ROBSON CLAUDIO FERREIRA LIMA

DOCUMENTO ELETRÔNICO

POSSÍVEIS USOS NA PMPR

Monografia apresentada ao Departamento de Contabilidade do Setor de Ciências Sociais Aplicadas, da Universidade Federal do Paraná, como requisito parcial à obtenção do título de Especialista em Planejamento e Controle da Segurança Pública.

Orientador Metodológico:
MÁRCIO SÉRGIO B. S. de OLIVEIRA

Orientador de Conteúdo:
Maj. PM LOEMIR MATTOS DE SOUZA

CURITIBA

2005

Dedico este trabalho à minha esposa, Silmara, pela compreensão, incentivo e pelo especial apoio dedicado aos assuntos afetos à minha carreira profissional.

Ao meu filho, Guilherme, meu amigo apoiador e carinhoso, pelos inúmeros abraços dispensados a cada dia, às vezes no meio da noite, quando retornava das aulas e de outras atividades afetas ao curso.

Aos meus pais, João e Lenize, pelo zelo na minha formação pessoal e profissional, despendido ao longo de toda minha vida, em especial durante este curso quando eu, a Silmara e Guilherme precisamos muito do seu apoio.

AGRADECIMENTOS

Ao Cap DERLY MACIEL DE CAMARGO e ao Sr. STEPHANO KUBIÇA, que por suas experiências profissionais e disposição em ajudar, muito contribuíram com este trabalho.

Aos Mestres que com sabedoria souberam transmitir os seus conhecimentos.

Aos meus companheiros de turma desejo sucesso e realização profissional, na esperança de tornar duradouros os laços de amizade e companheirismo, onde quer que nos encontremos ao final do curso.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

AC Raiz	- Autoridade Certificadora Raiz
AC	- Autoridade Certificadora
AIIM	- Association for Information and Image Management International
API	- Application Programming Interface
AR	- Autoridades de Registro
ASCII	- American Standard Code Information Interchange
ASP	- Application Service Provider
BIT	- Binary digit do inglês, traduzindo-se como dígito binário
BMP	- Imagem bitmap ou mapa de bits
BPM	- Batalhão de Polícia Militar
CAD	- Computer Aided Design, do inglês, traduzindo-se como desenho assistido por computador
CALS	- Computer Aided Acquisition and Logistic Support
CAO	- Curso de Aperfeiçoamento de Oficiais
Cap.	- Capitão
CD-R	- Compact Disk Recordable
CD-ROM	- Compact Disk - Read Only Memory
Cel.	- Coronel
CELEPAR	- Companhia de Informática do Paraná
CENADEM	- Centro Nacional de Desenvolvimento do Gerenciamento da Informação
CG	- Comando-Geral
Ch.	- Chefe
Ch. EM	- Chefe do Estado-Maior
Cmt.	- Comandante
COLD	- Computer Output to Laser Disc
COLD/ERM	- Computer Output to Laser Disk/ Enterprise Report Management
COM	- Computer Output to Microfilm
Cosit	- Conselho Estadual de Sistemas de Informática e Telecomunicações
CPI	- Comissão Parlamentar de Inquérito
CR-RW	- Compact Disk - ReWritable
DETRAN	- Departamento de Trânsito
DETRANs	- Departamentos de Trânsito dos Estados
DI	- document imaging
DLL	- dynamic link library
DM	- Document Management
DMA	- Document Management Alliance
DMS	- Document Management System
DPI	- Dots Per Inch, do inglês, traduzindo-se como pontos por polegada
DTI	- Diretoria de Tecnologia da Informação
EBCDIC	- Extended binary coded decimal interchange code
ECM	- Enterprise Content Management, do inglês, traduzindo-se como Gerenciamento do Conteúdo Corporativo
EDI	- Electronic Data Interchange do inglês, traduzindo-se como intercâmbio de dados eletrônicos
EDMS	- Engineering Document Management Systems
EM	- Estado-Maior

ERM - Enterprise Report Management, do inglês, traduzindo-se como gerenciamento de relatório corporativo
ERP - Enterprise Resource Planning
GC - Gestão do Conhecimento
GED - Gerenciamento Eletrônico de Documentos
HEXA - Hexadecimal. Base numérica composta de dezesseis algarismos.
HTML - Hypertext Markup Language
IBGE - Instituto Brasileiro de Geografia e Estatística
ICP - Infra-estrutura de Chaves Pública
ICP-Brasil - Infra-estrutura de Chaves Pública Brasileiras
ICR - Intelligent Character Recognition
IDC - sem correspondência conhecida, empresa de consultoria com foco nos segmentos de Tecnologia da Informação e Telecomunicações
IDM - Integrated Document System, do inglês, traduzindo-se como sistema de documentos integrados ou sistema integrador de documentos
ISDN - Integrated Services Digital Network
ISO - International Organization for Standardization
ITI - Instituto Nacional de Tecnologia da Informação
ITSS - Information Technology Security Strategy
JDBC - Java Database Connectivity
KB - Kilobyte
KM - Knowledge Management, do inglês, traduzindo-se como gestão do conhecimento
LAN - Local Area Network do inglês, traduzindo-se como rede de área local
LASER - Light Amplification by Stimulated Emission of Radiation
Maj. - Major
MB - Megabyte
MP - Medida Provisória
OAB - Ordem dos Advogados do Brasil
OBM - Organização Bombeiro Militar
OCR - Optical Character Recognition do inglês, traduzindo-se como reconhecimento ótico de caracteres
PC - Polícia Civil
PDDE - Protocoladora Digital de Documentos Eletrônicos
PDF - Portable Document Format
PDM - Product Data Management
PM - Polícia Militar
PMPR - Polícia Militar do Paraná
ProUni - Programa Universidade Para Todos
QOPM - Quadro de Oficiais Policiais-Militares
RAID - Redundant array of inexpensive or independent discs
Redarf - Retificação de Documento de Arrecadação
SERPRO - Serviço Federal de Processamento de Dados
SESP - Secretaria de Estado da Segurança Pública
Siscomex - Sistema Integrado de Comércio Exterior
SisCOp - Sistema de Controle Operacional
TCP/IP - Transmission Control Protocol/Internet Protocol
TIFF - Tag Image File Format
TJ - Tribunal de Justiça
TJPR - Tribunal de Justiça do Estado do Paraná

TTP	- Trusted Third Party, do inglês, traduzindo-se como terceiro confiável
UFPR	- Universidade Federal do Paraná
UNCITRAL	- United Nations Commission on International Trade Law, do inglês, traduzindo-se como Comissão das Nações Unidas para Leis de Comércio Internacional
WAN	- Wide Area Network do inglês, traduzindo-se como rede de área ampla
WCM	- Web Content Management, do inglês, traduzindo-se como gerenciamento do conteúdo de informações
WORM	- Write once, read multiple
WWW	- World Wide Web
XML	- Extensible Markup Language

RESUMO

Este trabalho monográfico analisa a possibilidade de uso de documentos eletrônicos na Polícia Militar do Paraná, preocupando-se com aspectos de segurança, confiabilidade e legalidade. O uso de documentação eletrônica extrapola o entendimento corporativo, exigindo compreensão técnica e jurídica acerca do tema, vindo o presente trabalho a apresentar aspectos conceituais, doutrinários e legais sobre o assunto. Por tratar sobre segurança e documento eletrônico faz-se necessário o entendimento de conceitos sobre Gerenciamento Eletrônico de Documentos, Certificação Digital, Assinatura Eletrônica ou Digital, Tempestividade Digital, entre outros que, por extensão, merecem estudo e assimilação. Pensando em avanços tecnológicos, não pode a Polícia Militar do Paraná buscar soluções isoladas para o cumprimento constitucional de sua missão, basicamente a preservação da Ordem Pública. No conceito doutrinário de Defesa Social, vários órgãos buscam a proteção e o socorro públicos, através de prevenção, ou supressão de ilícitos penais ou infrações administrativas. A troca de informações entre esses órgãos é abordada neste trabalho procurando-se demonstrar a viabilidade para que isso ocorra em meio digital, observando-se os aspectos legais que regulamentam o assunto. Este trabalho não pretende apontar a solução de mercado para a gerência eletrônica de documentos na PMPR, traz uma visão teórica do assunto, procurando demonstrar para a Corporação a idéia de que um sistema estanque não permitirá o domínio da informação. Soluções combinadas com outros órgãos necessitam análise e estudos aprofundados para a viabilização da atividade fim da PMPR nos moldes que a sociedade paranaense espera. Estas soluções devem agilizar o trâmite de documentos, facilitar o acesso à informação, estabelecer ferramentas em níveis gerenciais e táticos que, uma vez alimentada pelo nível operacional, reverta esta informação sob a forma de planejamento eficiente, diminuindo esforços e otimizando meios para a execução da atividade finalística da PMPR. A gestão documental deve ir ao encontro às necessidades dos demais órgãos afetos ao ciclo de defesa social, possibilitando o intercâmbio de documentos alcançando a eficiência administrativa e, como conseqüência, resultando em atividades céleres, desburocratizadas e eficientes.

PALAVRAS-CHAVE: Polícia Militar do Paraná; Gerenciamento Eletrônico de Documentos; Confiança Documento Eletrônico; Possíveis Usos na PMPR.

1 INTRODUÇÃO

A proposição da Academia Policial Militar do Guatupê - APMG, apontada inicialmente como "DOCUMENTO ELETRÔNICO – POR QUE CONFIAR?" demonstra a necessidade de a Polícia Militar do Paraná - PMPR ter certeza de que se pode confiar na informação digital. Esta dúvida norteia toda a instituição, o distanciamento tecnológico da atividade policial impediu por muito tempo o acesso à informatização, o que não dizer então, de um assunto tão atual que se refere à informatização do trâmite de documentos.

A confiabilidade em meio digital é maior do que se você entregar seu cartão de crédito nas mãos de um frentista ou de um garçom, que o leva não se sabe onde para fazer, além de autorizá-lo na administradora, sabe–se lá o que.

O acesso a documentos e informações importantes pode ser controlado:

- Por recursos da rede: direitos de acesso individuais a partes da rede, servidores e diretórios/pastas compartilhadas, Firewall, etc.;
- Por recursos do programa: criptografia, sistemas de arquivos próprios, controle de acesso, controle de funções ou recursos do aplicativo;
- Por combinação das duas situações citadas anteriormente, o que é o mais comum.

Com a certeza de que existe segurança no meio digital, baseada na experiência profissional do autor e nas referências indicadas e detalhadas no desenvolvimento das pesquisas, adota-se o seguinte tema para este trabalho: DOCUMENTO ELETRÔNICO – POSSÍVEIS USOS NA PMPR. Pretende-se com este enfoque demonstrar não somente a segurança, mas apresentar as possibilidades de utilização da informação em meio eletrônico como alternativa viável.

Propositadamente, o texto apresenta uma visão empresarial acerca do tema, a maior parte das vezes citada a partir de uma referência renomada, em que se insere a visão do órgão ou do gestor de segurança pública. Desse modo procura-se colocar a administração pública, em especial a Polícia Militar, como uma empresa em busca da solução ideal para a ferramenta de Gerência Eletrônica de Documentos e todas as tecnologias decorrentes.

O trabalho encontra-se dividido em seis capítulos. A partir desta Introdução, vê-se a seguinte estrutura:

- **Capítulo 2** – Situação Atual, na qual é apresentada a visão empresarial que leva à decisão pelo investimento em tratamento eletrônico dos documentos; este capítulo avança demonstrando dados atuais sobre a utilização da tecnologia no Brasil;
- **Capítulo 3** – Gerenciamento de Documentos, Conceitos e Definições, como objetivo de esclarecer os pontos principais envolvidos no tratamento de documentos de forma eletrônica, apresentam-se as idéias básicas que são imprescindíveis ao seu entendimento;
- **Capítulo 4** – Meios de Armazenamento e Ferramentas para Gerenciamento, procura-se expor o ferramental disponível na atualidade, demonstrando maneiras práticas e para que se destina cada equipamento ou produto;
- **Capítulo 5** – Segurança e Aplicabilidade, além de reforçar conceitos de segurança e confiabilidade, demonstra a realidade atual da tecnologia nos órgãos afetos à Polícia Militar do Paraná;
- **Capítulo 6** – Conclusões e Sugestões, apresenta algumas propostas na expectativa de melhorar a operacionalização e/ou implantação de solução para o tratamento eletrônico de informações dentro da PMPR.

Pretende-se demonstrar que segurança e confiabilidade são inquestionáveis quando se digitaliza documentos, avança-se no assunto e demonstra-se sua aplicabilidade nos dias de hoje, contextualizando com alguns órgãos envolvidos no ciclo de defesa social dentro do Estado do Paraná.

O Centro Nacional de Desenvolvimento do Gerenciamento da Informação – CENADEM apresenta em sua página virtual (www.cenadem.com.br), as seguintes informações, às quais intitulou "Dados Interessantes":

> A humanidade gerou a mesma quantidade de informação nos últimos 50 anos que nos 5 mil anteriores. Esse número duplicará nos próximos 26 meses. Em 2010, a informação duplicará a cada 11 horas. Cada vez mais estamos gerando mais documentos em papel. Segundo a AIIM International – Association for Information and Image Management International, EUA, a maior associação do mundo sobre gerenciamento da documentação, 95% das informações dos Estados Unidos estavam em papel em 1990. Este ano, cerca de 92% das informações ainda estarão em papel.
> Essa avalanche de papel gera a cada dia maiores problemas:

- Um executivo gasta em média quatro semanas por ano procurando documentos.
- Faz-se, em média, 19 cópias de cada documento. Gasta-se US$ 250,00 para recriar cada documento perdido.
- A imagem de um documento digitalizada a 200 dpi (pontos por polegada) e comprimida a 10:1 requer 50KB de armazenamento. Um gigabyte acomoda 20 mil imagens.
- Quinhentas páginas de texto requerem 1 MB de armazenamento.
- Um arquivo de quatro gavetas, com 2.500 folhas de papel por gaveta, comporta, em média, 10 mil imagens de documento.
- Um CD-R mede 120mm de diâmetro e pode armazenar até 650 MB de informação. Isso corresponde a 13 mil páginas de documentos.
- Estudos revelam que os escritórios criam cerca de 1 bilhão de páginas de papel por dia. Segundo uma pesquisa do IDC, EUA, esse total é constituído de 600 milhões de páginas de relatórios de computador, 234 milhões de fotocópias e 24 milhões de documentos diversos. Isso somente nos Estados Unidos.

Apesar de toda informatização presente nos ambientes corporativos, o papel, ainda, é o maior problema operacional na maioria das empresas, órgãos governamentais e instituições. Correspondências, cheques, faturas, ordens de compra, desenhos de engenharia e formulários de todos os tipos são, em sua grande maioria, processados manualmente. No meio policial, era comum a feitura de Inquéritos Policiais ou o registro de ocorrências em máquinas de datilografia até meados da década de 90. Atualmente, por mais que exista informatização, os procedimentos administrativos são, na grande maioria, apenas digitados no computador, que passou a ser usado em substituição à máquina de escrever. Os sistemas dedicados para o trabalho policial aparecem no atendimento e despacho de ocorrências, permanecendo a área administrativa carente de sistemas dedicados. Surge, então, a necessidade de desenvolver métodos para o aumento da produtividade de funcionários de escritório, tais como engenheiros, bancários, secretárias, advogados e gerentes, e, principalmente, de melhorar a qualidade de sua produção. Na atividade policial, esses novos métodos permitem o emprego do profissional de segurança pública no exercício finalístico de suas atribuições, não desperdiçando o emprego de profissionais treinados para o policiamento no dia-a-dia do serviço burocrático.

As mudanças nas organizações, resultam de uma reestruturação econômico-financeira internacional e nacional, além de sucessivas adaptações do setor produtivo, i.e., inflação, estabilidade, etc. Essas estruturações aparecem para se adequar a uma sociedade típica deste tempo, que é a sociedade tecnológica, caracterizada pela automação progressiva do aparato material e intelectual, que

regula a produção, a distribuição e o consumo, e que se estende tanto às esferas públicas de existência como às particulares, tanto ao domínio cultural como ao econômico e político, MARCUSE (1988).

A revolução tecnológica fez com que as empresas precisassem de novas formas de integração e trabalho, levando-as aos sistemas de automação de escritórios visando a apoiar a execução dos processos e atividades, aumentando a disponibilidade de tempo de gerentes e outros profissionais, a fim de que com este tempo adicional disponível, pudessem ter condições de aumentar a eficiência. Com isso, torna-se possível agilizar os processos críticos da organização de forma a otimizar o binômio produtividade-qualidade.

Em pleno Século XXI, a Polícia Militar do Paraná conhece a necessidade de informatização, isto se vê pelas recentes aquisições de computadores em volume que alcança quase todos os setores. No entanto, a simples aquisição de ferramentas (computadores) não suprirá a necessidade de soluções corporativas que racionalizem a utilização da informática, urge, e cada vez mais, a necessidade de a Polícia Militar possuir sistemas integrados que otimizem o serviço burocrático.

Para a implementação de um processo administrativo automatizado, é preciso haver uma mudança brutal na rotina da PMPR, com novos procedimentos administrativos para auxiliar na consulta a documentos, que anteriormente pareciam inacessíveis. Este universo de mudanças não pode excluir a atividade operacional. O acesso imediato a informações permite agilização da atividade, liberando o profissional para novas tarefas ou ocorrências que, atualmente acumulam-se cada vez mais, deteriorando a qualidade do serviço.

A velocidade com que as informações chegam, cada vez mais instantâneas, torna obrigatória uma adequada absorção das mesmas na capacidade de agir e, também, na estrutura de trabalho. A modernização, a agilização e o aumento de qualidade contínuos são requisitos básicos de qualquer empresa, quiçá o serviço policial diante do clamor social em prol da segurança pública.

O Gerenciamento de documentos vem, cada vez mais, deixando de ser encarado como ferramenta para nichos específicos de mercado, e passando a ser visto como componente indispensável para a concepção e desenvolvimento de modernos sistemas de informação, D'ALLEYRAND (1995). Conforme FRUSCIONE (1996), um dos mais fortes movimentos atuais da indústria de sistemas de

informação é, sem dúvida, o acelerado crescimento da utilização de sistemas de gerência de documentos.

Para a AIIM, um sistema de gerência de documentos é um sistema de informação capaz de armazenar, recuperar e manter a integridade de documentos, entre outras funcionalidades. Diversas razões explicam a atual efervescência do mercado de gerência de documentos. A principal delas é a percepção da vital importância que os documentos possuem como repositório do conhecimento das organizações, uma vez que a maior parte de suas informações vitais estão contidas em documentos não-estruturados, SADIQ (1997). Logo, a facilidade em armazenar, recuperar e conservar a integridade deste verdadeiro patrimônio intelectual torna-se um imperativo para manter as organizações produtivas e competitivas nos dias atuais. Acrescente-se a isso as novas exigências, em termos de volume de documentos e necessidades de controle, ditadas por normas técnicas como as normas ISO 9000, delineando-se um panorama altamente favorável ao crescimento da utilização desses sistemas.

Segundo GATES (1999), as empresas que terão sucesso na década atual serão aquelas que utilizarem as ferramentas digitais para reinventar sua maneira de trabalhar. Essas empresas tomarão decisões com rapidez, atuarão com eficácia e vão atingir direta e positivamente seus clientes, ou no caso da PM os anseios da comunidade. Acrescentou, ainda, que se a empresa converter cada documento de papel em um arquivo digital, ela se tornará mais competitiva. Essa visão empresarial também vale para instituições públicas, a Polícia Militar deve direcionar o foco de suas ações para o atendimento do cliente, somos um grande prestador de serviços e a sociedade quando liga para o n° 190 precisa do produto "segurança pública", com toda a sua complexidade.

A visão empreendedora e os ensinamentos de GATES, acima apontados, nos permitem avaliar que com o passar dos anos é crescente o uso dos documentos eletrônicos no cotidiano, de uma forma geral, mostrando-se presentes tanto no uso doméstico quanto na área comercial, passando pela indústria, prestação de serviços e alcançando o serviço público em geral.

Torna-se comum às organizações substituir o papel pelo armazenamento eletrônico de documentos em redes locais, ou muitas vezes sem qualquer limitação geográfica, permitindo cada vez mais agilidade na obtenção da informação.

GANDINI (2001) defende que os documentos tradicionais, apostos em papel, não mais correspondem às necessidades de rapidez na circulação das informações. São evidentes as suas limitações, no que se refere à simples conservação, transmissibilidade ou segurança.

Ainda GANDINI (2001) lembra ensinamentos do maior pensador contemporâneo do mundo dos negócios, PETER DRUCKER, asseverando que a Revolução da Informação, que vem ocorrendo atualmente, encontra-se no mesmo ponto em que a Revolução Industrial estava no início da década de 1820, aproximadamente 40 anos após o aperfeiçoamento, por JAMES WATT, da máquina a vapor. Em breve conclusão, ainda DRUCKER discorre que: "A máquina a vapor era para a Revolução Industrial aquilo que o computador vem sendo para a Revolução da Informação".

2 SITUAÇÃO ATUAL

2.1 FATORES QUE LEVAM À IMPLANTAÇÃO DE UM GED

A Sexta Pesquisa de Mercado do CENADEM projetava o mercado de GED no Brasil para o período 2000-2001 e revelava que o crescimento seria de 98% para o biênio 2000/2001, ou seja, 49% ao ano. Entre 388 empresas e organismos do governo pesquisados, 76,5% pretendiam implantar algum tipo de sistema de GED. Quase todas as empresas demonstravam a intenção de transformar seus documentos, processos e até documentos técnicos em mídias eletrônicas e discos ópticos, devido ao fato de que têm maior pressa em localizar os documentos de forma rápida e precisa. Quase todas as grandes organizações brasileiras já possuíam um sistema de GED com expansão para outras aplicações.

Na mesma pesquisa, foram diagnosticadas as 16 principais razões pelas quais os sistemas de GED estavam sendo implantados no Brasil:

- Absoluto controle nos processos de negócios;
- Alta velocidade e precisão na localização de documentos;
- Criação de facilidades para o trabalhador do conhecimento na empresa virtual;
- Disponibilização instantânea de documentos sem limites físicos;
- Eliminação de fraudes. Principalmente em agências governamentais;
- Gerenciamento automatizado de processos, minimizando recursos humanos e aumentando a produtividade;
- Grande melhoria no processo de tomada de decisões;
- Grande redução de espaço físico;
- Ilimitadas possibilidades para indexação de documentos;
- Impossibilidade de extravio ou falsificação de documentos;
- Integração com outros sistemas e tecnologias;
- Maior agilidade nas transações entre empresas;
- Maior velocidade na implementação de mudanças nos processos. Exigência da alta competitividade;

- Melhor atendimento ao cliente. O GED proporciona respostas precisas e instantâneas;
- Obtenção de vantagem competitiva sustentável; e
- Possibilidade da empresa virtual sem limites físicos.

A utilização de um sistema de Gerenciamento eletrônico de documentos pode levar as empresas a um diferencial competitivo, basicamente de três maneiras:

- Através do aumento da qualidade e da produtividade do trabalho: Com o GED, cria-se uma base corporativa de informações de rápido e fácil acesso. Novos documentos podem ser gerados a partir de outros, bastando salvá-lo com outro nome e alterá-lo para as novas necessidades. Assim, a informação não fica somente restrita a poucos, mas passa a ser um ativo corporativo, acessado e compartilhado por todos;
- Através da redução de custos proporcionada pelo aumento da produtividade. Com a facilidade de se consultar e acessar os documentos através do seu perfil, diminui-se o tempo de procura, de recuperação e de elaboração. Com isso, os serviços acabam absorvendo menos tempo de trabalho e ficam potencialmente mais baratos.; e
- Através da obtenção da certificação ISO 9000: As ferramentas de GED, por controlarem de forma sistemática o acervo de documentos, sua localização, utilização, versões e principalmente a segurança dos documentos, têm sido muito utilizadas para dar suporte à necessidade de registros demandada na certificação ISO 9000. Quando os auditores da ISO vão a uma empresa que usa o GED, o processo de auditoria da certificação fica simplificado, uma vez que uma ferramenta automatizada controla todo o processo de geração, acesso e manutenção dos documentos.

Muitas empresas já perceberam que o conhecimento é o seu maior patrimônio, mas ainda não o utilizam como deveriam. Muitas vezes, o conhecimento fica restrito ao funcionário que o adquiriu e não o compartilhou na empresa. O gerenciamento desse capital intelectual passou a ser vital no mundo globalizado e competitivo em que vivemos. O *Knowledge Management*, ou simplesmente KM, é o

tão procurado "Santo Graal" pelas empresas. Ele está prometendo sucesso e vantagem competitiva sustentável.

Esse assunto vem sendo acompanhado por administradores e economistas. Foi abordado no último livro do maior guru da administração moderna, Peter Druker. O KM é hoje o que todas as empresas precisam para se manter no mercado. Este gerenciamento e compartilhamento das informações tem sido feito através de ferramentas de Gerenciamento Eletrônico de Documentos, em que as pessoas registram seus conhecimentos em documentos e disponibilizam eletronicamente para os demais membros da organização.

2.2 SETORES QUE UTILIZAM GED

O CENADEM apresenta um banco de exemplos para demonstrar como o GED pode ser utilizado nos mais variados segmentos. Destacam-se nesse banco os seguintes segmentos:

- Acervos Históricos
- Administradora de Consórcio
- Advocacia
- Aeronaves
- Arquivologia
- Assembléia legislativa
- Agências Nacionais
- Bancos
- Biblioteca
- Bolsa de Valores
- Cartórios
- Centros de Pesquisa
- Clínicas
- Colégios
- Comunicação
- Câmara
- Construção
- Contabilidade
- Correios
- Cultura
- Documentação Histórica
- Energia
- Ensino
- Engenharia
- Empresas Aéreas
- Financeira
- Fornecedores de GED
- Fundações
- Governo Estadual
- Governo Federal
- Governo Municipal
- Hidroelétrica

- Hospitais
- IBGE
- Imobiliárias
- Imprensa Oficial
- Indústrias
- Institutos
- Informática
- Juntas Comerciais
- Laboratórios
- Mineração
- Ministérios
- Petroquímica
- Polícias
- Prefeituras
- Previdência
- Publicidade
- Receita Federal
- Recursos Hídricos
- Recursos Humanos
- Saúde
- Secretaria de Fazenda
- Secretaria de Segurança
- Seguradoras
- Serpro
- Siderúrgicas
- Telecomunicações
- Tribunal Federal
- Universidade
- Usinas

2.3 SITUAÇAO ATUAL NO BRASIL

Segundo o CENADEM, o Gerenciamento Eletrônico de Documentos está em crescimento no Brasil, que tem o maior mercado em toda a América Latina. Acrescenta, ainda, que nenhuma outra tecnologia da informação está crescendo tão rapidamente no Brasil. Isto se deve à redução de custos, aumento de produtividade e melhoria no atendimento ao cliente.

Pesquisa realizada pelo CENADEM em 2003 apresentou os seguintes indicadores:

- As áreas dos governos federal, estadual e municipal são as que demonstram mais interesse em GED e tecnologias afins: 18,4% dos respondentes.
- As empresas que pretendem ter algum tipo de sistema de GED em 2004/2005 são 40,9% do total. Desses, 67,1% pretendem que a implantação seja já em 2004.

- Perguntou-se quais os planos da organização para o tratamento do e-mail como documento, controle de temporalidade, disponibilização corporativa etc. Apenas 24,6% já têm algum sistema em uso, enquanto a maioria, 41,6%, ainda está pensando no assunto. 11,1% não estão preocupadas.
- Essa 10ª Pesquisa mapeou também a intenção das empresas em ter *eBusiness*, GED, *Workflow* e COLD na web. O resultado apontou que 23,4% da empresas pretendem ter e 29% já têm tais sistemas em uso. Apenas 0,5% pretendem utilizar o ASP - *Application Service Provider*.

Quase todas as empresas querem transformar seus documentos, processos e até documentos técnicos em mídias eletrônicas e discos ópticos, devido ao fato de que têm maior pressa em localizar os documentos de forma rápida e precisa. Quase todas as grandes organizações brasileiras já possuem um sistema de GED com expansão para outras aplicações.

3 GERENCIAMENTO DE DOCUMENTOS, CONCEITOS E DEFINIÇÕES

3.1 DOCUMENTO E OUTROS TERMOS

3.1.1 Documento

AURÉLIO BUARQUE DE HOLANDA FERREIRA (1996) conceitua a palavra documento como: "1. Qualquer base de conhecimento, fixada materialmente e disposta de maneira que se possa utilizar para consulta, estudo, prova, etc; 2. Escritura destinada a comprovar um fato; declaração escrita, revestida de forma padronizada, sobre fato(s) ou acontecimento(s) de natureza jurídica".

No uso policial deve ser considerado o entendimento jurídico sobre o assunto, fundamental se faz uma busca doutrinária do termo e sua aplicação prática. A partir da pesquisa jurídica elaborada por GANDINI (2001), pode-se analisar diversas interpretações acerca do documento e seu uso como prova:

> Os autores, ao conceituar documento, dividem-se em duas correntes. A primeira se apega à matéria e ao meio de fixação física do mesmo, enquanto que a segunda procura destacar o seu conteúdo. Nesta segunda posição, podemos destacar a presença dos juristas, visto que estes visualizam o documento como sendo o instrumento cuja finalidade é a prova de algum fato.
> JOSÉ FREDERICO MARQUES, ao conceituar documento, discorre: "A prova histórica real consistente na representação física de um fato". Portanto, seria ele a prova documental, de representação exterior e concreta do factum probandum em alguma coisa.
> GIUSEPPE CHIOVENDA entende que "documento, em sentido amplo, é toda representação material destinada a reproduzir determinada manifestação do pensamento, como uma voz fixada duradouramente (vox mortua)".
> MOACYR AMARAL SANTOS define documento como sendo "a coisa representativa de um fato e destinada a fixá-lo de modo permanente e idôneo, reproduzindo-o em juízo".
> ARRUDA ALVIM define documento como sendo uma prova real, de modo que todo documento é uma coisa. Afirma que este não se destina somente a fixar um pensamento, como é mais comumente utilizado, mas pode também fixar um fato. A fixação de um fato é mais ampla que a fixação de um pensamento.
> HUMBERTO THEODORO JUNIOR reconhece documento em seu sentido amplo e estrito. Em um aspecto geral, seria "não apenas os escritos, mas toda e qualquer coisa que transmita diretamente um registro físico a respeito de algum fato, como os desenhos, as fotografias, as gravações sonoras, filmes cinematográficos etc". Já em sentido estrito, assevera que documento abrangeria somente os escritos, pois estes

> teriam a finalidade de registrar, através da palavra escrita, em papel ou outro material adequado, a existência de algum fato.
> AMAURI MASCARO DO NASCIMENTO define documento como: "Todo objeto, produto de um ato humano, que representa a outro fato ou a um objeto, uma pessoa ou uma cena natural ou humana".
> A idéia acentuada que existe é que o documento se consubstancia numa coisa, fixada materialmente; por essa razão, muitos entendem que o elemento-conteúdo é inseparável de seu suporte físico.

Procurando definir o termo "documento", trazendo uma visão à atualidade, ainda GANDINI (2001), afirma:

> Diante da evolução da sociedade devemos tender cada vez mais para a flexibilização dos conceitos. Por isso, podemos entender como documento qualquer meio capaz de representar um significado compreensível, não sendo necessário que seja escrito a mão ou por quaisquer outros meios mecânicos. A título exemplificativo, podemos citar o conceito de documento, do ilustre autor Aurélio, já exposto anteriormente, onde preceitua que o mesmo consiste em uma escritura revestida de forma padronizada. No entanto, entendemos que tal conceito encontra-se ultrapassado, uma vez que seu suporte não é o mais relevante, que o que interessa, realmente, é seu conteúdo. O documento tradicional, aposto em papel, não mais se adequa à necessidade atual de dar agilidade à circulação de informações. São evidentes as suas limitações, tanto em relação à conservação, como à transmissibilidade e segurança.

Há que se ter em mente que o conceito de documento necessita desvincular-se do aspecto de materialidade, motivo pelo qual as construções doutrinárias até hoje desenvolvidas são insuficientes para açambarcá-lo em toda sua plenitude.

No âmbito do comércio eletrônico, a lei modelo da UNCITRAL (Comissão das Nações Unidas para Leis de Comércio Internacional), que busca uniformização internacional da legislação sobre o tema, estabelece em seu art. 5º que "não se negarão efeitos jurídicos, validade ou eficácia à informação apenas porque esteja na forma de mensagem eletrônica".

Pode-se encontrar, com auxílio do especialista AUGUSTO TAVARES ROSA MARCACINI, membro da Comissão Especial de Informática Jurídica da OAB-SP e da Comissão de Informática da Faculdade de Direito da USP, um conceito mais evoluído de documento:

> A característica de um documento é a possibilidade de ser futuramente observado; o documento narra, para o futuro, um fato ou pensamento presente. Daí ser também definido como prova histórica. Diversamente, representações cênicas ou narrativas orais, feitas ao vivo, representam um fato no momento em que são realizadas, mas não se perpetuam, não registram o fato para o futuro. Se esta é a característica marcante do documento, é lícito dizer que, na medida em que a técnica evolui

> permitindo registro permanente dos fatos sem fixá-los de modo inseparável de alguma coisa corpórea, tal registro também pode ser considerado documento. A tradicional definição de documento enquanto coisa é justificada pela impossibilidade, até então, de registrar fatos de outro modo, que não apegado de modo inseparável a algo tangível.

Diante desse entendimento, sendo o documento íntegro e confiável para a representação de um fato, não importa sua forma de apresentação, não persistindo a idéia de vinculação de seu conteúdo com seu elemento continente. GANDINI (2002).

3.1.2 Gerenciamento Eletrônico de Documentos - GED

Considera-se o termo Gerenciamento Eletrônico de Documentos a parte da disciplina mais ampla de sistemas de informação. Pode-se classificar a informação em duas formas: informação codificada e informação documental. O uso do termo informação documental, distinta de documento, é significante porque sugere que existe algo intrínseco acerca da natureza desse tipo de informação, que é independente do meio em papel ou seu equivalente eletrônico.

Segundo KOCK (1998), GED é a somatória de todas as tecnologias e produtos que visam gerenciar informações de forma eletrônica. Quando se fala em informações, precisa-se definir as formas como se apresentam sejam elas na forma de voz, texto ou imagens.

O GED visa gerenciar o fluxo das informações desde sua captura até o seu arquivamento.

As informações podem, originalmente, estar registradas em mídias analógicas ou digitais. Podem ser criadas em papel, revisadas no papel, processadas a partir de papel e arquivadas em papel dentre outras formas, como o microfilme.

O Gerenciamento Eletrônico de Documentos – GED é ao mesmo tempo : um método, um sistema e uma tecnologia, para a conversão e processamento de documentos como informação eletrônica digital. Essa ferramenta surgiu a partir da necessidade de as empresas gerenciarem a informação que se encontrava desestruturada, visando facilitar o acesso ao conhecimento explícito da corporação.

O GED promove a automação do ciclo de vida dos documentos, provendo um repositório comum, o qual possibilita capturar, armazenar e indexar documentos de qualquer formato/suporte físico (texto, imagens, páginas html, documentos escaneados, formatos multimídia). Deve também assegurar a integridade e reutilização do documento, integração e escalabilidade.

GED pode ser definido como a "tecnologia que facilita o armazenamento, localização e recuperação de informações estruturadas ou não, em formato digital, durante todo o seu ciclo de vida". De forma geral, essas soluções são compostas pelos módulos de Document Imaging, COLD/ERM e Document Management:

- **Document Imaging** (DI) – Gerenciamento de Imagens: esse módulo é responsável pela transformação do documento papel em uma imagem digital, permitindo a sua manipulação nesse ambiente. Esse processo abrange três etapas: a digitalização do documento por meio de um scanner, seu armazenamento (gravação em CD-ROM, DVD, Disco Óptico ou Disk Array) e o gerenciamento (consultas, pesquisas etc.) das informações em meio digital.
- **COLD/Enterprise Report Management** - Gerenciamento de Relatórios Corporativos: COLD (Computer Output to Laser Disk) substitui a tecnologia COM (Computer Output to Microfilm) como forma de armazenar grandes volumes de dados provenientes de sistemas computadorizados (arquivos spool). Em vez de serem impressos, os relatórios são gravados em mídia magnética/óptica e disponibilizados aos usuários, para consulta, no vídeo, por meio de um visualizador próprio.
- **Document Management** (DM) – Gerenciamento de Documentos: tem por objetivo o controle e armazenamento de documentos produzidos por programas de computador, tais como: Word, Excel, PowerPoint etc. Uma funcionalidade interessante de módulos desse tipo é a utilização de serviços de biblioteca que possibilitam o controle das diversas versões de um documento.

Com o crescimento da Internet, surgiu o termo Web Content Management (WCM), que trata do gerenciamento do conteúdo de informações e o que o diferencia do DM, pelo simples fato da publicação desse conteúdo na Web.

3.1.3 Enterprise Content Manager – ECM

Segundo o CENADEM, os fornecedores de GED são, em grande parte, representantes de soluções norte-americanas ou da Europa. Portanto, quando os conceitos chegam ao Brasil, sofrem adequações para nossa realidade.

Atualmente, muito se fala em ECM – Enterprise Content Management. A definição da AIIM - Association for Information and Image Management para ECM é "as tecnologias, ferramentas e métodos usados para captar, gerenciar, armazenar, preservar e distribuir conteúdo pela empresa. No nível mais elementar, as ferramentas e estratégias de ECM permitem o gerenciamento de informação não-estruturada de uma organização, enquanto aquela informação existir". Qualquer semelhança com o que se entende por GED não é mera coincidência.

A questão toda está centrada apenas em nomenclatura. Quando o GED chegou ao Brasil, seu equivalente nos Estados Unidos era o EDMS – Electronic Document Magement System. Hoje, naquele país fala-se também em IDM – Integrated Document System, que para nós corresponde ao Document Management, um dos componentes do GED. Para especialistas atuando no Brasil, o ECM é, numa maneira mais simplificada de se explicar, o GED com a sofisticação que a web permite mas, em essência, é a mesma coisa. Os recursos da comunicação pela Internet, incorporados às ferramentas, tecnologias e métodos do GED resultam numa amplitude das capacidades das funcionalidades inerentes ao GED. Existem diferentes termos para ECM: DI, DM. As diferenças são fruto de como os fornecedores pensam em confronto com o que os usuários pensam. "A indústria de ECM deve pensar em reduzir custos e conduzir negócios usando colaboração. Essas tecnologias oferecem ferramentas para cumprir normativas e objetivos, reduzir custos e atender conformidades", afirma JOHN MANCINI, presidente da AIIM International.

3.1.4 Workflow

Uma vez organizada a informação na empresa, precisa-se conhecer o fluxo do processo do negócio, em outras palavras, o seu Workflow. Este é um conceito antigo que sempre existiu nas organizações. A novidade está na automação do

controle do fluxo dos processos e o Workflow funciona como elemento aglutinador das ações pontuais de cada uma das etapas dos processos.

O foco principal reside em saber quem fez que parte do trabalho, em que ordem e sob quais condições (os 3Rs do Workflow – Routes /Rotas, Roles/Papéis e Rules/ Regras). Para sua utilização é primordial que o trâmite de documentos, com as etapas e atividades envolvidas, esteja completamente sistematizado.

Podemos conceituar Workflow como o elemento responsável por gerenciar o fluxo dos processos da empresa permitindo um controle automático de tarefas, eventos e prazos, com o intuito de atingir os objetivos do negócio. As diversas soluções de Workflow podem ser grupadas nas seguintes classes:

- **Produção**: processos de missão crítica de relevante valor agregado, com alto grau de estruturação nas regras de roteamento, controle e acompanhamento e com volume significativo de ocorrências repetitivas.
- **Colaborativo**: coordenação das atividades de um grupo de pessoas, trabalhando juntas para a execução de um projeto, porém com regras e fluxos de baixo grau de estruturação.
- **Administrativo**: processos administrativos com baixo valor agregado ao negócio e orientados para o roteamento de formulários e de documentos com baixo grau de estruturação.
- **Ad-hoc**: processos eventuais com regras e fluxos com baixo grau de estruturação.

Enquanto em um sistema tradicional o trâmite do processo necessita de intervenção humana, ou seja, é passivo, em um sistema de Workflow isso é realizado de forma automática. Para tal, os sistemas de Workflow, independente de sua classe, abrangem diversas funções, dentre as quais podemos destacar:

- **Seqüenciamento**: controle da seqüência de execução das diversas atividades do processo;
- **Controle de Tempo**: estabelecimento de limites de tempo para a realização das tarefas;
- **Roteamento**: caminhos alternativos de execução das tarefas (seqüencial, paralelo e condicional);

- **Atribuição de Papéis**: capacidade de rotear uma ação para um papel/perfil de usuário quando uma condição for satisfeita ou um prazo se esgotar;
- **Monitoramento**: facilidade de acompanhar a situação das tarefas e o trâmite das ações tomadas no processo.

3.2 A SOCIEDADE DO CONHECIMENTO

Gestão do conhecimento não é mais uma moda que surge para substituir outras práticas administrativas ou para resolver todos os problemas organizacionais. Pelo contrário, a GC está baseada em recursos com os quais a organização, eventualmente já conta, como gestão de sistemas de informação, de mudança organizacional ou de recursos humanos.

A Gestão do conhecimento não substitui outras práticas administrativas, ela convive bem com a atual estratégia de negócios da empresa. O diferencial é que ela pode ajudar a organização a fazer, de uma forma melhor, uma enorme gama de atividades que já desenvolve.

Conforme KOTLER (2000), para permanecer competitivo no ambiente cada vez mais dinâmico e complexo da nova economia, toda empresa deveria trabalhar duro para obsoletar sua própria linha de produto antes que os competidores o façam. A chave para isso é a inovação contínua.

Segundo CARL FRAPPAOLO, citado por ANDRADE (2002), gestão do conhecimento é "um conjunto de ferramentas para a automação dos relacionamentos entre informações, usuários e processos. O conhecimento é a informação residente na mente das pessoas, utilizada para a tomada de decisões em contextos desconhecidos". Fica evidente que a Gestão do Conhecimento visa, conectar detentores do conhecimento e usuários deste através do uso de tecnologias. Já JAY BROMBEREK, da Doculabs, define KM como "o processo de obter, gerenciar e compartilhar a experiência e especialização dos funcionários utilizando-se de tecnologias para alavancar isto de forma corporativa".

Quando se fala em conhecimento, este pode ser classificado em dois opostos:

- **Explícito** - quando o conhecimento é facilmente mapeado e passível de ser aprendido por terceiros.
- **Tácito** - refere-se ao conhecimento pessoal, empírico, calcado em experiências pessoais com insumos subjetivos.

Assim, pode-se concluir que o maior desafio para as organizações é a captação do conhecimento tácito já que aí reside o conhecimento com maior valor estratégico para estas.

Gestão do conhecimento envolve uma revisão dos processos, políticas e tecnologias da empresa a partir de uma melhor compreensão do seu papel intelectual e dos fluxos mais importantes relacionados à criação, identificação, organização, disseminação e uso de conhecimento estratégico para a organização.

Entende-se, ainda, que a GC é um processo corporativo focado na estratégia empresarial e que envolve:

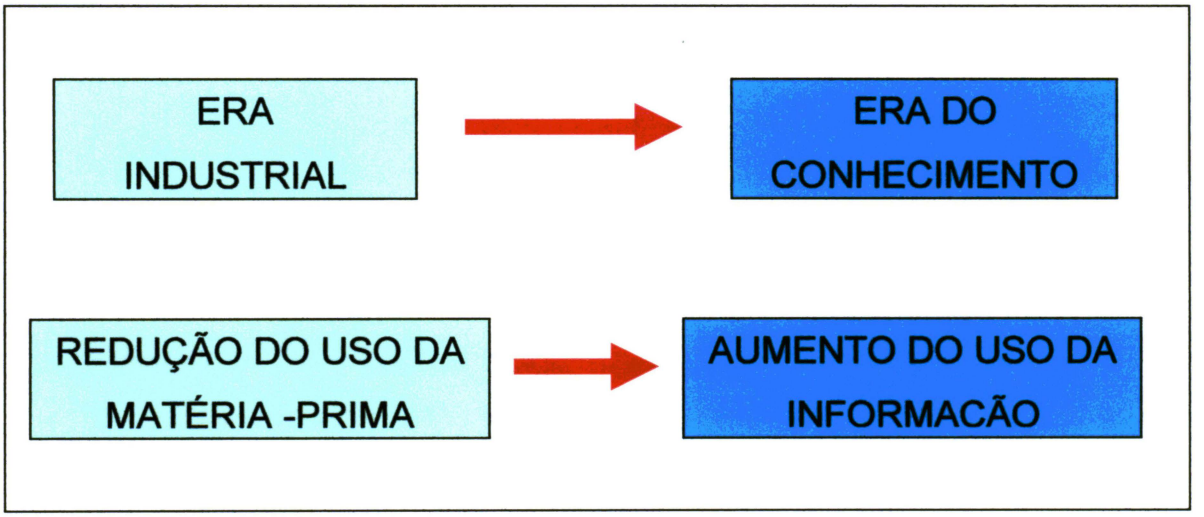
- **Gestão de Competências** - conhecimento, habilidade, experiência, julgamento de valor e redes sociais;
- **Gestão do Capital Intelectual**
  - *Capital humano* (pessoas e seus conhecimentos, intelecto e experiência), capacidade de suprir as exigências do mercado;
  - *Capital estrutural* (patentes, processos, manuais, marcas, conceitos, sistemas administrativos, banco de dados, tecnologias, estruturas); e
  - *Capital de clientes* (relacionamento com as pessoas que se atende ou faz negócios).
- **Aprendizagem Organizacional** – capacidade de criar, adquirir e transferir conhecimentos, modificar comportamentos, detectar e corrigir erros;
- **Inteligência Competitiva** – processo contínuo e formal que avalia o mercado, seus concorrentes atuais e potenciais, visando auxiliar na criação de vantagens competitivas; e
- **Educação Corporativa** - modelo baseado em competências, aprendizagem continuada e flexível, novas práticas (ensino a distância, etc.).

Para acompanhar este novo processo de desenvolvimento do mundo onde os serviços e a criatividade dão o tom, o capital físico, que era a variável-chave do crescimento econômico, perde lugar hoje para o capital humano, representado pelo conjunto de capacitações que as pessoas adquirem através da educação, de programas de treinamento e da própria experiência para desenvolver seu trabalho com competência, bem como pelo desenvolvimento de várias competências do ponto de vista profissional. A teoria do Capital Humano foi desenvolvida na década de 60 por dois economistas que mais tarde receberiam o prêmio Nobel (THEODORE SCHULTZ e GARY BECKER). Segundo essa teoria, poderíamos dizer de forma resumida que o progresso de um país é alavancado pelo investimento em pessoas.

Essa nova sociedade que está se formando, e que tem por base o capital humano ou intelectual, é chamada de **Sociedade do Conhecimento**. Nessa sociedade onde as idéias, portanto, passam a ter grande importância, estão surgindo em várias partes do mundo os *Think Thanks*, que nada mais são do que grupos ou centros de pensamento para a discussão de idéias. Esses centros têm por objetivo a construção de um mundo, de uma sociedade mais saudável do ponto de vista econômico e social, que possa desfrutar de uma melhor qualidade de vida.

Pode-se afirmar que a sociedade vem evoluindo conforme a figura a seguir:

FIGURA 1: EVOLUÇÃO DA SOCIEDADE DO CONHECIMENTO.



FONTE: Pesquisa de campo.

Na Sociedade do Conhecimento, as mudanças e as inovações tecnológicas ocorrem num ritmo tão acelerado, que além dos fatores tradicionais de produção,

como capital, terra e trabalho, é fundamental identificar e gerir inteligentemente o conhecimento das pessoas nas organizações. Esta nova era pressupõe uma imensa oportunidade de disseminar democraticamente as informações, utilizá-las para gerar conhecimento que nos leve em direção a uma sociedade mais justa. Pressupõe continuar estudando...

3.3 CERTIFICAÇÃO DIGITAL

É necessário levar-se em conta de que em vista de ser passível de adulteração sem deixar qualquer rastro, para que possa fazer prova, deve o documento eletrônico apresentar **assinatura digital**, pois apenas nessa circunstância é que se pode atribuir-lhe as características de autenticidade e de integridade.

Diferentemente do papel, que se alterado deixa marcas, perceptíveis por meio de perícia técnica, o documento eletrônico trata-se de uma seqüência de bits, reproduzíveis sem que sejam detectáveis quaisquer diferenças, que apresenta cópia exatamente igual ao original.

Não se pode descurar, também, que experimentamos um progresso notável na área de informática, em que inovações ocorrem diariamente. Dessa forma, embora nos dias de hoje possa afirmar-se que a certificação digital por meio de criptografia assimétrica reveste o documento eletrônico de segurança quanto aos aspectos de autenticidade e integridade, antes relatados, nada garante que não seja desenvolvido sistema que desvende o conteúdo criptográfico dos algoritmos hoje aplicados.

TREVISAN (2004) estabelece uma ampla visão dos princípios observados no comércio eletrônico e na legislação Federal sobre Segurança, privacidade e certificação digital, a qual transcreve-se:

> Embora a idéia de rede de comunicação consubstancie-se em conceito amplo que abrange qualquer espécie de sistema que conecte dois ou mais interlocutores, não existe dúvida que a face mais reluzente é a Internet, que provocou significativas mudanças no processo de comunicação. Segundo divulgado pela Câmara Brasileira de Comércio Eletrônico, o paradigma que emerge dessa revolução no mundo digital é o da informação eletrônica, gerador de novas relações econômicas e sociais. Ainda conforme a Câmara **as transações eletrônicas devem estar resguardadas**

> **pelos seguintes requisitos: disponibilidade**: o documento ou informação deve estar disponível ininterruptamente para novo tratamento ou utilização; **integridade**: fidelidade do documento ao teor original, sem sofrer qualquer alteração; **confidencialidade**: a informação relacionada a um indivíduo, empresa ou entidade deve ser protegida da ação indevida de terceiros, seja para conhecer ou tratar essa informação; **autenticidade**: há que ser garantida a autoria, origem e destino do documento eletrônico; **irretratabilidade**: é a garantia de que uma transação depois de efetuada não pode ser negada. Tais requisitos acham-se configurados no Decreto nº 3.505, de 13 de junho de 2000, que instituiu a **Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal** e que define como um dos objetivos da Política da Informação "estabelecer normas, padrões, níveis, tipos e demais aspectos relacionados ao emprego dos produtos que incorporem recursos criptográficos, de modo a assegurar a confidencialidade, a autenticidade, a integridade e o não-repúdio, assim como a interoperabilidade entre os Sistemas de Segurança da Informação". Relativamente às características antes apontadas, MARCACINI (2000) tem um posicionamento mais restritivo. No seu entender pode-se atribuir ao documento eletrônico, desde que por meio de criptografia assimétrica, duas qualidades essenciais: autenticidade e integridade. **(grifos nossos)**

Sabe-se que a criptografia, em si, é considerada tão antiga quanto a própria escrita. Indícios comprovam que técnicas para sua utilização foram conhecidas no Egito, Mesopotâmia, Índia e China, na Antigüidade. O primeiro livro sobre o tema, denominado Poligrafia, foi publicado em 1.510, por JOHANNES TRITHEMIUS, abade alemão, hoje considerado pai da moderna criptografia. Consiste tal método na cifragem de dados de maneira a se ocultar a informação contida na mensagem.

Descreve-se a criptografia em um conjunto de métodos e técnicas destinadas a proteger o conteúdo de uma informação, tanto em relação a modificações não autorizadas quanto à alteração de sua origem, ou à simples restrição do conhecimento a quem não deve tê-lo.

Vale ressaltar, de modo sucinto, que existem duas espécies de criptografia:

- **Simétrica** em que emissor e receptor partilham a chave de acesso e
- **Assimétrica** em que o emissor dispõe de uma senha pública, de conhecimento geral e outra privada, somente por ele conhecida.

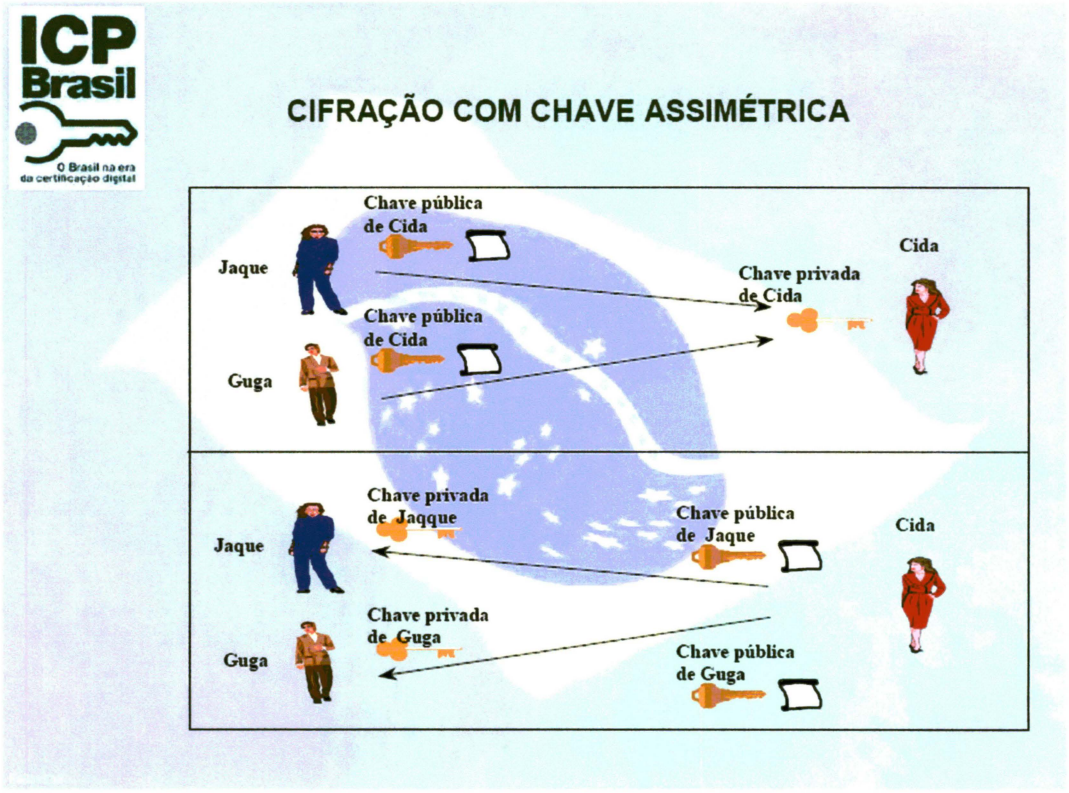
FIGURA 2: CRIPTOGRAFIA SIMÉTRICA.

FONTE: ICP-Brasil.

A criptografia assimétrica baseia-se em algoritmos que utilizam duas chaves diferentes, relacionadas matematicamente através de um algoritmo, de forma que o texto cifrado pela chave 1 do par somente poderá ser decifrado pela chave 2 do mesmo par.

As duas chaves envolvidas na criptografia assimétrica são denominadas chave pública e chave privada. A chave pública pode ser obtida pelo público em geral, enquanto que a chave privada somente deve ser de conhecimento de seu titular. Da mesma forma que no sistema de criptografia simétrica, a segurança da comunicação depende da garantia de segredo da chave privada, que só deve ser de conhecimento do de seu titular.

FIGURA 3: CRIPTOGRAFIA ASSIMÉTRICA.



FONTE: ICP-Brasil.

O emissor processa seu documento com a chave pública do receptor, que é conhecida. O texto cifrado somente poderá ser decifrado pelo receptor previsto, uma vez que somente ele tem a chave privada relacionada à chave pública que orientou a criptografia do documento emitido. Desta forma, fica atendido o requisito de confidencialidade da informação.

Assinaturas são geralmente usadas para se provar a autoria de documentos. DINEMAR ZOCCOLI, citado por TREVISAN (2004) traz o entendimento de FLÁVIA LOZZI segundo o qual preconiza ser a assinatura um gesto de próprio punho que contém forte significado simbólico, suficiente, por si só, para declarar próprias as afirmações externadas, sob as quais a firma vem aposta, dificilmente esquivando-se o signatário do reconhecimento dela como sua. Aduz, inclusive, a interpretação do *Information Technology Security Strategy* (ITSS), grupo de trabalho sobre matérias legais, patrocinado pelo governo do Canadá, segundo o qual a necessidade da assinatura em um documento eletrônico é tratada sob o enfoque seguinte:

> No mundo eletrônico, o original de um documento eletrônico é indistinguível de uma cópia, não existe assinatura escrita de próprio punho e ele não está sobre o papel. O potencial para fraudes é grande, devido à facilidade de interceptação e alteração dos

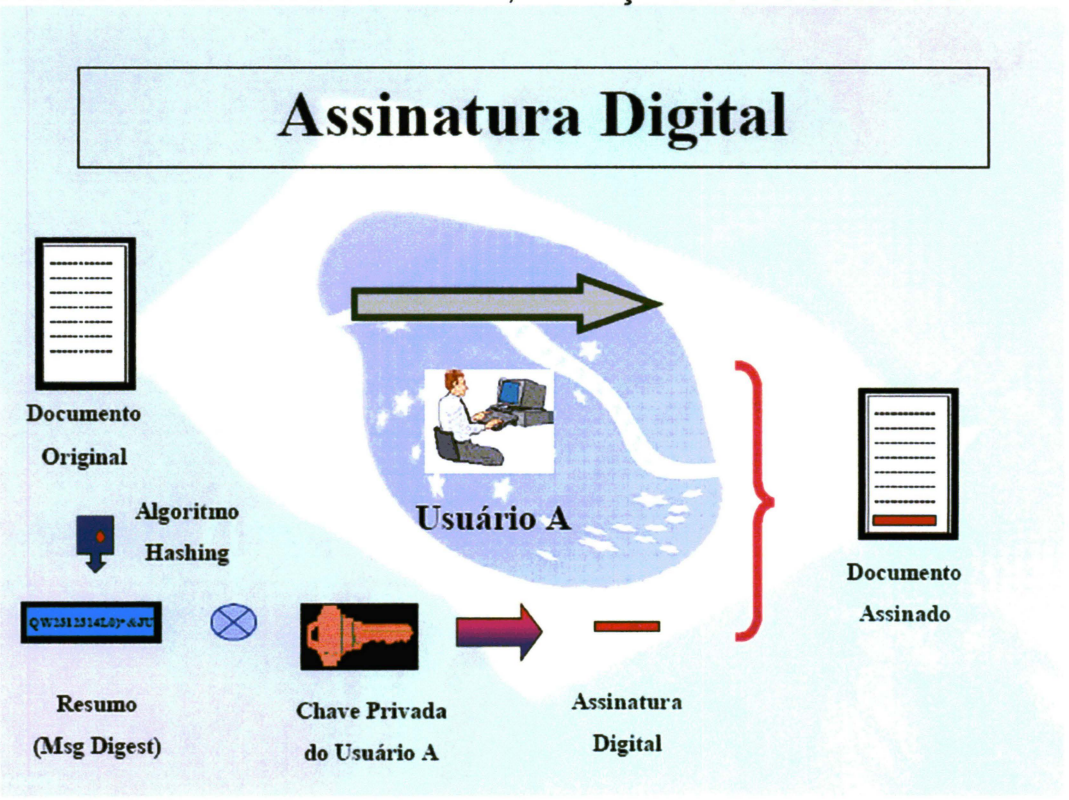
> documentos eletrônicos, e à velocidade de processamento de múltiplas transações. Sempre que as partes tratem entre si com muita freqüência, ou onde não existam conseqüências legais, uma assinatura pode não ser necessária. Todavia, existindo um alto potencial para disputa, ou uma assinatura tradicional ou uma assinatura digital é requerida.

Esse vínculo entre a assinatura e suporte tornou-se tão significativo que gerou dificuldades para se aceitar a idéia segundo a qual a função da assinatura pudesse ser explicada também sobre suportes diferentes e com sistemas diferentes, como é o caso do meio eletrônico.

A cifração do documento eletrônico atende ao requisito de confidencialidade da informação transmitida. Para atender aos requisitos de integridade e autenticidade são implementadas outras ações, gerando um documento assinado digitalmente.

A primeira etapa do processo de geração de um documento assinado digitalmente é aplicar uma função de resumo (*hash*) ao documento eletrônico, obtendo-se uma seqüência de tamanho fixo, única para cada documento. Nota-se que, a partir do resumo, nome dado ao resultado da função *hash*, não é possível recuperar o documento original, ou seja, a função *hash* é unidirecional.

FIGURA 4: ASSINATURA DIGITAL, GERAÇÃO DO DOCUMENTO.

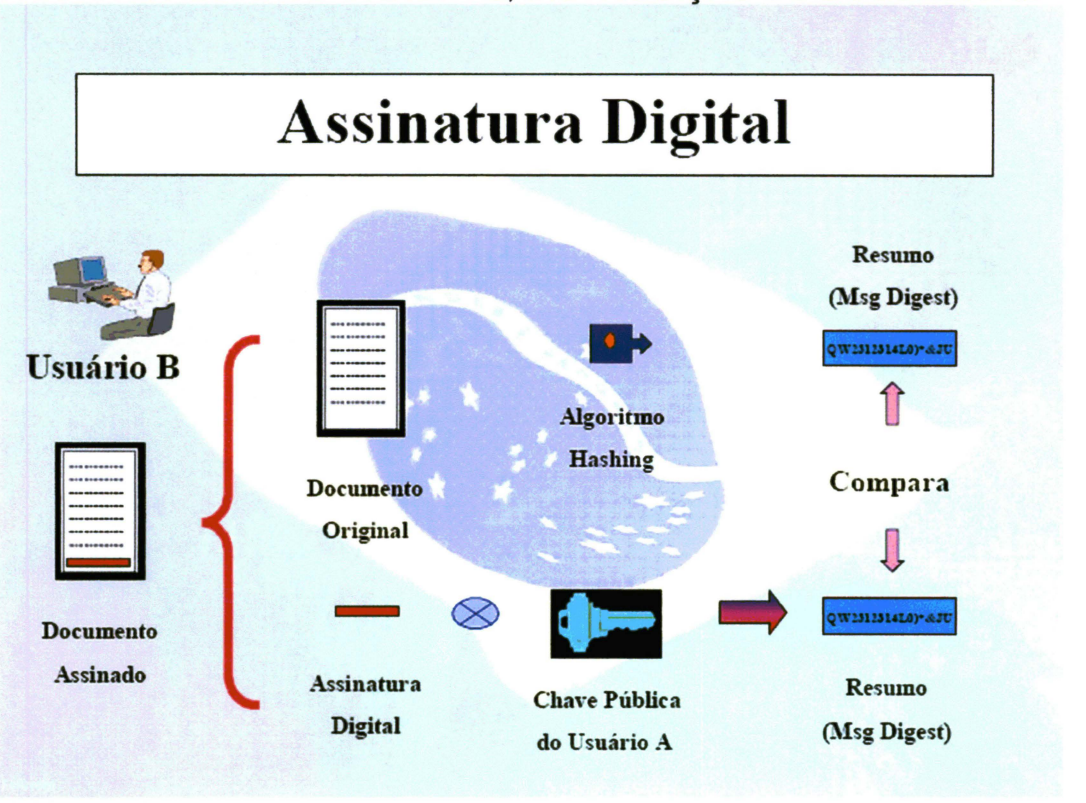


FONTE: ICP-Brasil.

Na segunda etapa do processo, esse resumo será então cifrado com a chave privada do emissor do documento, gerando um arquivo eletrônico que representará a assinatura digital do emissor. Essa assinatura será anexada ao documento eletrônico original, compondo a mensagem ou arquivo, que será transmitido ao receptor. Uma assinatura digital está associada a cada documento emitido.

Na terceira etapa do processo, o receptor recebe a mensagem ou arquivo – o documento original mais a assinatura. Aplica a função de *hash*, ao documento original, obtendo um resultado, aqui chamado resumo 1.

FIGURA 5: ASSINATURA DIGITAL, DISTRIBUIÇÃO DO DOCUMENTO.



FONTE: ICP-Brasil.

Em seguida, a assinatura é decifrada utilizando-se a chave pública do emissor, obtendo-se assim o resumo. Compara-se o resumo com o resumo 1. Caso os resumos sejam iguais, é possível concluir que:

- O documento está íntegro; e
- O documento foi realmente enviado pelo emissor porque a chave pública do receptor conseguiu decifrá-lo;

MARCACINI (2000) aduz que em vista de que documentos eletrônicos podem ser alterados sem deixar vestígios e dada a impossibilidade de se lançar

sobre eles assinatura autógrafa, a literatura jurídica produzida até meados da década de 1990 não os aceitava como prova documental.

Pode-se definir, sem adentrar-se em detalhes técnicos, assinatura digital como o resultado da operação de cifragem do documento eletrônico aplicando-se a chave privada de seu titular. Sua conferência processa-se com o uso da chave pública, reputando-se autêntica e íntegra se puder ser decifrada sem inconsistências.

TREVISAN (2004) defende que ao se utilizar um sistema que envolva chave pública, o gerenciamento de chaves passa a ter dois novos aspectos: primeiro, deve-se previamente localizar a chave pública de qualquer pessoa com quem se deseja comunicar e, segundo, deve-se obter uma garantia de que a chave pública encontrada seja proveniente daquela pessoa. Sem essa garantia, um terceiro (intruso) pode convencer os interlocutores de que chaves públicas falsas pertencem a eles. Dessa forma, quando um interlocutor envia uma mensagem a outro solicitando sua chave pública, um terceiro (intruso) poderá interceptá-la e devolver-lhe uma chave pública forjada por ele. Tal procedimento pode ocorrer com o emissor e o receptor da mensagem.

A garantia para se evitar este tipo de ataque é representada pelos certificados de chave pública. Tais certificados consistem em chaves públicas assinadas por uma pessoa de confiança, denominada terceiro confiável (TTP – acrônimo para *Trusted Third Party*) e servem para evitar tentativas de substituição de uma chave pública por outra. O certificado, além da chave pública, contém informações pessoais sobre seu titular e é assinado digitalmente por uma terceira parte confiável (autoridade certificadora) que associa o nome (e atributos) de uma pessoa ou instituição a uma chave criptográfica pública.

O certificado eletrônico, segundo definição da Ordem dos Advogados do Brasil, Seção São Paulo, consiste em uma declaração de um ente certificante, acerca da titularidade das chaves de uma outra pessoa que está sendo certificada. Esse ente é conhecido como "terceiro de confiança" pois sua declaração deve gerar, para o destinatário da informação, a certeza quanto a sua autoria. AUGUSTO MARCACINI (2000), no contexto que envolve os aspectos de autenticidade e integridade, define o certificado eletrônico como a forma mais prática de se demonstrar a titularidade da chave pública.

Sob a óptica jurídica, pode ser entendido como uma declaração de uma pessoa (ente certificante), em relação à chave pública de uma outra pessoa, atestando essa titularidade. No campo técnico, trata-se de arquivo eletrônico, assinado pelo certificante com sua chave privada contendo a chave pública e informações pessoais do titular desta chave pública.

O trabalho do estudante JOSÉ ROBERTO LENOTTI, citado por TREVISAN (2004), enfatiza que um único terceiro confiável, uma única autoridade certificadora, não é suficiente para garantir a funcionalidade do sistema. Para se obter serviços de segurança no relacionamento com terceiros, são necessárias várias autoridades certificadoras interligadas. Esse conjunto forma uma infra-estrutura de segurança na qual os usuários podem se basear. Quando essa infra-estrutura é projetada para lidar com o gerenciamento de chaves públicas ela é denominada infra-estrutura de chaves públicas (ICP) e pode apresentar duas formações básicas:

- **hierárquica**: ocorre quando há uma Autoridade Certificadora central que autoriza outras certificadoras a emitirem certificados, bem como fiscaliza a atuação dessas outras. Essa autoridade central é conhecida como Autoridade Certificadora Raiz;
- **rede** (ou mista): há uma rede de Certificadoras Digitais independentes, cada uma cruzando certificados privados e públicos com as outras. Este sistema de cruzamento de informações de certificados digitais é chamado de *Cross Certificate Pair*.

Considerando-se que a conferência do certificado é feita com a utilização da chave pública do ente certificante, resta saber se a chave pública que assinou o certificado é realmente do ente certificante. No caso de infra-estrutura hierárquica, há o pressuposto que os usuários do sistema acreditam na autenticidade de uma chave inicial, a chamada chave raiz, que é auto-assinada, isto é, seu certificado é assinado com a própria chave privada do par.

BRASIL (2000) afirma que no entendimento da UNCITRAL, para ter o documento virtual a mesma função e ser considerado como documento escrito, tal qual o documento convencional, é preciso que ele fique disponível para consultas posteriores, sendo que o objetivo desta norma é a possibilidade de reprodução e leitura ulterior.

Ainda BRASIL (2000) defende que para o reconhecimento da assinatura no documento eletrônico a UNCITRAL prescreve que ela deve estar de modo a identificar a pessoa por algum método, e é obvio que esse método a que se refere é a Criptografia, pois é a única forma segura de garantir a autenticidade do assinante. Vários países já adotaram o modelo da UNCITRAL, como os Estados Unidos, a Alemanha, a França, a Argentina, Colômbia e outros que estão ultimando as suas legislações.

BARROS (2004) salienta que um dos pontos que traz mais dificuldade aos profissionais são os sistemas de criptografia e certificação digital. A grande quantidade de aspectos a serem avaliados acaba confundindo até mesmo quem é especialista em segurança. Algoritmos e tamanhos de chaves são alguns dos aspectos que freqüentemente são levantados, mas não é tudo o que é necessário saber sobre um sistema de criptografia. Uma falha comum nas avaliações aparece por conta da forte propaganda de produtos que utilizam criptografia em torno do tamanho das chaves utilizadas. É comum encontrar afirmações que dizem que dado produto é seguro porque utiliza chaves de "tantos" bits. Também é comum ver pessoas fazendo comparações de tamanhos de chaves de algoritmos que funcionam sob conceitos distintos, chegando a conclusões inadequadas. Os algoritmos simétricos mais usados hoje, por exemplo, utilizam chaves entre 128 e 256 bits. Algoritmos assimétricos utilizam chaves de até 4096 bits, e não podem ser considerados mais seguros por conta disso. O que cada um destes sistemas realiza, qual o significado do tamanho dessas chaves e quando deve ser utilizado um ou outro, são algumas das questões que o profissional deve saber na hora de avaliar as características de criptografia de um produto.

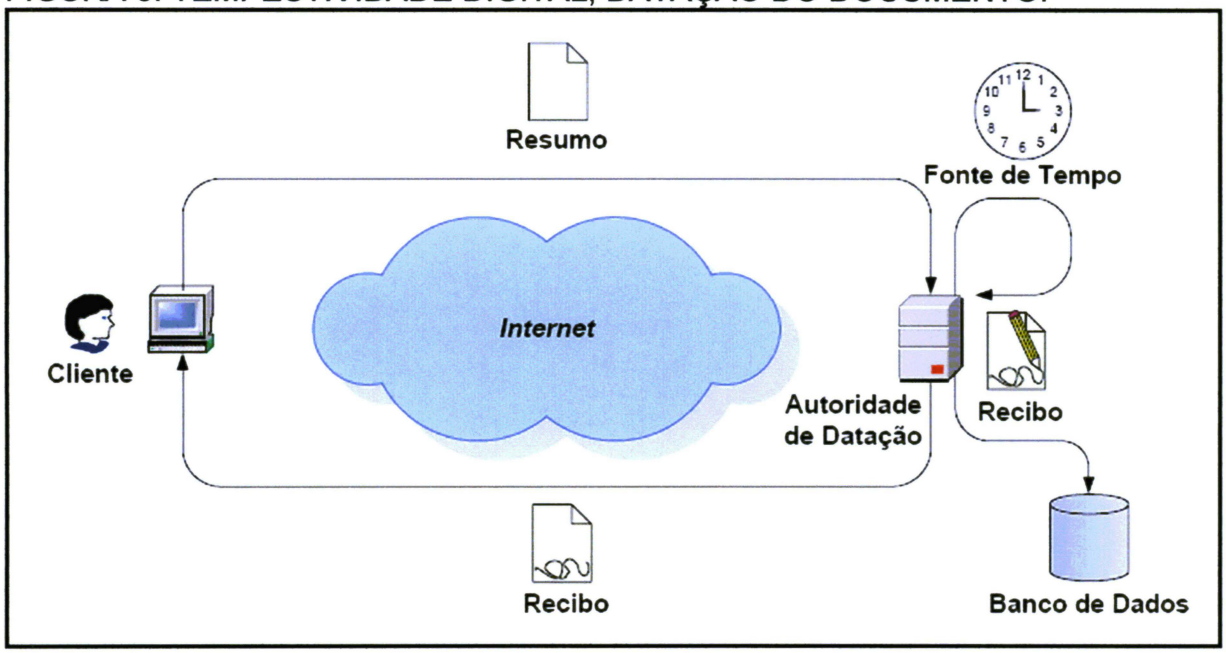
Como quaisquer outras ferramentas, a criptografia e a certificação digital ajudam a resolver problemas específicos. Mais importante do que saber o que estas ferramentas podem fazer é saber o que elas não podem fazer. A certificação digital, apesar de sua sólida base em criptografia, depende de uma série de processos que são tão ou mais importantes que o tamanho das chaves e qualidade dos algoritmos utilizados. São processos que visam reduzir riscos que não podem ser mitigados pela criptografia. Um dos maiores especialistas na área, BRUCE SCHNEIER, diz que "se você acha que criptografia vai resolver o seu problema ou você não conhece seu problema ou não conhece criptografia". Com esta visão e com o conhecimento necessário, o profissional de segurança pode avaliar corretamente

como a criptografia e a certificação digital são utilizadas em cada caso, podendo obter o que as ferramentas oferecem de melhor.

3.4 TEMPESTIVIDADE DIGITAL

O avanço da informática e a disseminação das redes de computadores permitiram o uso de transações eletrônicas em larga escala. Estas transações são realizadas através da troca de documentos eletrônicos entre entidades. O que antes era realizado usando papel, passou agora a ser realizado na forma digital. Com isso, faz-se necessário uma mudança no conceito de documento, de forma a adaptá-lo ao meio eletrônico, atribuindo-lhe a mesma confiança já consolidada no meio papel. COSTA (2003).

FIGURA 6: TEMPESTIVIDADE DIGITAL, DATAÇÃO DO DOCUMENTO.



FONTE: COSTA (2003).

Quando se falou em certificação digital, esclareceu-se que para os documentos eletrônicos serem considerados válidos juridicamente, é necessário que alguns requisitos de segurança sejam satisfeitos, dentre os quais: integridade, autenticidade, irrefutabilidade e tempestividade. Os três primeiros requisitos são atendidos através da utilização da assinatura digital. Já o requisito tempestividade

requer que os documentos eletrônicos sejam datados de maneira confiável. A Protocoladora Digital de Documentos Eletrônicos - PDDE é a entidade responsável por datar os documentos eletrônicos. Entretanto, para que a data adicionada ao documento pela PDDE seja confiável, é necessário que sejam realizados procedimentos de auditoria que fiscalizem o correto funcionamento da PDDE.

STEFANO KUBIÇA (2005, (b)), estabelece uma visão muito clara e abrangente do termo:

> A palavra tempestividade é muito usada nos meios jurídicos para designar "dentro do prazo" e, segundo o dicionário HOUAISS, quer dizer: oportunidade, no tempo próprio, o que ocorre no momento certo, oportuno no tempo devido. Aplicada no mundo digital, a tempestividade pode comprovar que um evento realmente aconteceu em determinado momento. É importante não confundir tempestividade com temporalidade porque esta tem relação com período de tempo, e no gerenciamento de documentos eletrônicos, por exemplo, trata do ciclo de vida do documento. Por sua vez, a tempestividade pode, por exemplo, comprovar os instantes de chegada e saída de um documento eletrônico nas etapas de um processo com fluxo de trabalho automatizado (workflow). Na verdade, a Tempestividade Digital já vem sendo estudada, pesquisada e até viabilizada em algumas organizações há algum tempo. É um conceito genérico que engloba termos como: datação eletrônica, carimbo de tempo, selo cronológico digital, estampilha temporal, carimbo digital, protocolos digitais, etc.(...) A Tempestividade Digital tem fundamental importância no gerenciamento de documentos eletrônicos e pode cumprir um requisito que a Certificação Digital não atende. Um documento que contém assinatura digital pode garantir integridade e autenticidade, mas quando precisa ser enviado ou recebido com a produção de um protocolo, é necessário que se considere a data e hora legal nesse protocolo. Por essa razão, existe hoje preocupação de se regulamentar a Tempestividade Digital dentro da Infra-estrutura de Chaves Públicas brasileira – ICP-Brasil. RENATO MARTINI, diretor de Infra-estrutura de Chaves Públicas do Instituto Nacional de Tecnologia da Informação - ITI, avalia alternativas possíveis para que a Tempestividade Digital dentro da ICP-Brasil seja segura e economicamente viável. Considera que a questão deve ser tratada sob quatro aspectos básicos. O primeiro diz respeito a uma política tecnológica baseada em padrões abertos e em consonância aos estabelecidos por organismos internacionais como forma de garantir a interoperabilidade. O segundo ponto é o fato de o Observatório Nacional ser, por lei, o mantenedor do tempo, ou seja, é o órgão que estabelece a hora legal do Brasil. Assim, é necessário que resoluções complementares criem modelos para que esse horário possa ser usado por prestadores de serviço de tempo. Outro ponto levantado por MARTINI é a importância de se entender que Certificação Digital não é apenas um modelo jurídico, mas também e principalmente uma questão tecnológica, sendo necessário criar utilidade e oportunidades para a adoção dessa tecnologia. Como quarto aspecto básico, MARTINI faz considerações sobre a necessidade de se ter um custo viável para definir um modelo. Com a regulamentação da Tempestividade Digital dentro da ICP-Brasil, RENATO MARTINI prevê para 2005 o desenvolvimento do projeto de Gestão Eletrônica de Documentos (GED) para a Esplanada dos Ministérios, que deverá agregar dois itens fundamentais: a datação eletrônica e a Certificação Digital.

Integrando-se a tempestividade digital à certificação digital, completa-se um ciclo virtuoso na gestão de documentos e processos eletrônicos, possibilitando seu uso nas esferas administrativas e jurídicas. A ferramenta para se alcançar isso, passa a ser o GED/ECM (*Enterprise Content Management*), que provê funcionalidades para elaboração/captação, armazenamento, gerenciamento, preservação e distribuição. A Certificação Digital pode garantir assinatura, autenticação, integridade e sigilo. Por sua vez, a Tempestividade Digital pode comprovar a data e hora em cada etapa do ciclo de vida de um documento, no trâmite de documentos eletrônicos em processos automatizados (WORKFLOW). Assim será possível saber e provar quando uma operação eletrônica foi efetivada, o que, em muitos casos, é tão importante quanto ter certeza da origem ou da integridade do seu conteúdo KUBIÇA (2005, (b)).

3.5 CONCEITOS PRÁTICOS E PRODUTOS ENVOLVIDOS NA CERTIFICAÇÃO DIGITAL

Certificado Digital é um arquivo no computador que identifica o usuário. Alguns aplicativos de software utilizam esse arquivo para comprovar a identidade do usuário para outra pessoa ou outro computador. Dois exemplos típicos são:

- Quando você consulta seu banco on-line, este tem que se certificar de que você é a pessoa que pode receber a informação sobre a conta. Como uma carteira de motorista ou um passaporte, um Certificado Digital confirma sua identidade para o banco on-line.
- Quando você envia um e-mail importante, seu aplicativo de e-mail pode utilizar seu Certificado Digital para assinar "digitalmente" a mensagem. Uma assinatura digital faz duas coisas: informa ao destinatário que o e-mail é seu e indica que o e-mail não foi adulterado entre o envio e o recebimento deste.

Um Certificado Digital normalmente contém as seguintes informações:

- Sua chave pública (para mais informações;- Seu nome e endereço de e-mail;
- A validade da chave pública;

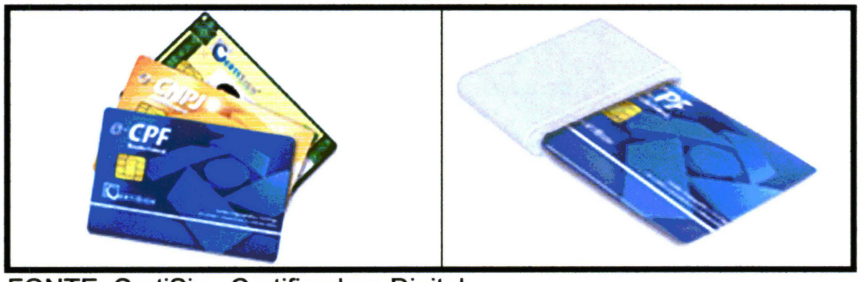
- O nome da empresa, Autoridade Certificadora – AC, que emitiu seu Certificado Digital;
- O número de série do Certificado Digital;
- A assinatura digital da AC.

SmartCard é um cartão criptográfico capaz de gerar e armazenar as chaves criptográficas que irão compor os certificados digitais. Uma vez geradas essas chaves, elas estarão totalmente protegidas, não sendo possível exportá-las para uma outra mídia nem retirá-las do smartcard. Mesmo que o computador seja atacado por um vírus ou, até mesmo um hacker, essas chaves estarão seguras e protegidas, não sendo expostas a risco de roubo ou violação.

Os múltiplos níveis de proteção que compõem a solução - incluindo recursos físicos e lógicos - asseguram a identificação do assinante, permitirão que a integridade e o sigilo das informações sejam protegidos e impossibilitarão o repúdio do documento em momento posterior.

Leitora é um dispositivo projetado para conectar um cartão inteligente (SMARTCARD) a um computador. A leitora se encarregará de fazer a interface com o cartão, enquanto o computador suporta e gerencia as aplicações. Instalar uma leitora de cartões inteligentes é um procedimento simples, que dispensa conhecimentos técnicos. Uma vez instalada, a leitora permitirá o acesso seguro a serviços na Internet já preparados para a certificação digital e aplicações de Internet Banking.

FIGURA 7: SMARTCARD E LEITORA.



FONTE: CertiSign Certificadora Digital.

O **token** é um hardware capaz de gerar e armazenar as chaves criptográficas que irão compor os certificados digitais. Uma vez geradas estas chaves, estarão totalmente protegidas, pois não será possível exportá-las ou retirá-las do token (seu hardware criptográfico), além de protegê-las de riscos como roubo ou violação.

Sua instalação e utilização é simples: conecte-o a qualquer computador através de uma porta USB depois de instalar seu driver e um gerenciador criptográfico (software). Dessa forma, logo que o token seja conectado, será reconhecido pelo sistema operacional.

FIGURA 8: TOKEN.

FONTE: CertiSign Certificadora Digital.

São características do token, incluindo recursos físicos e lógicos: assegurar a identificação do portador (que precisa de uma senha pessoal e intransferível para utilizá-lo), permitir que a integridade e o sigilo das informações contidas nele, proteger e armazenar essas informações (as chaves e os certificados) e impossibilitar a separação da chave criptográfica do hardware criptográfico.

4 MEIOS DE ARMAZENAMENTO E FERRAMENTAS PARA GERENCIAMENTO

Nos dias atuais ainda é forte a predominância do armazenamento dos documentos em papel, isto se deve, boa parte em função de que a troca de grande volume de informações ainda é feita através deste mecanismo, até mesmo por imposição legal. A certificação digital, apesar de regulamentada, só tem valor enquanto o documento estiver no meio digital, uma vez impresso, necessário se faz a autenticação do mesmo.

Alguns documentos já são gerados a partir de um software específico, como por exemplo o Autocad ou MS-Word, e, armazenados eletronicamente, para fins de consultas nos vários setores da empresa ou de órgãos públicos. Existem também outros documentos, como os vídeos que são armazenados em fitas próprias para este fim. Processos judiciais, inquéritos policiais já são, no Estado do Paraná, elaborados em sistemas corporativos e armazenados em servidores próprios.

Existem várias maneiras diferentes de se descrever o ciclo de vida de um documento. GARG, citado por FANTINI (2001), propõe, no que se refere à produção de documentos eletrônicos, a classificação encontrada no quadro a seguir:

QUADRO 1: ETAPAS DO CICLO DE VIDA DO DOCUMENTO.

Pesquisa	A aquisição de informação, incluindo a interpretação da informação contida nos documentos.
Autoria	Criação dos novos documentos.
Aprovação	Revisão dos documentos com a finalidade de fazê-los conforme com uma certa estrutura e padrão de conteúdo.
Publicação	Transformação dos documentos em uma forma de apresentação específica (por exemplo: papel, CD-ROM, Internet).
Armazenamento	Nesta etapa, os documentos devem ser guardados em um meio de armazenamento que ofereça confiabilidade e facilidade de localização e acesso aos documentos.

FONTE: GARG citado por FANTINI (2001).

FANTINI (2001) afirma que, ao contrário de outras visões para o ciclo de vida de documentos, a divisão nas cinco etapas anteriores ajuda a diferenciar os passos que envolvem o processo automatizado daqueles que envolvem interações humanas com a informação contida nos documentos.

4.1 ACESSIBILIDADE DOS DOCUMENTOS

Muito comum se faz, na atualidade o uso de computadores para gerar e manipular documentos. A maior parte desses documentos é armazenada para consulta futura ou mesmo para servir de base para criação de novos documentos.

Não obstante ser comum a idéia de se armazenar todos os documentos em um só formato de consulta como .tif ou .pdf, na verdade usa-se seu formato nativo ou original. Como exemplo disso vemos o Boletim do Comando-Geral que é disponibilizado em .pdf e .rtf, para facilitar o acesso por usuários de toda a PMPR. Isto acaba sendo bastante útil, uma vez que há necessidade de geração de novos documentos baseados nesses, anteriormente disponibilizados.

Considerando a inexistência de um sistema GED na PMPR, bem como de previsibilidade orçamentária para sua aquisição não é suficiente apresentar soluções de mercado para autoria, aprovação e divulgação; quando se buscar tal solução, as ferramentas de mercado serão outras. Por esse aspecto, este item do trabalho aponta conceitualmente soluções de GED e a maneira como instituições tratam sua informação e os meios de armazenamento.

A criação de um documento pressupõe que este será utilizado em dado momento em algum processo de uma organização. A INTRANET da PMPR (http://10.47.1.19) tem facilitado a distribuição de ordens, doutrina, normas, boletins gerais, portarias, diretrizes, entre outros documentos. De acordo com o quesito 4.5 da ISO 9001, que rege o controle de documentos e de dados, os documentos devem estar disponíveis em todos os locais onde são executadas as operações essenciais para o funcionamento efetivo do sistema da qualidade, isto pode ser alcançado pela INTRANET. Esta disponibilidade pode ser em forma de papel, eletrônica ou outros meios apropriados, como por exemplo, em vídeo.

Informações, às vezes caras e extremamente valiosas para uma organização, podem desaparecer pela constante mudança no quadro de profissionais e, principalmente, pela falta de documentação dos processos de trabalho. A normatização para elaboração de documentos existe, principalmente quando se trata de documento de Estado-Maior, no entanto sua distribuição e armazenamento podem ser falhos.

Em todo o mundo, muitos documentos são arquivados de forma aleatória, sem uma estrutura que facilite a sua localização quando se fizer necessário. A PMPR não foge à regra, armários, pastas suspensas, ordenações das mais variadas (alfabética, cronológica, por assunto, nome, etc) dificultam a localização de documentos. Outros são expostos a fatores que podem provocar danos irrecuperáveis, como por exemplo a deterioração pela ação do tempo, umidade, fungos, ataques de pragas como ratos, traças, baratas e outros que costumam danificar os papéis, fitas de vídeo, guias de recolhimento de impostos, recibos de pagamentos diversos, etc.

Os documentos eletrônicos geralmente são armazenados em microcomputadores que são acessados por vários usuários locais ou em rede que interliga vários computadores. A localização do arquivo ocorre de forma convencional, onde são estipulados os locais (pastas/diretórios) em que os mesmos estão armazenados. Este método demanda tempo na busca do documento, as vezes indeterminado, proporcional à estrutura disponível e à capacidade de assimilação do conhecimento por parte dos usuários.

Outro ponto crítico é o controle de versões. Quando um documento sofre uma alteração, este é disponibilizado pela versão mais atual. Uma eventual necessidade de consulta a uma versão anterior, normalmente provoca um backup inverso, visto que no método convencional não existe a preocupação com o armazenamento de versões anteriores.

Os sistemas de GED preservam as características visuais e espaciais, e a aparência do documento original em papel, gerencia o ciclo de vida das informações desde sua criação até o arquivamento, e podem estar registradas em mídias analógicas ou digitais em todas as fases de sua vida. O documento pode ser exibido ou impresso em papel onde e quando necessário em apenas alguns segundos.

O GED permite capturar, recuperar e transmitir documentos contendo todos os tipos de informação, tais como: manuscritas, criadas por computador, diagramas, fotografias, desenhos de engenharia e impressões digitais.

As informações podem ser criadas em mídias eletrônicas (por exemplo, um engenheiro gerando um desenho em produto CAD - *Computer Aided Design*), revisadas a partir de mídias eletrônicas, processadas a partir destas mídias e arquivadas eletronicamente, não sendo necessária em nenhum momento sua impressão. No entanto, é muito comum pessoas imprimirem os documentos que

recebem, pelo simples inconveniente de não estar familiarizado com o microcomputador, descartando-os após leitura e revisão, que poderiam ocorrer no meio eletrônico.

O GED é a melhor forma de tornar documentos disponíveis de forma extremamente eficiente para o usuário, permitindo a recuperação desses documentos através de estruturas eletrônicas. Essa eficiência na hora de localizar os documentos é possível através da atribuição de múltiplos índices eletrônicos que permitem a recuperação mais rápida dos dados. Daí chamar-se o sistema de gerenciamento eletrônico porque as mídias usadas para guardar os documentos são eletrônicas, como discos magnéticos e ópticos.

4.2 TECNOLOGIAS UTILIZADAS NO GERENCIAMENTO ELETRÔNICO DE DOCUMENTOS

KOCH (1998), afirma existirem no mercado de Gerenciamento Eletrônico de Documentos uma diversidade de soluções, pois, por baixo da expressão GED encontra-se uma gama de tecnologias, algumas já citadas anteriormente no capítulo 3, onde cada uma delas tem um objetivo específico para atender aplicações específicas, conforme descritas abaixo:

- Imagem (document imaging) - Tendo como foco o gerenciamento de documentos estáticos, esta ferramenta oferece produtos que armazenam imagens de documentos em estruturas pré-definidas de índices, e boa parte dos produtos reproduzem estruturas do tipo pasta/subpasta/documento. Outros indexam documentos diretamente. É mera substituição de mídias com alguma sofisticação adicional como múltiplos índices. Alguns exemplos são aplicações de recursos humanos e pastas de clientes com informações para efeito de crédito.
- Integração com sistemas de processamento de dados (imaging enable) – São bibliotecas de sub -rotinas de produtos de document imaging que podem ser integradas em programas tradicionais de processamento de dados, permitindo o acesso a funções de imagem (imaging) a partir destes. Esta integração pode ser feita através de uma série de recursos

como DLL, API, etc., e fornece informações em forma de dados e de imagem sobre determinado assunto, exibidas simultaneamente. Contas a pagar e recursos humanos são casos em que dados necessitam ser complementados com imagens de documentos.

- EDMS (Engineering Document Management Systems) - São produtos voltados ao gerenciamento de documentos técnicos, e possuem algumas características adicionais quando comparados a produtos de imaging quanto a controle de versões; manuseio de arquivos em formato TIFF (Tagged Image File Format), CALS (Computer Aided Acquisition and Logistic Support) e gerados por CAD; funções de red-line (faz marcas nos desenhos para futuras revisões); gerenciamento de periféricos com capacidade de manusear documentos do tamanho A0 etc. E, ainda, esses produtos gerenciam tanto arquivos imagem (raster) como arquivos CAD (vector). Normalmente, são utilizados para o gerenciamento de documentos técnicos como plantas de engenharia, manuais e listas de materiais.
- OCR (Optical Character Recognition) e ICR (Intelligent Character Recognition) - São utilizadas para obter dados processáveis por sistemas de processamento de dados a partir de imagens. OCR é utilizado para a conversão de caracteres gerados de forma mecânica (datilografia, impressa). O ICR é usado para a conversão de caracteres gerados de forma manuscrita. A conversão de imagens para caracteres ASCII, EBCDIC ou HEXA pode ser feita das seguintes formas:na primeira técnica, a matriz resultante do processo de digitalização é comparada a um banco de dados de matrizes e a matriz mais semelhante é escolhida; na segunda técnica, são analisadas as características da imagem para a identificação de caracteres semelhantes. Contudo, é necessária uma base de grafia que contenha a grafia a ser reconhecida, i.e., por exemplo, se na base não tiver um ç, não há como reconhecê-lo.
- Full Text Retrieval - São utilizados para recuperar documentos a partir de qualquer palavra do conteúdo do texto. Os documentos são

digitalizados e submetidos a um processamento de OCR para a extração de seu conteúdo e criação de base de índices.

- COLD (Computer Output to Laser Disk) aplica-se ao gerenciamento de relatórios feitos em sistemas de processamento de dados (relatórios gerados em arquivos spool, que estão armazenados em discos ópticos, como extratos, relatórios contábeis, gerenciais e de cobrança), armazena arquivos com relatórios em forma de dados cuja recuperação é através de diversos índices, e diversas formas, tais como servidor de fax, monitor ou impressora, além de integrar recursos de imagem para o armazenamento de máscaras de relatórios pré-impressos. Permite que sejam feitas anotações sobre o relatório sem afetar o documento original. Os relatórios contidos nos discos podem ser recuperados e visualizados, impressos, transmitidos por fax ou enviados eletronicamente para terminais de microcomputadores. Os sistemas de COLD são de baixo custo, de alta capacidade e eficiência na distribuição eletrônica de dados, eliminação ou diminuição de papel, eliminação de risco de extravio e deterioração e melhoria na prestação de serviços. Essa tecnologia pode ser integrada com ferramentas de data warehouse e data mining, para criação de um ambiente de business intelligence. Além disso, pode ser integrada a pacotes de ERP e a sistemas de gerenciamento de documentos, dando uma visão corporativa de todos os relatórios da empresa (SALLES, 2000).
- COM (Computer Output to Microfilm) - é a saída de computador diretamente para microfilme. Tecnologia que está aos poucos sendo substituida pelo COLD.
- Workflow de produção - gerencia fluxos de trabalho e a integração de ferramentas em processos estruturados, possuindo interface gráfica para o desenho do fluxo e mecanismos sofisticados de controle do processos que envolvam altos valores e volumes, como por exemplo, no mercado nacional, os processos de concessão de crédito, câmbio e sinistro em seguros.
- Workflow ad-hoc - são produtos que não possuem interface gráfica para a fluxogramação de processos. São voltados ao roteamento de

informações não estruturadas, além de serem utilizados para gerar infra-estrutura de comunicação e integração de ferramental de automação de escritórios.

- Forms Processing – Processamento eletrônico de formulários: A digitalização converte imagens de documentos para o mundo digital. A etapa seguinte transforma essa imagem em dados processáveis por um sistema de computação. A tecnologia de processamento eletrônico de formulários permite reconhecer as informações nos formulários e relacioná-las com campos nos bancos de dados. O processamento eletrônico de formulários está automatizando o processo de digitação em muitas empresas. Essa tecnologia já vem sendo utilizada por alguns bancos para agilizar o processamento dos formulários de abertura de contas. Outra grande aplicação dessa tecnologia é o reconhecimento de todos os formulários manuscritos do censo 2000 no Brasil, feito pelo IBGE – Instituto Brasileiro de Geografia e Estatística.
- Produtos integrados - são combinações de produtos/ferramentas, p.ex. integração de CAD (vector) com "imaging" (raster), "imaging" com estrutura de recuperação "full text retrieval" onde os índices foram obtidos através de OCR; "imaging" com COLD; "workflow" de produção com "imaging".

FANTINI (2001) afirma que de todos os elementos dos sistemas de Gerenciamento Eletrônico de Documentos, a preparação de documentos é tarefa bastante trabalhosa e que não deve ser abandonada, mesmo com os mais modernos sistemas automatizados. Pode ser feita pela própria equipe ou por um birô de serviços. De fato, o manuseio de documentos, o cuidado e organização relacionados neste processo exigem uma dedicação elevada das pessoas envolvidas.

Os escaners utilizam mecanismos de transporte de papel (de rotação ou de mesa) semelhantes aos das câmeras de microfilme rotatórias, dos dispositivos de fotocópia e das máquinas de facsímile. Portanto, a preparação dos documentos requer a remoção de grampos, clipes e outros prendedores. Alguns documentos em papel contêm informações que não podem ser comunicadas em preto e branco (por exemplo, números de contabilidade demonstrando valores negativos em vermelho),

pois a maioria dos escaners reconhece apenas o preto e branco. Portanto, como parte de preparação é importante identificar por escrito o que está em cores no original, antes da digitalização.

Três tipos de escaner de documentos podem ser encontrados no mercado:

- escaners vetoriais, utilizados em sistemas CAD (computer-aided design, ou projeto assistido por computador) para a criação de desenhos de engenharia;
- escaners de OCR (reconhecimento óptico de caracteres), que convertem todos os números e letras do texto num código ASCII para processamento de dados e textos;
- escaners raster (digitalizadores), que convertem a imagem num bitmap, processo conhecido como bitmapping.

Existem escaners com alimentadores para várias páginas, escaners de mesa para a digitalização de material encadernado, alimentadores de cartões-janela etc. Muitos permitem que o operador altere a resolução da digitalização, e a maioria dos escaners funciona de forma semelhante a uma fotocopiadora, mas existem unidades especiais para diferentes tipos de entrada.

O bitmapping é utilizado na conversão de documentos para uma representação digital binária eletrônica nos sistemas de Gerenciamento Eletrônico de Documentos para documentos comerciais que utilizam discos WORM (uma gravação, várias leituras) e discos ópticos regraváveis. O bitmapping (digitalização) trata uma imagem ou documento como um conjunto retangular de pontos, chamados picture elements, ou pixels. Nesse processo, usa-se uma técnica digital binária para representar os pixels escuros (pretos ou quase pretos) e claros (brancos ou quase brancos).

O projeto de índexação é muito importante não só porque ele é a chave para a localização de documentos, mas porque ele tem uma grande influência sobre os cronogramas de conversão e os custos iniciais, e também contínuos, do sistema. Geralmente, os dados de índices são armazenados em discos magnéticos, pois os discos ópticos não recuperam informações de índice com a velocidade necessária para as pesquisas. Em uma visão mais simplista pode-se dizer que uma indexação mal feita resulta naquilo que se vê cotidianamente em escritórios ou seções

desorganizadas, a procura de um documento, que, apesar de existir não se sabe onde foi guardado.

KOCH (1998) alerta para o fato de que há confusão quanto ao uso da expressão CD-ROM como forma de referenciar discos ópticos, que são para informações e automação de documentos. Isto pode implicar em erros de entendimento, pois um disco óptico WORM de 12 polegadas nunca poderá ser lido em um drive de CD-ROM e um CD-ROM nunca será regravável.

Portanto, a seguir faz-se a conceituação:

- CD-ROM (Compact Disk Read Only Memory): são discos ópticos gerados através de um processo de masterização a partir de um original, em instalações industriais sofisticadas, em pequeno número, principalmente em S. Paulo e Manaus. Tem, aproximadamente, capacidade de 650 Mb de informações, em dados e/ou imagens em suas 4 3/4 polegadas de diâmetro. Não pode ser alterada qualquer informação. São discos lidos em drives de CD ou em equipamentos que permitem o armazenamento de uma biblioteca destes, conhecidas por jukebox (com capacidade para 1.478 discos CDROM). A cor destes discos é prateada. Esta mídia é ideal para grandes quantidades de cópias de informações estáticas como enciclopédias, listas de componentes farmacêuticos, catálogos, etc. A principal aplicação do CD-ROM é a publicação, geralmente comercial, tais como catálogos, softwares, listas, enciclopédias, materiais para consulta, etc. Após configurado o sistema de réplica, são necessários apenas alguns segundos para se produzir cada CD-ROM duplicado. A criação do master original é cara e, portanto, só compensa para mais de 50 cópias. Um CD-ROM é gravado em apenas um lado e as informações são contidas numa única trilha que segue em espiral do centro para sua circunferência. Através de uma técnica chamada velocidade linear constante (CLV), a unidade de disco varia constantemente a velocidade com que o disco gira.
- CD-R (Compact Disk - Recordable ou Writable): são discos ópticos com o mesmo padrão de leitura do CD-ROM, mas com a possibilidade de gravação em instalações de empresas ou casa, bastando ter uma unidade de gravação para esta mídia. Em geral, a mídia CD-R é dourada, o que

torna fácil distinguir esta do CD-ROM (prateado). Esses discos podem ser lidos com os mesmos periféricos para a leitura do CD-ROM, pois têm o mesmo formato. Esta mídia é utilizada quando o número de cópias da mesma informação é baixo e/ou para o armazenamento de informações dinâmicas, em que o tempo necessário para a geração de um CD-ROM tornariam estas obsoletas. As informações dos CD-R, assim como as dos CD-ROM, são contidas numa única trilha que segue em espiral do centro do disco para a margem externa. Após gravadas, as informações não podem ser modificadas ou removidas.

- CD-RW (Compact Disk Rewritable): são discos ópticos com o mesmo padrão de leitura do CD-ROM, mas é possível fazer gravação nas instalações da empresa ou em casa, se tiver uma unidade de gravação. O CD-RW é regravável e o CD-R não permite regravação.
- DVD (Digital Video Disk): são discos ópticos mais recentes, os substitutos do CD, e tem a mesma dimensão do CD (4 3/4" ou 120 mm). Podem ser gravados em uma face, uma camada, uma face, duas camadas ou duas faces duas camadas através de feixes de laser mais fracos ou mais intensos. A capacidade máxima anunciada no mercado é de 4,7 GB para uma face, uma camada, 9GB para uma face, dupla camada, e 17 GB para duas faces, duas camadas.
- DISCOS ÓPTICOS WORM (Write Once, Read Multiple): são discos ópticos onde o processo de gravação é físico e altera a superfície, mas não possibilita alterar a gravação, pois só podem ser gravados uma vez, mas com ilimitadas leituras. Apresentam tamanhos de 5 1/4, 12 e 14 polegadas cuja capacidade varia de 650 MB a 25 GB. Considera-se que esta mídia deverá ter preferência no uso em aplicações onde se deseja valor legal para a informação. Através da velocidade angular constante (CAV), o disco WORM sempre gira na unidade de disco com a mesma velocidade. Um disco WORM, na unidade adequada, pode ser gravado por praticamente qualquer computador. As informações, na maioria dos discos WORM, são dispostas em círculos concêntricos chamados trilhas, que, por sua vez, são divididas radialmente em setores. A principal aplicação dos discos WORM é o armazenamento de todos os tipos de

documentos comerciais, como correspondência, faturas, vouchers, formulários preenchidos de todos os tipos e desenhos de engenharia. Os documentos podem ser gravados no disco WORM durante um período indefinido, até que o disco esteja cheio. As informações podem ser recuperadas e utilizadas durante esse período. As principais diferenças entre o disco WORM e o CD-ROM são: o primeiro é criado pelo usuário, e o segundo geralmente é criado por um publicante. Ambos precisam de unidades diferentes para leitura.

- DISCOS ÓPTICOS REGRAVÁVEIS: podem ser apagados para novo processo de gravação e podem ter diferentes formas de se fazer isto, sendo o magnetoóptico e o phase change os mais comuns. Têm tamanhos de 3 1/2, 5 1/4 e 12 polegadas, com capacidades entre 128 MB e 15 GB. Assim como os discos WORM, podem ser lidos em unidades standalone ou em jukebox. A principal aplicação dos discos regraváveis é o armazenamento de todos os tipos de documentos comerciais em que a admissibilidade legal não é um requisito ou esse requisito seja atendido por meio de microfilmes ou da manutenção de documentos em papel.

Todos os sistemas de discos ópticos utilizam a codificação digital binária para armazenar as informações, um raio laser de alta potência para gravar e um de baixa potência para ler as informações. Por ser lido com uma fonte de laser, não ocorre desgaste, independentemente de quantas vezes é utilizado.

FANTINI (2001) ressalta a importância de que a mídia deve ser armazenada de acordo com os padrões nacionais e as recomendações do fabricante, antes e depois da gravação. No caso do microfilme, supõe-se que o filme bruto tenha uma expectativa de vida de ao menos cem anos.

QUADRO 2: DURABILIDADE DAS MÍDIAS.

Mídia	Temperatura ° C	Umidade Relativa %	Durabilidade Anos
CD-ROM	40	80	2
	30	60	10
	20	40	50
	10	25	200
WORM	40	80	5
	30	60	20
	20	40	100
	10	25	200
CD-R	40	80	2
	30	60	5
	20	40	30
	10	25	100
MAGNETÓPTICO	40	80	2
	30	60	5
	20	40	30
	10	25	100
MICROFILME com qualidade arquivista (prata)	40	80	20
	30	60	50
	20	40	200
	10	25	500

FONTE: CENADEM citado por BALDAM (2002).

O quadro acima mostra dados que dão idéia da longevidade das diversas mídias para o armazenamento de informações. Na prática, a maior preocupação que se deve ter não é realmente se a mídia irá durar ou não algo em torno de cem anos. A maior preocupação deve ser imediata, buscando saber se nos próximos cinco anos, ou tempo que interessa ao armazenamento da informação, ainda haverá equipamentos (drives) que permitam ler essas mídias.

Fácil é recordar que no fim da década de 80 e início de 90 muito comum se fazia o uso do disco flexível de 5 ¼" ou 5,25 polegadas. Nos dias de hoje torna-se impossível encontrar *drives* para leitura dessas mídias.

Além das mídias ópticas existem as mídias magnéticas (disco rígido, disco flexível e fitas), as quais tem um uso mais comum disponibilizado pelo disco rígido (Hard Disk – HD). O HD é o mais rápido dispositivo disponível para armazenamento de massa documental. Atualmente, existem produtos de grande capacidade a custo totalmente acessível, além disso, eles podem ser agrupados em sistemas RAID possibilitando gigantescos volumes de informação, mais baratos, rápidos e duráveis do que soluções similares para discos ópticos (jukebox).

5 SEGURANÇA E APLICABILIDADE

A falta de confiança em recursos tecnológicos é uma constante observada no relacionamento de profissionais com tecnologias digitais, mas o conhecimento mais aprofundado sobre os métodos e vantagens que podem ser obtidas a médio e longo prazo, podem trazer estes mais para perto do uso eficaz dessas ferramentas em seu dia-a-dia. É preciso promover maior intimidade e cumplicidade para aquisição de confiança. É preciso estar atento às inovações da Sociedade do Conhecimento.

Em um Brasil com eleições eletrônicas copiadas para o mundo inteiro, em um universo globalizado de comércio eletrônico e automação bancária é inquestionável a confiabilidade no assunto.

Sabe-se que toda informação de ambientes corporativos revestem-se de determinado grau de sigilo, que muitas vezes confunde-se com segurança. A classificação de níveis de sigilo usada para documentação lembra muito os parâmetros indicados no Regulamento para Salvaguarda de Assuntos Sigilosos – RSAS, tendo os seguintes níveis:

- Público;
- Restrito;
- Confidencial;
- Secreto; e
- Supersecreto.

5.1 CONFIABILIDADE DA INFORMAÇÃO ELETRÔNICA

Sistemas e redes corporativas exigem níveis de segurança e confiabilidade dos mais variados, desde simples senhas de acesso, passando por criptografia, servidores Proxy, *Firewall*, etc.

A confiança de que sistemas corporativos funcionem vão do controle de acesso à necessidade de planejamento contingencial para que a informação não se perca. Sistemas como META4 e SisCOp necessitam de equipamentos (servidores)

de alta confiabilidade e performance, sem os quais estariam comprometidos meses de trabalho e volumosas somas do erário público.

Confiabilidade não se resume em acreditar na informação disponível, é preciso que ela esteja disponível. Para isso, o aprimoramento continuado em tecnologia da informação é algo imprescindível, não se pode mensurar o valor da informação, sem ela o comprometimento institucional é algo catastrófico, um preço caro de mais a se pagar pela falta de investimentos.

Se a informação de uma instituição está disponível em sistemas desenvolvidos com certa finalidade, acredita-se que seu conteúdo e suas atualizações sejam monitorados, mantendo-se um registro de quem fez o que e quando o fez, isto torna os sistemas corporativos confiáveis.

Quando essa informação, na forma de documento, precisa ser enviada a outro órgão, entram em cena a certificação e assinatura digital, sem o que não se pode confiar no documento eletrônico.

No dia 29 de junho de 2001, o Diário Oficial da União veiculou a Medida Provisória n° 2.200. Este diploma legal instituiu a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil para garantir a autenticidade e a integridade de documentos eletrônicos através da sistemática da criptografia assimétrica. CASTRO (2001).

A MP supra citada estabelece a organização da ICP-Brasil, comportando uma autoridade gestora de políticas (Comitê Gestor da ICP-Brasil) e uma cadeia de autoridades certificadoras composta pela Autoridade Certificadora Raiz - AC Raiz (Instituto Nacional de Tecnologia da Informação - ITI), pelas Autoridades Certificadoras - AC e pelas Autoridades de Registro - AR.

Compete à AC Raiz, primeira autoridade da cadeia de certificação, emitir, expedir, distribuir, revogar e gerenciar os certificados das AC (de nível imediatamente subseqüente ao seu), sendo vedado emitir certificados para o usuário final. Às AC, órgãos ou entidades públicas e pessoas jurídicas de direito privado, compete emitir, expedir, distribuir, revogar e gerenciar os certificados de usuários finais. Às AR, entidades operacionalmente vinculadas a determinada AC, compete identificar e cadastrar usuários, na presença destes, e encaminhar solicitações de certificados às AC.

CASTRO (2001) reconhece que o modelo centralizado adotado, vedando a certificação não derivada da AC Raiz, gerou profundas críticas. Nas edições subseqüentes da MP n° 2.200, apesar de mantido o modelo centralizado, único

gerador da presunção de veracidade em relação ao signatário do documento eletrônico, admitiu-se a utilização de outros meios de comprovação de autoria e integridade, inclusive os que utilizem certificados não emitidos pela ICP-Brasil. Outro aspecto digno de menção é a definição de que o par de chaves criptográficas será gerado sempre pelo próprio titular e sua chave privada de assinatura será de seu exclusivo controle, uso e conhecimento.

A Comissão Especial da Câmara dos Deputados aprovou, com várias alterações, o Substitutivo do Relator (Deputado JÚLIO SEMEGHINI), isto já no final de setembro de 2001. A rigor, o novo texto ajustou-se à Medida Provisória da ICP-Brasil, aceitando a autoridade certificadora raiz. Foi criado um credenciamento provisório até a completa operacionalização do modelo da ICP-Brasil.

Considerado resolvido o dilema legal, CASTRO (2001) afirma que o problema da identificação e da integridade dos documentos eletrônicos encontrou solução por meio da assinatura digital, baseada na criptografia assimétrica. "A assinatura digital, vale registrar, é apenas uma das espécies de assinatura eletrônica, abrangente de vários métodos ou técnicas, tais como: senhas, assinaturas tradicionais digitalizadas, chancela, biometria (íris, digital, timbre de voz), entre outras".

5.2 O GED E A CERTIFICAÇÃO DIGITAL NA PMPR

Na consecução do objetivo maior deste trabalho monográfico, utilizou-se por princípio, o estudo das necessidades de informatização de documentos na visão do comando da instituição, comparando-se com a realidade implantada e a visão da Diretoria de Tecnologia da Informação - DTI.

Para chegar à indicação de possíveis usos de documentação eletrônica desenvolveram-se pesquisas bibliográficas e documentais, incluindo legislação e entrevistas, que fundamentam teórica e praticamente a aplicabilidade da tecnologia que envolve o GED.

Como fonte de pesquisa para o levantamento de necessidades institucionais, considerou-se a entrevista às seguintes autoridades:

- Comandante-Geral da PMPR, Cel. QOPM DAVID ANTÔNIO PANCOTTI;

- Chefe do Estado-Maior e Subcomandante da PMPR, Cel. QOPM JOSÉ PAULO BETTES;
- Diretor de Tecnologia da Informação da PMPR, Maj. QOPM LOEMIR MATTOS DE SOUZA;
- Diretor do Departamento de Informática do TJPR, GESLER LUIS BUDEL;
- Analista de Informática da CELEPAR, STEFANO KUBIÇA.

Todo o texto apontado de agora em diante reflete a análise e as opiniões pessoais dos entrevistados. Estas entrevistas transcorreram de maneira muito informal, o que possibilita apresentar a idéia de todos, consolidadas em um entendimento pessoal por parte do autor deste trabalho, assumindo desta forma qualquer má interpretação observada no decorrer das entrevistas ou da pesquisa, que aproveitou material disponibilizado pelos entrevistados e outros colaboradores.

Não há que se falar em certificação eletrônica sem se pensar em GED. Nesse contexto todas as instituições consultadas possuem ou fornecem o desenvolvimento de soluções corporativas para o tratamento eletrônico das informações pertinentes à sua área de atuação.

A CELEPAR desenvolve soluções para os órgãos do poder executivo ,dentre elas a INTRANET do Estado, com todo o aparato de equipamentos de rede, servidores, e programas necessários, sendo o órgão responsável por sua administração e controle.

O TJPR possui estrutura própria, com quadro funcional e desenvolvimento próprio de sistemas, possuindo o JUDWIN que automatiza toda a documentação processual elaborada pelos cartórios das diversas varas da justiça espalhadas pelo Estado do Paraná. Possui, ainda, solução de EDMS (GED para desenhos em CAD) para o controle informatizado do Departamento de Engenharia e Arquitetura, além do inovador AUDIÊNCIA DIGITAL, que registra em vídeo e áudio as audiências judiciais, na maioria das vezes, sequer necessitando degravação de seu conteúdo.

A PMPR possui o SisCOp, ferramenta desenvolvida na Corporação, em substituição ao anterior Sistema de Despacho de Viaturas – SDV, o qual era fornecido e manutenido pela CELEPAR. Outras soluções são utilizadas em parceria com diversos órgãos do governo, os quais, por muitas vezes permitem o acesso da PMPR a suas bases de dados, buscando informações das mais variadas, como por

exemplo: multas, condutor, veículos, pessoas procuradas, pessoas desaparecidas, licitações, pregão eletrônico, META4 dentre outros.

A Polícia Civil - PC, mesmo não tendo sido incluída no roteiro de pesquisa possui sistema informatizado para tratamento eletrônico de seus documentos, sendo possível a elaboração de Inquéritos Policiais além de boa parte de seu serviço cartorial em meio digital.

O Boletim Único, que trataria com um único registro todo o encaminhamento de ocorrências policiais é algo que vem sendo trabalhado e, apesar de alguns adiamentos, deverá logo entrar em operação facilitando o tratamento de informações inter-organizacional. Pretende-se que a ocorrência uma vez iniciada, por exemplo na PMPR, tenha seu encaminhamento à PC, possibilitando o acompanhamento do Ministério Público e Poder Judiciário em qualquer fase do processo, centralizando a informação em um banco de dados padronizado e disponibilizado simultaneamente a todos os órgãos.

O estreito relacionamento entre TJ e órgãos da SESP facilita o desenvolvimento de novas rotinas de trabalho, evitando-se dessa forma a realização de tarefas duplicadas. Um exemplo desse relacionamento que vem facilitando o acesso à informação por vários órgãos, incluindo-se a PMPR, é a liberação de acesso aos antecedentes criminais por parte do TJ. Isso evita, por exemplo que cerca de 150.000 certidões de antecedentes criminais sejam cadastradas, economizando-se um volume de trabalho que, com o efetivo atual da Vara de Execuções Penais e Delegacia de Vigilância e Capturas, levaria aproximadamente seis meses de trabalho continuado.

Forte indício de que em breve a certificação digital será rotina em órgão públicos, percebe-se na utilização do serviço denominado como MALOTE DIGITAL, onde o TJ encaminha todo o processo em rede informatizada às instâncias superiores, que ao receberem fazem a importação de dados para os seus sistemas.

STEFANO KUBIÇA lembra que para tratar da Certificação Digital no Estado do Paraná, em março de 2003 foi criado o Grupo de Trabalho (GT) Pagamento Eletrônico e Certificação Digital. Este grupo é composto por representantes de todos os órgãos de Governo e tem como objetivo planejar e coordenar ações visando viabilizar o pagamento eletrônico dos serviços prestados pelo Governo Estadual na Internet e a utilização de certificação digital. A proposta de trabalho do grupo inclui reuniões mensais.

No Paraná como um todo, os órgãos estaduais ainda não estão utilizando serviços de certificação digital, assinatura eletrônica e tempestividade digital de forma efetiva e sistematizada. A Companhia de Informática do Paraná, a CELEPAR, está em fase de estruturação e capacitação técnica para atender às demandas do governo. Aguarda-se a disseminação das novas tecnologias. Tem-se como previsão o desenvolvimento das primeiras aplicações ainda neste ano de 2005 e o início de operações a partir do ano que vem. Para isso, o grupo de trabalho de governo eletrônico, que trata da certificação digital, está definindo políticas, padrões, forma de viabilização e diretrizes para o marco regulatório. Acredita-se que uma vez definidos esses padrões, os demais órgãos ainda alheios ao processo, sejam convocados a colaborar. As definições têm como referência as diretrizes do Instituto de Tecnologia da Informação - ITI, órgão ligado à Presidência da República. Baseado nessas definições, a CELEPAR está desenvolvendo uma proposta para internalização de assinatura, certificação e tempestividade digital no âmbito da administração pública estadual, através de palestras e cursos, elaboração de cartilhas e vídeo, e a viabilização de infra-estrutura KUBIÇA (2005).

Sabe-se que referente ao embasamento legal, já existe legislação federal regulamentando o assunto. A Medida Provisória 2.200-2/2001 instituiu a Infra-estrutura de Chaves Públicas (ICP-Brasil) que garante equivalência entre um documento eletrônico com assinatura digital e um documento em papel com assinatura manuscrita. No Congresso Nacional, tramita o projeto de lei 7.316 que deverá substituir a MP 2.200-2, trazendo uma série de inovações, entre elas a possibilidade de utilização de documentos de habilitação e identificação eletrônicos, como passaporte, RG e carteira de habilitação.

Como exemplo de uso por órgãos públicos da certificação digital, apesar de não estar no Paraná, cita-se a Secretaria da Receita Federal do Ministério da Fazenda, que já instituiu o e-CPF, Cadastro de Pessoa Física Eletrônico, podendo ser apresentado como comprovante de inscrição, em conformidade com a Instrução Normativa SRF n° 461/2000. Este e-CPF foi apresentado na FIGURA 7, com ele o contribuinte realiza uma série de procedimentos a partir do computador de casa, sem fila, como a consulta de sua situação cadastral e emissão de certidões no *site* da Receita Federal, pedidos de Redarf, utilização do Siscomex, credenciamento no ProUni, peticionamento eletrônico, escrituração fiscal para as Secretarias de Fazenda, entre outros serviços.

Objetivando identificar o grau de importância e apontar as principais características na implantação de base de dados, com vista à informatização de procedimentos, os entrevistados pertencentes à PMPR preencheram questionários que se encontram transcrito como anexo deste trabalho.

Na primeira pergunta, era solicitado que se atribuísse valoração do grau de importância às bases de dados, dentro da seguinte escala:

1 Grande;

2 Média;

3 Pequena;

4 Nenhuma.

Em resumo às respostas apontadas, temos o seguinte quadro:

QUADRO 3: IMPORTÂNCIA PARA IMPLANTAÇÃO DE BASE DE DADOS.

		CG	EM	DTI	Média
1	Cadastro de Pessoal	1	1	1	1,0
2	Relatórios Adm. Mensais (Séc. do EM, Frota, Armas, etc.)	1	1	1	1,0
3	Boletim de Ocorrência	1	1	1	1,0
4	Procedimentos Administrativos (IPM, CD, CJ, Sind.)	2	2	1	1,7
5	Boletim do Cmdo-Geral	3	1	1	1,7
6	Diretrizes	1	2	3	2,0
7	Legislação	1	2	3	2,0
8	Procedimentos Operacionais	2	1	3	2,0
9	Estudos de Caso	2	2	3	2,3
10	Ordens de Serviço	3	2	2	2,3
11	Editais (concursos em geral)	4	2	1	2,3
12	Planos de Operações	3	3	2	2,7
13	Diário Oficial do Estado	4	3	3	3,3

FONTE: Pesquisa de campo.

Pela análise da questão colocada, optou-se por dividir a resposta em quatro grupos, ordenados crescentemente pela média, em seguida pela nota atribuída pelo CG e em seguida pela nota atribuída pelo Ch. EM. Os itens estão agrupados na seguinte ordem: Grupo 1, itens 1 a 4; Grupo 2, itens 5 a 8 e Grupo 3, itens 9 a 13.

Percebe-se na PMPR, como na iniciativa privada, a importância da base de dados cadastrais, estando em primeiro lugar o cadastro de pessoal, ponto nevrálgico dentro do Estado, pois com suas informações, torna-se possível a identificação, localização de pessoal além do cálculo da folha de pagamento.

O cadastro de pessoal envolve um número muito grande de pessoas, não é à toa que uma primeira iniciativa de implantação de solução completa em GED se deu na Diretoria de Pessoal. Essa implantação ocorreu em um processo lento e bastante complexo, pois envolvia o escaneamento de fichas individuais para posterior controle e manutenção informatizados. Como já fora levantado anteriormente, a preparação de documentos é tarefa bastante trabalhosa e que não deve ser abandonada, mesmo com os mais modernos sistemas automatizados. A dificuldade de implantação, constantes mudanças no quadro funcional e a demora em produzir resultados, levou este processo à sucumbência, sendo substituído por uma solução vinda da Secretaria de Estado da Administração e Previdência. A Solução apresentada pelo META4 não permite que sejam deixados de lado o registro histórico que, atualmente encontra-se em papel. Os arquivos de pastas suspensas são enormes e seu manuseio é diário.

Investigando um pouco mais as respostas, vêem-se três pontos tidos como prioritários nos assuntos seguintes:

- Relatórios Administrativos Mensais;
- Boletim de Ocorrência; e
- Procedimentos Administrativos.

O Boletim de Ocorrência encontra-se em processo parcialmente informatizado dentro do SisSOp, trata-se do efetivo serviço da PMPR, disponível 24 horas por dia e 7 dias por semana para atender à população. Sem esse controle informatizado, seria impossível responder aos 12.000 chamados diários feitos através de ligações telefônicas para o n° 190 ou chamando-se diretamente um policial-militar. Este tema já foi tratado quando se falou do Boletim Único, sendo identificado não só pela PMPR, mas também pelos demais órgãos que integram o conceito de defesa social como uma grande prioridade a ser implantada no serviço público como um todo.

Nos quatro itens identificados com maior grau de importância, para a implantação de base de dados, sabe-se já existir informatização, no entanto, também é sabido que sistemas estanques não atendem o volume de informação que nos é ofertado diariamente.

Aprofundando a análise percebe-se a necessidade e conscientização por parte da PMPR do controle externo da polícia, da prioridade em bem administrar serviços e informações que, como veremos a seguir tomam destino a outros órgãos.

QUADRO 4: CARACTERÍSTICAS PRINCIPAIS PARA IMPLANTAÇÃO DE BASE DE DADOS.

		Informatizado Confecção	Informatizado Distribuição	Merece Distribuição	Segue outro Orgão	Data Atualização Importante	Soma
1	Cadastro de Pessoal	3	3	3	3	3	15
2	Relatórios Adm. Mensais (Sec do EM, Frota, Armas, etc.)	3	3	3	2	3	14
3	Boletim de Ocorrência	3	3	3	3	2	14
4	Procedimentos Adm. (IPM, CD, CJ, Sind.)	3	3	3	2	3	14
5	Procedimentos Operacionais	3	3	3	1	3	13
6	Legislação	3	3	3	1	3	13
7	Diretrizes	3	3	3	0	2	11
8	Boletim do Cmdo-Geral	3	3	3	0	2	11
9	Planos de Operações	3	2	3	0	2	10
10	Ordens de Serviço	2	3	3	0	2	10
11	Editais (concursos em geral)	2	2	2	2	2	10
12	Estudos de Caso	2	3	3	0	1	9
13	Diário Oficial do Estado	0	0	0	0	1	1

FONTE: Pesquisa de campo.

O QUADRO 4: CARACTERÍSTICAS PRINCIPAIS PARA IMPLANTAÇÃO DE BASE DE DADOS, apresenta, propositadamente uma relação com o ciclo de vida de um documento e com a idéia de identificar se a tempestividade digital é algo importante no trato das informações da PMPR.

A classificação dos assuntos dentro do quadro atendeu ao seguinte de escalonamento vertical: ordem decrescente somando-se o número de respostas obtidas por cada um dos entrevistados, em seguida mantendo a ordem decrescente, ordenação nos quesitos distribuição e informatização. A Opção pelo quesito distribuição se deve pelo fato de a disponibilização da informação ser até mesmo uma exigência para a implantação de programas de qualidade. Os itens estão agrupados na seguinte ordem: Grupo 1, itens 1 a 4; Grupo 2, itens 5 a 8 e Grupo 3, itens 9 a 13.

A relação que se estabelece entre o ciclo de vida de um documento, a tempestividade digital e o questionário, está esclarecida no quadro que segue:

QUADRO 5: RELAÇÃO DO QUESTIONÁRIO COM O CICLO DE VIDA DE UM DOCUMENTO.

CICLO DE VIDA DE UM DOCUMENTO	QUESTIONÁRIO
PESQUISA e AUTORIA	INFORMATIZADO CONFECÇÃO
APROVAÇÃO	SEGUE OUTRO ORGÃO
PUBLICAÇÃO	INFORMATIZADO DISTRIBUIÇÃO e MERECE DISTRIBUIÇÃO
TEMPESTIVIDADE DIGITAL	DATA ATUALIZAÇÃO IMPORTANTE

FONTE: Pesquisa de campo.

Comparando-se os quadros 3 e 4 percebem-se duas coincidências:

1 - Os quatro primeiros itens (Grupo 1) se repetem sem diferença alguma, apontando para a seguinte conclusão: a priorização de implantação de base de dados ou soluções GED com certificação digital obedece aos critérios que envolvem o trâmite dos documentos.

2 – No Grupo 2, os itens são idênticos em ambos os quadros, alternando-se apenas sua ordem dentro do grupo, possibilitando a análise de que todos os entrevistados estabeleceram uma coerência lógica para responder às duas questões apresentadas.

Percebe-se, ainda, que no primeiro grupo aparecem assuntos que têm relacionamento com a visão comunitária da PMPR, o atendimento ao público e o resultado do seu trabalho. No segundo grupo, estão temas que fazem referência à normatização da atividade policial e a distribuição do Boletim do Comando-Geral, não menos prioritárias para a implantação de GED.

6 CONCLUSÕES E SUGESTÕES

6.1 CONCLUSÕES

É inquestionável o importante papel na história das civilizações que os documentos sempre tiveram. Isso é comprovado, por exemplo, pelas escritas arqueológicas que relatam os costumes e a vida de variadas sociedades ancestrais. Não fossem por esses testemunhos físicos, talvez ainda hoje não se conheceria nada a respeito da existência dos povos antigos.

Muito oportunamente STEFANO KUBIÇA lembra que no Brasil, a utilização do processo eletrônico em substituição ao analógico, caminha a passos largos. O sistema bancário brasileiro é um dos mais avançados do mundo no processo de transações financeiras via Internet, por cujo meio se propagam vários tipos de comércios e serviços similares à certificação. Também no setor público, o Brasil já está exportando tecnologia. O voto eletrônico é um bom exemplo. Até os norte-americanos vêm aqui para aprender. Hoje, mais de 90% dos contribuintes brasileiros fazem suas declarações de renda pela Internet. Superadas algumas barreiras de ordem cultural, a resistência natural do ser humano dificulta as mudanças A assinatura, certificação e tempestividade digital deverão aos poucos mudar a forma como as pessoas, empresas, organizações e governos se relacionam.

Atualmente, a documentação eletrônica é uma realidade global. Os documentos tomaram diferentes formas e padrões, mas continuam mantendo a sua função principal de registrar o conhecimento humano sobre um assunto específico. Por diversos meios multimídia, por meios de comunicação, por meio dos computadores, rede que os interliga e softwares adequados, é possível a publicação de informações de forma quase instantânea, na medida em que elas vão sendo geradas, por exemplo, a transmissão em tempo real das diversas sessões das CPIs que se instalaram no Congresso Nacional. Este avanço não retrata apenas a característica de eficiência dos sistemas de computador e outros meios eletrônicos em publicar ou divulgar a informação, mas também reflete a idéia de fazer com que outras pessoas desfrutem das informações distribuídas de forma rápida e simples.

O melhor exemplo deste aspecto é a World Wide Web (WWW), junto com o conjunto de tecnologias associadas que permitem o seu acesso e utilização (web browsers, servidores de aplicações, repositório de dados distribuído, programas Java etc.).

Ao se utilizar documentos através de um sistema de informação, é preciso observar dois problemas principais. O primeiro deles é que a informação dos documentos, por possuir uma organização de complexidade variável, não permite o seu acesso de maneira simples através de aplicações diferentes. O segundo problema é que muitos documentos possuem um formato de armazenamento proprietário, comprometendo a sua reutilização e o seu compartilhamento entre os diferentes sistemas. Os documentos são repositórios de dados muito flexíveis, que admitem tanto o armazenamento de dados sem qualquer estrutura lógica quanto o armazenamento de dados mais complexos. Pode-se concluir que o excesso de informação pode ser danoso se ela não for bem administrada.

Uma grande quantidade de produtos e tecnologias variadas dominam o segmento, e como os computadores são vistos como ferramentas com capacidade de produzir algo mais do que documentos em papel, os produtores de software estão competindo entre si para integrar capacidades de autoria de documentos nos seus produtos. O mercado de produção de software de Gerenciamento Eletrônico de Documentos é um dos mais complexos e voláteis da indústria da computação. Essa volatilidade já foi abordada anteriormente, impedindo a apresentação de determinada solução mercadológica para suprir a necessidade da PMPR. Como a compra não se dará de agora até o final de 2006, não há o que se apresentar, visto que o mercado se atualizará e poderemos encontrar uma nova geração de produtos quando houver disponibilização orçamentária. Nessa linha de pensamento, resta também a certeza de que o Estado do Paraná precisa estabelecer padrões que permitam a interoperabilidade de sistemas, já que nenhum órgão poderá trabalhar isoladamente em um mundo globalizado ou na Sociedade do Conhecimento. Por interoperabilidade entenda-se a capacidade de seus sistemas e de seus computadores falarem entre si, trocarem informações entre si.

Um sistema GED atende às exigências de programas de certificação, como ISO 9000, que cobra controle efetivo dos documentos e processos, justificam-se ou viabilizam-se ainda, a implantação de projetos desse tipo a partir da preocupação com segurança, redundância e em especial a proteção contra catástrofes além

disso, em arquivos eletrônicos é mais simples o procedimento de criação de cópias de segurança.

A possibilidade de aumento da produtividade e competitividade é intrínseca a sistemas GED, pois as mídias analógicas (papel e microfilme) são mídias que em situações de freqüente acesso não conseguem trazer ganhos de produtividade aos processos tradicionais. A passagem de documentos para o meio eletrônico foi um passo natural, as pessoas estão aprendendo a gerenciar os documentos e informações eletronicamente, facilitando assim, a sua rotina de trabalho com consideráveis ganhos de produtividade.

No entanto, para uma implantação de um projeto de gerenciamento eletrônico eficaz, e verdadeiramente produtivo, deve-se começar a partir de um estudo criterioso das reais necessidades da PMPR, dos usuários e das perspectivas em vista. O Estado do Paraná possui um grupo de trabalho que estuda o assunto; as diretrizes do Governo do Estado para a informática pública estadual defendem soluções corporativas preferencialmente em software livre. O problema está na ausência de coordenação, harmonização e padronização dos múltiplos sistemas em operação. Pensando nisso, eventuais iniciativas tratadas isoladamente devem obedecer à orientação do Cosit.

No mundo da tecnologia da informação, não existem fórmulas padronizadas que atendam a 100% das expectativas e necessidades apresentadas pelos usuários, prova disso é a morosa implantação do META4, especialmente para a PMPR que possui características atípicas e peculiares, diferindo de tudo o que se conhece no mundo empresarial.

Toda mudança gera alguns transtornos, prescinde de fases de adaptação, porém pode ser tranqüila quando se leva em conta as particularidades de cada projeto, evitando, assim, surpresas desagradáveis tais como: objetivos não atendidos, incompatibilidades com a plataforma existente, falta de precisão no núcleo do projeto, etc. O que preocupa é que estas surpresas podem gerar imagens negativas para as soluções de GED, por passar a imagem de que esta tecnologia não atende às necessidades da instituição. O insucesso inicial de um projeto deve ser medido, sua continuidade é fundamental, passa a ser um compromisso com o erário público.

JOAQUIM FALCÃO, mestre em direito pela Universidade Harvard, diretor da Escola de Direito da Fundação Getúlio Vargas do Rio de Janeiro, professor de

direito constitucional da UFRJ e grande defensor da desburocratização do poder público, afirma que existe desafio latente e crescente que não se pode mais adiar para os governos. Trata-se da interoperabilidade de sistemas de informática. Os sistemas das polícias estaduais precisam falar entre si. Os tribunais estaduais falar com os tribunais superiores. E estes entre si. Este desafio implica duas conseqüências. Por um lado, faria, é verdade, o Estado mais poderoso e eficiente, com maior capacidade para cumprir as leis e fazê-las cumprir pelos cidadãos. Cresceria a eficiência dos poderes públicos para "fiscalizar" a sociedade. Por outro lado, traria inegáveis vantagens para todos. Acrescenta-se ao seu pensamento o controle externo sobre as polícias, a continuidade do serviço iniciado por determinado órgão, o atendimento mais eficiente ao cidadão que não verá uma repetição de esforços por todos os órgãos por que passa atualmente. Imaginem as vantagens para o motorista se os DETRANs estaduais falassem entre si. A carteira de motorista poderia ser tirada em qualquer Estado e não apenas, como hoje, no Estado original. O controle de veículos roubados seria muito maior. Imaginem se os computadores das secretarias de segurança estaduais e a polícia federal falassem entre si. A captura de criminosos seria muito mais agilizada.

A segurança do cidadão seria reforçada. Imaginem se os tribunais falassem entre si. As partes poderiam acompanhar os processos em primeira, segunda e terceira instância através de um único sistema operacional. Os custos do acesso à justiça diminuiriam. Os exemplos são infindáveis, assegura Falcão.

6.2 SUGESTÕES

A Sociedade do Conhecimento nos traz a convicção de que a adoção da tecnologia de Gerenciamento Eletrônico de Documentos envolve várias mudanças, entre elas culturais e filosofia de trabalho. Esses tópicos carecem de estudos aprofundados a fim de se diagnosticarem os motivos que levam as pessoas a demonstrarem resistência quando se trata de novas tecnologias. As conseqüências em não-adesão a inovações tecnológicas, testadas e validadas em um mundo globalizado, impedem o crescimento local, deixando para trás organizações que não se atualizam à era do conhecimento.

Diante destas considerações, ousa-se apresentar assuntos para projetos futuros que visem a implantação de sistemas corporativos, baseados ou não em GED, Certificação Digital, dentre outros. Apresentam-se também idéias de como tratar o assunto "Tecnologia da Informação" dentro da PMPR:

- Um desafio a ser alcançado seria a criação de um modelo que indicasse quais os itens que contribuem no custo do gerenciamento de documentos, e, quanto representa financeiramente os benefícios alcançados com a implantação do GED.
- Estudo das resistências e mudanças no comportamento das pessoas, fator que determinará um processo mais lento na implantação de qualquer tecnologia, podendo servir de base inclusive para soluções para a gestão de pessoas, contribuindo ainda, para que este processo seja facilitado nas futuras implantações.
- Estudo de viabilidade para implantação de programas de qualidade, principalmente aqueles que exigem normatização de procedimentos e revisão de processos organizacionais.
- Definição de equipe multidisciplinar que busque a padronização de procedimentos automatizados para implantação de documentação eletrônica nas diversas áreas de atuação da PMPR. Esta padronização poderá servir de base para orientar o desenvolvimento de soluções, preferencialmente em software livre, ou a aquisição de soluções completas.
- Manter constante elo de contato técnico-profissional com os órgãos envolvidos na defesa social, além da CELEPAR, com o objetivo específico de se alcançar a interoperabilidade de sistemas.
- Analisar o emprego de profissionais de segurança pública como administradores, gestores, desenvolvedores ou técnicos dentro da DTI.
- Analisar o aspecto do fornecimento de sistemas por terceiros, estabelecendo quanto representa financeiramente os benefícios entre desenvolvimento próprio, aquisição de produtos prontos, desenvolvimento de soluções específicas por parte da CELEPAR ou de outra empresa terceirizada.

GLOSSÁRIO

Ad-Hoc	Não estruturado.
API	Application Programming Interface. A Interface de Programação de um Aplicativo é um conjunto ou biblioteca de rotinas e/ou funções que podem ser utilizadas por outro aplicativo.
ASCII	American Standard Code for Information Interchange. Formato padrão para geração de arquivo de dados em microcomputadores, um sistema largamente usado para codificação de cartas, algarismos, pontuação, marcas e sinais como números binários.
ASP	Application Service Providers. Provedor que gerencia e distribui serviços e soluções com base em software para clientes por meio de uma WAN ou de uma central de dados. Na essência, ASP é uma maneira de as companhias terceirizarem parte ou todos os aspectos neces sários a sua área de tecnologia de informação.
Autocad	Software de desenvolvimento de projetos de engenharia.
Autoridade certificadora	Uma AC (Autoridade Certificadora) é a empresa que emite um Certificado Digital para você. A sua AC pode ser a empresa para a qual você trabalha ou uma empresa que você paga para emitir Certificados Digitais.
Backbone	Espinha dorsal. Principal caminho das transmissões enviadas pela Internet, de onde derivam as ramificações.
Backup	Procedimento de cópia de segurança dos dados armazenados.
Batch	Em lote, conjunto de programas processados consecutivamente pelo sistema operacional de um microcomputador.
Binário	Pertencente a um sistema de números com uma base de dois.
Bit	Binary digit, representa o código binário (0 ou 1) com que o computador funciona.
Bookmark	Lista de Tarefas.
Browser	Programa para navegar na Internet.
Business intelligence	É a utilização de uma séries de ferramentas para coletar, analisar e extrair informações, que serão utilizadas no auxílio ao processo de gestão e tomadas de decisão de empresas e organizações. Esse nome foi escolhido como metáfora das decisões governamentais baseadas em espionagem e análise de dados (caso da CIA)
Byte	Conjunto de oito Bits.
CALS	Computer-Aided Acquisition and Logistics Support. Uma iniciativa do Departamento de Defesa Norte-Americano para auxiliar o intercâmbio eletrônico dos documentos de engenharia entre os contratantes e as agências governamentais.
Cartão-janela	Cartão com uma ou mais aberturas projetadas especificamente para a instalação ou inserção de microfilme antes ou após o GED.

Chip	Circuito eletrônico produzido em uma pastilha de silício. O chip mais importante presente no micro é o processador, que funciona como se fosse o "motor" do computador.
Coopers & Lybrand	Empresa de consultoria e auditoria, com escritórios em várias cidades do mundo.
Data entry	Entrada de dados (captação dos dados e sua entrada no computador).
Data mining	O Data Mining é um processo de garimpo para a formulação de teorias e modelos. É uma inferência sobre a realidade. Ele analisa uma grande quantidade de dados provenientes do Data Warehouse. Este processo analisa os dados de forma a fornecer modelos e correlações que não poderiam ser conseguidos de outra forma.
Data warehouse	Armazém de dados, sistema que guarda e organiza todas as informações espalhadas pelos vários sistemas dentro de uma empresa. Termo genérico para um tipo de banco de dados que consiste num sistema de armazenamento, recuperação e gerenciamento de grandes quantidades de quaisquer tipos de dados. Os softwares da espécie freqüentemente incluem sofisticadas técnicas, inclusive de compactação, para buscas mais rápidas de dados, assim como filtros avançados.
Digitalizar	Utilizar scanner para converter documentos em imagens eletrônicas codificadas digitalmente.
Disco	Mídia de gravação.
Disco magnético	Disco com superfície magnética na qual podem ser armazenados dados pela magnetização de áreas de sua superfície.
Disco óptico	Mídia que aceita e mantém informações sob a forma de marcas numa camada de gravação que pode ser lida com um raio óptico.
Disco óptico regravável	Disco óptico em que são gravados os dados, que podem ser excluídos, posteriormente, para que outros dados sejam gravados.
DLL	dynamic link library. Biblioteca de funções usada em desenvolvimento de software
Document Imaging	Tecnologia de gerenciamento de documentos estáticos.
Drive	Leitor de discos.
E-commerce	Comércio Eletrônico. Atividade comercial que acontece por processos digitais através de uma rede. Boa parte das novas transações empresa-empresa e empresa-consumidor está se efetuando pela Internet.
Escaner	Scanner, dispositivo que converte de maneira eletro-óptica um documento em códigos binários (digitais) pela detecção e medida da intensidade da luz refletida ou transmitida.
Extranet	Muito similar a uma Intranet com o recurso adicional de que a informação contida pode ser acessada externamente por parceiros de negócios.

Firewall	Um sistema de segurança (hardware e/ou software) cujo principal objetivo é filtrar os acessos a uma rede. As empresas utilizam o firewall para proteger as suas redes internas conectadas à Internet contra a entrada de pessoas não autorizadas. (Hackers). Existem diversas tecnologias possíveis para a construção de um Firewall. Atualmente na 4.a geração, estão se transformando em SECURITY APPLIANCES, com hardware específico, para se conseguir velocidade e confiabilidade.
Groupware	Software que permite que um grupo de usuários em uma rede colabore num determinado projeto; incorpora e-mail, desenvolvimento colaborativo de documentos, programação e rastreamento
Hash	Termo que se refere a resumo da mensagem (palavra original da língua inglesa).
Hipertexto	Ligação de texto com outros documentos contendo mais informações sobre o mesmo tópico ou sobre tópico correlato
Home page	Página publicada na Internet.
Host	Um computador que oferece serviços especiais aos usuários
HTML	HyperText Markup Language. É um conjunto de especificações (símbolos) que determinam como o browser irá formatar o texto, e qual a função que cada pedaço do texto terá no documento Web.
ICP-Brasil	É um conjunto de técnicas, práticas e procedimentos, a ser implementado pelas organizações governamentais e privadas brasileiras com o objetivo de estabelecer os fundamentos técnicos e metodológicos de um sistema de certificação digital baseado em chave pública.
Imagem	Representação digital de um documento
Imaging	Processo de capturar, armazenar e retirar documentos independentemente do formato original, utilizando micrografia e/ou imaging eletrônico.
Indexação	Numa solução de imagens, indica a criação de índices que permite recuperar um documento armazenado em discos ópticos.
Interface	Em termos genéricos, uma interconexão comum entre dois componentes ou algum conjunto de instruções comuns que são compartilhados por dois ou mais programas.
Intranet	Rede projetada para organizar e compartilhar informações, e realizar transações digitais dentro de uma empresa. A intranet emprega aplicativos associados à Internet, tais como páginas WEB, browsers, e-mail, news groups e mailing lists, mas só é acessível aos que fazem parte da organização.
ISO	International Organization for Standardization. Organização Internacional de Normas.
ISO 9000	Série de normas do tipo procedimento que incluem diretrizes e modelos para a garantia da qualidade.
Java	Linguagem de programação

JDBC	Componenete para banco de dados interligados na linguagem JAVA
Jukebox	Dispositivo para acomodar diversos discos ópticos para acesso por meio de um sistema de computador.
Lap-top	Computador portátil.
Link	Ligação entre 2 grupos de arquivos de dado de modo que ambos se atualizarão ao mesmo tempo.
META4	Empresa responsável pelo desenvolvimento de solução informatizada para a gestão de pessoas e folha de pagamento dentro da Secretaria de Estado da Administração e Previdência. A Meta4 é um dos principais fornecedores mundiais de soluções para gestão de capital humano e intelectual.
Mídia	Meio físico para armazenar informações ou distribuí-las.
MS-Office	Pacote de ferramentas de automação de escritório, da Microsoft.
MS-Word	Editor de textos da Microsoft.
Pixel	Picture element, menor elemento da imagem digital.
Plugin	Extensões das funcionalidades dos browsers, oferecendo recursos adicionais de multimídia.
RAID	Redundant array of inexpensive or independent discs. Conjunto de discos rígidos interdependentes.
Raster	Descrição de um conjunto retangular ou quadrado formado por várias linhas de digitalização horizontais com diversos elementos da figura.
Rede	Caminho de comunicações entre computadores ou entre terminais e computadores.
Roteador	Dispositivo responsável pelo encaminhamento de pacotes de comunicação aos seus destinatários em uma rede ou entre redes, selecionando a rota mais eficiente disponível no momento.
Sistema	Coleção organizada de hardware, software, telecomunicações, suprimentos, pessoas, manutenção.
Sistemas estanques	Sistemas que não compartilhavam as informações.
Site	Site web.
Site web	Endereço da World Wide possuído e controlado por uma pessoa ou organização.
TCP/IP	Transmission Control Protocol/Internet Protocol. Conjunto de padrões da Internet que orienta o tráfego de informações e define o endereçamento e o envio de dados.
TIFF	Tag Image File Format. Alguns consideram como o padrão de fato para representação de imagens em bits.
Trilha	Caminho percorrido pelo raio laser de gravação ou leitura.
Web browsers	Browser. Programa para navegar na Internet.
Web	World Wide. Internet
Workflow	Fluxo de documentos em processos diversos, podendo ser eletrônico ou manual. Processo que permite o controle eletrônico do fluxo de documentos dentro de uma organização.

World Wide Web	Internet
World Wide	World Wide Web. Internet
WORM	Write Once Read Many. São os discos ópticos que são gravados por drives especiais e apenas podem ser lidos.
XML	Extensible Markup Language. Uma linguagem mais estruturada para representação de dados na Web, é utilizado na Internet e suporta uma grande variedade de aplicações.

REFERÊNCIAS

AIIM INTERNATIONAL. **Home page da AIIM INTERNATIONAL**. Disponível em: <http://www.aiim.org.> Acesso em 25 ago. 2005.

AIIM INTERNATIONAL. **Introduction to DMA.** Disponível em: <http://nfocentrale.net/dmware/> Acesso em 25 ago. 2005.

ANDRADE, Marcus Vinicius Mendonça. **Gerenciamento eletrônico da informação: ferramenta para a gerência eficiente dos processos de trabalho.** Niterói. 2002. 16 f. p. Núcleo de Documentação - Universidade Federal Fluminense.

BARROS, Augusto Quadros Paes de. **Criptografia e certificação: ferramentas úteis, mas pouco conhecidas**. 2004. Disponível em: <http://www.infoguerra.com.br/infonews/viewnews.cgi?newsid1094136453,57872,#> Acesso em 02 nov. 2005.

BRASIL, Angela Bittencourt. **O documento físico e o documento eletrônico.** Jus Navigandi, Teresina, a. 4, n. 42, jun. 2000. Disponível em: <http://www1.jus.com.br/doutrina/texto.asp?id=1781>. Acesso em 25 ago. 2005.

CASTRO, Aldemario Araujo. **O documento eletrônico e a assinatura digital. Uma visão geral.** Jus Navigandi, Teresina, a. 6, n. 54, fev. 2002. Disponível em: <http://www1.jus.com.br/doutrina/texto.asp?id=2632>. Acesso em: 05 ago. 2005.

CENADEM. **Home page do Centro Nacional de Desenvolvimento do Gerenciamento da Informação.** São Paulo. Disponível em: <http://www.cenadem.com.br> Acesso em 25 ago. 2005.

COSTA, Vanessa. et al. **Protocolação digital de documentos eletrônicos**. Florianópolis: Laboratório de Segurança em Computação. Universidade Federal de Santa Catarina. 2003. Disponível em: <http://www.bry.com.br/downloads/artigo/Protocolacao%20Digital%20de%20Documentos%20Eletronicos.pdf > Acesso em: 02 nov. 2005.

D'ALLEYRAND, Marc R. **Workflow em Sistemas de Gerenciamento Eletrônico de Imagens**. São Paulo: Cenadem, 1995.

FANTINI, Sérgio Rubens. **Aplicação do gerenciamento eletrônico de documentos: estudo de caso de escolha de soluções**. Florianópolis, 2001. 118 f. p. Dissertação (mestrado em Engenharia de Produção, especialidade em Inteligência Aplicada) - Programa de Pós-Graduação em Engenharia de Produção da Universidade Federal de Santa Catarina.

FERREIRA, Aurélio Buarque de Holanda. **Novo dicionário da língua portuguesa.** 2. ed. rev. Rio de Janeiro: Nova Fronteira, 1996, p. 605.

FRUSCIONE, James. **Workflow automatizado: como desenvolver projetos gerais e planejamento de suporte**. São Paulo: Cenadem, 1996.

GANDINI, João Agnaldo Donizeti; SALOMÃO, Diana Paola da Silva et al. **A segurança dos documentos digitais.** Teresina, Jus Navigandi, 2002. Disponível em: <http://www1.jus.com.br/doutrina/texto.asp?id=2677> Acesso em: 05 ago. 2005.

GATES, Bill. **A empresa na velocidade do pensamento: como um sistema nervoso digital**. São Paulo: Companhia das Letras, 1999.

_____. **A estrada do futuro.** São Paulo: Companhia das Letras, 1995.

GRIGSBY, Mason. **COLD – computer output to laser disk.** São Paulo: Cenadem, 1995.

KOCH, Walter W. **Gerenciamento eletrônico de documentos: conceitos, tecnologias e considerações gerais**. São Paulo: Cenadem, 1998.

KOTLER, P. **Administração de marketing: edição do novo milênio.** São Paulo: Prentice Hall, 2000.

KUBIÇA, Stefano. **Certificação Digital: Cartório Eletrônico.** Revista Bate Byte n° 147, Abril, Maio, Junho/ 2005 (a). CELEPAR. Curitiba

_____. **Comprovação Digital: Tempestividade Digital.** Revista Bate Byte n° 147, Abril, Maio, Junho/ 2005 (b). CELEPAR. Curitiba

LIMA NETO, José Henrique Barbosa. **Aspectos jurídicos do documento eletrônico**. Disponível em: <http://www.jus.com.br/doutrina/docuelet.html> Acesso em 25 ago. 2005.

MACEDO, Geraldo Majela Ferreira de. **BASES PARA A IMPLANTAÇÃO DE UM SISTEMA DE GERENCIAMENTO ELETRÔNICO DE DOCUMENTOS – GED ESTUDO DE CASO.** Florianópolis, UFSC, 2003.

MARCACINI, Augusto Tavares Rosa. **A certificação eletrônica na legislação brasileira atual.** 2000, Disponível em: <www.cbeji.com.br/br/novidades/artigos/index.asp?id=1424> Acesso em 02 out. 2005.

_____. **Direito e informática. Uma abordagem jurídica sobre criptografia.** 1ª ed. Rio de Janeiro: Forense, 2002, p. 10.

_____. **O documento eletrônico como meio de prova.** 2000. Disponível em: <http://www.advogado.com/internet/zip/tavares.htm.> Acesso em 02 out. 2005.

Revista Exame Digital. São Paulo: Abril, edição 710, ano 34, n. 6, mar. 2000, p. 113.

SADIQ, W.; ORLOWSKA, M. **Applying a Generic Conceptual Workflow Modeling Technique to Document Workflow**. In: AUSTRALIAN DOCUMENT COMPUTING SYMPOSIUM, 2., 1997. **Proceedings.** Melbourne: [s.n.], 1997.

STRINGHER, Ademar. **Aspectos legais da documentação em meios micrográficos, magnéticos e ópticos**. São Paulo: INIB, 1997.

_____. **Guia Brasileiro de software para gerenciamento eletrônico de documentos e knowledge management**. São Paulo: Cenadem, 1997.

TREVISAN, Antônio Carlos. **Papel ou arquivo eletrônico?** . Jus Navigandi, Teresina, a. 8, n. 482, 1 nov. 2004. Disponível em: <http://www1.jus.com.br/doutrina/texto.asp?id=5850> Acesso em: 05 ago. 2005.

VALLA, Wilson Odirley. **Doutrina de Emprego de Polícia Militar e Bombeiro Militar**. Curitiba: Optagraf Editora e Gráfica Ltda. 1999.

LEGISLAÇÃO

BRASIL. Lei nº 9.983, de 14 de julho de 2000. Altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal e dá outras providências

BRASIL. Medida Provisória nº 2.200-2, de 24 de agosto de 2001. Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, e dá outras providências.

BRASIL. Decreto-lei nº 3.505, de 13 de junho de 2000. Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, e dá outras providências.

BRASIL. Decreto nº 3.872, de 18 de julho de 2001. Dispõe sobre o Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira - CGICP-Brasil, sua Secretaria-Executiva, sua Comissão Técnica Executiva e dá outras providências.

BRASIL. Decreto nº 3.996, de 31 de outubro de 2001. Dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal.
ICP-Brasil. Resolução nº 1, de 25 de Setembro de 2001. Aprova a Declaração de Práticas de Certificação da AC Raiz da ICP-Brasil.

ICP-Brasil. Resolução nº 2, de 25 de Setembro de 2001. Aprova a Política de Segurança da ICP-Brasil.

ICP-Brasil. Resolução nº 3, de 25 de Setembro de 2001. Resolve designar a seguinte Comissão para auditar a Autoridade Certificadora Raiz - AC Raiz e seus prestadores de serviços.

ICP-Brasil. Resolução nº 4, de 22 de Novembro de 2001. Altera a Declaração de Práticas de Certificação da AC Raiz da ICP-Brasil.

ICP-Brasil. Resolução nº 5, de 22 de Novembro de 2001. Aprova o Relatório de auditoria da AC Raiz.

ICP-Brasil. Resolução nº 6, de 22 de Novembro de 2001. Aprova os critérios e procedimentos de credenciamento das entidades integrantes da ICP-Brasil.

ICP-Brasil. Resolução nº 7, de 12 de Dezembro de 2001. Aprova os requisitos mínimos para políticas de certificado na ICP-Brasil.

ICP-Brasil. Resolução nº 8, de 12 de Dezembro de 2001. Aprova os requisitos mínimos para as declarações de práticas de certificação das autoridades certificadoras da ICP-Brasil.

ICP-Brasil. Resolução nº 9, de 12 de Dezembro de 2001. Estabelece regras transitórias para a ICP-Brasil.

ICP-Brasil. Resolução nº 10, de 14 de Fevereiro de 2002. Estabelece as diretrizes da política tarifária da Autoridade Certificadora Raiz - AC Raiz da ICP-Brasil.

ICP-Brasil. Resolução nº 11, de 14 de Fevereiro de 2002. Altera os requisitos mínimos para as políticas de certificado na ICP-Brasil, a declaração de práticas de certificação da AC Raiz da ICP-Brasil, delega atribuições para a AC Raiz e dá outras providências.

ICP-Brasil. Resolução nº 12, de 14 de Fevereiro de 2002. Estabelece regras processuais para credenciamento na ICP-Brasil.

ICP-Brasil. Resolução nº 13, de 26 de Abril de 2002. Altera a declaração de práticas de certificação da AC Raiz da ICP-Brasil, os critérios e procedimentos de credenciamento das entidades integrantes da ICP-Brasil, os requisitos mínimos para as declarações de práticas de certificação das autoridades certificadores da ICP-Brasil, os requisitos mínimos para as políticas de certificado na ICP-Brasil, e dá outras providências.

ICP-Brasil. Resolução nº 14, de 10 de Junho de 2002. Altera os critérios e procedimentos para credenciamento das entidades integrantes da ICP-Brasil e a Resolução nº12, de 14 de fevereiro de 2002, que estabelece regras processuais para credenciamento na ICP-Brasil.

ICP-Brasil. Resolução nº 15, de 10 de Junho de 2002. Estabelece as diretrizes para sincronização de freqüência e de tempo na Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil.

ICP-Brasil. Resolução nº 16, de 10 de Junho de 2002. Estabelece as diretrizes para sincronização de freqüência e de tempo na Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil.

ENTREVISTAS

BETTES, José Paulo. Cel. QOPM. Chefe do Estado-Maior e Subcomandante da PMPR.

BUDEL, Gesler Luis. Diretor do Departamento de Informática do TJPR.

KUBIÇA. Stefano. Analista de Informática da CELEPAR.

PANCOTTI, David Antônio. Cel. QOPM. Comandante-Geral da PMPR.

SOUZA, Loemir Mattos de. Maj. QOPM. Diretor de Tecnologia da Informação da PMPR.

ANEXOS

ANEXO 1 - Questionário para Comandantes

1 - Qual a importância que se atribui para a implantação das seguintes bases de dados:

Escala: 1-Grande 2-Média 3-Pequena 4-Nenhuma

( ) Procedimentos Operacionais
( ) Cadastro de Pessoal
( ) Diretrizes
( ) Estudos de Caso
( ) Planos de Operações
( ) Ordens de Serviço
( ) Diário Oficial do Estado
( ) Boletim do Cmdo-Geral
( ) Legislação
( ) Editais (concursos em geral)
( ) Relatórios Adm. Mensais (Sec do EM, Frota, Armas, etc.)
( ) Boletim de Ocorrência
( ) Procedimentos Administrativos (IPM, CD, CJ, Sind.)
( ) Outras Descrever: _____

_____

_____

2 - Para análise de viabilidade de implantação se faz necessário identificar para cada um dos tópicos acima, suas características principais. Marque com "X" a coluna correspondente a cada informação.

	Informatizado Confecção	Informatizado Distribuição	Merece Distribuição	Segue outro Orgão	Data Atualização Importante
Procedimentos Operacionais					
Cadastro de Pessoal					
Diretrizes					
Estudos de Caso					
Planos de Operações					
Ordens de Serviço					
Diário Oficial do Estado					
Boletim do Cmdo-Geral					
Legislação					
Editais (concursos em geral)					
Relatórios Adm. Mensais (Sec do EM, Frota, Armas, etc.)					
Boletim de Ocorrência					
Procedimentos Administrativos (IPM, CD, CJ, Sind.)					
Outros:					
Outros:					

ANEXO 2 - Questionário para CELEPAR

1 – Existe algum trabalho no Governo do Estado que oriente a uma padronização para a gerencia eletrônica de documentos?

2 – Os órgãos da Justiça Estadual participam nesse projeto?

3 – Pretende-se incluir a PMPR? Qual a previsão para que isso ocorra?

4 – Como a CELEPAR vê o assunto tratado diretamente pelos órgãos de governo independentemente? Existe alguma possibilidade dos diversos setores não se falarem por falta de padronização?

5 – Existe previsão de se trabalhar em um projeto GED com certificação digital na PMPR?

6 – Na sua opinião quais as aplicabilidades do assunto GED em instituições policiais?

ANEXO 3 - Questionário para Tribunal de Justiça

1 - Qual a fase em que se encontra a implantação de processos informatizados no TJ?

2 – Existe algum trabalho conjunto com o poder Executivo que oriente a uma padronização para a gerencia eletrônica de documentos?

3 – Uma vez que o Condutor da prisão em flagrante depõe no processo, se faz necessária a certificação digital do Boletim de Ocorrências correspondente? Ela pode ser substituída por um extrato autenticado extraído de um sistema corporativo onde foi transcrito o BO?

DECRETO Nº 3.505, DE 13 DE JUNHO DE 2000

Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.

O PRESIDENTE DA REPÚBLICA, no uso da atribuição que lhe confere o art. 84, inciso IV, da Constituição, e tendo em vista o disposto na Lei nº 8.159, de 8 de janeiro de 1991, e no Decreto nº 2.910, de 29 de dezembro de 1998,

DECRETA:

Art. 1º Fica instituída a Política de Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal, que tem como pressupostos básicos:

I - assegurar a garantia ao direito individual e coletivo das pessoas, à inviolabilidade da sua intimidade e ao sigilo da correspondência e das comunicações, nos termos previstos na Constituição;

II - proteção de assuntos que mereçam tratamento especial;

III - capacitação dos segmentos das tecnologias sensíveis;

IV - uso soberano de mecanismos de segurança da informação, com o domínio de tecnologias sensíveis e duais;

V - criação, desenvolvimento e manutenção de mentalidade de segurança da informação;

VI - capacitação científico-tecnológica do País para uso da criptografia na segurança e defesa do Estado; e

VII - conscientização dos órgãos e das entidades da Administração Pública Federal sobre a importância das informações processadas e sobre o risco da sua vulnerabilidade.

Art. 2º Para efeitos da Política de Segurança da Informação, ficam estabelecidas as seguintes conceituações:

I - Certificado de Conformidade: garantia formal de que um produto ou serviço, devidamente identificado, está em conformidade com uma norma legal;

II - Segurança da Informação: proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento.

Art. 3º São objetivos da Política da Informação:

I - dotar os órgãos e as entidades da Administração Pública Federal de instrumentos jurídicos, normativos e organizacionais que os capacitem científica, tecnológica e administrativamente a assegurar a confidencialidade, a integridade, a autenticidade, o não-repúdio e a disponibilidade dos dados e das informações tratadas, classificadas e sensíveis;

II - eliminar a dependência externa em relação a sistemas, equipamentos, dispositivos e atividades vinculadas à segurança dos sistemas de informação;

III - promover a capacitação de recursos humanos para o desenvolvimento de competência científico-tecnológica em segurança da informação;

IV - estabelecer normas jurídicas necessárias à efetiva implementação da segurança da informação;

V - promover as ações necessárias à implementação e manutenção da segurança da informação;

VI - promover o intercâmbio científico-tecnológico entre os órgãos e as entidades da Administração Pública Federal e as instituições públicas e privadas, sobre as atividades de segurança da informação;

VII - promover a capacitação industrial do País com vistas à sua autonomia no desenvolvimento e na fabricação de produtos que incorporem recursos criptográficos, assim como estimular o setor produtivo a participar competitivamente do mercado de bens e de serviços relacionados com a segurança da informação; e

VIII - assegurar a interoperabilidade entre os sistemas de segurança da informação.

Art. 4º Para os fins deste Decreto, cabe à Secretaria-Executiva do Conselho de Defesa Nacional, assessorada pelo Comitê Gestor da Segurança da Informação de que trata o art. 6º, adotar as seguintes diretrizes:

I - elaborar e implementar programas destinados à conscientização e à capacitação dos recursos humanos que serão utilizados na consecução dos objetivos de que trata o artigo anterior, visando garantir a adequada articulação entre os órgãos e as entidades da Administração Pública Federal;

II - estabelecer programas destinados à formação e ao aprimoramento dos recursos humanos, com vistas à definição e à implementação de mecanismos capazes de fixar e fortalecer as equipes de pesquisa e desenvolvimento, especializadas em todos os campos da segurança da informação;

III - propor regulamentação sobre matérias afetas à segurança da informação nos órgãos e nas entidades da Administração Pública Federal;

IV - estabelecer normas relativas à implementação da Política Nacional de Telecomunicações, inclusive sobre os serviços prestados em telecomunicações, para assegurar, de modo alternativo, a permanente disponibilização dos dados e das informações de interesse para a defesa nacional;

V - acompanhar, em âmbito nacional e internacional, a evolução doutrinária e tecnológica das atividades inerentes à segurança da informação;

VI - orientar a condução da Política de Segurança da Informação já existente ou a ser implementada;

VII - realizar auditoria nos órgãos e nas entidades da Administração Pública Federal, envolvidas com a política de segurança da informação, no intuito de aferir o nível de segurança dos respectivos sistemas de informação;

VIII - estabelecer normas, padrões, níveis, tipos e demais aspectos relacionados ao emprego dos produtos que incorporem recursos critptográficos, de modo a assegurar a confidencialidade, a autenticidade, a integridade e o não-repúdio, assim como a interoperabilidade entre os Sistemas de Segurança da Informação;

IX - estabelecer as normas gerais para o uso e a comercialização dos recursos criptográficos pelos órgãos e pelas entidades da Administração Pública Federal, dando-se preferência, em princípio, no emprego de tais recursos, a produtos de origem nacional;

X - estabelecer normas, padrões e demais aspectos necessários para assegurar a confidencialidade dos dados e das informações, em vista da possibilidade de detecção de emanações eletromagnéticas, inclusive as provenientes de recursos computacionais;

XI - estabelecer as normas inerentes à implantação dos instrumentos e mecanismos necessários à emissão de certificados de conformidade no tocante aos produtos que incorporem recursos criptográficos;

XII - desenvolver sistema de classificação de dados e informações, com vistas à garantia dos níveis de segurança desejados, assim como à normatização do acesso às informações;

XIII - estabelecer as normas relativas à implementação dos Sistemas de Segurança da Informação, com vistas a garantir a sua interoperabilidade e a obtenção dos níveis de segurança desejados, assim como assegurar a permanente disponibilização dos dados e das informações de interesse para a defesa nacional; e

XIV - conceber, especificar e coordenar a implementação da infra-estrutura de chaves públicas a serem utilizadas pelos órgãos e pelas entidades da Administração Pública Federal.

Art. 5º À Agência Brasileira de Inteligência - ABIN, por intermédio do Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações - CEPESC, competirá:

I - apoiar a Secretaria-Executiva do Conselho de Defesa Nacional no tocante a atividades de caráter científico e tecnológico relacionadas à segurança da informação; e

II - integrar comitês, câmaras técnicas, permanentes ou não, assim como equipes e grupos de estudo relacionados ao desenvolvimento das suas atribuições de assessoramento.

Art. 6º Fica instituído o Comitê Gestor da Segurança da Informação, com atribuição de assessorar a Secretaria-Executiva do Conselho de Defesa Nacional na consecução das diretrizes da Política de Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal, bem como na avaliação e análise de assuntos relativos aos objetivos estabelecidos neste Decreto.

Art. 7º O Comitê será integrado por um representante de cada Ministério e órgãos a seguir indicados:

I - Ministério da Justiça;
II - Ministério da Defesa;
III - Ministério das Relações Exteriores;
IV - Ministério da Fazenda;
V - Ministério da Previdência e Assistência Social;
VI - Ministério da Saúde;
VII - Ministério do Desenvolvimento, Indústria e Comércio Exterior;
VIII - Ministério do Planejamento, Orçamento e Gestão;
IX - Ministério das Comunicações;
X - Ministério da Ciência e Tecnologia;
XI - Casa Civil da Presidência da República; e
XII - Gabinete de Segurança Institucional da Presidência da República, que o coordenará.

§ 1º Os membros do Comitê Gestor serão designados pelo Chefe do Gabinete de Segurança Institucional da Presidência da República, mediante indicação dos titulares dos Ministérios e órgãos representados.

§ 2º Os membros do Comitê Gestor não poderão participar de processos similares de iniciativa do setor privado, exceto nos casos por ele julgados imprescindíveis para atender aos interesses da

defesa nacional e após aprovação pelo Gabinete de Segurança Institucional da Presidência da República.

§ 3º A participação no Comitê não enseja remuneração de qualquer espécie, sendo considerada serviço público relevante.

§ 4º A organização e o funcionamento do Comitê serão dispostos em regimento interno por ele aprovado.

§ 5º Caso necessário, o Comitê Gestor poderá propor a alteração de sua composição.

Art. 8º Este Decreto entra em vigor na data de sua publicação.

Brasília, 13 de junho de 2000; 179º da Independência e 112º da República.

FERNANDO HENRIQUE CARDOSO
José Gregori
Geraldo Magela da Cruz Quintão
Luiz Felipe Lampreia
Pedro Malan
Waldeck Ornélas
José Serra
Alcides Lopes Tápias
Martus Tavares
Pimenta da Veiga
Ronaldo Mota Sardenberg
Pedro Parente
Alberto Mendes Cardoso

(Diário Oficial da União, de 14 de junho de 2000)

LEI Nº 9.983, DE 14 DE JULHO DE 2000.

Mensagem de Veto nº 961

Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal e dá outras providências.

O PRESIDENTE DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

Art. 1º São acrescidos à Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, os seguintes dispositivos:
"Apropriação indébita previdenciária" (AC)*
"Art. 168-A. Deixar de repassar à previdência social as contribuições recolhidas dos contribuintes, no prazo e forma legal ou convencional:" (AC)

"Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa." (AC)

"§ 1º Nas mesmas penas incorre quem deixar de:" (AC)

"I – recolher, no prazo legal, contribuição ou outra importância destinada à previdência social que tenha sido descontada de pagamento efetuado a segurados, a terceiros ou arrecadada do público;" (AC)

"II – recolher contribuições devidas à previdência social que tenham integrado despesas contábeis ou custos relativos à venda de produtos ou à prestação de serviços;" (AC)

"III - pagar benefício devido a segurado, quando as respectivas cotas ou valores já tiverem sido reembolsados à empresa pela previdência social." (AC)

"§ 2º É extinta a punibilidade se o agente, espontaneamente, declara, confessa e efetua o pagamento das contribuições, importâncias ou valores e presta as informações devidas à previdência social, na forma definida em lei ou regulamento, antes do início da ação fiscal." (AC)

"§ 3º É facultado ao juiz deixar de aplicar a pena ou aplicar somente a de multa se o agente for primário e de bons antecedentes, desde que:" (AC)

"I – tenha promovido, após o início da ação fiscal e antes de oferecida a denúncia, o pagamento da contribuição social previdenciária, inclusive acessórios; ou" (AC)

"II – o valor das contribuições devidas, inclusive acessórios, seja igual ou inferior àquele estabelecido pela previdência social, administrativamente, como sendo o mínimo para o ajuizamento de suas execuções fiscais." (AC)

"Inserção de dados falsos em sistema de informações" (AC)

"Art. 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano:" (AC)

"Pena – reclusão, de 2 (dois) a 12 (doze) anos, e multa." (AC)

"Modificação ou alteração não autorizada de sistema de informações" (AC)

"Art. 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente:" (AC)

"Pena – detenção, de 3 (três) meses a 2 (dois) anos, e multa." (AC)

"Parágrafo único. As penas são aumentadas de um terço até a metade se da modificação ou alteração resulta dano para a Administração Pública ou para o administrado." (AC)

"Sonegação de contribuição previdenciária" (AC)

"Art. 337-A. Suprimir ou reduzir contribuição social previdenciária e qualquer acessório, mediante as seguintes condutas:" (AC)

"I – omitir de folha de pagamento da empresa ou de documento de informações previsto pela legislação previdenciária segurados empregado, empresário, trabalhador avulso ou trabalhador autônomo ou a este equiparado que lhe prestem serviços;" (AC)

"II – deixar de lançar mensalmente nos títulos próprios da contabilidade da empresa as quantias descontadas dos segurados ou as devidas pelo empregador ou pelo tomador de serviços;" (AC)

"III – omitir, total ou parcialmente, receitas ou lucros auferidos, remunerações pagas ou creditadas e demais fatos geradores de contribuições sociais previdenciárias:" (AC)

"Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa." (AC)

"§ 1º É extinta a punibilidade se o agente, espontaneamente, declara e confessa as contribuições, importâncias ou valores e presta as informações devidas à previdência social, na forma definida em lei ou regulamento, antes do início da ação fiscal." (AC)

"§ 2º É facultado ao juiz deixar de aplicar a pena ou aplicar somente a de multa se o agente for primário e de bons antecedentes, desde que:" (AC)

"I – (VETADO)"

"II – o valor das contribuições devidas, inclusive acessórios, seja igual ou inferior àquele estabelecido pela previdência social, administrativamente, como sendo o mínimo para o ajuizamento de suas execuções fiscais." (AC)

"§ 3º Se o empregador não é pessoa jurídica e sua folha de pagamento mensal não ultrapassa R$ 1.510,00 (um mil, quinhentos e dez reais), o juiz poderá reduzir a pena de um terço até a metade ou aplicar apenas a de multa." (AC)

"§ 4º O valor a que se refere o parágrafo anterior será reajustado nas mesmas datas e nos mesmos índices do reajuste dos benefícios da previdência social." (AC)

Art. 2º Os arts. 153, 296, 297, 325 e 327 do Decreto-Lei nº 2.848, de 1940, passam a vigorar com as seguintes alterações:

"Art. 153. ....."

"§ 1º-A. Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública:" (AC)

"Pena – detenção, de 1 (um) a 4 (quatro) anos, e multa." (AC)

"§ 1º (parágrafo único original)....."

"§ 2º Quando resultar prejuízo para a Administração Pública, a ação penal será incondicionada." (AC)

"Art. 296. ....."

"§ 1º .....

....."

"III – quem altera, falsifica ou faz uso indevido de marcas, logotipos, siglas ou quaisquer outros símbolos utilizados ou identificadores de órgãos ou entidades da Administração Pública." (AC)

"....."

"Art. 297. .....

....."

"§ 3º Nas mesmas penas incorre quem insere ou faz inserir:" (AC)

"I – na folha de pagamento ou em documento de informações que seja destinado a fazer prova perante a previdência social, pessoa que não possua a qualidade de segurado obrigatório;" (AC)

"II – na Carteira de Trabalho e Previdência Social do empregado ou em documento que deva produzir efeito perante a previdência social, declaração falsa ou diversa da que deveria ter sido escrita;" (AC)

"III – em documento contábil ou em qualquer outro documento relacionado com as obrigações da empresa perante a previdência social, declaração falsa ou diversa da que deveria ter constado." (AC)

"§ 4º Nas mesmas penas incorre quem omite, nos documentos mencionados no § 3º, nome do segurado e seus dados pessoais, a remuneração, a vigência do contrato de trabalho ou de prestação de serviços." (AC)

"Art. 325. ....."

"§ 1º Nas mesmas penas deste artigo incorre quem:" (AC)

"I – permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da Administração Pública;" (AC)

"II – se utiliza, indevidamente, do acesso restrito." (AC)

"§ 2º Se da ação ou omissão resulta dano à Administração Pública ou a outrem:" (AC)

"Pena – reclusão, de 2 (dois) a 6 (seis) anos, e multa." (AC)

"Art. 327. ....."

"§ 1º Equipara-se a funcionário público quem exerce cargo, emprego ou função em entidade paraestatal, e quem trabalha para empresa prestadora de serviço contratada ou conveniada para a execução de atividade típica da Administração Pública." (NR)

"....."

Art. 3º O art. 95 da Lei nº 8.212, de 24 de julho de 1991, passa a vigorar com a seguinte redação:

"Art. 95. *Caput*. Revogado."

"a) revogada;"

"b) revogada;"

"c) revogada;"

"d) revogada;"
"e) revogada;"

"f) revogada;"

"g) revogada;"

"h) revogada;"

"i) revogada;"

"j) revogada."

"§ 1º Revogado."
"§ 2º ....."

"a) ....."

"b) ....."

"c) ....."

"d) ....."
"e)....."

"f)....."

"§ 3º Revogado."

"§ 4º Revogado."
"§ 5º Revogado."

Art. 4º Esta Lei entra em vigor noventa dias após a data de sua publicação.

Brasília, 14 de julho de 2000; 179º da Independência e 112º da República.

FERNANDO HENRIQUE CARDOSO
José Gregori
Waldeck Ornelas

Publicado no D.O. de 17.7.2000

MEDIDA PROVISÓRIA Nº 2.200-2, DE 24 DE AGOSTO DE 2001.

Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências.

O PRESIDENTE DA REPÚBLICA, no uso da atribuição que lhe confere o art. 62 da Constituição, adota a seguinte Medida Provisória, com força de lei:

Art. 1º Fica instituída a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.

Art. 2º A ICP-Brasil, cuja organização será definida em regulamento, será composta por uma autoridade gestora de políticas e pela cadeia de autoridades certificadoras composta pela Autoridade Certificadora Raiz - AC Raiz, pelas Autoridades Certificadoras - AC e pelas Autoridades de Registro - AR.

Art. 3º A função de autoridade gestora de políticas será exercida pelo Comitê Gestor da ICP-Brasil, vinculado à Casa Civil da Presidência da República e composto por cinco representantes da sociedade civil, integrantes de setores interessados, designados pelo Presidente da República, e um representante de cada um dos seguintes órgãos, indicados por seus titulares:

I - Ministério da Justiça;

II - Ministério da Fazenda;

III - Ministério do Desenvolvimento, Indústria e Comércio Exterior;

IV - Ministério do Planejamento, Orçamento e Gestão;

V - Ministério da Ciência e Tecnologia;

VI - Casa Civil da Presidência da República; e

VII - Gabinete de Segurança Institucional da Presidência da República.

§ 1º A coordenação do Comitê Gestor da ICP-Brasil será exercida pelo representante da Casa Civil da Presidência da República.

§ 2º Os representantes da sociedade civil serão designados para períodos de dois anos, permitida a recondução.

§ 3º A participação no Comitê Gestor da ICP-Brasil é de relevante interesse público e não será remunerada.

§ 4º O Comitê Gestor da ICP-Brasil terá uma Secretaria-Executiva, na forma do regulamento.

Art. 4º Compete ao Comitê Gestor da ICP-Brasil:

I - adotar as medidas necessárias e coordenar a implantação e o funcionamento da ICP-Brasil;

II - estabelecer a política, os critérios e as normas técnicas para o credenciamento das AC, das AR e dos demais prestadores de serviço de suporte à ICP-Brasil, em todos os níveis da cadeia de certificação;

III - estabelecer a política de certificação e as regras operacionais da AC Raiz;

IV - homologar, auditar e fiscalizar a AC Raiz e os seus prestadores de serviço;

V - estabelecer diretrizes e normas técnicas para a formulação de políticas de certificados e regras operacionais das AC e das AR e definir níveis da cadeia de certificação;

VI - aprovar políticas de certificados, práticas de certificação e regras operacionais, credenciar e autorizar o funcionamento das AC e das AR, bem como autorizar a AC Raiz a emitir o correspondente certificado;

VII - identificar e avaliar as políticas de ICP externas, negociar e aprovar acordos de certificação bilateral, de certificação cruzada, regras de interoperabilidade e outras formas de cooperação internacional, certificar, quando for o caso, sua compatibilidade com a ICP-Brasil, observado o disposto em tratados, acordos ou atos internacionais; e

VIII - atualizar, ajustar e revisar os procedimentos e as práticas estabelecidas para a ICP-Brasil, garantir sua compatibilidade e promover a atualização tecnológica do sistema e a sua conformidade com as políticas de segurança.

Parágrafo único. O Comitê Gestor poderá delegar atribuições à AC Raiz.

Art. 5º À AC Raiz, primeira autoridade da cadeia de certificação, executora das Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil, compete emitir, expedir, distribuir, revogar e gerenciar os certificados das AC de nível imediatamente subseqüente ao seu, gerenciar a lista de certificados emitidos, revogados e vencidos, e executar atividades de fiscalização e auditoria das AC e das AR e dos prestadores de serviço habilitados na ICP, em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor da ICP-Brasil, e exercer outras atribuições que lhe forem cometidas pela autoridade gestora de políticas.

Parágrafo único. É vedado à AC Raiz emitir certificados para o usuário final.

Art. 6º Às AC, entidades credenciadas a emitir certificados digitais vinculando pares de chaves criptográficas ao respectivo titular, compete emitir, expedir, distribuir, revogar e gerenciar os certificados, bem como colocar à disposição dos usuários listas de certificados revogados e outras informações pertinentes e manter registro de suas operações.

Parágrafo único. O par de chaves criptográficas será gerado sempre pelo próprio titular e sua chave privada de assinatura será de seu exclusivo controle, uso e conhecimento.

Art. 7º Às AR, entidades operacionalmente vinculadas a determinada AC, compete identificar e cadastrar usuários na presença destes, encaminhar solicitações de certificados às AC e manter registros de suas operações.

Art. 8º Observados os critérios a serem estabelecidos pelo Comitê Gestor da ICP-Brasil, poderão ser credenciados como AC e AR os órgãos e as entidades públicos e as pessoas jurídicas de direito privado.

Art. 9º É vedado a qualquer AC certificar nível diverso do imediatamente subseqüente ao seu, exceto nos casos de acordos de certificação lateral ou cruzada, previamente aprovados pelo Comitê Gestor da ICP-Brasil.

Art. 10. Consideram-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos de que trata esta Medida Provisória.

§ 1º As declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil presumem-se verdadeiros em relação aos signatários, na forma do art. 131 da Lei nº 3.071, de 1º de janeiro de 1916 - Código Civil.

§ 2º O disposto nesta Medida Provisória não obsta a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento.

Art. 11. A utilização de documento eletrônico para fins tributários atenderá, ainda, ao disposto no art. 100 da Lei nº 5.172, de 25 de outubro de 1966 - Código Tributário Nacional.

Art. 12. Fica transformado em autarquia federal, vinculada ao Ministério da Ciência e Tecnologia, o Instituto Nacional de Tecnologia da Informação - ITI, com sede e foro no Distrito Federal.

Art. 13. O ITI é a Autoridade Certificadora Raiz da Infra-Estrutura de Chaves Públicas Brasileira.

Art. 14. No exercício de suas atribuições, o ITI desempenhará atividade de fiscalização, podendo ainda aplicar sanções e penalidades, na forma da lei.

Art. 15. Integrarão a estrutura básica do ITI uma Presidência, uma Diretoria de Tecnologia da Informação, uma Diretoria de Infra-Estrutura de Chaves Públicas e uma Procuradoria-Geral.

Parágrafo único. A Diretoria de Tecnologia da Informação poderá ser estabelecida na cidade de Campinas, no Estado de São Paulo.

Art. 16. Para a consecução dos seus objetivos, o ITI poderá, na forma da lei, contratar serviços de terceiros.

§ 1º O Diretor-Presidente do ITI poderá requisitar, para ter exercício exclusivo na Diretoria de Infra-Estrutura de Chaves Públicas, por período não superior a um ano, servidores, civis ou militares, e empregados de órgãos e entidades integrantes da Administração Pública Federal direta ou indireta, quaisquer que sejam as funções a serem exercidas.

§ 2º Aos requisitados nos termos deste artigo serão assegurados todos os direitos e vantagens a que façam jus no órgão ou na entidade de origem, considerando-se o período de requisição para todos os efeitos da vida funcional, como efetivo exercício no cargo, posto, graduação ou emprego que ocupe no órgão ou na entidade de origem.

Art. 17. Fica o Poder Executivo autorizado a transferir para o ITI:

I - os acervos técnico e patrimonial, as obrigações e os direitos do Instituto Nacional de Tecnologia da Informação do Ministério da Ciência e Tecnologia;

II - remanejar, transpor, transferir, ou utilizar, as dotações orçamentárias aprovadas na Lei Orçamentária de 2001, consignadas ao Ministério da Ciência e Tecnologia, referentes às atribuições do órgão ora transformado, mantida a mesma classificação orçamentária, expressa por categoria de programação em seu menor nível, observado o disposto no § 2º do art. 3º da Lei nº

9.995, de 25 de julho de 2000, assim como o respectivo detalhamento por esfera orçamentária, grupos de despesa, fontes de recursos, modalidades de aplicação e identificadores de uso.

Art. 18. Enquanto não for implantada a sua Procuradoria Geral, o ITI será representado em juízo pela Advocacia Geral da União.

Art. 19. Ficam convalidados os atos praticados com base na Medida Provisória nº 2.200-1, de 27 de julho de 2001.

Art. 20. Esta Medida Provisória entra em vigor na data de sua publicação.

Brasília, 24 de agosto de 2001; 180º da Independência e 113º da República.

FERNANDO HENRIQUE CARDOSO
José Gregori
Martus Tavares
Ronaldo Mota Sardenberg
Pedro Parente

DECRETO Nº 3.872, DE 18 DE JULHO DE 2001.

Dispõe sobre o Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira - CG ICP-Brasil, sua Secretaria-Executiva, sua Comissão Técnica Executiva e dá outras providências.

O PRESIDENTE DA REPÚBLICA, no uso das atribuições que lhe confere o art. 84, incisos IV e VI, da Constituição, e tendo em vista o disposto na Medida Provisória nº 2.200, de 28 de junho de 2001,

DECRETA:

Art. 1º O Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira - CG ICP-Brasil, instituído pela Medida Provisória nº 2.200, de 28 de junho de 2001, exerce a função de autoridade gestora de políticas (AGP) da referida Infra-Estrutura.

Art. 2º O CG ICP-Brasil, vinculado à Casa Civil da Presidência da República, é composto por onze membros, sendo quatro representantes da sociedade civil, integrantes de setores interessados e sete representantes dos seguintes órgãos, todos designados pelo Presidente da República:

I - Casa Civil da Presidência da República, que o coordenará;

II - Gabinete de Segurança Institucional da Presidência da República;

III - Ministério da Justiça;

IV - Ministério da Fazenda;

V - Ministério do Desenvolvimento, Indústria e Comércio Exterior;

VI - Ministério do Planejamento, Orçamento e Gestão; e

VII - Ministério da Ciência e Tecnologia.

§ 1º Os representantes da sociedade civil serão designados para períodos de dois anos, permitida a recondução.

§ 2º A participação no CG ICP-Brasil é de relevante interesse público e não será remunerada.

§ 3º O CG ICP-Brasil terá uma Secretaria-Executiva.

§ 4º As decisões do CG ICP-Brasil serão aprovadas pela maioria absoluta de seus membros.

§ 5º Os membros do CG ICP-Brasil serão, em seus impedimentos, substituídos por suplentes designados na forma do **caput**.

§ 6º Poderão ser convidados a participar das reuniões do CG ICP-Brasil, a juízo do seu Coordenador ou do próprio Comitê, técnicos e especialistas de áreas afins.

Art. 3º Compete ao CG ICP-Brasil:

I - adotar as medidas necessárias e coordenar a implantação e o funcionamento da Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil;

II - estabelecer a política, os critérios e as normas para licenciamento das Autoridades Certificadoras - AC, das Autoridades de Registro - AR e dos demais prestadores de serviços de suporte à ICP-Brasil, em todos os níveis da cadeia de certificação;

III - estabelecer a política de certificação e as regras operacionais da Autoridade Certificadora Raiz - AC Raiz;

IV - homologar, auditar e fiscalizar a AC Raiz e os seus prestadores de serviço;

V - estabelecer diretrizes e normas para a formulação de políticas de certificados e regras operacionais das AC e das AR e definir níveis da cadeia de certificação;

VI - aprovar políticas de certificados e regras operacionais, licenciar e autorizar o funcionamento das AC e das AR, bem como autorizar a AC Raiz a emitir o correspondente certificado;

VII - identificar e avaliar as políticas de ICP externas, quando for o caso, certificar sua compatibilidade com a ICP-Brasil, negociar e aprovar, observados os tratados, acordos e atos internacionais, acordos de certificação bilateral, de certificação cruzada, regras de interoperabilidade e outras formas de cooperação internacional; e

VIII - atualizar, ajustar e revisar os procedimentos e as práticas estabelecidas para a ICP-Brasil, garantir sua compatibilidade e promover a atualização tecnológica do sistema e a sua conformidade com as políticas de segurança.

Art. 4º O CG ICP-Brasil será assistido e receberá suporte técnico da Comissão Técnica Executiva - COTEC, coordenada pelo Secretário-Executivo do Comitê Gestor, e integrada por representantes indicados pelos membros do CG ICP-Brasil e designados pelo Chefe da Casa Civil da Presidência da República.

§ 1º Serão convidados permanentes às reuniões da COTEC representantes:

I - do Ministério da Defesa;

II - do Ministério da Previdência e Assistência Social;

III - do Ministério da Saúde; e

IV - da Autoridade Certificadora Raiz - AC Raiz.

§ 2º Poderão ser convidados a participar das reuniões da COTEC, a juízo do seu Coordenador ou da própria Comissão, representantes de outros órgãos e entidades públicos.

§ 3º Compete à COTEC:

I - manifestar-se previamente sobre todas as matérias a serem apreciadas e decididas pelo CG ICP-Brasil;

II - preparar e encaminhar previamente aos membros do CG ICP-Brasil expediente contendo o posicionamento técnico dos órgãos e das entidades relacionados com as matérias que serão apreciadas e decididas; e

III - cumprir outras atribuições que lhe forem conferidas por delegação do CG ICP-Brasil.

§ 4º Os membros da COTEC serão, em seus impedimentos, substituídos por suplentes designados na forma do **caput**.

Art. 5º O CG ICP-Brasil estabelecerá a forma pela qual lhe será prestada assessoria pelo Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações - CEPESC.

Art. 6º A Secretaria-Executiva do CG ICP-Brasil é chefiada por um Secretário-Executivo e integrada por assessores especiais e por pessoal técnico e administrativo.

§ 1º O Secretário-Executivo será designado por livre escolha do Presidente da República.

§ 2º A Secretaria-Executiva receberá da Casa Civil da Presidência da República o apoio necessário ao exercício de suas funções, inclusive no que se refere aos cargos de assessoria e ao apoio técnico e administrativo.

Art. 7º Compete à Secretaria-Executiva do CG ICP-Brasil:

I - prestar assistência direta e imediata ao Coordenador do Comitê Gestor;

II - preparar as reuniões do Comitê Gestor;

III - coordenar e acompanhar a implementação das deliberações e diretrizes fixadas pelo Comitê Gestor;

IV - coordenar os trabalhos da COTEC; e

V - cumprir outras atribuições que lhe forem conferidas por delegação do Comitê Gestor.

Art. 8º Este Decreto entra em vigor na data de sua publicação.

Brasília, 18 de julho de 2001; 180º da Independência e 113º da República.

FERNANDO HENRIQUE CARDOSO
José Gregori
Pedro Parente

Este texto não substitui o publicado no D.O.U. 19.7.2001

DECRETO Nº 3.996, DE 31 DE OUTUBRO DE 2001.

Dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal.

O VICE-PRESIDENTE DA REPÚBLICA, no exercício do cargo de Presidente da República, usando das atribuições que lhe confere o art. 84, incisos II, IV e VI, alínea "a", da Constituição, e tendo em vista o disposto na Medida Provisória nº 2.200-2, de 24 de agosto de 2001,

DECRETA:

Art. 1º A prestação de serviços de certificação digital no âmbito da Administração Pública Federal, direta e indireta, fica regulada por este Decreto.

Art. 2º Somente mediante prévia autorização do Comitê Executivo do Governo Eletrônico, os órgãos e as entidades da Administração Pública Federal poderão prestar ou contratar serviços de certificação digital.

§ 1º Os serviços de certificação digital a serem prestados, credenciados ou contratados pelos órgãos e entidades integrantes da Administração Pública Federal deverão ser providos no âmbito da Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil.

§ 2º Respeitado o disposto no § 1º, o Comitê Executivo do Governo Eletrônico poderá estabelecer padrões e requisitos administrativos para a instalação de Autoridades Certificadoras - AC e de Autoridades de Registro – AR próprias na esfera da Administração Pública Federal.

§ 3º As AR de que trata o § 2º serão, preferencialmente, os órgãos integrantes do Sistema de Administração do Pessoal Civil - SIPEC.

Art. 3º A tramitação de documentos eletrônicos para os quais seja necessária ou exigida a utilização de certificados digitais somente se fará mediante certificação disponibilizada por AC integrante da ICP-Brasil.

Art. 3º-A. As aplicações e demais programas utilizados no âmbito da Administração Pública Federal direta e indireta que admitirem o uso de certificado digital de um determinado tipo contemplado pela ICP-Brasil devem aceitar qualquer certificado de mesmo tipo, ou com requisitos de segurança mais rigorosos, emitido por qualquer AC integrante da ICP-Brasil. (Incluído pelo Decreto nº 4.414, de 7.10.2002)

Art. 4º Será atribuída, na Administração Pública Federal, aos diferentes tipos de certificados disponibilizados pela ICP-Brasil, a classificação de informações segundo o estabelecido na legislação específica.

Art. 5º Este Decreto entra em vigor na data de sua publicação.

Art. 6º Fica revogado o Decreto nº 3.587, de 5 de setembro de 2000.

Brasília, 31 de outubro de 2001; 180º da Independência e 113º da República.

MARCO ANTONIO DE OLIVEIRA MACIEL
Martus Tavares
Silvano Gianni

Este texto não substitui o publicado no D.O.U. 5.11.2001