2010), setenta por cento das transações econômicas mundiais trafegam pela internet todos os dias.

Conforme destacou a referida companhia, mesmo com o avanço e acrisolamento de todas as ferramentas de segurança da informação, os prejuízos causados por fraudes galgam a casa dos bilhões de dólares.

Por isso, sempre visando a evitar a captura e a espionagem de seus documentos durante as transações digitais em meios públicos, como a rede mundial de computadores, a informática emprestou e melhorou os conceitos da criptografia antiga, também objetivada em transformar os seus dados, deixando-os irreconhecíveis a estranhos.

A criptografia moderna está apoiada em algoritmos com diversos graus de complexidade – os quais convertem o valor original em códigos secretos, através de um procedimento denominado de cifragem, gerando criptogramas, onde o transmissor possui uma chave de codificação a qual é compartilhada com o receptor. Sem ela, jamais o criptograma voltará para o seu talho legítimo.

Outro venábulo utilizado para a segurança, diretamente ligado aos sistemas de informação, é o esquema de autenticação e liberação, por meio de usuário e senha. Mas este modelo só restringe o acesso, sem distorcer o real significado do conteúdo, logo, é menos seguro, pois se a senha for descoberta seu teor será facilmente revelado. Então se sugere para operar com autenticação e cifração dos dados ao mesmo tempo.

Existem diversas funções e modelos de chaves, algoritmos e redes de dados, como a função algébrica booleana, chaves reutilizáveis e não reutilizáveis, algoritmos simétricos e assimétricos.

Portanto, o sucesso da proteção das informações, garantindo a confiabilidade, autenticidade, integridade e confidencialidade dos dados das pessoas, dependerá

da escolha e aplicação correta de tais itens. Afinal esta temática é bastante delicada e complexa, requerendo um estudo infinitamente perscrutado.

Narrados alguns pontos relevantes sobre os motivos e os procedimentos para se embaular informações importantes, a seguir serão fundamentados alguns termos utilizados a princípio, a fim de facilitar o entendimento do leitor e justificar as decisões a serem tomadas ao projeto em tese.

2.1. Chaves e Algoritmos

Para Sousa (1999), a chave é uma sequência de bits (zeros e uns) utilizada com o propósito de codificar os dados em outro formato, e pode ser gerada de maneira aleatória pelos próprios computadores. A decodificação ou a exibição do formato original só é possível com o seu conhecimento.

A fim de exemplificar, abaixo segue um modelo utilizando a função algébrica booleana, onde uma chave simples de 11 bits “00111001101” é repetida e somada aos bits da mensagem original:

Tabela 1 – Definição da Álgebra de Boole

$0 + 0 = 0$
$1 + 0 = 1$
$0 + 1 = 1$
$1 + 1 = 0$

Tabela 2 – Exemplo de Criptografia com a Álgebra de Boole

Mensagem original:	01110100100101000101101010111010001011
Chave:	00111001101001110011010011100110100111
Mensagem cifrada:	01001101001100110110111001011100101100

Quanto maior a quantidade de bits utilizada pela chave, mais sólida e forte ela será. O exemplo acima utilizou apenas 11 bits, a fim de simplificar a transformação e facilitar o entendimento. Uma chave começa a ficar segura a partir de 90 bits.

Assunte que a mensagem original é distinta do criptograma. Ele só poderá ser traduzido e compreendido, através do processo de inversão, se a chave for

conhecida pelo receptor, do contrário jamais será desvelado.

Há pelo menos dois tipos diferentes de chaves, uma reutilizável e outra não reutilizável.

O caso antecessor usou uma chave de 11bits, contando com a álgebra de Boole. Ela pode ser reutilizada quantas vezes forem necessárias, em outras circunstâncias. Porém, reutilizá-la frequentemente é uma fraqueza, pois esse modo de agir facilitará a sua descoberta, reduzindo assim sua fidúcia.

Sousa (1999) definiu que a chave não reutilizável é concebida ocasionalmente e com o cumprimento da mensagem, sendo um cifrário perfeito, mas incômodo de empregar, porque o ideal é operar com chaves inferiores ao tamanho das mensagens a serem transmitidas.

Sobre os algoritmos, eles podem ser simétricos ou assimétricos.

No caso do algoritmo simétrico uma única chave é compartilhada entre emissor e receptor. É um método questionável, todavia depende de como a chave é informada ao destinatário. Caso ela seja interceptada por um terceiro durante o transporte e esse venha a ter acesso à mensagem, a proteção se esvaírá.

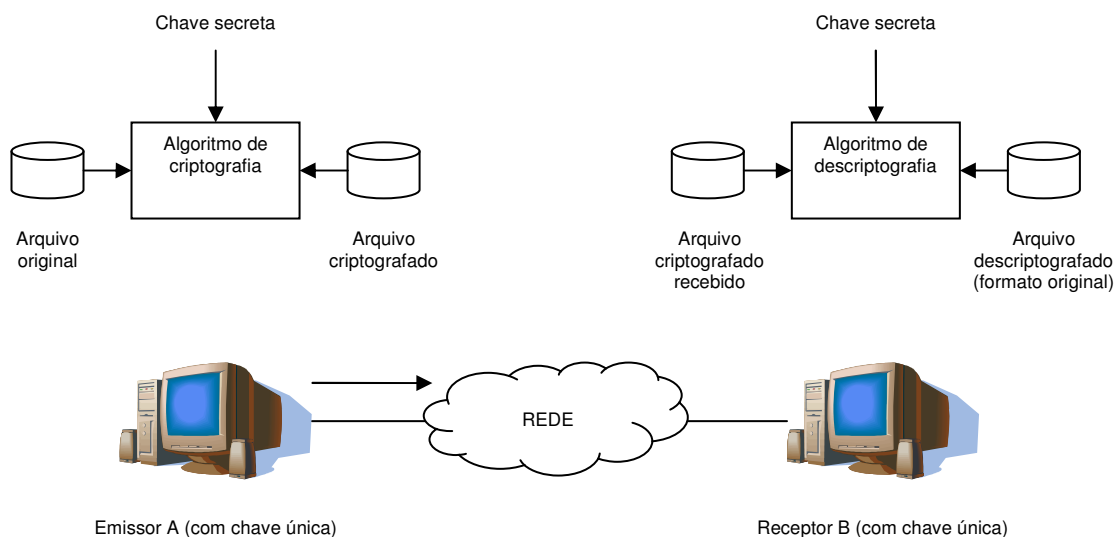


Figura 3 – Diagrama do Funcionamento do Algoritmo Simétrico³

O computador A está enviando um arquivo ou mensagem cifrada ao computador B, por meio de uma rede de dados. O computador B, ao recebê-lo e conhecendo a chave utilizada, consegue decifrar o criptograma, conforme ilustra a

³ SOUSA, Lindeberg Barros. **Redes de Computadores: Dados, Voz e Imagem**. São Paulo: Érica, 1999. 206 p. il.

figura 3.

Sendo um cifrário composto e utilizando uma *string* alfanumérica como chave de cifragem e decifragem, o algoritmo simétrico mais utilizado é o DES (*Data Encryption Standard*).

Diferentemente do algoritmo simétrico, o algoritmo assimétrico ou algoritmo de “chave pública”, como é comumente conhecido, trabalha com duas chaves. Enquanto uma delas (chave pública ou chave direta) cifra a outra (chave privada ou chave inversa) decifra a mensagem. Esse modelo proporciona maior segurança, porque o criptograma criado com a chave pública só pode ser decodificado com a chave privada do destinatário.

Sousa (1999) aponta o algoritmo assimétrico RSA como o mais popular. Também recomenda utilizá-lo com chave privada de mais de 90bits. Este cifrário foi criado em 1978 por *Ronald Rivest, Adi Shamir e Leonard Adleman*. O acrônimo é a concatenação das iniciais dos sobrenomes deles. Suas chaves são geradas a partir de números primos.

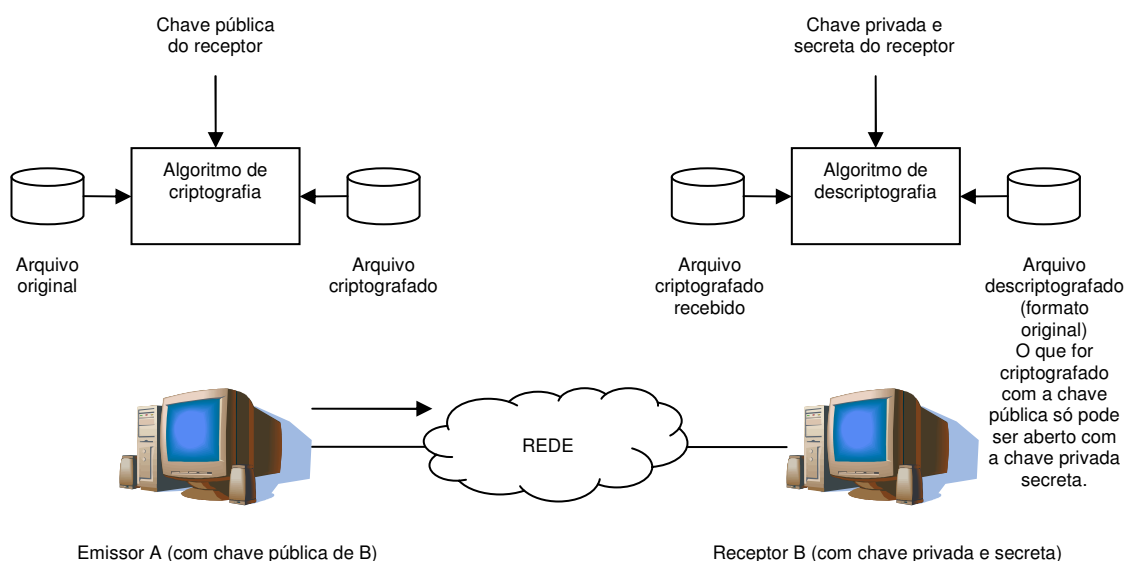


Figura 4 – Diagrama do Funcionamento do Algoritmo Assimétrico⁴

O computador A está enviando um arquivo ou mensagem cifrada ao computador B, que foi criptografada com a chave pública de B, por meio de uma rede de dados. O computador B, ao recebê-la, consegue decifrar o criptograma com sua chave privada e secreta, conforme ilustra a figura 4.

⁴ SOUSA, Lindeberg Barros. **Redes de Computadores: Dados, Voz e Imagem**. São Paulo: Érica, 1999. 208 p. il.

Por ser muito difícil ou impossível decompor um número composto, a fim de descobrir por quais outros ele foi gerado, a chave pública é divulgada abertamente em uma lista. Porém a chave privada é mantida secretamente pelos usuários.

Contudo, através do método de “pesquisa exaustiva”, *crackers* podem tentar a decomposição, testando vários números primos até identificar os dois utilizados para a geração da chave pública. Mas isso requer muito tempo, chegando a levar anos para a concretização do feito.

A técnica criptográfica utilizando o algoritmo assimétrico possibilitou a invenção da “assinatura digital”, abordada no item seguinte.

2.2. Certificação e Assinatura Digital

Como asseverar a origem ou destino de um arquivo ou mensagem, a fim de manter a confidencialidade e integridade da informação trocada entre computadores, mesmo embaulando o verídico significado?

Para garantir a validade e autenticidade da chave pública pertinente ao usuário, criou-se o processo de certificação com assinatura digital.

Na vida real, quando uma pessoa física ou jurídica necessita provar a veracidade de sua assinatura, ela se dirige a um cartório de registro ou cartório tradicional e solicita o reconhecimento de firma. O selo do cartório autentica o valor do documento, tornando-o confiável e irrefutável.

A certificação digital é análoga ao processo do parágrafo antecessor, onde uma Autoridade Certificadora ou *Certification Authority* (AC ou CA), também conhecida como “Cartório Eletrônico”, fornece o certificado digital, com prazo de validade, ou seja, o certificado tem um tempo de vida útil, deixando de valer depois de expirado o tempo previamente determinado pelo órgão regulador, porém pode ser revalidado.

Há dois tipos de certificado: A-1 e A-3. No primeiro, os dados da pessoa e a assinatura digital ficam armazenados em mídias como o disco compacto (CD). No segundo, as chaves dos usuários permanecem depositadas em *smart cards* ou *tokens*.

Um país pode ter diversas ACs, todavia elas precisam ser reconhecidas pela

Infraestrutura de Chave Pública ou *Public Key Infrastructure* (ICP ou PKI), uma instituição suprema que autoriza o funcionamento das Autoridades Certificadoras. No Brasil, a autoridade suprema se chama ICP-Brasil. Consentaneamente com a Intel Corporation (2010), ela controla oito ACs de primeiro nível, a saber: Presidência da República, Secretaria da Receita Federal, Serpro (Serviço Federal de Processamento de Dados), Caixa Econômica Federal, AC Jus, Imprensa Oficial de São Paulo, Serasa e CertiSign. Sem o aval desses órgãos, um certificado perde seu valor legal.

O certificado digital conseguiu resolver um dos maiores problemas dos tempos modernos, proporcionando uma comunicação com mais fidúcia e solidez aos fins comerciais e de lazer, pois o órgão regulador possui os dados do proprietário da chave pública, conseguindo deste modo garantir a veracidade da identificação por reconhecer o seu verdadeiro dono.

Desta forma, sabendo que a chave pública é realmente do destinatário, o emissor fica tranquilo e pode gerar o criptograma com plena segurança.

Através da assinatura digital, é impossível negar a origem da informação.

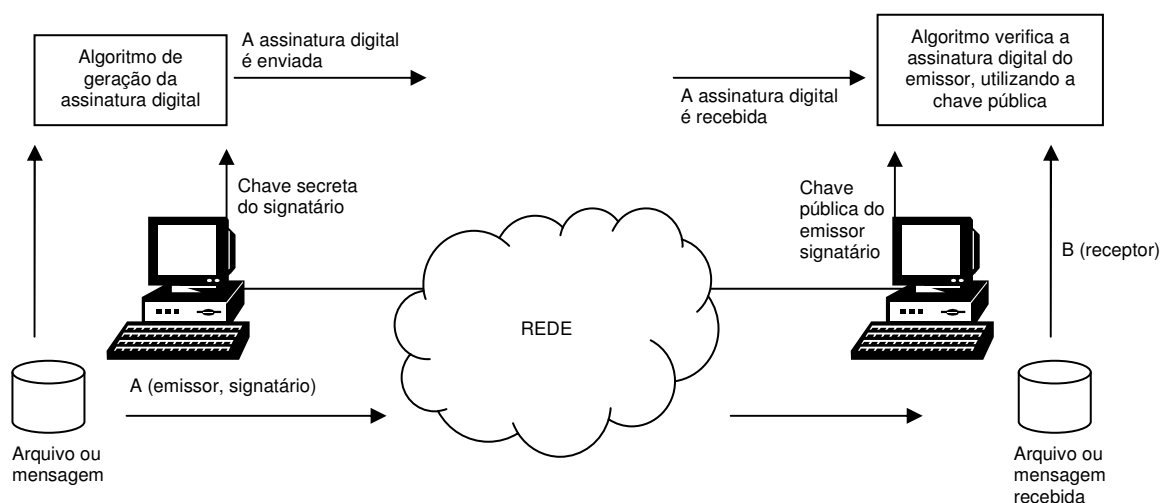


Figura 5 – Autenticação de Usuário Utilizando Cifrado Assimétrico⁵

O processo de cifração do sistema assimétrico é paulatino se comparado com o simétrico, afinal seu algoritmo possui mais elementos.

Sua vantagem está na segurança, todavia ele não apresenta o risco de interceptação da chave quando da transferência da mensagem ou arquivo, conforme

⁵ SOUSA, Lindeberg Barros. **Redes de Computadores: Dados, Voz e Imagem**. São Paulo: Érica, 1999. 215 p. il.

apresenta a figura 5.

2.3. Segurança da Informação

No primórdio da era digital, a preocupação com a fidúcia da informação guardada nos computadores restringia-se a aspectos físicos, afinal eles se comunicavam no máximo através de uma rede local.

A realidade atual é bem egrégia daquela, afinal as tecnologias da informação estão em constante mutação e se tornam excessivamente complexas a cada dia.

Inicialmente os sistemas eram centralizados em mainframes, máquinas de grande porte situadas em centrais de processamento de dados ou CPDs. O acesso a esses equipamentos limitava-se a poucos. Mas com o surgimento, aceitação e disseminação do microcomputador esses sistemas se tornaram distribuídos, complicando drasticamente o gerenciamento da informação.

Equiparados com as máquinas hodiernas, aqueles computadores são arcaicos, rudimentares. Porém, evitavam a redundância da informação. Com a distribuição dos sistemas, isso deixou de acontecer. A capacidade de armazenamento se tornou demasiadamente maior, contudo, é mal utilizada. Uma mesma informação, às vezes, fica armazenada em mais de uma máquina, ocupando desnecessariamente as memórias. Outro fator problemático é a inconsistência, porque essas informações ou dados podem ser alterados simultaneamente, transmutando ou distorcendo o lítico significado.

Ambientes virtuais seguros são raros ou inexistentes, pois, como os computadores estão interligados em redes de dados abertas, qualquer falha poderá culminar com a invasão de crackers ou a entrada de um vírus.

Narrados alguns pontos próceros, surge uma dúvida: como salvaguardar a solidez dos sistemas e ambientes físicos e virtuais, assegurando a integridade e confidencialidade dos dados?

A resposta a esta indagação está na utilização da função de “*hashing*” ou de checagem por meio do controle de acesso, autenticação, criação de túneis virtuais seguros para o transporte da informação em redes públicas, geração de *backup*, entre outros, sempre pensando na segurança dos arquivos, equipamentos e

instalações físicas.

O controle de acesso tem por objetivo conceder ou revogar o acesso de usuários a sistemas, aplicações e instalações físicas, conforme as alçadas peculiares dos funcionários ou atores. E pode ser através de senhas de acesso ou autenticação, como identificação biométrica e cartão magnético ou “inteligente”, palavras-chave, firewall.

O processo de autenticação por criptografia é um dos mais seguros. Ele oferece total sigilo na troca das identificações. Alguns protocolos desenvolvidos aperfeiçoaram significativamente esse tipo de operação, tais como: PAP (*Password Authentication Protocol*), *Tacacs* e *Radius*.

Outro aspecto positivo da autenticação é o não repúdio ou irretratabilidade, pois a autoria ou identidade da pessoa ou empresa fica registrada, impossibilitando a negação dos fatos.

Para Sousa (1999), a autenticação se sucede entre os participantes num acesso ou entre os dados da mensagem, permitindo às partes a garantia de identidade, envolvendo usuários versus sistemas ou clientes versus servidores.

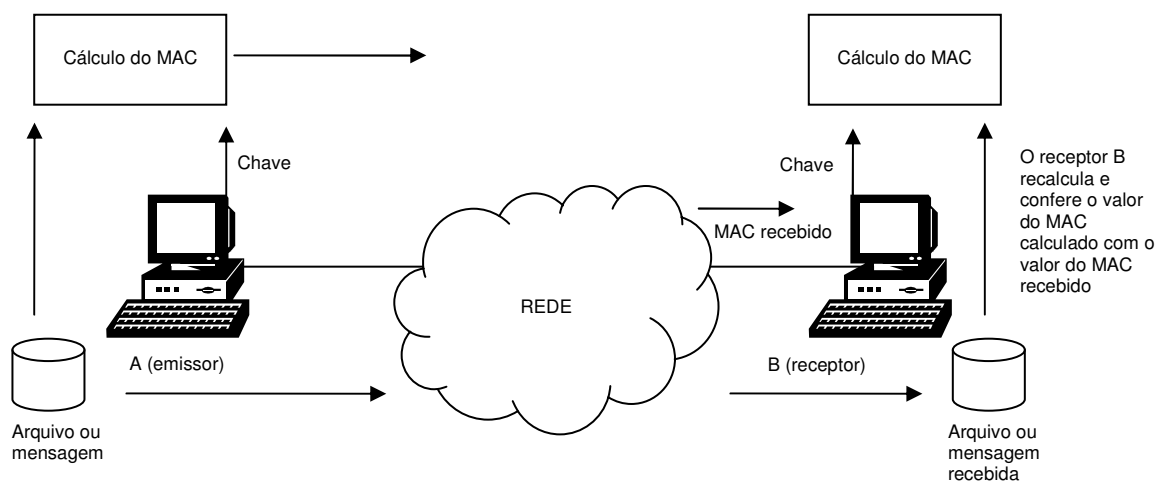


Figura 6 – Autenticação Baseada nos Dados do Documento em Sistemas Simétricos⁶

A fim de exemplificar, suponha que alguém queira enviar um documento autenticado, pela rede de dados, assegurando sua integridade e autoria. Nesse caso, a autenticação será embasada nos dados do referido arquivo, usando o algoritmo simétrico, por criar o criptograma mais rapidamente.

⁶ SOUSA, Lindeberg Barros. **Redes de Computadores: Dados, Voz e Imagem**. São Paulo: Érica, 1999. 214 p. il.

Contando com parâmetros diversos como data, hora, criptografia e fazendo uso da chave DES, o algoritmo calcula um valor final chamado de MAC (*Message Authentication Code*).

Sousa (1999) descreveu o MAC como um bloco de informações anexado ao final do documento.

Caso o documento sofra avarias no percurso, esse dano poderá ser apurado pelo receptor, conforme apresenta a figura 6. Isso é possível visto que ao receber tal arquivo, o destinatário irá recalculá-lo. Se esse valor for divergente do MAC incluso ao final, é porque o arquivo sofreu alterações antes de atingir o destino. Logo, deve ser descartado.

Com relação aos túneis virtuais criados, a partir dos procedimentos de autenticação e criptografia, criou-se o conceito de rede privada virtual ou *virtual private network* (VPN).

Igualmente mostra a figura 7, a rede privada é arquitetada sobre as redes públicas, gerando túneis de comunicação cifrada ou “tunneling”, como se fosse um canal privativo e dedicado, proporcionando colossal segurança, pois somente os computadores autorizados podem integrar essas conexões, portanto, o teor dos dados é inacessível a terceiros.

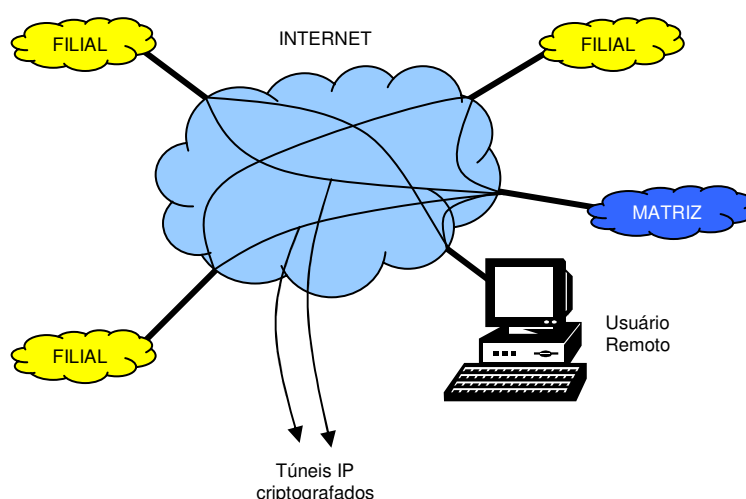


Figura 7 – Rede Virtual Privada por Meio da Internet⁷

Sousa (1999) traçou seu desenho e determinou os componentes básicos, como: autenticação – para garantir a identidade dos usuários e servidores,

⁷ SOUSA, Lindeberg Barros. **Redes de Computadores: Dados, Voz e Imagem**. São Paulo: Érica, 1999. 216 p. il.

privacidade e segurança, integridade, cifragem e decifragem dos dados.

O sucesso de uma rede desse naipe depende da sua capacidade de suportar e transportar diferentes protocolos, tais como o IP, IPX, Netbios, entre outros, da garantia da solicitação e execução da autenticação, da interligação dos túneis de comunicação com protocolos do tipo L2TP (*Layer 2 Tunneling Protocol*), IPSec, PPTP (*Point to Point Tunneling Protocol*).

Até o momento a ênfase foi ao ambiente virtual, mas, e o ambiente físico, seria menos relevante?

O ambiente físico é tão importante quanto o virtual. Os dados precisam ser depositados em servidores protegidos contra alterações e perdas, principalmente no que tange às intempéries, portanto, livres de desastres ambientais e danos acidentais.

O local onde serão construídos os datacenters para hospedar os servidores necessita ser muito bem estudado, planejado. De acordo com Halla (2010), jamais eles podem ser construídos próximos de vizinhos nocivos, tais como: depósitos de empresas de qualquer natureza, embaixadas, fábricas, presídios, enfim, longe de lugares sujeitos a incêndio, manifestações populares, enchentes, terremotos e vulcões, tornados e furacões, avalanches e deslizamentos.

Partindo a uma visão mais abrangente e realista, países alvo de guerra devem ser evitados ou, então, o ideal é construí-los subterraneamente, com estrutura específica para aguentar vários megatons, a fim de suportar a uma explosão atômica. Veja o ilustrado nas figuras 8 e 9.

Como todo equipamento é suscetível a soft crash – falha do sistema – e a hard crash – falha da mídia, pensando em *recovery* (recuperação), os servidores operam em sincronismo ou em RAID (*Enterprise Redundant Array of Independent Drives ou Redundant Array of Inexpensive Drives* – Conjunto Redundante de Discos Independentes). Entretanto, uma falha bastante evidente é manter os servidores paralelos ou em sincronismo no mesmo ambiente, pois, ocorrendo uma eventualidade, todo o sistema será afetado. O correto é instalar os servidores de segurança em outras localidades.

Para efeito de ilustração, o ataque terrorista sucedido no World Trade Center em Manhattan, Nova York, em 11 de setembro de 2001, derrubou ambas as torres, destruindo-as plenamente. Se as companhias da torre A mantivessem seus servidores de backup na torre B, teriam perdido seus bens mais valiosos – a

informação, indo à falência.

Finalmente, o recinto onde serão alocados os equipamentos precisa contar com boa ventilação e refrigeração do ar, instalações elétricas adequadas e protegidas contra falhas, mobília de trabalho apropriada. Ainda, as pessoas devem ser treinadas constantemente, sempre visando a assegurar as operações dos equipamentos e manutenção da rede, conforme ilustram as figuras 8 e 9.

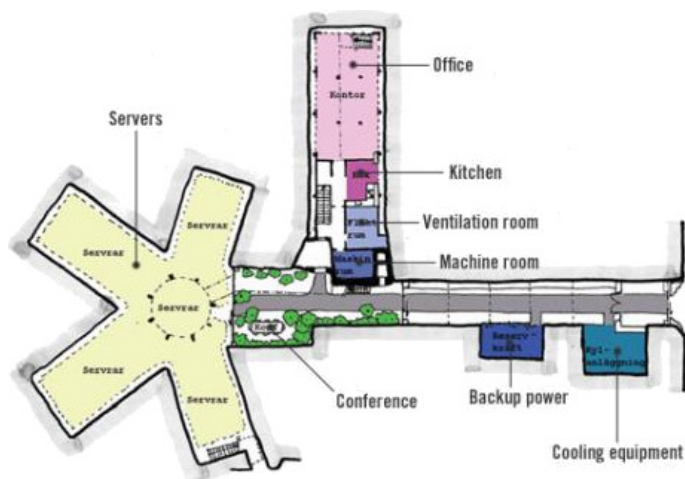


Figura 8 – Planta Baixa do Datacenter Pionen White Mountains Subterrâneo⁸



Figura 9 – Outras visões do Datacenter Pionen White Mountains Subterrâneo⁹

⁸ Fonte: <<http://cybervida.com.br>>

⁹ Fonte: <<http://cybervida.com.br>>

Muito embora o Datacenter Pionen White Mountains pareça ser ficção científica, ele é pura realidade e está instalado onde antes era um abrigo anti-nuclear escavado em pedras, 30 metros abaixo de Estocolmo, na Suécia.

2.4. Reformulação do Modelo de Identidade Individual do Cidadão

Tendo em vista a inédita iniciativa da Prefeitura Municipal de Curitiba, Paraná, a de substituir o documento de identidade individual do cidadão de papel por um modelo eletrônico, este projeto apresentará, a partir de agora, uma proposta para a implementação da nova AC e demais fatores envolvidos.

A nova identidade, além da função de identificação peculiar do indivíduo, servirá a outros fins, concedendo acesso a diversos serviços oferecidos pela referida prefeitura, portanto, fazendo uso da certificação digital.

Para tanto, os cidadãos deverão ser recadastrados, a fim de atualizar os dados, tornando-os consistentes e evitando possíveis erros ou redundância. Também, o recadastramento possibilitará a criação de uma ficha ampla, com novos campos, tais como e-mail e telefone.

Por se tratar de informação séria e sigilosa, o banco de dados necessitará de extrema proteção. Como construir uma sala com a infraestrutura mínima necessária para armazená-lo despenderia altas cifras, o ideal será terceirizar o serviço de hospedagem a um datacenter confiável, robusto e disponível no mercado brasileiro.

Por fim, o projeto contemplará um plano especificando os processos de treinamento aos colaboradores, troca do documento de identidade de papel pelo eletrônico e definição dos cargos dos envolvidos.

2.5. Banco de Dados

Adotando a linguagem padrão SQL (*Structured Query Language* – Linguagem Estruturada de Pesquisa), o Modelo Entidade-Relacionamento (Modelo ER) deverá ser escolhido ao banco de dados.

Devido à facilidade de manipulação e entendimento, ele é o mais popular entre os desenvolvedores, porque parte da percepção de que o mundo real é constituído de entidades se relacionando, ou seja, objetos e atores interagindo.

Machado (2008) demonstrou como a SQL pode manipular objetos de diferentes classes entre as funções de um SGBD (Sistema Gerenciador de Banco de Dados), por ser uma linguagem de numerosas aplicações, como demonstra a figura 10.

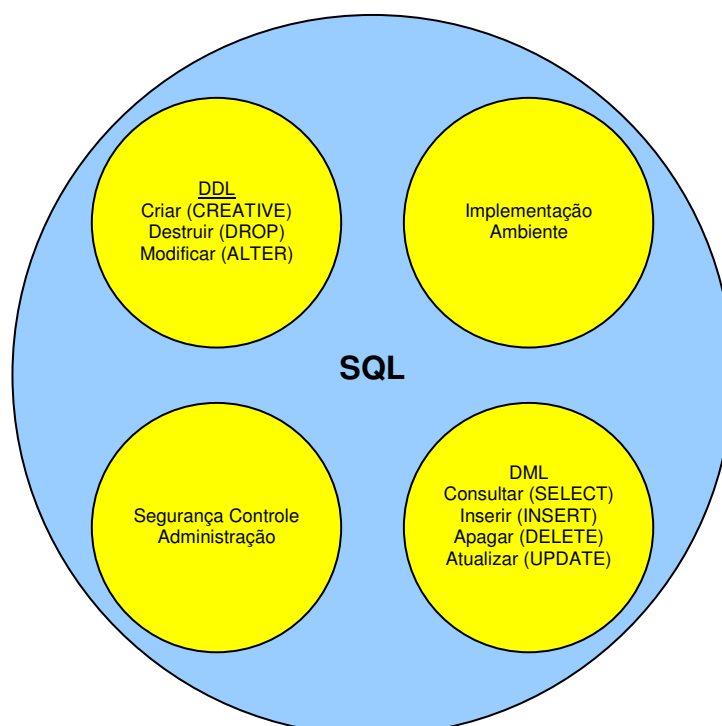


Figura 10 – Aplicações da Linguagem SQL¹⁰

O modelo ER proporciona uma comunicação otimizada entre os usuários e os desenvolvedores de sistemas, pois possui um elevado grau de semântica. É composto de três classes de objetos, a saber: entidades, relacionamentos e atributos.

As entidades são responsáveis pelo armazenamento das informações de toda e qualquer coisa do mundo real. Seus exemplos: pessoas físicas ou jurídicas, objetos físicos ou abstratos tipo CPF (Código de Pessoa Física), RG (Registro Geral), CNH (Carteira Nacional de Habilitação), endereço, bairro, cidade, estado, telefone e e-mail.

¹⁰ MACHADO, Felipe Nery Rodrigues. **Projeto e Implementação de Banco de Dados**. São Paulo: Érica, 2008. 317 p. il.

As associações existentes entre as entidades formam os relacionamentos ou interligação entre elas.

Os atributos descrevem as características peculiares das entidades, representando suas propriedades.

De maneira sucinta, a arquitetura do banco de dados onde serão registrados todos os dados dos cidadãos pode ser vista na figura 11.

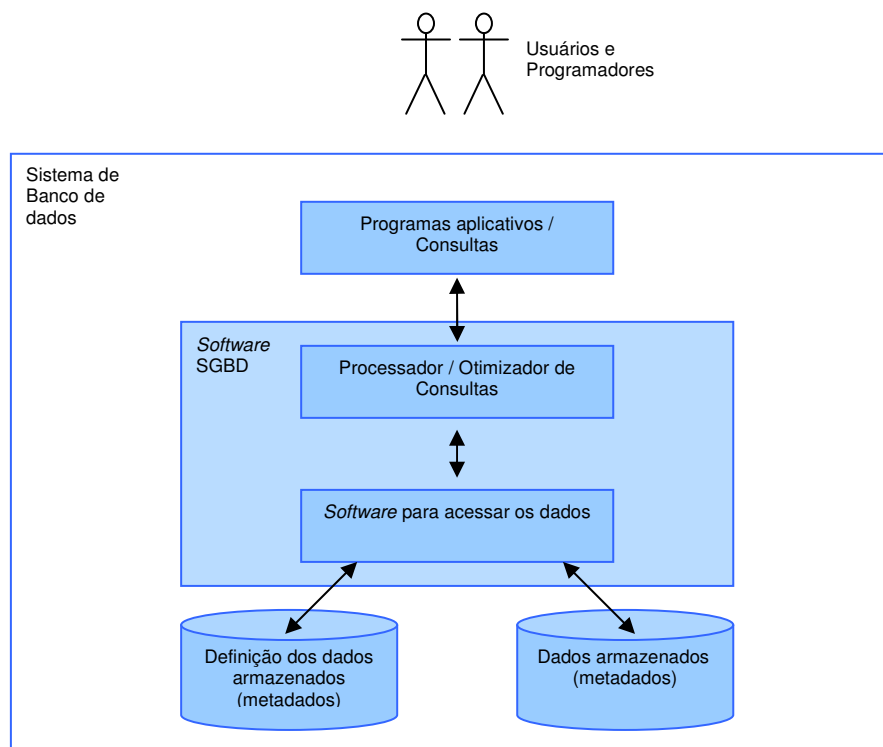


Figura 11 – Diagrama da Arquitetura do Sistema de Banco de Dados¹¹

2.6. Nova Infraestrutura de Chave Pública – ICP

Um Servidor Linux gerará as chaves públicas e privadas dos cidadãos, enquanto um Servidor Windows se responsabilizará pelo armazenamento dos dados das pessoas bem como a Chave Pública e CRL ou LRC (Lista de Revogação de Certificados).

O CRL é necessário para evitar o uso indevido ou não autorizado de um certificado, sempre que alguém desistir de utilizá-lo ou quando ele for furtado. Em

¹¹ UNIVERSIDADE PAULISTA. **Apostila de Administração de Banco de Dados**. São Paulo: [s.n.], 2009. 6 p. il.

outras palavras, é uma lista negra dos certificados anulados, a qual deve ser consultada impreterivelmente por todos os processos envolvendo uma ICP.

Outro Servidor Linux assumirá o papel de rodar as aplicações web, a fim de permitir o acesso aos diversos serviços disponibilizados pela prefeitura, tais como: acessar informações e solicitar documento de identidade eletrônico.

O acesso aos serviços online será protegido por um roteador com firewall, para assegurar a fidedignidade das transações.

A figura 12 apresenta o exposto acima com maiores detalhes.

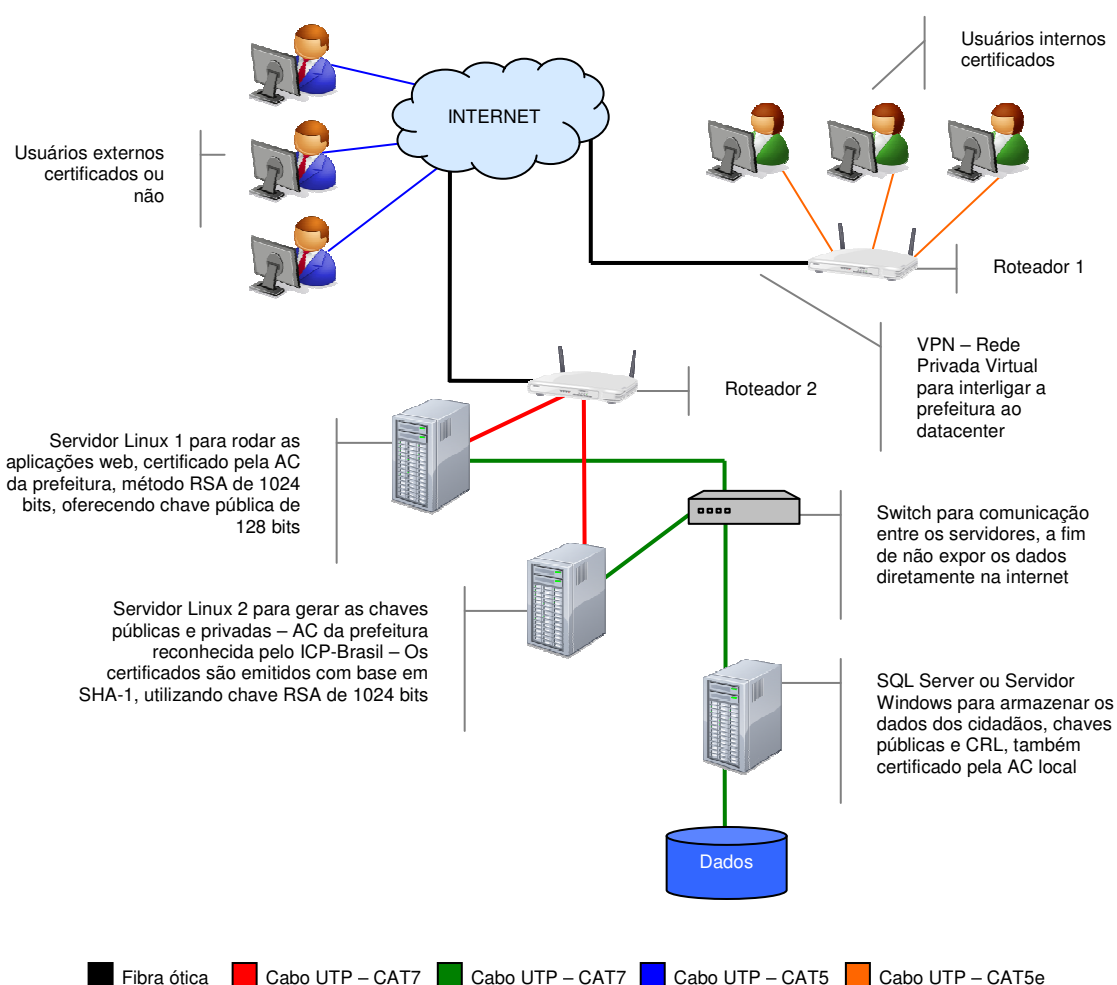


Figura 12 – Diagrama da Nova ICP

O usuário externo não cadastrado deverá, primeiramente, acessar o servidor de aplicação web, através da porta 80. Ao solicitar o domínio, o roteador indicará automaticamente o Servidor Linux 1.

Depois de registrado e liberado, quando o usuário externo efetuar acesso autenticado, ele será direcionado ao Servidor Linux 1, porém o referido servidor irá

consultar o SQL Server a fim de averiguar a validade do certificado digital.

Um diferencial bastante significativo e de extrema valia é a utilização do protocolo SSL (*Secure Sockets Layer*) e não HTTP (*Hypertext Transfer Protocol*) para as transações. A conexão via SSL é mais confiável, porque se realiza com a utilização de um certificado digital. Logo, é criptografada.

Os usuários internos acessarão os servidores apenas através de autenticação digital, por meio de uma rede privada virtual, garantindo assim sigilo absoluto.

O projeto todo deverá ser realizado num prazo máximo de doze meses, incluindo a compra dos servidores, definição dos cargos, contratação e capacitação de pessoal, estabelecimento de contato com os órgãos competentes para a liberação e aprovação do funcionamento da nova AC, entre outros.

2.7. Política de Segurança

Este projeto visa mais a parte estrutural e de arquitetura da nova AC, não adentrando nas peculiaridades dos sistemas ou modelos adotados.

Entretanto, é de suma importância salientar a relevância das políticas de segurança, afinal instituições isentas de um esquema de fidúcia bem planejado e implantado ficam suscetíveis a sucumbirem ou definharem diante de ataques inesperados.

Nos tempos atuais, faz-se necessário operar preventivamente. O certo é evitar ações corretivas e isoladas.

Antivírus e senhas de acesso apenas são insuficientes para asseverar a solidez e robustez da segurança, tornando obrigatório o desenvolvimento de uma política, através da qual os colaboradores serão educados conforme os critérios, necessidades e visões do local onde estão inseridos, ou seja, tomarão conhecimento das regras formais de acesso às tecnologias e recursos disponíveis.

A política de segurança deverá determinar os seguintes procedimentos:

- O que fazer e como acessar o correio eletrônico;
- O que fazer e como acessar a internet;
- Como, quem e quando instalar novos softwares;

- Responsável e como fazer e armazenar backups;
- Comprimento e periodicidade das senhas;
- Determinação de penalidades explícitas para o não cumprimento dos itens;
- Quem serão os integrantes da equipe de segurança;
- Período de vigência;
- Entre outros.

Acima de tudo, as pessoas necessitam trabalhar com ética.

O ambiente de trabalho serve para a resolução de problemas da empresa ou instituição. Os interesses e as obrigações particulares precisam ser sanados fora da esfera empresarial.

Caso um usuário do sistema tente baixar um vídeo pela internet, esse comprometerá toda a rede, causando lentidão às demais transações e prejudicando todo o fluxo operacional dos sistemas, contudo, atrapalhando os negócios prioritários.

Baixar e instalar programas piratas são os erros mais graves, pois esse modo de agir pode enganar firewall e burlar os antivírus, vindo a alojar e disseminar um arquivo nocivo por toda a rede, comprometendo plenamente os sistemas e colocando as bases de dados em perigo.

Finalizando, o documento denominado de política de segurança visa a abolir as falhas aludidas, proporcionando muita tranquilidade às operações.

2.8. Processo de Substituição de Identidade

O novo modelo de identidade será solicitado impreterivelmente pela internet, por todos os curitibanos.

Para os municípios ainda não contemplados pela inclusão digital, a prefeitura destinará um espaço de auto-atendimento em seu prédio, com vinte e cinco terminais, além de liberar as bibliotecas entre outras repartições públicas a tal fim. O novo espaço permanecerá aos diversos serviços eletrônicos oferecidos, e funcionará analogamente ao sistema bancário vigente.

O cadastramento in-loco acontecerá com cronograma configurado por bairro e

data.

Dois terminais de auto-atendimento serão destinados àqueles que deixarem de comparecer no dia convocado, a fim de evitar tumultuo ou aglomeração de gente.

Segundo o IBGE, em 2008 o número de habitantes de Curitiba passava de um milhão e oitocentos mil.

Considerando o tempo de dez minutos por cadastro, num total de sete horas diárias de atendimento, cada terminal realizará o equivalente a quarenta e dois registros diariamente. Sendo vinte e cinco máquinas no novo espaço, por dia serão realizados 1050 cadastros. Esse valor não contempla as solicitações realizadas pelos internautas e em demais locais.

Caso todos os cidadãos resolvessem se dirigir à prefeitura, seriam necessários aproximadamente um mil e setecentos dias ou quatro anos e seis meses para a conclusão do serviço. Entretanto, espera-se menos de 30% da população nos postos de atendimento físicos.

O tempo máximo para a substituição do documento antigo é de dois anos, podendo ser prorrogado, se for irremissível.

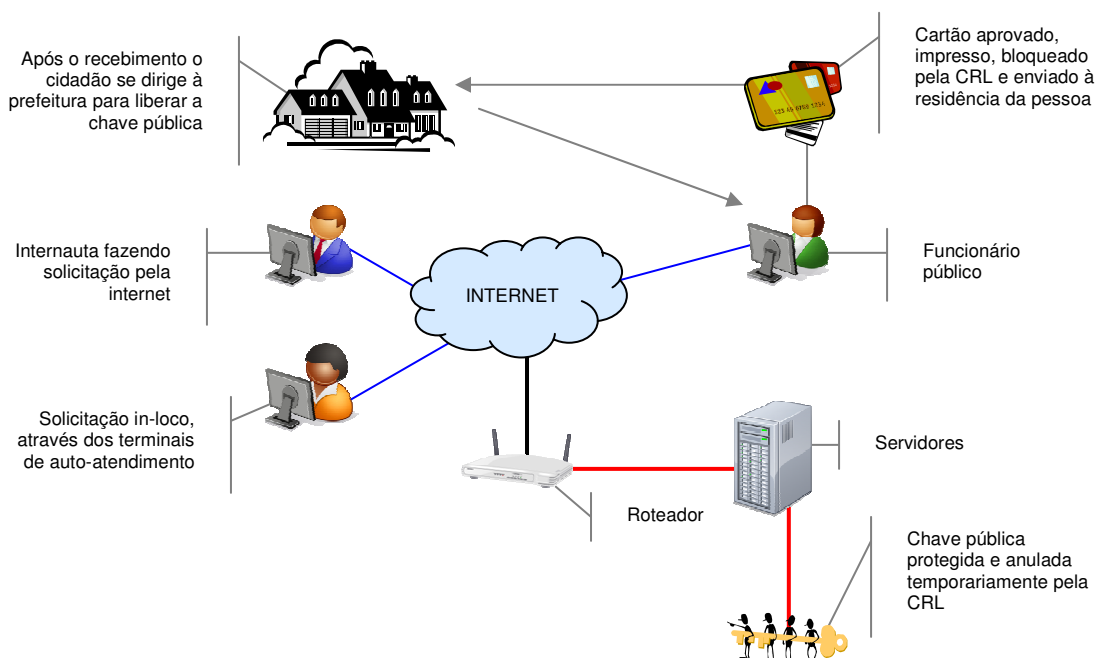


Figura 13 – Diagrama do Processo de Substituição de Identidade

Após análise e aprovação da nova identidade, o documento será enviado via correio às residências das pessoas. Essas, por sua vez, necessitarão entrar em contato para a liberação e entrega da cédula antiga. Ausente de liberação, a nova

chave deixará de funcionar, pois estará criteriosamente incluída na CRL. Contudo, o processo de liberação consiste em excluir a chave pública relacionada ao documento da CRL, conforme apresenta a figura 13.

2.9. Recrutamento, Contratação e Plano de Treinamento

Consistentemente com Oliveira (2007), o processo de recrutamento é a fase mais importante da formação de uma equipe ou time. Todo o sucesso depende de como o cargo é descrito e da determinação da qualificação, juntamente com requisitos básicos, como a experiência, escolaridade, responsabilidade, conhecimento técnico, condições de trabalho, enfim, dos fatores exigidos de seus ocupantes para um efetivo e promissor desempenho.

Recrutar, selecionar e contratar profissionais essenciais ao funcionamento de um serviço ou departamento, não é tarefa frívola. Requer a contratação de uma empresa terceirizada e especializada em processos de transição de recursos humanos e realização de concursos públicos.

A descrição da tarefa, função e cargo precisa ser muito bem planejada. Logo, essa tarefa ficará a cargo da empresa mancomunada. Este projeto simplesmente sugerirá o perfil ideal e imprescindível para a ocupação dos cargos.

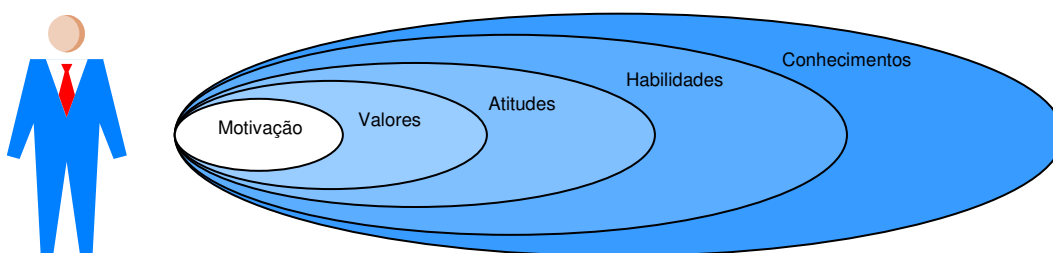


Figura 14 – Comportamento a ser desenvolvido¹²

Apenas pessoas concursadas, egressas do ensino médio para cargos x e formadas em nível superior para cargos y, bilíngue para cargos z, com formação profissionalizante ou similar em informática, comunicativa, sociável, paciente, confiável, dinâmica, ética, educada e apresentável, poderão compor a nova equipe

¹² BOOG, Gustavo G.; BOOG, Magdalena T. **Manual de Treinamento e Desenvolvimento: Gestão e Estratégias / Coordenação**. São Paulo: Pearson Prentice Hall, 2006. 185 p. il.

da central de atendimento ao cidadão.

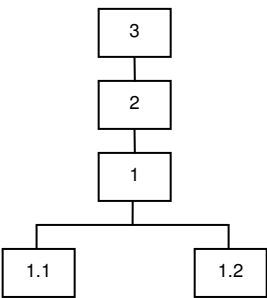
Após a fase de recrutamento e contratação de pessoal, os colaboradores ingressos passarão por um treinamento de integração, a fim de terem seus conhecimentos modelados, além de adquirirem novos saberes.

Com a capacitação espera-se desenvolver os comportamentos: motivação, valores, atitudes, habilidades e conhecimento, conforme mostra a figura 14. Como dizem Boog e Boog (2006), o conhecimento é a base para construir o restante.

2.9.1. Modelo Sugestivo de Cargo

Embasado no exemplo de Oliveira (2007), a seguir um único modelo sugestivo de cargo, com uma composição completa, estabelecendo critérios e técnicas para a empresa contratada prosseguir com o recrutamento e seleção de pessoal.

Tabela 3 – Modelo Sugestivo de Cargo

Prefeitura Municipal de Curitiba	Departamento: Central de Atendimento
Cargo: Atendente	
Área: Recepção	Setor: Atendimento ao Cliente
Local: Nova sala da prefeitura, onde estarão os terminais de auto-atendimento	
ORGANOGRAMA DE LOCALIZAÇÃO	
 <pre> graph TD 3[3] --- 2[2] 2 --- 1[1] 1 --- 1.1[1.1] 1 --- 1.2[1.2] </pre>	3. Diretor Executivo 2. Gerente de Atendimento 1. Coordenador de Atendimento 1.1. Supervisor de Atendimento 1.2. Atendente
Objetivo final (missão do cargo): Atender os cidadãos de maneira eficiente e satisfatória.	
Fornecedor: Todos os departamentos ou órgãos envolvidos, tais como: datacenter, autoridade certificadora interna, desenvolvedores, entre outros.	
Cliente: Cidadãos e departamentos ou órgãos dependentes dos serviços prestados.	

Atividades não delegadas

- Solicitar senha do usuário.
- Auxiliar e liberar acesso aos usuários internos e externos à internet.
- Indicar treinamentos.
- Modificar os procedimentos e metodologias operacionais.
- Alterar as políticas definidas.
- Deixar de cumprir as obrigações.

Atividades delegadas

- Atender, recepcionar e orientar clientes internos e externos.
- Notificar o superior imediato sobre qualquer anormalidade que possa comprometer as transações normais.
- Participar de treinamentos quando convocado, certificando-se de que outro colaborador assumiu seu posto, a fim de evitar possíveis transtornos.

Contatos internos

Departamentos: auxiliar a sanar dúvidas oriundas de cadastros problemáticos.
 Atendimento: levantar problemas decorrentes da atualização ou instalação de novos sistemas.
 Diretoria: viabilização de planos ou recursos.
 Central de atendimento: dúvidas relacionadas ao atendimento.

Contatos externos

Fornecedores de soluções tecnológicas: cursos referentes às novas tecnologias ou atualizações.

Análise do cargo

Nível decisório: o cargo tem autoridade para resolver problemas relacionados às dúvidas dos cidadãos.

Dimensões: não tem subordinado direto.

Qualificação: ensino médio. Formação profissionalizante ou similar em informática. Dois anos de experiência em atendimento ao público. Bilíngue.

Aprovação:

Ocupante:

Data:

Superior Imediato: Coordenador de atendimento

2.9.2. Treinamento

Boog e Boog (2006) afirmaram que uma empresa ou instituição será tão grande quanto for a qualidade das pessoas que nela trabalham.

Para Grubbs-West (2007), a contratação deve ser baseada na filosofia de vida, entretanto, a contratante precisa fornecer um treinamento para a função. Um

dos princípios de lealdade determinado por ela, chama bastante a atenção: “contrate quem é *bom*, pois não é possível treinar ninguém para ser *bom*”.

Tais visões explicitam a importância de um excelente treinamento ao desenvolvimento e ascensão pessoal e profissional dos colaboradores, mesmo depois de ter contratado os melhores.

A eficiência e eficácia de um curso de capacitação profissional são subalternas de um bom planejamento, através da construção de um plano, onde serão especificados os detalhes relevantes, inerentes e indispensáveis, conforme sugere a tabela a seguir:

Tabela 4 – Plano de Treinamento

CONTEÚDO PROGRAMÁTICO	RECURSOS INSTRUCIONAIS	DINÂMICA	CARGA HORÁRIA	AValiação	INSTRUTOR
Integração 1.1. Apresentação da base organizacional e tecnológica 1.2. Definição da missão e visão 1.3. Cultura organizacional 1.4. Introdução das políticas organizacionais 1.5. Exibição das metodologias adotadas 1.6. Apresentação formal da equipe	- Apostilas - Vídeos - Mapas - Retroprojeter - Slides - Lousa	- Aulas expositivas - Apresentação de vídeos - Trabalho em grupo - Visita a campo - Dinâmica de grupo	Dois turnos de quatro horas, num total de oito horas	- Abertura de diálogo com interação por meio de indagações orais - Questionários - Observações	Superintendente do depto. RH e pessoal do depto. qualidade
Conhecimento técnico específico 1.1. Apresentação das tecnologias, através de aulas práticas 1.2. Realização de testes laboratoriais 1.3. Aplicação de exercícios práticos 1.4. Conceitos e fundamentos 1.5. Conclusão	- Apostilas - Vídeos - Mapas - Retroprojeter - Slides - Lousa - Computadores	- Aulas expositivas - Apresentação de vídeos - Trabalho em grupo	Doze turnos de quatro horas, totalizando quarenta e oito horas	- Abertura de diálogo com interação por meio de indagações orais - Questionários teóricos - Teste prático - Observações	Pessoal do depto. engenharia de <i>software</i> e demais fornecedores das novas tecnologias
Oficialização 1.1 Entrega dos certificados 1.2 Alocação de pessoal	-x-	- Reconhecimento dos colaboradores e gesto de agradecimento	-x-	-x-	Superintendente do depto. RH ou coordenador local

2.10. Legislação

Todas as tecnologias e demais fatores envolvidos, a serem adquiridos para a formação e consolidação do novo departamento, deverão atender ao disposto na lei 8.666¹³, de 21 de junho de 1993, a qual regulamenta o art. 37, inciso XXI, da Constituição da República Federativa do Brasil, instituindo normas para licitações e contratos da Administração Pública e dando outras providências.

A preferência será pelos serviços e produtos produzidos ou prestados por empresas brasileiras de capital nacional; produzidos no país; produzidos ou prestados por empresas brasileiras; produzidos ou prestados por empresas que invistam em pesquisa e no desenvolvimento de tecnologia no país; conforme estabelece o terceiro artigo da referida lei, em seu segundo parágrafo.

De acordo com o sétimo artigo da aludida lei, a execução de obras e a prestação de serviços, impreterivelmente, obedecerá à seguinte ordem: projeto básico, projeto executivo e execução das obras e serviços. Do contrário estará em desconformidade, podendo tal licitação ser caçada, revogada. Todavia as etapas antecessoras, com exceção do projeto executivo, podem ser realizadas concomitantemente à execução das obras e serviços, havendo o consentimento da Administração Pública.

Sem a existência de um projeto básico, aprovado pela autoridade competente, e disponível para consulta pelos interessados em participar do processo licitatório; e com ausência de um orçamento minucioso para expressar a composição de todos os custos unitários; também sem uma previsão de recursos orçamentários para asseverar a quitação das obrigações decorrentes das obras e serviços a serem executadas no exercício financeiro em curso, conforme o cronograma; e, finalmente, sem que o produto dela esperado esteja contemplado nas metas estabelecidas no Plano Plurianual, se for o caso; as obras ou os serviços não poderão ser licitados, cabendo sanções aos infratores.

Sobre os custos ou valores a cobrar pelo serviço, passa a valer a lei 9.648, de 27 de maio de 1998. Salvo os casos expressamente previstos em lei, as licitações serão julgadas pelo menor valor da tarifa do serviço público a ser prestado; a maior

¹³ Fonte: <http://www.planalto.gov.br/ccivil_03/Leis/L8666cons.htm>

oferta, quando de pagamento ao poder concedente pela outorga da concessão; a melhor proposta técnica, com preço fixado no edital; a melhor proposta em razão da combinação dos critérios de menor valor da tarifa do serviço público a ser prestado com o de melhor técnica; entre outros.

A respeito da contratação e treinamento dos novos colaboradores, a seção IV, dos Serviços Técnicos Profissionais Especializados, deverá ser consultada. Ela trata dos estudos técnicos, planejamentos e projetos básicos ou executivos; pareceres, perícias e avaliações em geral, fiscalização, supervisão ou gerenciamento de obras ou serviços; treinamento e aperfeiçoamento de pessoal; entre outros. Ainda, ressalva em seu primeiro parágrafo que os contratos para a prestação de serviços técnicos profissionais especializados deverão, preferencialmente, ser celebrados mediante a realização de concurso público, com estipulação prévia de prêmio ou remuneração.

3. CONCLUSÃO

Conclui-se com este estudo e projeto que não há sistemas com fidiúcia perfeita, entretanto, existem métodos eficazes para se dificultar o acesso a informações por estranhos. A fim de embaular o lítico teor de uma mensagem, o recurso mais utilizado é a criptografia. Há vários tipos de algoritmos e chaves. Porém o sucesso da operação depende do modelo adotado.

O algoritmo mais seguro e robusto é o assimétrico, pois ele independe de transportar a chave anexada à mensagem. O criptograma é gerado a partir da chave pública do destinatário, e só pode ser decifrado com a sua chave privada. Do contrário, jamais será desvelado.

Ficou explícito que o certificado da identidade eletrônica precisa ser confiável e seguro. Dado a isso, considerou-se o tipo SHA-1 – o qual utiliza chave RSA de 1024 bits.

Entretanto, notou-se que isoladamente a tecnologia é insuficiente para asseverar a solidez dos sistemas e assegurar a rigidez das instituições diante de ameaças. Sobretudo, é imprescindível a definição de uma política de segurança, envolvendo a cultura dos colaboradores.

Referente ao investimento predial, edificar uma sala adequada para hospedar os servidores despenderia altas cifras, contudo, necessitando de fortaleza e custo acessível, o ideal é hospedar os servidores em datacenters.

A respeito da base de dados, o banco de dados necessita de uma linguagem de fácil manipulação e entendimento, a qual parta da percepção do relacionamento das entidades do mundo real. Para tanto, adotou-se a linguagem SQL e o modelo ER, pois, além de atenderem os requisitos esperados, são populares entre os desenvolvedores.

A integridade das pessoas também deve ser salvaguardada, todavia o vazamento de informações pode causar um estrago catastrófico, com proporções incomensuráveis. Para tanto, o acesso a nova Infraestrutura de Chave Pública se sucederá por meio do protocolo SSL. Para coibir o uso indevido e não autorizado, a chave pública dos certificados será automaticamente bloqueada no CRL. Apenas o responsável poderá solicitar sua liberação.

Às fases de recrutamento e seleção, por serem extremamente relevantes e

fundamentais ao êxito do negócio, optou-se pela contratação de uma empresa especializada em processos de transição de recursos humanos e realização de concursos públicos.

Os novos colaboradores precisam ser treinados, afinal as instituições são tão grandes quanto a qualidade das pessoas que nelas trabalham.

Os licitantes deverão atentar-se à lei 8.666, de 21 de junho de 1993, pois ela é fundamental às licitações e deve ser seguida impreterivelmente. Caso seu conteúdo seja menosprezado, os infratores se sujeitarão a sanções.

Finalmente, ficou evidente que o projeto é inovador e desafiante. Todavia, depois de implantado e reajustado, servirá de arquétipo a outras cidades.

REFERÊNCIAS BIBLIOGRÁFICAS

SOUSA, Lindeberg Barros de. **Redes de computadores: Dados, Voz e Imagem.** São Paulo: Érica, 1999.

GRUBBS-WEST, Lorraine. **Como transformar sua equipe no seu maior patrimônio.** Rio de Janeiro: Sextante, 2007.

BOOG, Gustavo G; BOOG Magdalena T. **Manual de treinamento e desenvolvimento: gestão e estratégias/coordenação.** São Paulo: Pearson Prentice Hall, 2006.

OLIVEIRA, Aristeu de. **Manual de descrição de cargos e salários.** São Paulo: Atlas, 2007.

MACHADO, Felipe Nery Rodrigues. **Projeto e implementação de banco de dados.** São Paulo: Érica, 2008.

BROWN, Dan. **O símbolo perdido.** Tradução de Fernanda Abreu. Rio de Janeiro: Sextante, 2009.

UNIVERSIDADE PAULISTA. **Apostila de Modelagem de Sistemas de Informação, Gestão Estratégica de Recursos Humanos, Segurança da Informação e Planejamento Estratégico de Tecnologia da Informação.** São Paulo: [s.n.], 2010.

UNIVERSIDADE PAULISTA. **Apostila de Matemática Aplicada, Administração de Banco de Dados e Sistemas de Informação.** São Paulo: [s.n.], 2009.

HALLA, Victor. **Slide sobre segurança da informação.** São Paulo: Universidade Paulista, 2010.

WIKIPEDIA. **Enciclopédia livre.** [S.l.]: Wikimedia Foundation, Inc., 2010. Disponível em: <http://pt.wikipedia.org/wiki/Cifra_ma%C3%A7%C3%B3nica>. Acesso em: 22/05/2010.

PLANALTO. **Site oficial da presidência da república.** [S.l.]: Casa Civil, 2010. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L8666cons.htm>. Acesso em: 22/05/2010.

INTEL SEMICONDUTORES DO BRASIL LTDA. **Apostila de certificação digital.** São Paulo: [s.n.], 2010.