Pontifícia Universidade Católica de São Paulo

MBIS - Master Business Information System

"A Importância do Escritório sem Papel na Segurança da Informação"

David César de Jesus Nery

Orientador: Prof. Alexandre Campos Silva

MBIS 2003

Ficha Catalográfica

Nery, David César de Jesus, 2004

A Importância do Escritório sem Papel na Segurança da Informação, David César de Jesus Nery, São Paulo, 2004

Bibliografia

1. Introdução *2. Aspectos do Escritório sem papel*

3. Segurança da Informação *4. Pontos Críticos de Sucesso*

5. Conclusão

Agradecimentos

A Deus, pela oportunidade em participar do MBIS e pela sabedoria em concluí-lo.

Aos meus pais, Christovam e Nair, por ter plantado em mim, desde a infância, a semente do saber.

Ao Prof. Alexandre Campos Silva, pela orientação, acompanhamento e apoio na elaboração desta monografia e aos demais professores do MBIS pelos ensinamentos.

Ao Sr. Antonio Carlos Del Cielo, por ter acreditado em meu potencial, aprovando a bolsa de estudos.

Ao Banco Bradesco S.A., por ter patrocinado o curso, integralmente.

Resumo

Esta monografia descreve aspectos relacionados ao "Escritório sem Papel", sua origem e características. Por outro lado, atento para o crescente uso do papel no dia-a-dia das corporações, apesar de toda tecnologia disponível, como gestão integrada de documentos e processos.

Além disso, estabelece uma parceria com a Segurança da Informação visando reduzir riscos, vulnerabilidades e garantir a integridade dos dados, através de uma política de segurança bem definida.

Para isso, explico rotinas e procedimentos, comparando possíveis adversários e ameaças à segurança, e, analisando ferramentas tecnológicas e defesas indispensáveis a qualquer organização, seja pequena, média ou grande.

Sumário

1. Introdução

Quando o ser humano passou a se comunicar por palavras, percebeu que a comunicação era imprescindível, porém sua trajetória acabou por culminar num volume inimaginável de informações. Ao longo da história, o modo de expressão através de imagens evoluiu muito.

Se voltarmos no tempo, podemos vislumbrar os desenhos gravados em cavernas, feitos pelo homem pré-histórico, a invenção da escrita, os papiros egípcios e os pergaminhos, até a invenção do papel pelos chineses e a produção gráfica.

Na década de 80, marcou-se o início da utilização de computadores pessoais nos escritórios, deixando de utilizar as máquinas de escrever.

Nos anos 90, fixou-se a idéia de microcomputadores ligados em rede, utilizando correio eletrônico, datawarehouse, software para workflow e um número ilimitado de outros recursos para eliminar o papel dos escritórios.

Atualmente, pode-se observar que, documentos e arquivos são manuseados de forma constante nas empresas, estando presentes em artigos, notas, esboços, recados, post-it e fotografias nas mesas; revistas, diários e livros nas prateleiras, enquanto que em armários e arquivos, muitas vezes, esses papéis são amontoados, levando a informações desconexas, incompletas e irreconciliáveis. Até mesmo em escritórios de alta tecnologia, os papéis ocupam espaço e estão largamente espalhados.

O volume de informações é de real importância, merecendo tratamento diferenciado e organizado seguindo critérios, muitas vezes, generalizados dentro do âmbito de arquivamento e documentação, ou criados pelas empresas com base em seu "core-business" e pela necessidade específica do processo de negócio, tomada de decisão, prova ou como fonte de conhecimento.

Para as corporações, a informação passa a ser tudo o que é gerado, processado, recebido e distribuído, pois é o coração dos documentos e dos dados. Elas passam a gerir a validade dessas informações e podem classificá-las em: estruturadas e não-estruturadas:

- **Informações estruturadas** são tudo o que está cadastrado em banco de dados, inseridas a partir de programas ou formulários eletrônicos.

- **Informações não-estruturadas** são cartas, cópias, e-mails, fax, contratos, e um sem número de papéis impressos, inclusive materiais da Web que, na maioria das vezes são deixados sobre a mesa, ou jogados no lixo sem critério algum de segurança. Essas informações compõem mais de 80% do corpo documental das empresas e são tratadas de forma muito simples. Assim, muito da história e memória técnica das organizações acaba sendo perdida.

Diante de um cenário formado por um volume enorme de informações, as empresas não sabem por onde começar a administrar seus documentos. Pois, a grande questão é o modo que a informação será mantida e acessada.

Além disso, a falta de controle, torna os documentos inacessíveis quando mais se precisa deles. A distribuição manual de documentos em papel gera lentidão no fluxo de trabalho e aumento no custo de arquivamento e recuperação, tornando o gerenciamento muito caro.

Outro fator é verificar informações importantes ou fundamentais e, separar a informação inútil. Falta às empresas uma estratégia para tratá-las, mantê-las e assegurá-las quanto a possíveis vulnerabilidades, pois informações protegidas garantem autenticidade e integridade, ou seja, garantir que a informação não seja violada e evitar que seja acessada por pessoas não autorizadas.

Uma vez que, o conhecimento é gerado pelas atividades: produzir e analisar a informação. [SELLEN e HARPER, 2003] comparam o dia moderno a gerações passadas: "Considerando que nossos avós trabalhavam em fábricas que faziam qualquer coisa, desde navios a tecidos. Hoje, provavelmente trabalha-se em um escritório onde usamos nossas habilidades para produzir e analisar a informação".

As mídias em que se armazenam e transmitem as informações também são componentes fundamentais para o conhecimento, sendo necessário desenvolvimento contínuo.

A idéia principal do "escritório sem papel" é estabelecer um novo conceito nos ambientes de trabalho, onde o papel passa a ser cada vez menos necessário. Assim, uma série de processos tenta reduzir a necessidade de papel nas organizações, tentando minimizar a falta de convergências entre dois mundos: papel e eletrônico, pois eles têm andado de forma separada, quando deveriam ser visivelmente conectados.

Este trabalho visa estabelecer uma parceria entre o "escritório sem papel" e a "segurança da Informação", usando a tecnologia para gestão integrada de documentos e processos para reduzir a constante preocupação com a segurança dos dados em ambientes corporativos.

Além disso, busca a redução de custos e riscos, e, proteção contra ameaças e ataques que surgem diariamente, uma vez que, os crimes eletrônicos estão se tornando uma constante em nossa sociedade, sendo praticados a todos os instantes.

1.1. O uso do papel

Há milhares de anos, povos gravaram fatos, pensamentos e idéias em pedra, madeira, couro, tecido, entre outros materiais rústicos. Enquanto o comércio crescia, surgia a necessidade de uma nova forma de guardar as informações, pois o material utilizado era pesado e difícil de manusear.

O papiro foi inventado pelos egípcios e apesar de sua fragilidade, muitos deles duram até hoje. O pergaminho era mais resistente, utilizando pele animal, porém o custo era mais elevado.

A invenção do papel, segundo os historiadores é atribuída a um oficial da Corte chinesa, chamado T'Sai Lun, que teria fabricado o papel, a partir de plantas trituradas, trapos velhos e restos de rede de pesca, no início do século II.

Curiosamente, o papel levou muito tempo até chegar ao Ocidente: antes disso, foi largamente difundido entre os árabes, que instalaram a primeira fábrica de papel na Europa, após a invasão da Península Ibérica, na Espanha, em 1150.

Em meados do século XIX, a demanda de papel ganhou um grande impulso com a impressão de livros, jornais e a fabricação de outros produtos de consumo.

Daí em diante, foram utilizados diferentes produtos químicos que deram lugar à grande variedade de papéis existentes.

Hoje, o papel é considerado o principal suporte para a difusão da escrita, da informação e de todo o conhecimento humano. As necessidades das pessoas têm um poder enorme sobre o desenvolvimento de novas tecnologias. Na história da humanidade, boa parte da tecnologia que conhecemos, surgiu da necessidade humana, na sociedade e na economia.

Apesar da chegada eminente do "escritório sem papel" ser proclamada nos últimos 30 anos, a Internet permitiu a qualquer estação de trabalho acessar documentos criados em outros equipamentos, aumentando o uso da impressão.

Quando se fala no "escritório sem papel", geralmente pensa-se no volume de papel consumido a cada ano. A utilização de papel nos escritórios continua crescendo, enquanto o armazenamento eletrônico aumenta exponencialmente. Além disso, outros fatores influenciam a demanda por papel, como aspectos demográficos, condições econômicas e emprego da população. Veja a seguir, o consumo de papel:

Anos	Consumo de Papel (milhões de toneladas)			
	Mundo		Brasil	
	Papéis	Coated	Papéis	Coated
1990	237,4	33,8	4,7	1,2
2000	323,3	99,1	7,2	2,3
2003	339,0	103,9	7,8	3,8
2012	563,1	172,6	13,4	6,3

Fonte: Consumo Mundial: American Forest & Paper Association – Consumo no Brasil: BRACELPA e BNDES

Apesar do consumo do papel coated (para imprimir e escrever) parecer insignificante no consumo total, constitui o segundo maior segmento do setor, logo após o segmento de embalagem.

Gostaria de abordar problemas no uso do papel dividindo em três classes: problemas simbólicos, de custo e interação.

- **Problema simbólico:** usar o papel como símbolo do passado, muitas vezes, é uma opção mais cara e menos eficiente. [SELLEN e HARPER, 2003] exemplificam numa rápida história sobre um empregado de laboratório de pesquisa que projetava novas tecnologias, porém seu escritório estava infestado de massas de papel aparentemente desorganizadas. Embora o empregado fosse excepcionalmente eficiente, ao entrar no escritório se tinha uma má-impressão através daquela imagem, pois se imaginava que o laboratório também fosse assim, demonstrando um erro simbólico.

- **Problema de custo:** Para documentos em papel, os custos são problemáticos após os documentos serem gerados. Considerando que, o custo com documento digital e de impressão são mínimos comparados ao custo inicial de implantação de novas tecnologias. Uma vez que, após a implementação, uma companhia possui uma enorme massa de documentos em papel e o armazenamento e manutenção são caros, incluindo a entrega e recuperação do papel, contrapondo-se aos sistemas eletrônicos e também custos menos diretos. Cada decisão passa a ser minuciosamente estudada.

- **Problema de interação:** são funções que o papel não dispõe, ou seja, as limitações impostas pela natureza do papel como um meio físico para interação, assim, documentos em papel:
  - É usado localmente, não podendo ser acessado remotamente;
  - Ocupa espaço físico, isto é, deve ser armazenado;
  - Requer entrega física, sendo necessário, alocar uma pessoa para trafegar um documento em papel;
  - É difícil de integrar com outros e também de reproduzir (sem tecnologias para reproduzir), sendo exibições estáticas, visuais.

Esses problemas demonstram razões por que pessoas poderiam querer eliminar ou pelo menos reduzir o uso de papel.

1.2. Origens do Escritório sem Papel

Nos idos de 1800, surgiram propostas a substituir métodos baseados em papel, a exemplo da idéia de transmitir dados utilizando eletricidade de Samuel Morse. E, ao final daquele século, o telégrafo, a máquina de teletipo e o telefone também apareceram. Mas algumas invenções foram vistas como possibilidades mais diretas para substituir o papel como o fonógrafo de Thomas Edison que sugeria aos gerentes gravar a voz no dispositivo e gravar quantas vezes fosse necessário, ao invés de ditar os relatórios às secretárias que escreviam, eliminando mensagens em papel e cartas, e, marcando o início do "escritório sem papel".

Décadas mais tarde, inventores prediziam dispositivos que não substituiriam comunicações baseadas em papel, mas reduziriam o uso de papel para impressão de documentos e armazenamento. Em 1945, Vannevar Bush descreveu um dispositivo para uso individual, de tipo mecanizado para arquivo e biblioteca, chamado "memex", que podia ser consultado rapidamente, armazenando as informações em forma de microfilme, surgindo a idéia de um modo alternativo de procurar e arquivar documentos.

Com o surgimento dos computadores, os microfilmes foram deixados para trás, enquanto os documentos passaram a ser compostos de bits e bytes.

Nos anos 50 e 60, o conceito original de Bush começou a se parecer com uma predição dos livros e bibliotecas digitais que conhecemos hoje. Joseph Licklider passou uma idéia de substituir os livros por dispositivos

facilitadores da informação, utilizando um sistema contendo entrada de dados e reconhecimento de voz, permitindo aos usuários especificar, aplicar, monitorar e se necessário revisar, examinando amplos repositórios de informação. Tanto Bush como Licklider previam a explosão da informação, reconhecendo que sistemas baseados em papel não proveriam soluções.

[SELLEN e HARPER, 2003] definem o "escritório sem papel" como uma expectativa criada sobre a tecnologia eletrônica que tornaria o papel no escritório uma coisa do passado, porém é difícil afirmar onde e quando o conceito foi introduzido. A idéia foi creditada ao centro de pesquisas da Xerox - PARC, localizado em Palo Alto, na Califórnia, onde também nasceram outras idéias que influenciariam o mundo tecnológico que conhecemos atualmente, como impressora laser, interfaces gráficas e rede Ethernet.

Não se sabe ao certo, mas qualquer que seja a veracidade dos fatos, os pesquisadores da PARC tiveram que trilhar um caminho cuidadoso em suas atividades. "A necessidade de reduzir o papel" passou a ser uma meta para o que era então o negócio principal da Xerox: a fabricação de dinheiro em papel.

Quando a PARC transformou os grandes computadores difíceis de manusear em dispositivos, como da concepção das máquinas de Babbage: utilizando como desktop, parecia óbvio a muitos que era um sinal do fim de papel. Afinal de contas, o sistema Xerox Star parecia ser projetado para reproduzir aspectos do papel, pois possuía uma tela capaz de exibir dois documentos lado a lado, ligada via rede Ethernet a outros computadores de mesma configuração.

Embora os pesquisadores da PARC poderiam ter pensado que não estavam no negócio de inventar o “escritório sem papel”, outros fizeram - particularmente jornalistas que queriam dar um "grande furo" sobre a revolução que estava a ponto de acontecer.

Então, em 1975, foi publicado um artigo na revista Business Week, descrevendo uma série de previsões sobre o fim da máquina de escrever e do papel, com a chegada do escritório do futuro. Esta reportagem afirmava que, uma equipe da PARC trabalhava em um projeto para verificar o que aconteceria se limitassem à utilização de uma resma de papel à empresa.

Ainda, por um conjunto de razões, não aconteceu a revolução no ambiente do escritório que parecia iminente. Em primeiro lugar, os custos dos sistemas Xerox inicialmente oferecidos eram muito altos, exceto para organizações mais abastadas. Além disso, o pessoal sênior julgava que não haveria futuro para tais produtos, independente do preço. Em todo caso, enquanto eles decidiam qual caminho de desenvolvimento tecnológico iriam tomar, a PARC foi se fragmentado: uma área visava redes, outra desenvolvia aplicativos e processadores de textos para computadores pessoais, culminando na divisão do grupo de pesquisa da PARC. Enquanto alguns ficaram desenvolvendo o sistema Star, outros se juntaram à nova área, porém, um terceiro grupo saiu da empresa levando algumas das idéias básicas e implementando-as. Esses esforços vieram a ser conhecido primeiramente como Apple Lisa e, mais tarde como Apple Macintosh.

O resultado final era uma "arquitetura de informação" inventado na PARC que permitia conexão direta entre usuários de rede, sendo implementada de modo limitado fora do laboratório (na divisão de produtos que desenvolveu o sistema Star), culminando numa conseqüência importante: o papel se tornou à conexão entre os usuários.

Em 1980, havia uma variedade de computadores pessoais no mercado (IBM e Apple eram dominantes) e os programas de um não podiam ser lidos em outros equipamentos. Em outras palavras, com exceções notáveis, o papel se tornou um substituto para rede, permitindo aos usuários com máquinas diferentes compartilhar documentos ou outros materiais que estavam trabalhando. E, apesar da tecnologia não oferecer tudo que precisavam e o desenvolvimento manter o seu passo, algo tinha transformado a vida no escritório. Porém, investimentos em computadores Apple e IBM levaram muitos a pensar que, o papel finalmente desapareceria, porque faziam um dos trabalhos mais importantes - conectar as pessoas - achando apoio em uma nova tecnologia: a Internet, uma nova forma de comunicação que ganhou o maior número de usuários em menor tempo na história da humanidade. O telefone, que foi uma verdadeira revolução em sua época, levou 70 anos para conquistar 50 milhões de usuários. Já a Web conseguiu este feito em apenas cinco anos.

A partir de uma linguagem de marcação bastante simples chamada HTML (Hyper Text Markup Language), tornou-se possível trafegar textos e informações de natureza científica, permitindo a qualquer computador conectado a rede, ler e exibir os documentos de qualquer outro computador.

Em efeito, evitava o problema intransigente de inoperabilidade entre diferentes processadores de texto e aplicativos gráficos. Considerando que, anteriormente, documentos do WordPerfect não pudessem ser lidos pelo Microsoft Word e vice-versa, com o HTML a maioria das aplicações poderia ser lida em qualquer equipamento, independente do aplicativo.

O aumento do acesso a Web assegurou que os benefícios do HTML pudessem ser mostrados, apesar do desejo das companhias de software ser outro. Assim, pessoas de uma organização passaram a se comunicar com outras, efetivamente, não só podendo enviar documentos eletrônicos de qualquer máquina ou sistema entre si, mas também fora da empresa. Podendo facilmente, criar e acessar a repositórios de documentos eletrônicos.

Quando se esperava que o "escritório sem papel" se firmasse, o consumo de papel aumentou [GIMSON, 1997]; a Internet serviu para aumentar a impressão feita em casa ou no escritório. Uma vez que, as pessoas tinham mais acesso às informações do que antes, preferiam usar a rede para pesquisar os dados e em seguida, imprimir, para leitura em papel.

Naquele momento, as grandes empresas atentavam em reduzir a impressão de grandes volumes. Esse processamento gerava custos elevados com impressão e foi reavaliado, reduzindo consideravelmente as despesas. Todavia não conseguiram abandonar ou reduzir o uso do papel.

Nos últimos anos, as exigências legais sobre a gestão de documentos em vários formatos e a necessidade de eliminar os gargalos nos processos de negócio estão empurrando as empresas para um novo patamar de integração tecnológica.

Pouco a pouco, o mercado está integrando numa só plataforma, gerenciamento de processos e documentos, prometendo dar mais transparência a informações e processos e, elevando o nível de produtividade das corporações.

Deste modo, o crescimento de demanda por plataformas de gerenciamento híbridas, envolvem a manipulação de documentos em vários formatos e mídias, e a integração de aplicações diversas, seja no nível corporativo ou no departamental.

Outro fator é a busca por produtividade nos processos de negócio. Utilizando ferramentas workflow associadas à gestão de conteúdo ajudam a eliminar o fluxo de papel e o gargalo dentro dos processos. Esses projetos podem envolver algumas áreas específicas da empresa, com soluções que usam uma ou várias tecnologias.

2. Aspectos do Escritório sem Papel

Desenvolver uma tecnologia para abranger todo tipo de informação através da integração de diferentes tecnologias, além de reduzir o consumo de papel tem sido a meta das empresas, independente do porte, sendo pública ou privada.

Para entender melhor essa tecnologia, faz-se necessário apresentar os aspectos tecnológicos, culturais e financeiros, além da legislação referente à utilização de documentos eletrônicos.

A partir dessa análise torna-se possível entender por quê e quais fatores permitirão que uma tecnologia tão importante, como o "escritório sem papel" alcance o devido espaço nas corporações.

2.1. Aspectos Legais

Apesar de todos os questionamentos, o fato é que a legislação de modo geral não aprova documentos em meios digitais com a mesma facilidade que aceita microfilmes. A maioria das aplicações em que o documento eletrônico é aceito está ligada às relações com o governo e embora exista muita pressão para homologação em geral do documento digital, este não pode ser considerado como plenamente aceito e em muitos casos existe a necessidade da guarda permanente de documentos em meio físico.

Para se adequarem às novas imposições do mercado financeiro e de capitais, as empresas precisam preservar cuidadosamente suas informações, significando gerenciar de forma eficaz documentos em vários formatos e mídias. E, ultimamente, com os escândalos envolvendo executivos da Enron e da WorldCom, essas iniciativas atingiram empresas brasileiras, exigindo olhar cuidadoso sobre os documentos gerados e armazenados, através da força da lei para elevar o crescimento do mercado de gestão integrada de documentos e processos.

A partir de novas regras, o enfoque sobre a gestão dos documentos poderá mudar nas empresas. Não se tratando apenas de gerenciar arquivos num formato de mídia específico, mas também todos os registros, independente da mídia utilizada, desde a criação até a destruição ou arquivamento permanente.

2.1.1. Sarbanes-Oxley Act

Nos Estados Unidos, a cultura "acionária" é amplamente difundida, assim, desde o pequeno poupador até os grandes fundos movimentam bilhões de dólares em carteiras de ações negociadas em bolsa (NYSE e NASDAq).

Com os escândalos corporativos de manipulação de dados contábeis nas empresas Enron e WorldCom, o Congresso norte-americano aprovou e o presidente George W. Bush sancionou em julho de 2002, a Lei Sarbanes-Oxley Act (uma referência a dois membros do congresso responsáveis pela elaboração: Paul S. Sarbanes e Michael Oxley), considerada a mais importante reforma legislativa do mercado de capitais desde os Securities Acts de 1933 e de 1934, logo após a quebra da bolsa de valores de Nova York em 1929.

A Lei foi criada devido à preocupação com maiores danos que poderiam ser causados e o impacto negativo. E, desta vez, o principal objetivo não foi dar mais informações ao mercado, e sim, elevar o padrão de conduta ética e estabelecer responsabilidades nos níveis mais altos: presidência e diretoria da empresa, incluindo auditorias e advogados contratados. Passando a introduzir regras de governança corporativa, dando transparência e confiabilidade aos resultados das organizações.

Para isso, estabelece que os principais executivos das principais companhias de capital aberto confiram os relatórios periódicos entregues a SEC - Securities and Exchange Comission. Atestando quanto à veracidade das informações, para que não ocorram declarações falsas ou omissas,

representando, de forma precisa, as condições financeiras e os resultados da companhia.

Além disso, exigem que o diretor presidente e o financeiro apresentem declarações que a companhia possui controles internos, estruturados de forma a assegurar que nenhuma informação relevante fuja ao conhecimento dos principais membros da administração. Não podendo mais alegar falta de conhecimento quanto às práticas contábeis adotadas nas empresas.

Em caso de violação da Lei, os envolvidos estarão sujeitos a penas que podem variar de dez a vinte anos de prisão e multas de até US$ 5 milhões.

Outro fator importante é a sua aplicabilidade às empresas estrangeiras que possuem valores mobiliários registrados na SEC, inclusive as brasileiras, que devem investir na guarda e gerenciamento de documentos em vários formatos, ampliando a definição de "destruição de documentos".

No Brasil, em maio de 2003, o Banco Central sancionou a Lei 3.081, que dispõe sobre a prestação de serviços de auditoria independente para as instituições financeiras. Determinando que o auditor independente deve elaborar como resultado do trabalho de auditoria realizado, relatórios de avaliação da qualidade e adequação do sistema de controles internos, inclusive sistemas de processamento eletrônico de dados.

2.1.2. Acordo da Basiléia II

Até pouco tempo, a prática de segurança da informação era uma decisão interna, mas isso está mudando com o Acordo da Basiléia II. Trazendo os riscos operacionais para a análise de riscos, inseriu-os dentro do limite teto de até 8% de implicação do capital total da empresa, somados ao risco de crédito e de mercado.

Assim, passou a ser considerado risco: erros do funcionário, falhas de computador, documentação irregular, fraudes eletrônicas e passivo judicial. Necessitando converter documentos em papel para eletrônicos, aplicar mecanismos de segurança como assinatura digital e reduzir custos.

Apesar do Tratado da Basiléia incidir sobre as empresas do ramo financeiro e de crédito, sua aplicação deve ser dar em efeito cascata, exigindo processos e metodologias recíprocas, com espelhos de segurança. Levando-se em consideração, a impossibilidade de reduzir os riscos operacionais sem uma prática geral do mercado e sem investimento na educação do usuário, desde o funcionário até o fornecedor e cliente final.

2.2. Aspectos Culturais

Um estudo realizado pela Universidade da Califórnia, em Berkeley, nos Estados Unidos, apontou que em 2002, a população mundial produziu uma quantidade de informação nova suficiente para encher 500 mil bibliotecas do Congresso norte-americano.

Para condução dos trabalhos, a escola de gerenciamento da universidade diluiu os números em 5 bilhões de gigabytes de novos dados, cerca de 800 megabytes por pessoa, o que equivale a uma pilha de livros de nove metros de altura. Essa quantidade de informação pode estar armazenada em mídia impressa, filme, disco magnético e óptico, sendo vista ou ouvida, considerando telefone, rádio, TV e Internet. E, há previsões que indicam que, em 2020, o conhecimento duplicará a cada 83 dias, atualmente duplica a cada quatro anos [JORNAL DO GED, 2004 - Nº 61].

Apesar da tecnologia disponível, o consumo de papel nas empresas aumenta constantemente. A quantidade de informação arquivada em papel, incluindo-se livros, jornais e documentos de escritório, aumentou 43% quando comparada com semelhante estudo realizado em 1999 [GIMSON, 1997].

Isso acontece porque o desenvolvimento da tecnologia não foi acompanhado pela mudança cultural: documentos em mídia digital são criados mais facilmente e em maior número e constantemente "baixados" no papel.

Exemplos comuns: alguns executivos determinam às secretárias imprimir os e-mails recebidos; em seguida, ditam ou esboçam uma resposta e determinam às mesmas que respondam via e-mail. Em outros casos, determinam à secretária que peça ao remetente que assine a cópia impressa do e-mail (por não acreditar na segurança de senhas). Num segundo momento, quando passam a responder às mensagens via e-mail (enviados pela secretária), determinam que a resposta seja impressa e que a secretária colete uma assinatura do destinatário na cópia, e evidentemente, todas essas cópias acabam sendo arquivadas.

Há algumas boas razões para que cópias em papel sejam geradas: DILLON [1992] adverte que usuários retêm 30% a mais do que lêem em papel do que em monitores. Outro fator a ser evidenciado são as resistências ao uso da tecnologia, por diversas origens, sendo que algumas são previsíveis:

- **Resistência à mudança:** por uma questão de pura inércia, às vezes, os funcionários não querem mudar a forma de trabalho, a qual estão habituados há muito tempo. Podendo não representar má vontade ou indiferença, e sim, que a mudança gera tensão nos envolvidos.

- **Manuseio do papel:** há muito tempo o papel é o principal meio físico utilizado para escrita ou desenho, tornando-se cômodo, prático, fácil de reproduzir e reconhecido por qualquer indivíduo, desde a infância. Tornando-se hábito comum e confortável, usar canetas em reuniões e durante a leitura de livros. Gerando desconforto inicial, usar somente documentos eletrônicos.

- **Visualização no monitor é de pior qualidade:** a resolução do texto impresso é muito melhor que aqueles apresentados em tela, devido a razões físicas e construtivas que fazem com que a visualização no monitor seja realmente de menor definição.

- **Segurança:** normalmente as pessoas acreditam que o papel é meio mais seguro, pois temem que salvando em meio eletrônico, podem se deteriorar, perdendo o conteúdo.

- **Ergonomia:** alguns poderão reclamar, muitas vezes com razão, que a exposição direta ao computador, sem as "folgas" de tempo longe dele, gera desconforto e tensão.

- **Sindicais:** não se pode ignorar o fato de que o aumento de produtividade pode significar tempo para tomada de decisão, mas pode significar também que novos postos de trabalho podem não surgir.

É preciso levar em consideração a cultura organizacional, quando se deseja mudar o "*modus operandi"* de uma empresa. Sendo imprescindível administrar as situações de medo e desconforto que irão aflorar, respeitando os valores das organizações.

Tornando-se necessário reconhecer os diversos tipos de pessoas que irão interagir com a mudança, para saber como transformá-los em aliados do projeto. Desde os contatos iniciais, com o medo do desconhecido e sua natural

rejeição, até o domínio pleno da tecnologia por meio do conhecimento de uso, chegando à fase de cooperação e interação.

Na primeira fase de implantação do "escritório sem papel", recomenda-se explorar os recursos do e-mail. Assim, as pessoas terão o primeiro contato com um documento eletrônico de forma menos agressiva que o usuário acostumado a ler documentos em papel, já que, teoricamente, a leitura de e-mails é feita no monitor. Sabendo-se que, inicialmente, ao receber um e-mail o usuário irá imprimir porque ainda quer ter os dados em papel, e com o passar do tempo, acabará abandonando esse costume.

2.3. Aspectos Financeiros

Vale a pena analisarmos questões financeiras, vejamos algumas pesquisas interessantes sobre o consumo de tempo e dinheiro que ocorre no gerenciamento de documentos:

- Executivos gastam em média 150 horas / ano, procurando, localizando, solicitando e esperando documentos [COOPERS & LYBRAND].
- Em cada 20 documentos, um se perde [COOPERS & LYBRAND].
- Executivos gastam 20% a 45% do tempo pensando, criando ou manipulando documentos [GARTNER GROUP].
- Um funcionário guarda em média 20.000 folhas de papel por ano em arquivos dos mais diversos tipos [GARTNER GROUP].
- Consome 12% a 15% de renda da empresa [GARTNER GROUP].
- Em média, 90% do tempo da vida útil de um documento é gasto em trânsito e filas. Ou seja, necessita gerenciamento [DELPHI CONSULTING].
- Gastam-se U$ 250 para recriar um documento de engenharia perdido [COOPERS & LYBRAND].
- As pessoas perdem entre 20% e 30% de seu tempo, localizando e recuperando informações [CYCO].
- Processos trabalhistas são perdidos por não se localizar o documento correto no prazo estipulado da Lei [FEM].

Por outro lado,

- 71% de executivos e gerentes pesquisados pela NFI Research gastam uma hora ou mais todos os dias, enviando, recebendo, lendo e escrevendo e-mails. [REVISTA BUSINESS STANDARD].

- Mais de 25% gastam três ou mais horas por dia com e-mails [REVISTA BUSINESS STANDARD].
- 68% dizem que 25% ou mais de seus e-mails não são necessários [REVISTA BUSINESS STANDARD].

No aspecto financeiro, o aumento da produtividade é fundamental, uma vez que, as organizações estão mais interessadas em se livrar da papelada desnecessária e reduzir custos com aluguel de espaço físico para comportar toneladas e mais toneladas de documentos. Assim, transferem documentos em papel para mídias eletrônicas, conseguindo mais agilidade na recuperação de informações e, conseqüentemente, mais competitividade no mercado numa economia cada vez mais globalizada.

O papel e o microfilme são mídias que em situações de freqüente acesso não conseguem trazer ganhos de produtividade aos processos tradicionais de negócios. A rápida localização de documentos ajuda a tornar mais eficiente o serviço prestado por uma empresa.

Outro fator importante é a redução de custos. Tendo em mente que a principal razão está no ganho em produtividade, e não na liberação do espaço físico. Além disso, nem sempre o custo/benefício da migração justifica a implantação da tecnologia, porém, em longo prazo, o papel poderá ser eliminado de forma contínua, devido a considerações tecnológicas.

É preciso fazer um levantamento bem feito de volume, tipos de documentos, estruturas de índices que se pretende atribuir aos documentos, qual o prazo de retenção para que os documentos fiquem no sistema, qual a plataforma de processamento de dados disponível e qual o produto que mais se aproxima aos requerimentos iniciais. Olhando sempre para dentro e avaliando o cenário da organização antes de optar pela tecnologia.

Outros fatores complementares ajudam a justificar ou viabilizar a tecnologia, tais como proteção contra catástrofes. É difícil fazer cópias de segurança de arquivos de papel, enquanto em arquivos eletrônicos, o procedimento de backup é trivial.

2.4. Aspectos Tecnológicos

Apesar das mudanças que ocorreram no desenvolvimento da tecnologia nas últimas três décadas, observa-se que algumas contribuíram para o aumento da impressão, geradas por duas tendências tecnológicas significantes:

Tendência 1 - A primeira tendência indica que a conectividade aumentou o acesso a informações que não havia anteriormente. Cada vez mais estações de trabalho estão completamente conectadas, e também em casa. Além disso, o aumento de impressão é fomentado com: a conexão mais barata, aumento na largura de banda, facilidade em trazer mais informação ao desktop, estar conectado a outras pessoas e a habilidade de enviar informação a outros.

Em uma pesquisa realizada em 150 empresas norte-americanas comprovou-se por informação dos gerentes que as redes com acesso à Internet, aumentaram notavelmente a impressão [SELLEN e HARPER, 2003]. Outro estudo realizado pela Pricewaterhouse Coopers concluiu que, o uso do e-mail corporativo vem causando um aumento considerável de 40% no consumo de papel.

Enquanto o uso de e-mail para enviar e distribuir documentos e mensagens, extinguiu os memorandos em papel, não acabaram completamente com o papel. Muitos e-mails tendem a ser impressos, inclusive anexos extensos. As pessoas adquirem mais mensagens do que recebiam se usasse o correio convencional. Parece que quanto mais recebem, mais

imprimem, comprovando que cada funcionário de escritório gera cerca de 125 quilos de papel impresso a cada ano [JORNAL DO GED, 2003 - Nº 57].

Tendência 2 - Uma segunda tendência é o avanço da tecnologia de impressão. Nos últimos vinte anos, houve mudanças bastante significativas no modo como os documentos são impressos e em que consistem. Previamente, se quisessem distribuir cópias de um documento a seus colegas, primeiro imprimiam, tirariam cópia (xerox) e, então distribuíam. Atualmente, em lugar de imprimir e distribuir, apenas distribui-se e então se imprimi. Em outras palavras, enviamos eletronicamente o arquivo ao destinatário, para que este imprima.

[GIMSON, 1997] cita que, entre 1988 e 1993, o número de copiadoras aumentou, pelo menos, 5% no mundo, enquanto que o número de impressoras aumentou 600% Além disso, as impressoras multifuncionais (impressora, fax, scanner e copiadora num único dispositivo) contendo modernas técnicas possibilitam imprimir cópias diretamente de uma fonte digital. Até mesmo quando o usuário fizer uma cópia de um documento em papel, primeiramente, o documento será analisado, convertido em arquivo digital, e então impresso.

Outro fato é impressão sob demanda. Anteriormente, a produção era freqüentemente terminada em grandes centros de impressão, em larga escala. Atualmente, conectar-se a impressoras digitais, permitem a impressão de documentos como e quando houver necessidade. Uma vez que, as impressoras estão mais baratas, mais rápidas e de melhor qualidade do que

antes. Um bom exemplo é da impressão colorida que, passou a ser comum, tanto em casa como no escritório, pois as pessoas e organizações têm mais controle no que imprimem, quando imprimem, e por onde imprimem.

Na última década, novas tecnologias proveram meios pelos quais podem-se produzir documentos em papel baratos, de alta qualidade e personalizados, tornando vantajoso, imprimir e consumir mais papel. Enquanto as tecnologias encorajam o uso de papel, também permitem trabalhar efetivamente com documentos digitais. Por exemplo:

- Processadores de texto substituíram virtualmente a máquina de escrever para a criação e modificação de documentos pessoais e relacionados ao trabalho como memorandos e cartas.
- O e-mail é tão comum e praticamente, erradicou os antigos memorandos nos escritórios. O envio de mensagens eletrônicas é o modo principal para enviar e distribuir documentos, mensagens e memorandos dentro e fora das organizações.
- Os computadores tornaram-se menores, mais leves, sem fios e com baterias mais duradouras. Pode-se trabalhar com documentos digitais com acesso a rede em qualquer lugar.
- Muitos documentos que antes eram exclusivos do meio físico passaram a ser digital, como: manuais de referência, dicionários, enciclopédias, documentação técnica, formulários, catálogos, relatórios informativos, revistas e diários.
- Conversão dos documentos em papel ao formato digital reduziu custos com arquivamento que passou a ser fácil de localizar.

- Arquivos em mídia digital mais baratos e eficientes estão tornando possível o armazenamento de enormes quantidades de informação digital, incluindo o CD-ROM, DVD, disco óptico, fita magnética e discos rígidos. Calcula-se que, em 1995, 95% de todos os documentos em organizações foram armazenados em papel permanecendo 5% em meio digital [JORNAL DO GED, 2003, Nº 57], a proporção de documentos armazenados em papel tem diminuído substancialmente nos últimos anos.

Em 1993, Paul Saffo comparou a situação a uma piñata eletrônica (balão de papel) cercada por uma fina camada de papel [THE ELETRONIC PIÑATA: A Paperless Future is waiting in the Wings, 1993, Institute for the Future]. Conforme o balão cresce, a superfície da esfera também cresce, porém a uma taxa muito mais lenta. Pensando assim, o volume de informação baseada em papel continuou crescendo mais ou menos linearmente, enquanto o volume de informação eletrônica aumentou exponencialmente.

Assim, a relação entre papel e tecnologia digital no escritório é muito mais complexa que se possa imaginar. Freqüentemente, novas tecnologias favorecem a utilização do papel ao invés de substituí-lo completamente, podendo alterar o trabalho no escritório: às vezes anulando a necessidade de papel e outrora criando mais demanda.

Para entender porque isto acontece, precisa-se entender a razão pelas quais, algumas atividades humanas são mais bem executadas com papel do que usando alternativas digitais. Algumas tecnologias são inferiores ao papel para determinadas tarefas-chave.

Por exemplo, designers dispensaram pouca atenção na fabricação dos “e-books”, não levando em consideração a necessidade das pessoas em navegá-los completamente. Uma vez que, essa tecnologia forneça igual ou melhor sustentação à maioria das tarefas que são do "trabalho central do conhecimento", o futuro do papel poderá ser diferente.

Assim, alternativas tecnológicas têm sido importantes para o escritório sem papel, conforme descrevo a seguir.

2.4.1. GED - Gerenciamento Eletrônico de Documentos

O GED - Gerenciamento Eletrônico de Documentos é um grupo de tecnologias, divididas em cinco funcionalidades básicas: captação, gerenciamento, armazenamento, distribuição e preservação. Dentro dessas funcionalidades, cada tecnologia tem uma função específica. Podendo trabalhar separadas ou em conjunto, promovem a organização de informações conforme a necessidade da empresa em adequação ao “core-business” e processos de negócio. Podendo significar a capacidade de dirigir e controlar todo o capital intelectual da empresa de forma muito mais eficiente.

A redução de espaço físico de armazenagem e do tempo necessário para a localização de um documento, o aumento de produtividade, a melhoria no atendimento ao cliente, maior segurança e controle no acesso aos documentos e a capitalização do conhecimento da empresa têm sido as principais vantagens apontadas, pois significam tornar documentos disponíveis de forma extremamente eficiente para o usuário e permitem 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.

Devendo ser considerado documento, como qualquer papel que contenha informação relevante, ou qualquer arquivo digital que possa ser impresso de forma legível e sendo transformado em documento em papel. Exemplos de documento:

- Desenho.
- Manuscrito.
- Arquivo de processador de texto.
- Formulários.
- Cheque ou outro documento financeiro.
- Nota fiscal.

2.4.1.1. Componentes do GED:

- **Armazenamento:** pode ser no próprio servidor de imagens ou outro ambiente computacional.

- **Documento:** pode estar em papel ou nativamente digital.

- **Estação de trabalho:** computador que permite consultar, criar novos documentos, cadastrar documentos existentes, etc.

- **Impressora:** usada para obter uma cópia física do documento.

- **Processador:** os sistemas GED podem instalados no servidor, em rede para distribuição das informações, ou ainda individualmente, nas estações de trabalho.

- **Rede:** meio de comunicação entre os diversos componentes do sistema.

- **Scanner:** equipamento usado para digitalizar documentos, ou seja, obter uma imagem do documento a ser armazenada eletronicamente.

2.4.1.2. Captação

É o modo como informações e documentos eletrônicos ou em papel, passar a um repositório de conteúdo para reutilizar, distribuir e armazenar.

- **Agregação:** o processo de combinar a entrada de dados de criação e auditoria de diferentes ferramentas e outros sistemas.

- **COLD/ERM:** embora o termo COLD (Computer Output to Laser Disk) seja bastante utilizado, pouco a pouco vem sem substituído por ERM (Enterprise Report Management), o objetivo desta aplicação é armazenar e indexar saídas de computador (inicialmente relatórios) em discos magnéticos, discos ópticos e fitas magnéticas. Uma vez armazenados, podem ser acessados, visualizados, impressos, transmitidos por fax ou distribuídos via Internet. Aplicações típicas: faturas de telefone, energia elétrica, água; extratos bancários; relatórios financeiros.

- **Categorização:** organiza documentos, páginas Web e outros conteúdos em um agrupamento lógico baseado no próprio conteúdo.

- **Document Imaging:** processo de captação, armazenamento e busca de documentos, independente do formato original.

- **E-forms/Webforms:** formulários desenhados, gerenciados e completamente processados num ambiente eletrônico.
- **Forms Processing:** tecnologias aplicáveis na captura de dados de formulários digitalizados em campos e linhas, por meio de padrões de reconhecimento inteligente como OCR, ICR, código de barras, marcas, e outros, visando alimentar banco de dados. Tendo como objetivo minimizar a grande aplicação de recursos em indexação e obtenção de dados que tradicionalmente são inseridos manualmente.
  - **OCR (Optical Character Recognition):** permite reconhecer caracteres impressos ou digitados em dados processáveis pelo computador. É o processo mais difundido, pois possui aplicação bem diversificada, especialmente na recuperação de documentos antigos.
  - **ICR (Intelligent Character Recognition):** permite reconhecer manuscritos em documentos. Utilizado em documentos preenchidos manualmente, como pesquisas, pedidos de material, formulários em serviços públicos, entre outros. Além disso, pode incluir capacidade para aprender fontes durante o processo ou usar o contexto para fortalecer as probabilidades de reconhecimento correto ou reconhecer caracteres manuscritos.
  - **OMR (Optical Mark Reader):** habilidade de detectar a presença de informações marcadas, como "listbox".
  - **BCR (Bar Code Reader):** habilidade de reconhecer / interpretar código de barras em dados processáveis.
  - **MICR (Magnetic Ink Coated Recognition)**: habilidade de reconhecer/interpretar conjuntos de caracteres altamente estilizados, impressos com tinta magnética para otimização do processo de

reconhecimento. Os reconhecimentos mais utilizados: CMC-7 para caracteres não sólidos, como cheques e E13-B para caracteres notadamente formados.

- **Indexação:** identificação e atributos específicos de um documento ou arquivo de base de dados para facilitar a busca.

2.4.1.3. Armazenamento

É onde se guarda o conteúdo e como pode ser encontrado.

- **Content Management System:** capacidade para gerenciar e rastrear o local e relacionamento entre conteúdo e repositório de dados.

- **Database:** coleção eletrônica de registros ou elementos de dados armazenados num arquivo central ou banco de dados relacional, acessíveis a muitos usuários.

- **Disco óptico (CD-ROM/DVD):** mídia que aceita e retém informações na forma de marcas ou densidade de modulação numa camada de gravação que pode ser lida com um feixe óptico.

- **Fita:** mídia de armazenamento magnética.

2.4.1.4. Gerenciamento

São ferramentas e técnicas pra mover conteúdo pela organização e monitorar seu desempenho.

- **Colaboração:** ferramentas (auditoria colaborativa, vídeo-conferência) que permitem a usuários trabalhar o mesmo conteúdo num ambiente comum.

- **Document Management:** software que controla e organiza documentos pela empresa, incorporação captação de conteúdo e documento, Workflow, sistemas de saída e busca de informações.

- **Web Content Management:** tecnologia para direcionar a criação do conteúdo, revisão, aprovação e processo de publicação de conteúdo baseado em Web.

- **Gestão Documental:** capacitar a empresa determinar um ciclo de vida específico a uma peça individual de informação corporativa desde a criação, recebimento, manutenção e uso para a última disposição dos registros. Um registro não é, necessariamente, o mesmo que um documento. Todos os documentos são potenciais registros, e não vice-versa, onde o registro é essencial ao negócio e documentos são containers de informação para se trabalhar.

2.4.1.5. Distribuição

Meio para conseguir o conteúdo correto ao público certo quando necessário.

- **PDF (Portable Document Format):** formato desenvolvido na Adobe Systems para publicação de documentos. Atualmente, a NPES - Association for Supplies of Printing, Publishing and Converting Technologies e a AIIM - Association for Information and Image Management estão juntas num projeto que pretende desenvolver um padrão internacional para definir o uso deste formato, batizado de PDF/A, será encaminhado a um grupo de trabalho da ISO - International Organization for Standartization, uma vez que não possui regras definidas para esse formato.

  Visando caminhar à necessidade cada vez maior de se armazenar documentos eletronicamente, a fim de assegurar a preservação de seus conteúdos por um longo período de tempo, e que, futuramente, possam ser localizados e recuperados. Incluindo documentos de múltiplas páginas, contendo imagens, textos, gráficos vetorizados, entre outros.

- **Compressão:** técnica usada para reduzir o número de bits num arquivo de imagem digital como tiff e jpeg.

- **Personalização:** relaciona o conteúdo ao indivíduo.

- **Transformação:** a troca do formato de um conteúdo para outro, conforme a necessidade da distribuição.

2.4.1.6. Preservação

Meio para conseguir o conteúdo correto ao público certo quando necessário.

- **Microfilme:** pode ser um registro micrográfico ou filme de grão fino para registrar imagens reduzidas em tamanho com relação ao original.

- **Papel:** secular, um dos modos de assegurar que documentos sejam lidos daqui a cem anos ou mais, desde que protegidos corretamente, porém ocupam espaço físico.

2.4.2.Workflow

[CRUZ, 2000] define "Workflow" como a automação de processos de negócio no todo ou em parte, em que documentos, informação ou tarefas são passadas de um participante a outro para ação, de acordo com regras estabelecidas. Um processo de negócio é um conjunto logicamente relatado de fluxos de trabalho, passos de trabalho e tarefas que provêm um produto ou serviço para clientes.

Essa tecnologia permite gerenciar de forma pró-ativa qualquer processo de negócio das empresas e, se aplica à descrição de uma sucessão de tarefas necessárias para processar documentos enquanto estes tramitam na organização.

2.4.2.1. Tipos de Workflow

- **Ad-hoc:** é aquele criado para ser usado dinamicamente por grupos de trabalho, cujos participantes necessitem executar procedimentos individualizados para cada documento processado, dentro do fluxo de trabalho. Normalmente é composto de regras que, dificilmente se repetem, por inteiro, a cada documento que tenha que ser trabalhado pela atividade. É o tipo mais elementar de workflow existente, pois é uma forma elementar de quebrar resistência cultural, como o e-mail.

- **Produção / Transação:** trata-se de um sistema voltado para o processamento de grandes volumes de dados, muita política de negócio e recursos financeiros em grande escala. Fazendo com que desenvolvimento e implantação tenham que ser cuidadosamente planejados. Os dados tratados por esse tipo de workflow têm duas origens: uma no próprio fluxo e outra em banco de dados, que suportam as aplicações ligadas ao sistema.

- **Administrativo:** é orientado para rotinas administrativas, sendo um pouco mais complexo que o ad-hoc e mais simples que o de transação. Pois têm características de sistemas de correio eletrônico, mas com algumas capacidades a mais, tornando ideal para o tratamento de documentos e formulários que servem de suporte para rotinas, que, embora repetitivas, e aparentemente sem complexidade, precisam ser realizadas corretamente. Exemplos desse tipo são rotinas de aprovação de despesas, controle de gastos de viagens, aprovação de ordens de compras e todo um conjunto de necessidades que genericamente são conhecidas como rotinas administrativas.

- **Orientado para Objeto:** são versões sofisticadas dos sistemas de workflow orientados para transações. Permitindo o desenvolvimento de aplicações mais complexas, permitindo facilidades que em outra tecnologia seria impossível, tanto na programação como no uso.

  Tem como características peculiares: encapsulamento, direito de herança, integridade referencial, procedimentos compostos, bibliotecas procedurais e ambiente gráfico baseado em ícones, todos encontrados no ambiente orientado a objetos.

- **Baseado no conhecimento:** esse tipo de workflow tem características e ferramentas que permitem aprender com seus próprios erros e acertos. Qualquer sistema baseado no conhecimento tem tecnologia para ir além da execução pura e simples das regras preestabelecidas e incorporar exceções a seus procedimentos. Inteligência artificial é uma das tecnologias que permitem a esse tipo de workflow, aprenderem consigo mesmo. Outra tecnologia são sistemas especialistas, desenvolvidos para poderem inferir solução a partir da vivência de fatos do cotidiano.

  Um sistema workflow baseado no conhecimento, desenvolvido com técnicas estatísticas, heurísticas, inteligência artificial e usando os mesmos princípios de reconhecimento de padrões com que são construídas as redes neurais, poderá ser a solução às freqüentes mudanças que o fluxo venha a sofrer para acompanhar a dinâmica do processo de negócio das organizações.

  "No dia em que surgir um sistema workflow baseado no conhecimento estará quebrando mais um paradigma na gestão de processos" [CRUZ, 2000].

2.4.3.Estudos de Caso

2.4.3.1. Setor Público

Organismos públicos, por serem grandes gerados de documentos e por terem cada vez mais a necessidade de atender melhor o cidadão, demonstram grande preocupação com a Gestão Documental e com a implantação das tecnologias do GED.

- **Copel - Companhia Paranaense de Energia:** os documentos gerados nas diversas áreas têm seus prazos de retenção determinados pelo que estabelece a legislação ou a necessidade empresarial. Após arquivamento nas áreas para uso corrente, são encaminhados ao arquivo geral para serem gerados arquivos eletrônicos, em microfilme ou digitalizado.

  Anteriormente, esse processo era manual, com auxílio de planilha eletrônica, aplicativos mainframe, não integrados e defasados tecnologicamente, além de estarem sem padrão, pois estavam baseados no conhecimento do quadro de pessoal, dos aplicativos, do fluxo e da localização física dos documentos.

- **TRT - Tribunal Regional do Trabalho da 3ª Região, em São Paulo:** implantou o programa de gestão de documentos, visando a racionalização do ciclo documental por meio de normas para a produção, fluxo, arquivamento e destinação final dos documentos, eliminação ou guarda permanente. Sendo classificados por assunto, prazos de guarda em cada setor e no arquivo geral. Tendo por objetivo a eliminação do papel para as requisições de documentos, como já ocorre na 1ª Instância, onde o prazo de cumprimento das requisições foi reduzido de seis dias para 48 horas.

- **TRT - Tribunal Regional do Trabalho da 4ª Região, em Porto Alegre:** escolheu a comunicação eletrônica para julgamentos de processos da segunda instância. Com isso, a pilha de 40 mil processos caiu para zero e os processos julgados por dia passaram de 120 para 200. O tempo médio das sessões do julgamento foi de dez horas para apenas seis. E principalmente, foram economizados cerca de R$ 240 mil com papel e impressão, já que 2,4 milhões de páginas não precisam ser impressas. Após o julgamento, o resultado é publicado, na íntegra, via Internet.

- **ANA - Agência Nacional de Águas:** a implantação do sistema de gestão documental iniciou-se com um sistema informatizado de gestão de documentos e arquivos que trouxe organização à Instituição e desburocratizando várias atividades, beneficiando servidores e cidadãos envolvidos com a documentação. Sendo possível substituir a prática informal pelo recebimento eletrônico de documentos; elaborar correspondências com base em modelos pré-definidos; obter numeração automática de documentos; emitir etiquetas com código de barras para identificar os documentos; possibilitar pesquisas via Intranet e Internet por meio de palavras-chave, assunto, data do documento, etc.; disponibilizar a imagem das correspondências recebidas por meio de digitalização e as produzidas por meio de anexação de arquivo digital ao registro cadastrado, entre outros serviços. Antes do sistema, não havia controle informatizado de gestão documental, exceto o Protocolo Geral. O controle era manual ou informal em sua maioria em cadernos de protocolos, e para saber sobre determinado processo, era necessário fazer uma ligação telefônica para determinado setor.

2.4.3.2. Setor Privado

O setor privado também investe em soluções GED.

- **EMI Music:** contratos originais assinados por Carmem Miranda e outros artistas do mundo da música é parte valiosa do acervo das quais um sistema GED está cuidando muito bem. Esses documentos determinam os percentuais negociados e assinalam todo o recolhimento de direitos autorais relativos à gravadora, bem como a participação dos artistas na venda da obra. O projeto foi dividido em oito etapas, onde fizeram levantamento documental e catalogação dos documentos com as análises e adequações que sustentaram a implantação de GED na empresa.

- **Stefanini:** batizado de NetDocs, o sistema para GED é totalmente web, permite o gerenciamento físico e digital de documentos. Instalado num servidor da empresa, disponibiliza documentos, de acordo com a permissão de acesso, para funcionários e parceiros via Internet ou Intranet. Possui os módulos workflow para controle de aprovação de formulários, via serviço de mensagens, com freqüência pré-determinada, pelas quais os envolvidos recebem aviso de trabalho pendente, e o módulo bibliotecário, subdividido em documentos físicos e eletrônicos, no ambiente físico, controla e reserva empréstimos de livros e revistas, já no eletrônico, armazena qualquer tipo de arquivo, permitindo visualização ou download, mantendo histórico com data e identificação do usuário.

- **Dow Química:** o departamento de Pesquisa e Desenvolvimento de Poliglicóis possui um acervo significativo de relatórios de pesquisa, artigos científicos e contribuições de pesquisadores. Por meio do programa de eliminação do papel, batizado de Zero Paper, buscava-se uma solução para a conversão desse material em meio digital. Utilizando a ferramenta Adobe Acrobat, permitiu o aproveitamento de variados recursos, com o desenho de uma base de documentos em PDF, descritos em metadados, alimentados numa estação usando recursos de formulário eletrônico. Após alimentação, os dados são migrados para dentro dos PDFs de cada documento, onde passam a ser pesquisáveis nos campos de autor, data e palavras-chave.

3. Segurança da Informação

Nos últimos anos, as redes de computadores foram utilizadas por pesquisadores universitários para enviar mensagens eletrônicas, e também, por funcionários de empresas para compartilhar periféricos. Sob essas condições, as redes nunca precisaram de maiores cuidados.

Naquela época, as informações eram armazenadas em papel e a segurança era relativamente simples. Com as mudanças tecnológicas e o uso do mainframe, a estrutura de segurança ficou mais sofisticada com controles centralizados.

Fatores como a chegada de computadores pessoais, redes departamentais e a Internet, elevaram os aspectos de segurança a um patamar de tamanha complexidade, surgindo a necessidade de desenvolvimento de equipes especializadas no gerenciamento dessa infra-estrutura.

A Internet constitui risco potencial à segurança da informação, pois conecta milhões de computadores. Nesse ínterim, um usuário comum realiza transações bancárias, trafega dados pessoais e compra em sites na Web, e caso não esteja protegido suas informações podem ser capturadas.

[TANEMBAUM, 2003] define a segurança como um assunto abrangente que inclui inúmeros tipos de problemas. Em sua forma mais simples, a segurança se preocupa em garantir que pessoas mal-intencionadas

não leiam, ou pior ainda, modifiquem secretamente mensagens enviadas a outros destinatários. Outra preocupação da segurança são pessoas que tentam ter acesso a serviços remotos que não estão autorizadas a usar. Além disso, lida com meios para saber se uma mensagem supostamente verdadeira é um trote. Tratando de situações em que mensagens legítimas são capturadas e reproduzidas, além de lidar com pessoas que tentam negar o fato de terem enviado determinadas mensagens.

A segurança da informação pode ser definida como um conjunto de medidas que, se constituem de controles e políticas de segurança, tendo como objetivo a proteção das informações dos clientes e da empresa, controlando o risco de revelação ou alteração por pessoas não autorizadas.

Na sociedade da informação, as informações fazem parte do patrimônio de uma empresa, estando contidas em sistemas computacionais e considerados recursos críticos, tanto para concretização de negócios e tomada de decisões. Pode-se imaginar o que ocorreria se informações institucionais fossem parar nas mãos da principal concorrente ou fossem corrompidas ou apagadas. Nunca foi tão fácil atacar os sistemas informatizados, uma vez que, sistemas de informação institucionais estão conectados a redes externas.

Outro aspecto a ser considerado é o fato que sistemas de informática devem operar de forma adequada e garantam a segurança das informações, necessitando de ambientes controlados, protegidos contra desastres naturais (incêndio, terremoto, enchente), falhas estruturais (interrupção no

fornecimento de energia elétrica, sobrecargas elétricas), sabotagens, fraudes, acessos não autorizados e outros, utilizando contingências.

Segurança é, portanto, a proteção de informações, sistemas, recursos e serviços contra desastres, erros e manipulação indevida e não autorizada, de forma a reduzir a probabilidade e o impacto de incidentes de segurança.

3.1. Política de Segurança

É a formalização de conceitos, normas e procedimentos de segurança que visam dar proteção, controle e monitoramento do processo de segurança implantado no ambiente de tecnologia. Devem ser levantados as ameaças, riscos e vulnerabilidades que podem ocorrer com as informações.

Sua principal função é informar sobre os direitos e obrigações para proteção da tecnologia e o acesso à informação. Proporcionando o direcionamento para implementações técnicas seja para adquirir, configurar ou auditar sistemas e redes, adequando aos requisitos propostos.

Também é responsabilidade da política de segurança ditar as regras, e expressar o que os usuários devem e não devem fazer em relação aos diversos componentes do sistema, incluindo o tipo de tráfego permitido na rede. Devendo ter a aceitação e o suporte de todos os níveis de empregados dentro da empresa, para que se torne apropriada e efetiva.

Constitui-se em:

- Integridade;
- Confidencialidade;
- Disponibilidade;
- Legalidade.

As informações da empresa são classificadas de acordo com o grau de importância:

- Informações confidenciais;
- Informações corporativas;
- Informações públicas.

A elaboração da política de segurança passa pelas etapas:

- Definir a equipe responsável pela implantação e manutenção da segurança;
- Analisar as necessidades e procedimentos utilizados pela empresa;
- Identificar os processos críticos;
- Classificar a Informação;
- Definir o Uso: Confidencial, Interno, Público;
- Elaborar normas e procedimentos para técnicos e usuários;
- Definir plano de recuperação a desastres ou plano de contingência;
- Definir sanções ou penalidades pelo não-cumprimento da política;
- Elaborar termo de compromisso;
- Comunicar a diretoria / presidência e aos funcionários;
- Divulgar a política;
- Implementar;
- Revisar a política.

3.2. Adversários da Segurança

[SCHNEIER, 2001] adverte que os adversários da segurança da informação são os mesmos que existem no ambiente físico: criminosos comuns procurando ganho financeiro, espiões industriais procurando vantagem competitiva, hackers procurando conhecimento secreto e, agências de inteligência militar. As pessoas não mudaram, simplesmente o ambiente virtual é um novo lugar para exercer suas atividades. Eles podem ser categorizados por objetivos, acesso, recursos, habilidade e risco.

- **Objetivos:** os adversários possuem objetivos variados como dano puro, lucro financeiro, informações e assim por diante. Um exemplo é que o objetivo de um espião industrial é diferente de um sindicato do crime organizado, e as medidas para evitar o primeiro, podem nem sequer intimidar o segundo. Entender os objetivos de prováveis atacantes é a primeira etapa para descobrir quais medidas de contra-ataque serão eficientes.
- **Níveis de acesso:** os adversários possuem diferentes níveis de acesso - um empregado interno possui muito mais acesso do que alguém de fora da organização.
- **Níveis de habilidade:** alguns ataques exigem muita habilidade, como desvendar um algoritmo de criptografia, por exemplo. Alguns adversários possuem um conhecimento da tecnologia em nível básico, sendo controlados por um desejo de entender. Outros podem ter uma habilidade considerável, maior que a dos projetistas originais do sistema, pois vêem o sistema do lado de fora como um atacante.

- **Níveis de recurso:** os adversários possuem acesso a diferentes níveis de recurso, alguns têm muito dinheiro, outros operam sem capital. O adversário rico é o mais flexível, pois pode trocar recursos por outras coisas, inclusive pagando a um empregado da empresa para acessar os dados, comprar tecnologia ou até contratar especialistas para invadir sistemas.
- **Níveis de risco:** diferentes adversários desejam tolerar diferentes níveis de risco. Terroristas dão-se por satisfeitos morrendo por sua causa. Crackers experientes arriscam passar um tempo na cadeia, roubando senhas de acesso a contas correntes, mas provavelmente não desejam se sacrificar em uma tentativa de assalto à banco. Os que buscam publicidade não querem ser presos.

O chefe de segurança do Setor de Crimes pela Internet da polícia de São Paulo, Mauro Marcelo de Lima e Silva no artigo "Os Crimes Digitais Hoje" [MODULO], avalia o perfil do criminoso de informática, baseando-se em pesquisa empírica e indica que os criminosos são jovens, educados, sexo masculino, com idade entre 16 e 32 anos, caucasianos, audaciosos e aventureiros, com inteligência bem acima da média e movidos pelo desafio da superação do conhecimento, além do sentimento de anonimato, que bloqueia seus parâmetros de entendimento para avaliar sua conduta como ilegal, sempre alegando ignorância do crime e, alegando ser apenas, uma brincadeira.

Exemplos de adversários mais comuns:

Adversário	Objetivo
Contador	Desviar dinheiro da empresa.
Corretor de Valores	Negar promessa feita a um cliente através de e-mail.
Craker	Testar o sistema de segurança; roubar dados.
Espião	Descobrir segredos militares ou industriais.
Estudante	Divertir-se, observando e-mails de outras pessoas.
Executivo	Descobrir a estratégia de marketing do concorrente.
Ex-funcionário	Vingar-se por ser demitido.
Terrorista	Descobrir segredos de armas bacteriológicas.
Vigarista	Roubar números de cartão de crédito e vendê-los.

3.2.1.Hackers

A palavra hacker possui várias denominações, desde um administrador de sistemas perito o suficiente para descobrir o funcionamento dos computadores até um adolescente com pouca ética que se diverte acabando com a rede. Não são criminosos, porém sua imagem é muito distorcida pela mídia. Na realidade, são especialistas em informática que procuram defeitos nos sistemas operacionais e programas e quando os descobrem, comunicam aos fabricantes, além de toda a comunidade interessada, através de informativos periódicos, listas de discussão ou "newsgroups". Esses indivíduos experimentam os limites dos sistemas por curiosidade intelectual ou mero prazer.

3.2.2.Crackers

São os adversários mais temidos da rede, pois são movidos pela fama e dinheiro. Sempre estão à procura de alguma brecha para invadir redes e roubar dados, ocasionando falhas em computadores, disseminando vírus e deformando páginas Web, além de escrever códigos maliciosos para invasão automática (spyware). Como geralmente agem em grupo, mantém páginas na Internet com informações e programas para invasão, além de serem muito solidários, quando fazem um bom programa, disponibilizam o código fonte na rede para que outros programadores retirem os defeitos do original e criem novas versões, mais avançadas, com recursos mais destrutivos.

No mundo virtual, o mais famoso é o norte-americano Kevin David Mitnick, que foi condenado por fraudes no sistema de telefonia, roubo de informações e invasão de sistemas, atualmente vive em liberdade condicional.

3.2.3.Carders

Estes criminosos solitários causam o aumento dos crimes relacionados a computador. Podem ser pessoas que têm acesso e que notam falhas nos sistemas, resolvendo explorá-las. Geralmente, se especializam na criação de programas que geram ou roubam números de cartão de crédito para conseguir dinheiro, possibilitando comprar em sites de comércio eletrônico, ou ainda roubar informações como nome e endereço para praticar extorsão.

3.2.4.Phreakers

São criminosos especializados em telefonia. Fazem parte de suas principais atividades as ligações gratuitas, tanto locais como interurbanas, reprogramação das centrais telefônicas e instalação de escutas, além de conseguir que um possível ataque a um sistema tenha como ponto de partida provedores de acessos em outros países, suas técnicas permitem não somente ficar invisível diante de um provável rastreamento, como também forjar o culpado da ligação fraudulenta.

O prejuízo causado pelos "Phreaker", no Brasil, gira em torno de 2% (dois por cento) do faturamento das operadoras de telefone móvel, aproximadamente, US$ 15 bilhões [MÓDULO, 2004].

3.2.5.Insiders Maliciosos

Um insider (pessoa que tem acesso a informações sigilosas) malicioso é um adversário perigoso e traiçoeiro. Pois já está dentro do sistema e pode ignorar defesas em torno dele. Normalmente, possui um alto nível de acesso e pode ser considerado confiável. Nem sempre ataca o sistema, e sim, corrompe para seus próprios fins. Não necessariamente é empregado, podendo ser consultor ou contratado.

Normalmente, sabe como o sistema funciona e onde estão os pontos fracos. Conhece a estrutura organizacional e como seria conduzida qualquer investigação contra suas ações.

3.2.6.Espionagem Industrial

O negócio é uma guerra e possui árbitros, que estabelecem regras e realizam o melhor para impô-las. Quando a técnica de investigação passa a ser ilegal, a inteligência competitiva termina e a espionagem industrial começa. Sendo motivada para obter vantagem sobre a concorrência, através do roubo de segredos comerciais dos concorrentes.

3.2.7.Hacktivista

Caracterizada por uma variedade de grupos ideológicos e indivíduos, essa categoria pode ser motivada por geopolítica ou etno-religião, ou por crenças morais e éticas. Geralmente se preocupam em causar danos a informações, de modo que suas técnicas estão ligadas à negação de serviço e destruição completa. Seus maiores objetivos são vingança, situações caóticas e publicidade sangrenta.

Em 1998, um grupo de hackers chamado The Legion of the Urderground declarou guerra à República da China e ao Iraque em uma conferência on-line. Era mais um passo do hacktivismo. E, este movimento está crescendo. "O futuro de qualquer ativista político está na grande rede", declarou Stanton McCandish, diretor da Eletric Frontier Foundation, há alguns anos iniciou a campanha pela liberdade de expressão na Internet.

3.2.8.Organizações de Inteligência

Para a maioria desses adversários, entrar em um site, ganhar inteligência competitiva ou roubar dinheiro é um jogo. Possuem muita verba para pesquisa, equipamentos, habilidades e mão-de-obra qualificada. Seus maiores objetivos são informações militares, projetos de armas e informações diplomáticas.

3.3. Principais Ameaças

[SCHNEIER, 2001] categoriza as principais ameaças à segurança da informação a ser descrita da seguinte maneira:

3.3.1.Software Malicioso

Provavelmente é a primeira interação que há em segurança de computador. Normalmente, o usuário comum nunca sabe o que acontece no computador e acaba rodando softwares não confiáveis, correndo riscos.

Nesse pacote podem estar vírus, cavalos de tróia e vermes, juntos são chamados de malware. Possuem dois componentes: a **"carga útil"**, que faz o dano e pode ser maligna, podendo modificar o controle de acesso, roubar chaves secretas e enviar por e-mail, re-formatar o disco rígido, ou, apenas mostrar uma mensagem incômoda na tela, ou ainda, não fazer absolutamente nada e o **"mecanismo de propagação"**.

3.3.2.Vírus de computador

É uma seqüência de código de computador que se prende a outro programa, não podendo viver por conta própria. Uma vez preso, se replica utilizando os recursos do programa para se autocopiar e prendê-las a outros programas, e assim por diante.

O primeiro vírus foi escrito por Fred Cohen, aluno da USC em 1983, que fez isso para demonstrar o conceito, pois muitas pessoas não acreditavam que seria possível. Atualmente, são mais de 60.000 vírus diferentes e a maioria foi escrita para PCs compatíveis com IBM, sendo categorizados em: infectadores de arquivos, vírus de boot e vírus de macro.

- **Infectadores de arquivos:** por um longo período foram os mais comuns. Funcionam prendendo-se aos arquivos de programas, como processadores de textos e jogos de computador. Quando uma aplicação é executada, se instala na memória, de modo que possa infectar para outras aplicações, podendo se espalhar para outras máquinas através de discos infectados ou via rede.

- **Vírus de boot:** são menos comuns. Eles residem em uma parte especial do disco, seja disquete ou disco rígido, carrega-se na memória quando o computador é inicializado. Uma vez carregado, pode infectar todos os discos rígidos e qualquer disquete que seja colocado na unidade, e depois se espalhar para outros sistemas.

- **Vírus de macro:** são escritos em linguagens de scripting e infectam arquivos de dados em vez de programas. Muitos programas de processamento de textos, planilhas e banco de dados possuem linguagens de scripting, também chamados macros e são usados para automatizar tarefas e armazenados como dados.

  O primeiro vírus de macro escrito para Microsoft Word, "Concept", foi observado inicialmente em 1995, porém já existiam em editores de texto

Emacs no início de 1992. Esses vírus podem se espalhar muito mais rápido do que outros, pois usuários trocam dados com mais freqüência do que programas. E à medida que, e-mails, colaboração e transferência de arquivos aumentaram, eles se espalharam rapidamente.

3.3.3.Vermes

Mais conhecido como "worms" é um pedaço de malware específico para computadores em rede, sendo um programa de autoduplicação, que não se esconde em outro programa, como faz o vírus. Em vez disso, existem por conta própria, vagando através das redes de computadores da melhor forma possível, realizando danos que foi programado para fazer.

Em 1988, Robert T. Morris lançou o verme mais famoso. Foi um verme de Internet, que causou a falha de 6.000 computadores: 10% dos computadores. Esse verme começava em uma máquina e tentava entrar em outras estações via rede, usando técnicas básicas. Quando tinha sucesso, enviava uma cópia de si mesmo para a nova máquina, duplicando o processo em outras máquinas.

Outro verme conhecido foi o PrettyPark, executável no Windows, como anexo de e-mail, após a execução do programa era enviado a todos os usuários cadastrados na lista de endereços do Outlook Express.

3.3.4.Cavalos de Tróia (Horse Trojan)

Cavalo de Tróia é um pedaço de malware incorporado em algum software, projetado para enganar o usuário para pensar que é benigno.

Na história do Cavalo de Tróia original, os gregos sitiaram a cidade de Tróia por dez anos, sem demonstrar sinais de queda. Odisseu mandou os soldados gregos construir um enorme cavalo de madeira com rodas e entrar nele. À noite, puseram o cavalo em frente aos portões da cidade como admissão de derrota, fingindo a retirada do exército. E o "presente" foi levado para dentro das muralhas. Na mesma noite, os gregos saíram do cavalo e abriram os portões para o restante da armada grega que massacrou os troianos, pilhando as riquezas.

Seguindo essa analogia, o cavalo de tróia digital ou "trojan" é um código que se instala secretamente no sistema e faz coisas que não se espera ou deseja, enquanto finge fazer algo útil. Podendo observar o buffer do teclado até que detecte o que parece ser uma seqüência de números de cartão de crédito e os envie via TCP/IP para alguém.

Back Orifice é um trojan popular para Windows. Instalado no computador, permite que outro usuário remoto se conecte e assuma o controle pela Internet, podendo fazer upload e download das informações, excluir arquivos, alterar configurações, reinicializar o computador, ver o que estiver na tela do servidor, etc.

Além do Back Orifice e outras ferramentas escritas por invasores, muitos programas de administração remotos podem servir como trojan. DIRT (Data Interception by Remote Transmission) é um trojan desenvolvido pelo governo dos Estados Unidos e disponíveis à polícia, sendo um canivete suíço dos cavalos de tróia, porém outros são mais sutis. Vários trojans podem coletar nomes de usuários e senha, enviando-os de volta ao criador. Também podem modificar sorrateiramente programas de criptografia para escolher chaves de um pequeno pool aleatório, enfraquecendo o espaço de chaves, incluindo certificado falso no computador e enganando o usuário para que confie em alguém.

3.3.5.JavaScript, Java e ActiveX

Algumas vulnerabilidades são encontradas nas linguagens a seguir:

- **JavaScript**

Essa linguagem permite trechos de código sejam incorporados em páginas Web, e todos os principais browsers aceitam. Podendo ser utilizados para abrir e fechar janelas, manipular formulários, ajustar configurações do browser, e assim por diante. Os ataques baseados nessa linguagem apareceram nos últimos anos, utilizando falhas de segurança. Alguns exemplos aleatórios surgiram em 1997, que permitiam monitorar quais sites o usuário visitava; em 1998, liam quaisquer arquivos na máquina do usuário e ainda interceptavam e-mails do usuário. Todos esses bugs foram consertados, porém a cada dia novas falhas são descobertas e rapidamente resolvidas.

- **ActiveX**

ActiveX é um conjunto de tecnologias que permite aos componentes de software interagir uns com os outros em um ambiente de rede, independentemente da linguagem em que os componentes foram criados [MICROSOFT].

Esse conjunto usa uma defesa de assinatura de código, onde cada trecho do código chamado "controle" possui uma assinatura digital verificada. Em seguida, o browser monta uma caixa de diálogo e mostra ao usuário o nome do programa ou a empresa que assinou o controle. Se o usuário concordar, é baixado pelo browser. Porém, existe um problema, após a aceitação do controle ActiveX, ele pode fazer o quiser na máquina do usuário, podendo re-formatar o disco rígido, mudar entradas de planilhas, coletar informações pessoais e assim por diante. Esse sistema é incrivelmente poderoso, muito mais flexível e acessível, mais interessante arquitetonicamente e inimaginavelmente mais perigoso do que qualquer outro semelhante em qualquer outro sistema operacional.

- **Java**

A linguagem Java utiliza um modelo completamente diferente denominado "applet", sendo executado via browser na Web, possuem três mecanismos:

1. **Verificador de código de bytes,** que analisa o código e garante sua correta formatação, para que não haja problemas.

2. **Carregador de classe,** que determina como e quando um applet pode ser incluído no ambiente Java, certificando-se que o applet não substituirá algo importante que já exista.
3. **Gerenciador de segurança,** que é consultado sempre que o applet Java tenta fazer algo questionável, como abrir um arquivo, acessar a rede e assim por diante.

   Mesmo assim, existem problemas de segurança.

3.3.6.Hacking de URL

Como a maior parte da informação que se movimenta pela Internet, se baseia no protocolo http que não é criptografado ou autenticado, muitos invasores procuram URLs, baseando-se no erro do usuário. A primeira classe de ataques consiste em diferentes maneiras como os servidores roubam tráfego um do outro, uma vez que alguns sites desejam que pessoas vejam suas homepages, tenta enganar os motores de busca, ajustando cuidadosamente textos em tags meta (comandos incorporados em páginas Web para dizer que se referem à página) ou palavras-chave para atuarem como isca para esses motores. Denominado "furto de página", permite que o motor de busca identifique suas páginas parecendo como um Web site popular. Durante a pesquisa, aparecem nos resultados logo acima do site popular, levando a usuários descuidados a acessarem o site falso.

Outro ataque chamado Pishing Scam é uma espécie de jogo de trapaça na Web, através de manipulação de endereços URL no site de um cliente, o atacante pode forçar a vítima a fazer toda a sua navegação através

de um determinado site. Este site pertencente ao hacker pode manter o registro de navegação, além das senhas de acesso, números de conta bancários, cartões de crédito.

3.3.7.Cookies

Cookies são um truque de programação embutido em browsers, são trechos de dados que um servidor Web dá a um browser, que guarda os dados no computador do usuário e os retorna ao servidor. Problemas são identificados quando alguns servidores usam cookies para rastrear usuários de um site para outro, e alguns utilizam para descobrir a identidade do usuário. Além disso, alguns sites podem enviar cookies via e-mail para identificar o usuário durante sua visita posterior.

3.3.8.Scripts da Web

Os ataques anteriores são direcionados contra o cliente, esse ataque usa o servidor como vítima. Ao realizar uma consulta na Web, o servidor Web envia o pedido a uma aplicação de banco de dados e depois formata o resultado para exibir ao usuário. O problema está nos scripts da Web que podem ser potencialmente um furo de segurança, podendo ser "hackeados" para fazer coisas não antecipadas, permitindo baixar todos os arquivos do servidor Web, exibir o conteúdo de um banco de dados, listas de clientes e seus registros pessoais, entre outras operações.

3.3.9.Privacidade na Web

Normalmente, a navegação na Web é anônima. Porém, existem maneiras de identificar o usuário. Além dos cookies, os servidores Web registram os acessos, gravando um log que inclui endereço IP do usuário, a hora do pedido da Web, a página solicitada e o login do usuário. No entanto, a maioria dos sites da Web abandona esses logs, uma vez que poucos sites comerciais se preocupam em proteger a privacidade dos usuários.

3.4. Requisitos da Segurança da Informação

No ambiente virtual, conectado e independente, criou-se expectativas que correspondem aos requisitos de segurança:

- **Anonimato** - garantir que o autor não seja identificado. Possuindo duas vertentes extremamente opostas. Positivamente, permite a qualquer pessoa não seja identificada em denúncias, na participação em newsgroups de sobreviventes de abuso, doenças como AIDS, entre outras atividades. Permitindo as pessoas falarem sem a necessidade de assinar seus nomes, ou ainda, permitir que sobreviventes de guerra enviem notícias sobre o conflito para outras partes de mundo, sem assumir o risco de ameaça de morte por revelar suas identidades. No lado negativo, permite as pessoas enviar e-mails ameaçadores, publicar discurso de ódio e outras difamações, dispersar vírus e vermes de computadores, e assim por diante.

- **Auditoria** – proteger os sistemas contra erros e atos cometidos por usuários autorizados. Para identificar autores e ações, são utilizadas trilhas de auditorias e logs, que registram o que foi executado no sistema, por quem e quando. Também projetadas para auxiliar causas judiciais.

- **Autenticação** – confirma que seu parceiro na comunicação é quem deve ser e não um impostor. Confirmar a identidade de um processo remoto, face à presença de um intruso mal-intencionado é difícil e exige protocolos complexos baseados em criptografia.

- **Confiabilidade** – garantir que, mesmo em condições adversas, o sistema atuará conforme esperado.

- **Consistência** – certificar-se de que o sistema atua de acordo com a expectativa dos usuários.

- **Controle de acesso** - Certificar que somente pessoas autorizadas possam fazer tudo o que estiverem autorizadas a fazer e que todos os outros não possam.

- **Disponibilidade** - a propriedade dos serviços de um produto estarem acessíveis quando necessários e sem atrasos impróprios, ou, estar acessível e utilizável sob demanda por uma entidade autorizada. As medidas relacionadas a esse objetivo podem ser duplicação de equipamentos / sistemas e backup. Um bom exemplo de ataque contra disponibilidade é a sobrecarga provocada por usuários ao enviar enormes quantidades de solicitação de conexão com o intuito de provocar "crash" nos sistemas.

- **Integridade** - garantir que os dados não sejam excluídos ou alterados por alguém que não tenha permissão, mantendo os dados sempre corretos, completos e atualizados. Evitando que sejam modificados desde sua criação, ou apagados, além de dirimir fraudes.

- **Privacidade ou confidencialidade** - evitar que usuários não autorizados tenham acesso a informações confidenciais.

3.5. O Fator Humano

Na visão de um usuário comum, um sistema é analisado em propriedades. Entre elas, existe a complexidade, pelo extenso número de componentes, que trabalham por si e interagem com outros componentes. Além disso, os sistemas fazem coisas que não são antecipados pelos usuários avançados ou projetistas. Essas propriedades possuem efeitos profundos sobre a segurança da informação.

No mundo real, as pessoas não entendem computadores, apenas acreditam no que os computadores mostram e querem realizar suas tarefas. Assim, não entendem os riscos, mesmo que imediato.

Pensando em segurança, as pessoas trancam portas e janelas, verificam se estão sendo seguidas ao passarem por um local obscuro, porém não entendem ameaças sutis. Não acreditam que um pacote possa ser uma bomba ou que uma pessoa de boa aparência possa vender números de cartão de crédito do outro lado da rua.

A segurança da informação funciona no âmbito digital. Para que o sistema de computador realize algo útil, terá que interagir com usuários de alguma forma, em algum momento ou por algum motivo. E essa interação é um risco à segurança de todos eles.

O movimento de informações para o âmbito digital é problemático; mantê-las lá é difícil. Como não há um "escritório sem papel", a informação

nunca permanece nos computadores, passa para o papel o tempo todo. Informação é informação, e para alguém com más intenções, a informação em arquivos em papel é tão valiosa quanto os arquivos digitais. Muitas vezes, o papel jogado no lixo é mais valioso do que os mesmos dados que estão gravados no computador, além de ser mais fácil de ser roubado e menos provável de ser perdido. Uma corporação que codifica seus dados nos computadores, mas não tranca seus arquivos ou não tritura seu lixo estará aberta a este tipo de ataque.

Geralmente, as pessoas não sabem analisar o risco, pois não podem olhar as vulnerabilidades e tomar uma decisão segura sobre o quanto ela é ruim. Também não conseguem ver um ataque e tomar uma decisão sobre a probabilidade, o mesmo acontece quanto à situação de segurança e na decisão sobre o que fazer. Normalmente superestimam os riscos para coisas que são fora de controle (envenenamento em restaurantes) e "sensacionalizadas" na mídia (ser vítima de um ataque terrorista). Porém subestimam riscos para coisas que são mundanas e comuns (cair da escada, participar de acidente de automóvel). Certamente, não ter informações suficientes agrava o problema.

As probabilidades permeiam a criptografia, a segurança de computador, avaliação de risco, contramedidas, porém o risco é uma probabilidade, igualmente a segurança.

[SCHNEIER, 2001] define "Risco" como a possibilidade de um ativo sujeitar-se a fatores e incidentes que possam resultar em perdas ou danos, comprometendo a continuidade das atividades de uma organização.

As pessoas se baseiam em crenças. Todos sabem que o sol nasce no leste porque assim acontecem há milhares de manhãs. Hoje, temos a evidência astronômica sólida, mas acreditavam no surgimento diário do sol no leste muito antes de Copérnico ter substituído Ptolomeu. Bebe-se a água que nem sempre se sabe a procedência e o tratamento adotado, porém acredita-se que a água não seja venenosa, talvez por que nunca foi venenosa.

Na segurança também funciona dessa maneira, a impressão digital não é necessariamente exclusiva; os sistemas de identificação biométrica poderiam ter uma chance de 0,1% de que uma pessoa não autorizada seja reconhecida como uma impressão digital válida. Tudo isso são probabilidades.

Geralmente, as pessoas acreditam que o "computador nunca comete erros" e isso é um perigo dos sistemas computadorizados. Como raramente cometem erros, os usuários não sabem como lidar com eles. Porém, na realidade há falhas no software que cometem erros o tempo todo e os invasores maliciosos tiram proveito disso.

Quando uma condição de erro ocorre poucas vezes por semana, normalmente as pessoas sabem o que fazer. Porém se acontecer uma única vez por ano, talvez não haja ninguém preparado para sanar o erro.

Muitas vezes, os usuários se acostumam a determinados erros, que não param o sistema, podendo constituir alarmes aleatórios e passam a ignorá-los, podendo ser uma brecha de segurança.

Isso é a natureza humana, as pessoas querem se comunicar independente do sistema de segurança. Contanto que não prejudique esse desejo.

3.5.1.Interface Homem-Máquina

O sistema mais desprotegido é aquele que não é usado. E freqüentemente, um sistema de segurança deixa de ser usado, pois é muito irritante. Fatores como a demora ao carregar ou ler o disco levam o usuário a perder a paciência e desabilitar o serviço. Além disso, nunca utilizam todos os recursos dos programas de segurança, como criptografia em e-mail.

As pessoas querem segurança, mas não querem vê-la funcionando. Todo indivíduo que tenha utilizado os computadores antes que houvesse senhas, permissões e limitações, certamente optará pelo sistema antigo, pois era mais fácil. Quando há necessidade de interação com a segurança e tomada de decisão baseada nela, sempre serão evitados. Uma vez que, para cada sistema que o usuário interaja há uma senha diferente que necessita ser trocada a um certo período. Devido à variedade de senhas, o usuário acaba esquecendo e perde o acesso. Neste caso, necessita enviar e-mail ao administrador para liberar o acesso, que por sua vez, tem inúmeros usuários com este tipo de problema.

Outra dificuldade está na tomada de decisões dos usuários, visando uma ação segura. Um exemplo é que mesmo após os sustos causados pelos vírus Melissa e Worm.ExploreZip em 1999, as pessoas continuam a abrir

anexos de e-mails que não estavam esperando, como foi o caso da infecção em massa do verme ILOVEYOU e suas dezenas de variantes. Os usuários continuam abrindo mensagens provindas de fontes não confiáveis, correndo riscos.

3.5.2.Transferência Homem-Máquina

Se todos os documentos fossem assinados digitalmente, todo mundo dependeria e confiaria no sistema de assinatura digital. Neste caso, a assinatura digital estaria legalmente regulamentada e válida em qualquer tipo de documento.

No âmbito digital, o usuário transfere a confiança ao computador com alguma garantia que o sistema funcionará corretamente. Ninguém sabe se determinadas aplicações exercem suas funções corretamente, principalmente se determinado equipamento for utilizado por várias pessoas e com múltiplas funções.

A esperança existirá se o equipamento for utilizado para única finalidade, sendo verificado por teste de segurança específico.

3.5.3.Funcionários Maliciosos

Nenhuma segurança de computador pode impedir ataques internos, embora mecanismos de auditoria determinem as partes culpadas após os fatos.

O programador que escreve um sistema de segurança pode deixar uma brecha, ou seja, uma abertura secreta para entrada de invasores, sem que o administrador perceba. A mesma coisa, acontece se o técnico que instala o firewall também tiver essa intenção. O auditor também pode deixar passar alguns detalhes, e assim por diante.

As empresas tentam reduzir os riscos de funcionários maliciosos de várias maneiras. Seja contratando "pessoas honestas" ou até realizando análise de integridade para determinadas funções. Outras difundem a confiança, visando limitar a quantidade de dano que uma pessoa possa causar. Porém, uma organização sempre estará à mercê de seu pessoal.

3.5.4.Ataques Externos por Persuasão - Engenharia Social

[ABAGNALE, 2004] define a Engenharia Social como a arte e a ciência de induzir pessoas a agirem de acordo com seus desejos. Não é uma maneira de controlar a mente, nem permitir que consiga fazer as pessoas realizarem descontroladamente tarefas fora de seu comportamento normal, longe de ser infalível. Envolve também mais do que simplesmente pensar rápido e utilizar uma variedade de sotaques divertidos. As vítimas confiam demais e são muito ingênuas.

Os criminosos utilizam características humanas como ambição, medo, ira, cobiça, vaidade, levando a um golpe muito eficiente, indo buscar a informação diretamente na fonte. Evitando criptografia, segurança de computador, de rede, e tudo o mais que for tecnológico.

Segundo uma análise divulgada pelo Gartner, a Engenharia Social será a principal ameaça aos sistemas tecnológicos de defesas das grandes corporações e usuários de Internet daqui a dez anos.

Infelizmente, este tipo de golpe pode estar tão próximo quanto se pode imaginar. Em uma única ligação telefônica, o invasor pode se fingir de administrador de rede ou gerente de segurança e obter informações como login, senha e outras informações confidenciais do empregado, baixando a guarda de qualquer sistema de segurança. Ou ainda, entrar em uma sala de computadores portando um PDA ou um crachá de vendedor, bastando para entrar no sistema, ou ainda entrar como visitante e conectar o notebook a uma rede desprotegida.

Há casos em que alguém se passa por funcionário de suporte técnico de um provedor de acesso a Internet, telefona para um usuário qualquer informando que a conexão está com algum tipo de problema e que para consertar necessita da senha. O usuário, na sua ingenuidade, fornece a senha e mais tarde, verifica no extrato mensal do provedor que utilizou recursos além do que realmente o tinha feito.

Há também, os sites anônimos que prometem horas grátis de acesso, bastando o usuário informar nome de usuário e senha. Na verdade, trata-se de um ataque de engenharia social, onde as informações para conseguir horas extras, serão utilizadas em favor dos golpistas.

A mesma técnica é adotada nos "Phishing Scam" de bancos, onde os usuários recebem um e-mail informando que os dados de suas contas precisam ser atualizados. Os correntistas acabam informando todos os dados necessários, uma vez que as pessoas são geralmente prestativas.

Para evitar problemas futuros, as pessoas precisam estar cientes dos perigos de se passar qualquer tipo de informação.

3.6. Tecnologias de Segurança da Informação

A segurança é comparada a uma corrente, pois sua composição possui muitos elos, e cada um é essencial para a força da corrente. Podemos implementar segurança da informação utilizando as seguintes tecnologias:

3.6.1.Senhas

A técnica tradicional de autenticação é uma senha. É utilizada em toda parte, ao conectar ao computador, acessar a rede e sistemas específicos, para fazer uma ligação telefônica usando cartão de chamada, ou para sacar dinheiro no caixa eletrônico.

Pode ser definida em duas etapas:

- **Identificação:** o usuário informa quem é.
- **Autenticação:** o usuário comprova quem é, informando a senha.

As senhas são algo que o usuário conhece. Outras técnicas de autenticação são baseadas em algo que o usuário é - biometria - ou algo que o usuário possui - token de acesso.

3.6.2.Conexão Única

Uma coisa que tem incomodado os usuários de computador em grandes ambientes seguros é o grande número de senhas. Os usuários digitam uma senha ao ligar o equipamento, outra para se conectar a rede, uma terceira para se conectar a Internet, e assim por diante.

A conexão única é a solução para esses problemas de utilização. Infelizmente há alguns problemas, como aplicações legadas e medidas de segurança que envolve risco adicional. Porém, existem produtos que possibilitam o funcionamento em algumas situações, como o caso dos Portais Corporativos.

3.6.3.Tokens de Acesso

Caracterizada como uma solução que usa o que o usuário tem: um token físico de algum tipo. É a forma mais antiga de controle de acesso: no meio físico, uma chave restringia o acesso a um cofre, sala ou prédio. A possessão do selo do rei autoriza alguém a atuar como seu representante. Sistemas mais modernos e automatizados utilizam chaves eletrônicas como as de quarto de hotel ou manuais como os crachás de empresa de acesso às instalações. A idéia básica é a mesma, o token físico serve para autenticar seu possuidor.

A forma mais simples é do possuidor provar que possui o token, assim o usuário conecta o token a uma entrada de dados e o computador verifica se ele está lá.

O problema mais sério com essa tecnologia é que os tokens podem ser roubados. Assim o sistema não autentica realmente a pessoa e sim, o token. A maioria dos sistemas combina tokens de acesso com senhas, chamadas de PINs ou números de identificação pessoal para contornar essa vulnerabilidade.

3.6.4.Smart Card

Também chamado de "Cartão Inteligente", consiste em um cartão contendo um chip responsável pela geração e o armazenamento de certificados digitais.

A presença do Smart Card no mercado já é uma realidade, devido a múltiplas aplicações como programas de fidelidade (cartão de relacionamento e facilidades), identificação pessoal, controle de acesso, consumo, ponto e estacionamento, tíquetes de alimentação, tíquetes eletrônicos para cooperativas, moedeiro eletrônico, cartão de descontos e servindo como ferramenta para Data Base Marketing registrando o perfil do cliente e hábitos de consumo.

Contribuindo à segurança, reduz a possibilidade de emissão de cartões clones e por tratar a informação no próprio cartão, elimina o risco da perda de dados por problemas de rede.

3.6.5.Protocolos de Autenticação

São formas criptográficas de autenticação por uma rede. O Kerberos é um protocolo de autenticação inventado no MIT em 1988, e tem sido usado no mundo UNIX desde então.

Outros protocolos de login usam a criptografia por chave pública como IPSec (IP Security) e SSL (Secure Socket Layer), orientados a conexões e utilizados para garantir segurança e sigilo das informações como os serviços de home banking. Alguns sistemas usam protocolos simples, porém secretos, como o protocolo que o telefone celular usa para provar que as ligações devem ser permitidas em uma rede específica.

3.6.6.Biometria

Possui uma idéia simples: o usuário é o autenticador. O reconhecimento físico é biométrico, sendo utilizado há muito tempo pelos nossos antepassados.

Existem muitos tipos diferentes de biometria: escrita à mão (aparência), padrões de voz, reconhecimento de face e impressões digitais, geometria da mão, padrões de digitação, varreduras de retina e íris,

geometria da assinatura (pressão da caneta, velocidade da assinatura e assim por diante) e outros.

Com o passar dos anos, os sistemas de identificação biométrica melhoraram na identificação dos falsos positivos e falsos negativos. Por exemplo, verificam se a pessoa realmente está viva, para alguém com um dedo de plástico ou com um dedo real cortado, possa enganar o leito de impressão digital.

Para a maioria das aplicações, a biometria precisa ser armazenada em um banco de dados como senhas.

3.6.7.Criptografia

O termo criptografia vem do grego e significa "escrita secreta", vindo a ser utilizada há muito tempo. Há milênios foi usada nos hieróglifos egípcios e ao longo da história, vem protegendo segredos de estado, sociedades secretas, confidentes e amantes. Entre os militares que teve o papel mais importante na definição das bases para a tecnologia.

Sua idéia principal é que um grupo de pessoas possa usar um conhecimento privado para manter as mensagens escritas secretas contra todos os outros. Provendo uma comunicação segura e, garantindo confidencialidade, autenticidade, integridade e não-repúdio.

As mensagens a serem criptografadas, conhecidas como **texto simples** são transformadas por uma função que é parametrizada por uma chave. Em seguida, a saída do processo de criptografia, conhecida como **texto cifrado** é transmitida sem que haja alterações por terceiros não autorizados. Se cair em mãos erradas, o adversário não conhece a chave para decodificar o texto e, portanto, fica difícil de fazê-lo. A arte de solucionar mensagens cifradas é chamada **criptoanálise**. Enquanto que, a arte de criar mensagens cifradas e solucioná-la é conhecida como **criptologia**.

As mensagens podem ser codificadas por códigos ou cifras:

- Por **códigos**, o conteúdo das mensagens é escondido através de códigos predefinidos entre duas partes.
- A **cifra** permite ao conteúdo da mensagem ser cifrado misturando as letras da mensagem original. A mensagem é decifrada fazendo-se o processo inverso. Consistem na implementação de longas seqüências de números e letras que determinarão o formato do texto cifrado através de algoritmos associados a chaves.

Este tipo de criptografia se baseia na classificação quanto ao número de chaves utilizadas, simétrica e assimétrica.

Na criptografia **simétrica**, os algoritmos utilizam a mesma chave para codificar e decodificar. Essa chave é uma seqüência de bits aleatórios de algum tempo: no ano 2000, 128 bits era um bom tamanho de chave devido a sua eficiência.

Os algoritmos simétricos são encontrados nos sistemas de codificação global e os mais comuns são DES e DES triplo, IDEA e Blowfish. AES é o Advanced Encryption Standard e será utilizado pelo governo dos Estados Unidos.

Na criptografia **assimétrica** são utilizados dois tipos de chaves, chave pública e chave privada, onde a criptografia da mensagem é feita utilizando a chave pública e a decriptografia é realizada com a chave privada, ou vice-versa. Visam proteger e-mails privados, arquivos pessoais, transações bancárias eletrônicas e código de disparo nuclear, protegendo a privacidade.

3.6.8.Assinatura e Certificação Digital

Com o crescimento da Internet, o aparecimento de uma infra-estrutura comum baseado no desenvolvimento de aplicações, houve a necessidade de criar um mecanismo comum de segurança para troca de mensagens e transações, os padrões de certificação viabilizaram o uso exclusivo de documentos eletrônicos em processos críticos entre pessoas físicas e jurídicas.

Um certificado é uma credencial, que é assinado por alguém em que se confia, sendo a ligação entre uma chave pública e uma identidade. Tecnicamente, é um arquivo que contém informações pessoais como nome, cargo, endereço de e-mail entre outras coisas, agregados aos dados sobre o certificado, como data de emissão e expiração, além de dados do emissor ou assinante e a chave pública. Consiste de um par de senhas, uma de

conhecimento público (chave pública), outra de conhecimento exclusivo da pessoa a ser certificada (chave privada).

O Certificado Digital realiza 4 itens básicos: a identificação das partes envolvidas em uma transação, garantia de integridade, sigilo e a impossibilidade de repúdio.

Esses certificados são emitidos por uma Autoridade Certificadora (CA - Certificate Authority), que pode ser um órgão governamental ou companhia privada, que também necessitam ser certificadas por outras CAs. No Brasil, as certificadoras homologadas são Certisign, Serasa, Serpro, Caixa Econômica Federal, Secretaria da Receita Federal e Presidência da República.

Em termos de legislação, o impulso para o uso das assinaturas digital certificadas foi a Medida Provisória 2.200, que instituiu a ICP-BR (Infra-estrutura de Chaves Públicas Brasileira) para regulamentar a implementação e utilização no país e atribui validade legal aos documentos assinados digitalmente.

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 [ICP Brasil, 2001].

3.7. Defesas de Segurança da Informação

3.7.1.Firewalls

[TANENBAUM, 2001] compara o firewall há uma adaptação moderna de uma antiga forma de segurança medieval: cavar um fosso profundo em torno do castelo. Esse recurso forçava todos aqueles que quisessem entrar ou sair do castelo a passar por uma única ponte levadiça, onde poderiam ser revistados por guardas.

No ambiente virtual, é possível utilizar o mesmo artifício, o firewall é um mecanismo que protege a rede ou estação, mantendo os intrusos do lado de fora e permitindo a entrada de usuários autorizados. Assim, para várias redes conectadas de forma arbitrária, todo o tráfego de entrada ou saída é filtrado através de uma ponte levadiça eletrônica.

Porém, ainda que o firewall esteja perfeitamente configurado, existem maneiras de vencer a segurança. Por exemplo, se um firewall for configurado para permitir a entrada de pacotes de redes específicas, um invasor fora do firewall pode inserir falsos endereços de origem para ultrapassar essa verificação. Se um usuário interno quiser transportar documentos para fora da empresa, poderá codificar ou transformar os documentos em imagens que passarão por qualquer filtro de palavras, tranqüilamente.

De acordo com um estudo realizado pelo Computer Security Institute em 1998, o fato é que 70% dos ataques vêm de dentro do firewall, podendo vir de funcionários insatisfeitos [SCHNEIER, 2001].

3.7.2.Redes Privadas Virtuais - VPN

Muitas companhias têm escritórios e fábricas espalhadas por muitas cidades, às vezes por vários países. Para manter a comunicação tornou-se necessário construir uma rede a partir dos computadores das empresas agregando linhas telefônicas dedicadas também chamada de rede privada. É um excelente meio de segurança, porém o arrendamento das linhas telefônicas gerou um custo alto de operação.

Para resolver o problema, foram criadas as VPNs (Virtual Private Networks) que são redes virtuais, com conexão segura em uma rede pública.

As VPNs possuem duas aplicações principais. A primeira é conectar pedaços separados da rede. Uma empresa pode ter dois escritórios em diferentes lugares, cada uma com sua rede local, e, ambas conectadas por uma VPN via Internet. O segundo uso é conectar usuários móveis: seja trabalhando em casa, prestando serviços ao cliente, ou ainda em quartos de hotéis. Aqui, o usuário conecta localmente a servidor de Internet, que roda uma VPN do computador do usuário até a rede.

Um projeto comum é equipar cada escritório com um firewall e criar túneis pela Internet entre todos os pares de escritório. Quando o sistema estiver funcionando, cada par de firewalls tem de negociar os parâmetros como serviços, modos, algoritmos e chaves.

3.7.3.Software Antivírus

O software antivírus tem como principal função bloquear a ação de vírus, cavalos de Tróia, worms e outros códigos maliciosos, mantendo o computador seguro e eliminando as ameaças em todos os pontos de entrada do computador, inclusive no correio eletrônico, na Internet e até mesmo na sincronização com o PDA.

Sua atividade consiste em monitorar constantemente o computador, barrando atividades suspeitas para evitar que qualquer nova ameaça se espalhe. Passando a ser executado continuamente em segundo plano no computador, varrendo arquivos regularmente e procurando mudanças incomuns no tamanho, além de programas que correspondam à base de dados de vírus conhecidos do software, anexos suspeitos de e-mail e outros sinais de alerta.

Os softwares antivírus também detectam aplicativos potencialmente indesejáveis, como spyware, adware e outros, removendo-os para proteger dados e privacidade dos usuários.

Alguns procedimentos preventivos de segurança:

- Nunca abra e-mail de origem desconhecida ou duvidosa. Caso não tenha solicitado e não conhece o remetente, delete o e-mail, sem abrir.
- Mantenha o seu programa antivírus sempre atualizado e ativo.
- Vacine sempre os disquetes antes de abrir.
- Cuidado com arquivos baixados de sites de procedência duvidosa.
- Não execute um arquivo recebido pela Internet, sem antes passá-lo por um programa de antivírus.

4. Pontos Críticos de Sucesso

Neste capítulo, abordaremos questões relevantes para que uma empresa encontre os pontos críticos e alcance o sucesso na implementação do escritório sem papel.

4.1. Pontos Positivos

- ✓ **Redução de custos:**

Um estudo realizado em 2004 comparou o custo de impressão entre as três tecnologias mais utilizadas - sem contabilizar o gasto com papel [ABRAFORM, 2004]:

Tecnologia de Impressão	Custo por Página - R$
Matricial (Dot Matrix)	0,008
Jato de Tinta (Ink Jet)	0,25
Toner (Laser)	0,08

Um pacote de papel comum custa em média, R$ 13,90 dividindo por 500 folhas, chega-se ao valor de R$ 0,0278 por folha.

Impressão	Custo por Página - R$		
	Impressão	Folha	Total
Matricial	0,008	0,0278	0,0358
Jato de Tinta	0,25	0,0278	0,2778
Laser	0,08	0,0278	0,1078

Outro estudo alertou que, cada funcionário imprime cerca de 33 páginas da Internet, diariamente [CENADEM, 2003]. Multiplicando o custo desse tipo de impressão, teremos:

Impressão	Custo por Página - R$		
	Fórmula	Diário	Anual
Matricial	0,0358 x 33	1,1814	431,21
Jato de Tinta	0,2778 x 33	9,1674	3.346,10
Laser	0,1078 x 33	3,5574	1.298,45

Durante um ano, uma empresa com mil funcionários, utilizando somente impressoras laser, gastará cerca de R$ 1.298.450,00 (quase um milhão e trezentos mil reais!!!), apenas com essa impressão, sem contabilizar a impressão de e-mails, relatórios e memorandos, que elevaria o custo.

- ✓ **Aumento de produtividade:**

Até pouco tempo era impossível prever o tempo que um documento importante levaria para ser aprovado, onde e com quem poderia estar parado, significando gargalo no processo de aprovação.

Atualmente, sistemas de workflow informam onde a documentação eletrônica está, o prazo previsto para aprovação e o próximo passo a ser tomado. Dando total transparência aos processos e aumentando a produtividade.

✓ **Redução do tempo em transações comerciais e financeiras:**

É uma conseqüência do ganho de produtividade e da automação do trâmite de papéis. Com a redução de gargalos e burocracia, transações são realizadas no menor tempo possível, através de acesso remoto, minimizando o volume de papéis e eliminando os extravios.

✓ **Melhor aproveitamento das fontes de documentação:**

Documentos se perdem a todo o momento, inclusive nas gavetas de funcionários. Em meio digital, são mais fáceis de encontrar, tendo destino certo. Além disso, permitem a consulta simultânea de pastas de documentos por várias pessoas em diferentes lugares, tanto na matriz como nas filiais.

✓ **Otimização do espaço físico:**

O armazenamento das informações em mídias eletrônicas possibilitará a análise do layout visando reestruturação e melhor aproveitamento do espaço físico disponível. Deste modo, os armários lotados de pastas poderão ser eliminados.

- ✓ **Implantação de novas tecnologias:**

Um erro grave que acontece nas organizações é a busca pela solução ideal. É necessário ter em mente o que a empresa realmente necessita, evitando decisões precipitadas. Haja vista, a dificuldade de encontrar uma ferramenta que solucione todos os problemas.

Um aspecto importante na escolha da solução é evitar sistemas complexos, que reúnem todos as funções de GED, desde a digitalização até o workflow, pois são pouco flexíveis ou ainda difíceis de customizar. Além disso, deixam a empresa refém do sistema, não permitindo a utilização de outras ferramentas. O ideal é procurar no mercado, o melhor aplicativo para cada situação.

Outro fator é não optar por formatos proprietários, uma vez que, os arquivos gerados pelo software devem interagir com outras aplicações.

Na área de infra-estrutura, é importante analisar a compatibilidade com sistemas operacionais existentes, aplicativos internos e protocolos utilizados. Avaliando a estabilidade na rede no horário normal de trabalho, evitando a queda de performance e comprometimento das atividades relacionadas com o sistema.

- ✓ **Integridade dos documentos:**

Documentos em papel podem ser acessados por qualquer pessoa, uma vez que, informações importantes podem ser jogadas no lixo sem nenhum critério.

Manter os dados corretos, completos e atualizados, evitando alteração ou exclusão por indivíduos não-autorizados é peça-chave na segurança da informação. Ferramentas simples permitem aos usuários criptografar os documentos, para serem lidos por pessoas autorizadas.

- ✓ **Preservação do histórico da empresa:**

As condições que os documentos em papel são submetidos podem definir o tempo de vida das informações. Estando digitalizados, podem ser guardados por mais tempo, preservando dados históricos da organização.

4.2. Pontos Negativos

- ✓ **Resistência a mudanças:**

A transição do processo em papel ao processo totalmente informatizado pode gerar impacto entre os funcionários. Haja vista, o ser humano vem utilizando o papel como ferramenta de informação.

Para reduzir o impacto, o ideal é escolher uma ferramenta que possua uma interface amigável e seja fácil de utilizar.

- ✓ **Necessidade de contingência:**

Um escritório totalmente digital deve manter um número mínimo dos formulários mais utilizados em papel, para atender situações atípicas, como queda de energia elétrica, problemas técnicos na rede, etc.

4.3. Facilitando a implantação do "escritório sem papel"

✓ **Conscientizar funcionários para o lixo "digital":**

Relatórios importantes podem conter informações extraídas de bases de dados, contendo dados sobre clientes, funcionários, fornecedores, transações financeiras, etc. Nota-se nas empresas, que parte não é arquivada e sim descartada, após avaliação do seu conteúdo. Essas informações são jogadas no lixo, sem nenhum critério.

A empresa deverá realizar uma campanha interna, conscientizando os colaboradores a triturar os documentos impressos após a utilização.

✓ **Integrar aplicativos de e-mail ao formato PDF:**

Vimos anteriormente que é comum, as pessoas imprimirem e-mails para ler em papel. Para reduzir essa impressão nas empresas, poderia ser instalado um driver de impressão PDF nas estações de trabalho. Além disso, seria necessário configurar os aplicativos de mailing para gerar o arquivo eletrônico em local específico da rede, no momento que o botão "Imprimir" fosse acionado.

✓ **Marketing ecológico:**

A empresa pode iniciar uma estratégia de marketing junto aos clientes e comunidade, pela consciência ecológica, visando a preservação dos recursos naturais.

Haja vista, com o "escritório sem papel", há redução do consumo de papel nas organizações, não gerando lixo. E, apesar de ser uma pequena parte do montante gerado diariamente, essa atitude contribui em reduzir a poluição do ar, solo e água, bem como evita a necessidade de instalar novas áreas para aterros sanitários.

Além disso, a queda do consumo de papel evita a demanda pela matéria-prima: a madeira, provocando uma redução no número de árvores derrubadas.

Deixando em evidência, a preocupação da empresa em melhorar o meio-ambiente, a partir de mudanças de atitude visando o bem estar de todos.

5. Conclusão

Por um longo tempo, o "escritório sem papel" foi considerado o "Santo Graal" para promover eficiência e economia no ambiente de trabalho. Apesar de todo mundo desejar, ninguém podia encontrá-lo. Na teoria parecia funcionar perfeitamente, contudo na prática era muito complicado. Muitas empresas tentaram e fracassaram.

Acredito que o escritório do futuro será diferente do que é hoje. Por um tempo, o papel ainda irá evoluir e mudar podendo desaparecer ou persistir, mantendo-se na maioria das atividades. Em outras palavras, continuará a predominar em atividades que envolvam trabalho do conhecimento ou que envolvam demonstrar idéias e ações.

A meta de implementação é difícil de ser alcançada, pois as organizações se preocupam apenas em retirar o papel, causando mudanças superficiais e impedindo que tarefas sejam alteradas. Assim, usuários não se afastam do papel e as empresas concluem que não vale o esforço.

No ambiente de trabalho é comum encontrarmos mesas divididas em setores: uma área reservada para equipamentos de informática (monitor, gabinete, teclado e mouse), outra reservada para papéis (jornais, revistas, circulares, pastas e outros artigos relativos ao conhecimento), ou ainda, podem dispor de uma terceira área para caixinhas de correspondência (entrada e saída de papéis).

Ao passar por uma mesa repleta de papéis, podemos pensar que o funcionário possa estar atolado em serviço, ou ainda, que não tenha capacidade para gerir o trabalho, uma vez que o papel transmite tipos de pensamento.

Esse método de empilhar documentos foi introduzido por nossos avós quando trabalhavam em fábricas. Após uma pausa, era mais prático retomar o trabalho, se os papéis estivessem empilhados e classificados em ordem de urgência, data, tema ou alfabética. Isso acontece, pois o nosso cérebro necessita "prender" as informações que ainda não foram categorizadas ou que não foram usadas, passando a classificar, naturalmente, toda a papelada como índice.

No entanto, faz-se necessário estabelecer metas de utilizar menos papel nas organizações, a partir da gestão integrada de documentos e processos.

Porém, a maior barreira para o "escritório sem papel" está no fato que alternativas digitais ainda são inadequadas para tarefas do dia-a-dia e as características particulares do papel facilitam a escolha para tarefas manuais. Se essas características não forem alcançadas ou se não houver uma evolução conjunta do papel e do ambiente de trabalho em todos os aspectos, será difícil prever um futuro sem papel.

Gradualmente, novas alternativas serão melhoradas e desenvolvidas, aproximando às características do papel e encontrando o próprio nicho. A partir daí, intensificarão características como: busca rápida, compartilhamento, armazenamento e acesso remoto, além de assumir atividades onde as mídias eletrônicas são melhores, como produção e distribuição de novos tipos de mídias incluindo áudio, vídeo, música e conteúdo multimídia interativo. Tudo irá depender do efeito causado pela mudança no trabalho e nos processos organizacionais.

Outro motivo para evitar o papel é o extravio de dados no tráfego de informações. O "escritório sem papel" pode contribuir à segurança da informação envolvendo aspectos fundamentais ao negócio, reduzindo riscos e agilizando processos.

As organizações devem estar preparadas para resistir a ataques, ameaças e vulnerabilidades, que vem crescendo a cada ano, reduzindo a preocupação com a segurança dos dados. A existência de uma política de segurança efetiva deve envolver as áreas de gestão e tecnologia, sendo fundamental conscientizar todos os colaboradores para o cumprimento das medidas de segurança e proteção dos recursos.

6. Bibliografia

- BALDAM, Roquemar, VALLE, Rodrigo e CAVALCANTI, Marcos. GED - Gerenciamento Eletrônico de Documentos. Editora Érica, 2002.
- BISHOP, Matthew A. Computer Security, 1ª Edição. A. Wesley Professional, 2002.
- CRUZ, Tadeu. Workflow - A Tecnologia Que Vai Revolucionar Processos - 2ª Edição. Editora Atlas, 2000.
- DILLON, A. Reading from paper versus reading from screens: a critical review of the empirical literature. Ergonomics, 1992.
- D'ALLEYRAND, Marc. Workflow em Sistemas de Gerenciamento Eletrônico de Imagens. Editora CENADEM, 1995.
- EXEC. FINANCEIROS. Vanderlei Campos. Agilidade e redução de custos no fluxo de documentos. *Revista Executivos Financeiros*, São Paulo, v. XV, n. 161, p. 36-38, junho/2004.
- E-MANAGER. Carla Baiense. Tudo num só lugar. *Revista E-Manager*, Vitória, v. XV, n. 77, p. 34-41, dezembro/2003.
- GED. Jornal do GED: São Paulo, CENADEM - Centro Nacional de Desenvolvimento do Gerenciamento da Informação, ano 2003, n. 55, 57, 58, ano 2004, n. 61, 62, 63, 64, Bimestral.
- GIMSON, Roger. Electronic Paper - Can it be real? Bristol, Hewlett Packard Labs. 1997.
- MONTEIRO, Luís. Do Papel ao Monitor Possibilidades e Limitações do Meio Eletrônico. Mestrando em Design - PUC-Rio, 2001.
- SCHNEIER, Bruce. Segurança.com - Segredos e Mentiras sobre a Proteção na Vida Digital. Editora Campos, 2001.
- SELLEN, Abigail J. e HARPER, Richard H.R. The Myth of the Paperless Office. MIT Press, Paperback Edition, 2003.
- TANENBAUM, Andrew S. Redes de Computadores. Tradução da Quarta Edição. Editora Campos, 2003.

7. Webografia

- ABAGNALE, Frank W., Cuidado com a Engenharia Social: entrevista com Frank W. Abagnale.
  Disponível em: <http://www.modulo.com.br/pt/page_i.jsp?page=3&catid=6&objid=75>
  Acesso em 13.12.2004
- ABRAFORM - Associação Brasileira Indústria de Formulários, Documentos e Gerenciamento da Informação, Estudo de custo por página impressa.
  Disponível em <http://www.abraform.org.br/informativo/info14.htm>.
  Acesso em 02.7.2004.
- CENADEM, O GED.
  Disponível em: <http://www.cenadem.com.br/ged/>.
  Acesso em 13.10.2004.
- ICP Brasil, Legislação.
  Disponível em: <http://www.cenadem.com.br/ged/>.
  Acesso em 29.10.2004.
- MODULO, Os crimes digitais hoje.
  Disponível em: <http://www.modulo.com.br/empresa3/noticias/artigo_entrevista/a-crimes.htm>.
  Acesso em 26.8.2004.
- MICROSOFT, Descrição das tecnologias ActiveX.
  Disponível em <http://support.microsoft.com/default.aspx?scid=kb;pt-br;154544>.
  Acesso em 30.8.2004.