Biblios
ISSN 1562-4730 (online)

Gestão e segurança da informação eletrônica: Exigências para uma gestão documental eficaz no Brasil

Sandra Buth Zanon

Academia Nacional de Polícia - ANP, Brasil

OPINION

Resumo

A gestão e segurança da informação, principal ativo das organizações, são questões imperativas na Era da Informação e do Conhecimento. A partir da prática na área de gestão documental e informacional em órgãos públicos do Brasil, observou-se a ausência de um modelo de gestão da informação eletrônica adequado às necessidades das organizações bem como de uma política de segurança da informação. Assim, apresenta-se uma reflexão sobre a necessidade premente de gestão das informações eletrônicas, visando a eficácia da gestão documental, e a importância da adoção de uma política de segurança da informação para assegurar sua integridade, confidencialidade, autenticidade, disponibilidade, não-repúdio e preservação a longo prazo.

Palavras-chave

Gestão da informação ; Segurança da informação ; Gestão documental ; Informações eletrônicas ; Brasil

Management and electronic information security: requirements for effective document management in Brazil

Abstract

The management and information security, the organization's main asset, are imperative issues at the Age of Information and Knowledge. Practicing at documentary and informational management field in public institutions from Brazil, it has been showed a lack of an appropriate electronic information management model suited to an organization also an information security policy. This paper reflects about an urgent necessity for electronic information management, aiming efficient document management, and the importance of adopting information security policy to ensure its integrity, confidentiality, authenticity, availability, non-repudiation and long term preservation.

Keywords

Information management ; Information security ; Document management ; Electronic information ; Brazil

Introdução

Em tempos de globalização o sucesso e competitividade das organizações dependem da informação. Enquanto ativo importante das organizações, a informação precisa ser adequadamente gerida e protegida.

A evolução tecnológica trouxe muitas mudanças em todas as áreas do conhecimento, alcançando também os modos de fazer da gestão documental. A informação orgânica não está mais contida apenas em suportes convencionais, como o papel, se fazendo presente cada vez mais os documentos em suportes informáticos, contribuindo para o acelerado aumento do volume documental e informacional. Em meio à gama de informações

diárias, importa selecionar aquelas que realmente são importantes para a organização e dispor de mecanismos para preservá-las a longo prazo, acessíveis a tempo e a quem de direito.

Neste contexto, o desafio está em definir um modelo adequado de gestão da informação eletrônica que atenda as necessidades das organizações de acesso rápido à informação e de garantia da sua confiabilidade, em conformidade com as normativas legais.

Não será abordada a importância indiscutível da gestão documental para a eficiência das organizações. O objetivo é tecer considerações sobre a gestão e segurança das informações eletrônicas nas organizações públicas, vez que se apresenta como questão crítica para uma gestão documental eficaz. A exemplo de Santos (2005, p. 114), entende-se que a discussão sobre gerenciamento de informações eletrônicas é produtiva para as organizações que tratam seus documentos arquivisticamente, vez que a "existência de uma política arquivística de gestão documental para documentos eletrônicos seria resultante da evolução de uma política iniciada com os suportes tradicionais".

Outrossim, gestão de documentos e informações, bem como a gestão do conhecimento, são conceitos que se complementam, conforme Santos (2008) e, apesar da gestão da informação ser mais ampla que a gestão documental, esta alcança aquela quando se trata de documentos arquivísticos que contém informações orgânicas.

Também Rosseau e Couture em 1998 (p. 61) já abordavam o lugar da Arquivística na gestão da informação dizendo que "este lugar situa-se num contexto administrativo e organizacional onde a informação deve ser considerada, organizada e tratada como um recurso tão importante quanto os recursos humanos, materiais ou financeiros."

Assim, as análises e sugestões que seguem foram formuladas a partir da prática da gestão documental em órgãos públicos do Brasil com o fim único de reflexão sobre a gestão e segurança da informação eletrônica e, quiçá, como inspiração para a melhoria dessas condições nessas organizações.

1 Gestão da informação eletrônica

É fato que o desenvolvimento das tecnologias da informação trouxe muitas vantagens ao mundo contemporâneo, impulsionando a globalização e influenciando todas as áreas do conhecimento, impondo mudanças nunca antes vistas nos modos de fazer. Relativamente à gestão documental, a sociedade ainda procura respostas para viabilizar a evolução do documento analógico para o digital suprindo questões legais e de preservação da informação. A problemática principal nesta área está relacionada à facilidade de produção e modificação das informações eletrônicas.

Acerca do conceito de informação e sua importância, Silva Filho (2010) diz que:

> Informação compreende qualquer conteúdo que possa ser armazenado ou transferido de algum modo, servindo a determinado propósito e sendo de utilidade ao ser humano. Trata-se de tudo aquilo que permite a aquisição de conhecimento. Nesse sentido, a informação digital é um dos principais, senão o mais importante, produto da era atual. Ela pode ser manipulada e visualizada de diversas maneiras. Assim, à medida que a informação digital circula pelos mais variados ambientes, percorrendo diversos fluxos de trabalho, ela pode ser armazenada para os mais variados fins, possibilitando ela ser lida, modificada ou até mesmo apagada.

Tomando por base esse conceito de informação, percebe-se que as organizações necessitam de sistemas de informação para gerenciar seu principal ativo. Embora um sistema de informação possa ser entendido como qualquer sistema que armazena e fornece acesso à informação, seja ele automatizado ou manual, será abordado neste artigo como um sistema que utiliza recursos de tecnologia da informação para processar dados e gerar informação, isto é, como um sistema informatizado.

A partir da prática da gestão documental em órgãos públicos observou-se que são utilizados, na mesma organização, inúmeros sistemas de informação para gerenciar as informações em meio eletrônico, inclusive sistemas de gerenciamento eletrônico de documentos (GED). Porém, apesar de seu uso ser indispensável para gerenciar a gama de informações, nem sempre a diversidade de sistemas de informação que, na maioria das vezes não estão integrados, oferece a eficiência necessária à organização na recuperação da informação para o apoio às operações diárias e a tomada de decisão.

A ausência de um sistema de informação abrangente para gerenciamento das informações eletrônicas contribui para o alastramento de sistemas de informação utilizados isoladamente nas diversas unidades de uma organização. Da mesma forma, divergem os gestores, os modelos de dados, os sistemas gerenciadores dos bancos de dados, as plataformas, as linguagens de programação, etc. desses sistemas, dificultando a integração de informações e o estabelecimento da gestão arquivística de documentos eletrônicos.

Todas as unidades de uma organização contam com informações orgânicas encontradas nos seus documentos, nos arquivos eletrônicos produzidos e nos seus diversos sistemas de informação. Os documentos, assim como as informações eletrônicas, na maioria das vezes estão organizados de forma empírica. Do ponto de vista arquivístico, conforme Rousseau e Couture (1998) informação orgânica é aquela produzida, enviada ou recebida em função das atividades-meio e fim de uma organização e que, uma vez registrada, dá origem aos arquivos dessa organização. Informação não-orgânica é aquela produzida fora do contexto de atividades da organização e que, muitas vezes, existe nos locais de trabalho, mas também em bibliotecas ou em centros de documentação.

O tratamento dos documentos oficiais públicos é regido pela legislação brasileira, além de normas institucionais que, juntas, dão as diretrizes para a correta e adequada gestão documental e consequente acesso às informações a curto e longo prazo. Uma vez que as normas de gestão documental para a Administração Pública já existem, cabe estendê-las à gestão das informações eletrônicas por dois simples motivos: primeiro porque o tratamento da informação independe do suporte; segundo porque o gerenciamento correto das informações eletrônicas é um treinamento importante para a produção e uso de documentos digitais.

Para tratar a informação é necessário, antes de qualquer coisa, qualificá-la. É a qualidade da informação que determina sua importância para a organização. Considerar a informação um bem não é uma invenção da Era da Informação e do Conhecimento, mas são as tecnologias da informação que estão revolucionando a noção de valor que se adicionou à informação.

Segundo Hubbard (2010) o método para calcular o valor da informação existe há décadas e consiste num desdobramento da teoria do jogo e da teoria da decisão, em outras palavras, o valor da informação é igual à probabilidade de estar errado vezes o custo de estar errado.

Moresi (2010), por sua vez, acredita que o valor da informação está associado a um contexto e que sua quantificação é relativa, relacionada a juízos de valor que também variam de acordo com o tempo e a perspectiva. Apesar do autor considerar que os valores de uso e troca da informação apenas serão úteis na definição de provável equivalência monetária, apresenta uma equação para cálculo do valor da informação que é igual ao resultado da divisão dos produtos e serviços da organização multiplicados pela qualidade dos mesmos, pelo resultado dos custos multiplicados pelo tempo de resposta.

Segundo Tonini (2010) a dificuldade de mensurar e quantificar os produtos e serviços de informação e documentação deve-se às suas características de intangibilidade e de simultaneidade. A autora apresenta uma fórmula de cálculo do custo da informação a partir da soma dos custos diretos e indiretos de produção e uso, incluindo custo da mão-de-obra e tempo consumido em cada atividade da organização.

Diante do exposto, verifica-se que valorar a informação não é tarefa fácil, além de divergirem as opiniões e as metodologias para sua quantificação e qualificação. Em todos os casos implica num estudo aprofundado dos usos da informação de uma organização, envolvendo a análise quantitativa de custos referentes à implantação e manutenção dos sistemas e a análise qualitativa que irá identificar a contribuição das informações para a tomada de decisões e definição de estratégias institucionais.

Quando, porém, as informações orgânicas e não-orgânicas da organização não atendem a um padrão de produção e tratamento, ficando misturadas, o mais importante e urgente é classificar a informação orgânica com o fim de quantificá-la e qualificá-la no futuro, visando seu gerenciamento. O tratamento da informação não-orgânica, por sua vez, é de responsabilidade de seu produtor.

A redução do volume de bytes e a consequente redução de custos de manutenção está relacionada diretamente à gestão das informações eletrônicas que compreende, entre outras coisas, separação de informações institucionais ou orgânicas de outros tipos de informações ou não-orgânicas, acessibilidade e segurança. Assim, embora o custo de manutenção das informações eletrônicas também não possa ser estabelecido sem um estudo aprofundado, certo

é que a gestão adequada das informações, além da conformidade legal e da segurança, proporcionará também a redução de custos.

As tecnologias da informação não mais estão restritas às áreas de informática, estando presentes em todas as áreas do conhecimento e sendo responsável pelo funcionamento total do ciclo de informações das organizações. A dificuldade está, porém, no fato de tais informações estarem separadas, distribuídas em diversas estruturas de sistemas de informação, em múltiplas plataformas e aplicativos. A informação fica no local em que é produzida, muitas vezes isolada. A situação se agrava quando essas informações estão fora de um sistema corporativo, isto é, produzidas e armazenadas aleatoriamente no desempenho diário de atividades diversas. Exemplo disso são as informações armazenadas nos computadores dos usuários e na rede.

Segundo Innarelli (2008, p.26) são três as formas de produção de informações eletrônicas na atualidade, a saber "por meio de sistemas informatizados através de dados contidos em sistemas gerenciadores de bancos de dados (SGBD), por processo de digitalização e/ou diretamente com uso de um software ou sistema específico".

Santos (2005, p. 117) em sua pesquisa sobre o tratamento de documentos eletrônicos nas instituições públicas de arquivo no Brasil também refere a problemática da dispersão das informações eletrônicas:

> A descentralização do armazenamento, pelo uso dos discos rígidos dos computadores setoriais ou disquetes, é uma das grandes dificuldades a ser contornada pelos arquivistas. É necessária uma gestão arquivística que englobe desde a produção documental até a destinação final dos documentos, caso contrário, corre-se o risco de perder informações por meio de atualizações de documentos, utilizados como modelo para novos, ou pelo apagamento completo do documento para liberação de espaço nos suportes de armazenamento.

Diante do exposto, recomenda-se a adoção de padrões com relação à forma de organização e ao local de armazenamento das informações eletrônicas orgânicas com o fim de garantir sua recuperação e preservação. Ao estabelecer o modelo de dados é apropriado utilizar a classificação de assuntos estabelecida pelo Conselho Nacional de Arquivos - CONARQ para os documentos da Administração Pública, Resolução nº 14/2001, tal como se utiliza para documentos analógicos, a fim de criar um único padrão, conhecido por todos. Exemplo: I. Nome das pastas: classe/subclasse; II. Nome dos arquivos: assunto ou tipo documental.

Rousseau e Couture em 1998 (p. 68) já recomendavam a elaboração do que chamaram de um sistema integrado de gestão da informação orgânica com o fim de tratar adequadamente os ativos informacionais da organização. Segundo os autores, todas as fases desse sistema são beneficiadas pela classificação e temporalidade dos documentos, visto representar "o elemento estabilizador que permite regular o crescimento exponencial da informação". Os autores completam ainda dizendo que:

> ...graças à tabela de seleção dos documentos, a informação será sistematicamente depurada e tratada em função do ciclo de vida que lhe foi atribuído, e os sistemas utilizados serão periodicamente aliviados, acelerando a comunicação da informação pertinente.

Além disso, cabe definir também os locais de armazenamento próprios para as informações orgânicas de modo que sejam facilmente identificadas e localizadas. Assim, considerando que a organização possua uma estrutura de rede, sugere-se que, quando as informações produzidas não integrarem um sistema corporativo específico, sejam armazenadas na rede, no espaço virtual criado para cada setor/atividade. O espaço da rede reservado a cada usuário, bem como o próprio computador do usuário, são locais que podem ser utilizados para armazenamento de informações não-orgânicas ou para backup, embora subentenda-se que as informações em rede contem com uma sistemática de backup. Desta forma, a gestão das informações orgânicas ficaria sujeito ao modelo de dados padrão adotado pela organização e sob responsabilidade do setor de informática no que se refere a segurança. As informações não-orgânicas, por sua vez, seriam de responsabilidade exclusiva dos seus produtores.

Cabe esclarecer que a classificação de informações orgânicas adotada na Administração Pública brasileira é a temática, segundo a qual as informações são classificadas por assunto, os quais encontram-se hierarquicamente distribuídos de acordo com as funções e atividades desempenhadas pela organização. São 10 grandes classes de assuntos, subdivididas em subclasses, grupos e subgrupos, partindo-se sempre do geral para o particular.

No meio eletrônico as classes, subclasses, grupos e subgrupos corresponderiam às pastas e os arquivos aos tipos documentais. O nome dos arquivos também merece a adoção de um padrão visando a rápida e eficiente recuperação das informações. Os padrões de nomeação devem ser definidos de comum acordo entre os usuários de forma a facilitar a identificação do conteúdo informacional dos arquivos e, posteriormente, ser amplamente divulgados. Na nomeação de arquivos deve-se considerar a utilização do menor número possível de caracteres, preferir traço em vez de espaço para separar palavras e utilizar elementos informativos usuais e importantes para a identificação da informação como número, data, interessado e tema.

As informações eletrônicas também necessitam ser classificadas segundo sua sensibilidade, isto é, a necessidade de proteção da informação contra exposição não autorizada, fraude, roubo ou abuso. A propósito, a classificação da informação por níveis de segurança antecede a classificação por assuntos, uma vez que aquela definirá a natureza da informação e, consequentemente, quem pode acessá-la e em que local deve ser armazenada.

A partir do exposto, apresenta-se na Figura 1 um modelo de dados para organização de informações eletrônicas apropriado para a gestão dessas informações nas organizações públicas.

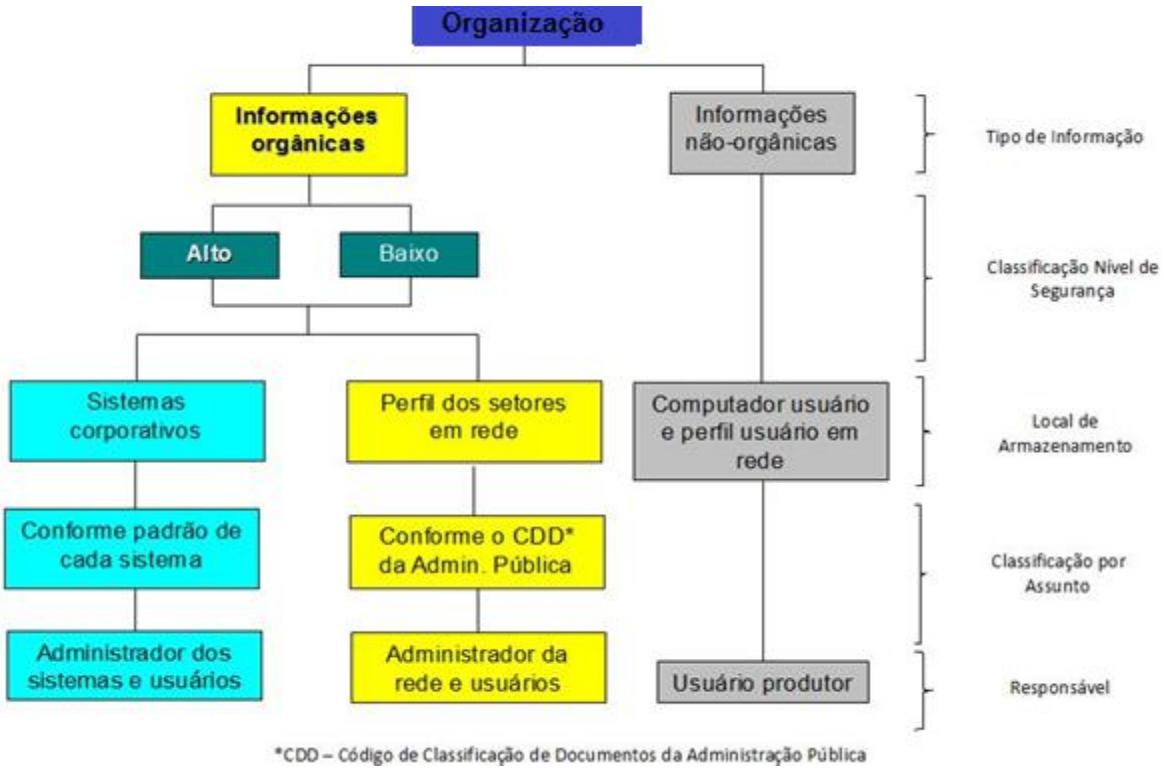

Figura 1 : Modelo de dados para organização de informações eletrônicas

2 Política de segurança da informação

Segurança da informação, segundo a NBR ISO/IEC 27002:2005, é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio.

A mesma norma prevê ainda que a segurança da informação está diretamente relacionada com a preservação da confidencialidade, da integridade e da disponibilidade da informação.

Considerando que a maioria das informações do mundo atual circulam e estão armazenadas em sistemas de informação, depreende-se que a qualidade dos serviços prestados pelas organizações depende desses sistemas,

uma vez que a informação é matéria-prima para a tomada de decisões, definição de estratégias e identificação das ameaças e oportunidades de negócio. Os sistemas de informação, por sua vez, dependem da segurança a eles oferecida, porquanto uma informação desatualizada, corrompida ou indisponível não atenderá às necessidades da organização.

As tecnologias da informação trouxeram a possibilidade real de gerenciamento da totalidade das informações, propiciando a gestão do conhecimento. Ao mesmo tempo, mudaram e aumentaram as formas de uso da informação, tornando-se importante a criação de mecanismos que garantam a integridade e privacidade das mesmas.

As vulnerabilidades estão presentes em todos os sistemas de informação e devem ser identificadas para a escolha correta de medidas de segurança. Em se tratando de redes de telecomunicação, as vulnerabilidades são ainda maiores e estão relacionadas a falhas de hardware, software e uso indevido. Como exemplo pode-se citar grampos em linhas, interceptação ilegal de dados e linhas cruzadas.

Em organizações que lidam com informações sensíveis, o estabelecimento de uma política de segurança da informação não é apenas importante, é absolutamente necessária para garantir sua probidade.

Segundo Dias *apud* Laureano (2010, p. 56), a política de segurança da informação é:

> ...um mecanismo preventivo de proteção dos dados e processos importantes de uma organização que define um padrão de segurança a ser seguido pelo corpo técnico e gerencial e pelos usuários, internos ou externos. Pode ser usada para definir as interfaces entre usuários, fornecedores e parceiros e para medir a qualidade e a segurança dos sistemas atuais.

Para Santos (2005, p. 127), o estabelecimento da política de segurança da informação é uma ação estratégica das organizações:

> ...a política de segurança da informação deve fazer parte do planejamento estratégico da instituição e tem fundamental participação na continuidade de suas atividades, na segurança de seus empregados ou servidores e na preservação de seu patrimônio mobiliário e imobiliário.

Em outras palavras, a política de segurança consiste na formalização dos anseios da organização quanto à proteção de suas informações. Inicialmente deve abordar aspectos simples como identificação de usuários dos sistemas de informação, classificação das informações conforme sua prioridade, controle de acesso aos sistemas de informação, controle de uso das informações para fins institucionais, monitoramento do tráfego de informações na rede institucional, incluindo o acesso a Internet e o uso do correio eletrônico e normatização da política de segurança com aplicação de auditoria e sanções no caso de não observância da mesma. Com base em diagnósticos e análises de risco, a política deve evoluir para o estabelecimento de um sistema de segurança da informação.

Um sistema de segurança da informação é abrangente e envolve ações de segurança operacional (por ex.: análise de riscos, normas e procedimentos, plano de contingência, etc.), segurança física (por ex.: câmeras de vídeo, alarmes, roletas, detectores de metal, etc.) e segurança lógica (detectores de cartão magnético, senhas, certificados digitais, criptografia, firewall, etc.). A política de segurança e o sistema de segurança da informação devem ser formulados em conjunto pela Administração e pelos colaboradores com conhecimentos específicos na área de tecnologia e segurança da informação.

Entre os objetivos de um sistema de segurança deve estar:

- Proteção das informações contra destruição e modificação não autorizadas, bem como contra vazamento;
- Capacidade de prevenir violações, detectar invasões e interromper as ameaças, bem como avaliar e reparar danos mantendo a operacionalidade dos sistemas computacionais caso ocorra invasão;
- Garantia da integridade, confidencialidade, autenticidade, disponibilidade e não-repúdio das informações.

São cinco os pilares da segurança da informação, segundo Silva Filho (2010):

1. Integridade: qualidade de informação que não foi alterada;
2. Confidencialidade: garante que a informação esteja disponível apenas a usuários autorizados;
3. Autenticidade: garante a verificação da origem da informação;
4. Disponibilidade: refere-se ao sistema estar pronto a responder requisições de usuários legítimos, disponibilizando a informação e os seus recursos.
5. Não-repúdio: garante que o autor da informação ou de uma operação em sistemas de informação não negue sua ação.

O estabelecimento de um sistema de segurança da informação compreende as seguintes fases:

a) Planejamento (análise riscos/custos e estabelecimento de política)

Em primeiro lugar é necessário saber o que é necessário proteger. Para tanto, um levantamento é requerido a fim de identificar as necessidades de segurança da informação e as vulnerabilidades a que estão sujeitas. Conhecidas as necessidades, deve-se definir prioridades e custos. As prioridades devem levar em consideração aspectos como conformidade com a legislação aplicável e interesses da organização e dos parceiros, entre outros. Quanto aos custos, o prejuízo de uma possível perda ou indisponibilidade de informações relevantes deve ser considerada na avaliação do custo-benefício de implementar ações de segurança. A partir disso, será possível planejar as ações de segurança da informação de acordo com as necessidades e possibilidades da organização. A política de segurança das informações também deve estar integrada com as políticas institucionais, metas e planejamento estratégico da organização, uma vez que os procedimentos e padrões de segurança não podem impactar no funcionamento do ambiente de tecnologia da informação e nem tampouco na continuidade dos serviços ou negócios.

b) Execução (definição de normas e procedimentos e plano de contingência)

O próximo passo é a definição de normas e procedimentos para a efetiva execução do plano de ação. Segundo Dias apud Laureano (2010, p. 56), “as normas dirão como a organização irá proceder na proteção, controle e monitoramento de seus recursos computacionais”. Além disso, também é imprescindível que sejam definidas as responsabilidades pelas ações de segurança, delineando as principais ameaças, riscos e impactos envolvidos. Deve ser de responsabilidade geral, no mínimo, o conhecimento da política de segurança, a aplicação da política e a comunicação de suspeitas relativas a problemas com a política. Demais responsabilidades devem ser distribuídas entre administrador de sistema, administrador de segurança, colaboradores/usuários e convidados. A infringência à política de segurança deve prever consequências e penalidades aos responsáveis, sob pena de não ser levada a sério. O plano de contingência em tecnologia da informação visa definir as ações a serem tomadas em casos de crise ou desastres que prejudiquem o acesso às informações da organização. Sua definição é importante na medida em que auxilia no restabelecimento em tempo mínimo do processamento de informações, considerando a criticidade destas, de tal forma a minimizar eventuais prejuízos.

c) Acompanhamento (auditoria)

O objetivo do acompanhamento é verificar a conformidade dos procedimentos da organização com a política de segurança da informação previamente estabelecida. Por outro lado, visa também verificar se os procedimentos de segurança da informação continuam adequados à realidade da organização no que tange suas necessidades de uso e proteção da informação. A auditoria é uma forma de acompanhar a efetiva e correta aplicação das políticas de segurança, bem como a única forma de avaliação e proposição de melhorias.

Definidas as fases básicas para o estabelecimento de um sistema de segurança da informação, pode-se dizer que os requisitos indispensáveis para um sistema eficaz são: autenticação de usuários; detectores de ataque e invasão como firewall; detectores de intrusão, como IDS (intrusion detection system) e antivírus; criptografia; e backup.

Embora não seja abordada na literatura específica voltada para sistemas de segurança da informação, a migração periódica das informações vitais da organização para novos programas e suportes é imprescindível para a acessibilidade a longo prazo e requisito indispensável da preservação digital de documentos eletrônicos, sendo esta ação unanimidade na área de gestão documental.

Estabelecer o sistema de segurança da informação, porém, não é a única medida que a organização precisa tomar. Deve se preocupar também com as condições necessárias para a efetividade desse sistema. A participação de todos os colaboradores/usuários é uma dessas condições, vez que a segurança precisa de coesão, isto é, não pode haver falha por parte de nenhum dos integrantes da cadeia, sob pena de deixar o todo vulnerável. Outro aspecto importante é o treinamento, entendido como forma viável de divulgação da política de segurança e as formas corretas de adoção da mesma. Além disso, o treinamento também deve instruir os usuários dos sistemas quanto à importância das informações e sua gestão adequada. Por fim, o controle do esquema de segurança da informação, incluindo análise e gerência de riscos, deve ser realizado continuamente com o objetivo de manter e melhorar o sistema, caracterizando a auditoria como ponto crucial e derradeiro para a eficácia do sistema de segurança da informação.

Ao tratar do gerenciamento eletrônico de documentos arquivísticos, Santos (2005, p.164) aponta a necessidade de existência de uma política arquivística paralelamente ao desenvolvimento de um sistema de segurança da informação e à capacitação e treinamento constate. Segundo o autor, são “as questões mais relevantes para a aplicação prática de uma gestão arquivística de documentos digitais”.

No Brasil, para o estabelecimento de uma política de segurança, devem ser observadas a NBR ISO/IEC 27001:2013 e 27002:2013, da Associação Brasileira de Normas Técnicas (ABNT), as quais, juntas, estabelecem um referencial para desenvolver, implementar e avaliar a gestão da segurança da informação, bem como para avaliar e tratar os riscos de segurança da informação voltados para as necessidades da organização.

A Política de Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal foi instituída no ano de 2000 através do Decreto 3.505/2000, cujos pressupostos devem ser atendidos quando do estabelecimento de políticas de segurança da informação nas organizações públicas. São pressupostos básicos da Política de Segurança da Informação, conforme a referida norma:

1. Assegurar a garantia ao direito individual e coletivo das pessoas, à inviolabilidade da sua intimidade e ao sigilo da correspondência e das comunicações, nos termos previstos na Constituição;
2. Proteção de assuntos que mereçam tratamento especial;
3. Capacitação dos segmentos das tecnologias sensíveis;
4. Uso soberano de mecanismos de segurança da informação, com o domínio de tecnologias sensíveis e duais;
5. Criação, desenvolvimento e manutenção de mentalidade de segurança da informação;
6. Capacitação científico-tecnológica do País para uso da criptografia na segurança e defesa do Estado; e
7. Conscientização dos órgãos e das entidades da Administração Pública Federal sobre a importância das informações processadas e sobre o risco da sua vulnerabilidade.

Além disso, há também a Resolução nº 39/2006, do Instituto Nacional de Tecnologia da Informação, que estabelece a política de segurança da ICP-Brasil e serve como um referencial para o estabelecimento da política de segurança da informação nas organizações públicas.

3 Considerações finais

O estabelecimento de políticas de gestão e segurança para as informações em meios eletrônicos é importante na medida em que o compartilhamento das informações constitui-se em uma necessidade para o bom desempenho da organização.

Assim, a adoção de padrões para a classificação da informação, local adequado de armazenamento e definição de responsabilidades, conforme apresentado neste artgo, é imprescindível para uma adequada gestão da informação eletrônica.

Quanto à política de segurança da informação nas organizações públicas, recomenda-se, prioritariamente, a instituição de comissão de segurança da informação, análise dos riscos a que as informações estão sujeitas e desenvolvimento de um sistema de segurança da informação.

Considerando que a evolução das tecnologias da informação em todas as áreas do conhecimento é um caminho sem volta, resultando na responsabilidade cada vez maior sobre os dados produzidos e mantidos em meio eletrônico para seu efetivo uso, é muito importante – e já não sem tempo - que as organizações se preocupem em iniciar uma política de segurança da informação. Somente a prática é capaz de apontar o caminho certo para a proteção das informações nesse meio virtual tão democrático e cheio de possibilidades e vulnerabilidades – encontram-se pessoas de todos os tipos, inclusive criminosos, com intenções de todos os tipos, inclusive maliciosas.

Laureano (2010, p. 57-58) sugere:

- Uma boa política hoje é melhor do que uma excelente política no próximo ano;
- Uma política fraca, mas bem-distribuída, é melhor do que uma política forte que ninguém leu;
- Uma política simples e facilmente compreendida é melhor do que uma política confusa e complicada que ninguém se dá o trabalho de ler;
- Uma política cujos detalhes estão ligeiramente errados é muito melhor do que uma política sem quaisquer detalhes;
- Uma política dinâmica que é atualizada constantemente é melhor do que uma política que se torna obsoleta com o passar do tempo;
- Costuma ser melhor se desculpar do que pedir permissão.

Concluindo, embora o estabelecimento de uma política de segurança da informação imponha a adoção de novas ações e atribuições, muitas vezes complexas, onerosas ou difíceis de solucionar, é melhor tê-la do que jamais ter se preocupado com essa questão.

Referências bibliográficas

ARQUIVO NACIONAL. Resolução nº 14, de 24 de outubro de 2001. Aprova a versão revisada e ampliada da Resolução nº 04, de 28 de março de 1996, que dispõe sobre o código de Classificação de Documentos de Arquivo para a Administração Pública: atividades de apoio, a ser adotado como modelo para os arquivos correntes dos órgãos e entidades integrantes do Sistema Nacional de Arquivos (SINAR), e os prazos de guarda e destinação de documentos estabelecidos na Tabela Básica de Temporalidade e Destinação de Documentos de Arquivo relativos às atividades de apoio da Administração Pública. Diário Oficial da União, Poder Executivo, Brasília, DF, 08 fev. 2002. Seção 1, p. 2.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27002 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão de segurança da informação. Rio de Janeiro: ABNT, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27001 – Tecnologia da informação – Técnicas de segurança – Sistemas de gestão da segurança da informação – Requisitos. Rio de Janeiro: ABNT, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27002 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão de segurança da informação. Rio de Janeiro: ABNT, 2013.

BRASIL. Decreto n. 3.505, de 13 de junho de 2000. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. Diário Oficial da União, Poder Executivo, Brasília, DF, 14 jun. 2000.

HUBBARD, Douglas. Como lidar com as incertezas das análises de custo-benefício nos projetos de tecnologia. CIO, ago. 2007. Disponível em: <http://cio.com.br/gestao/2007/08/21/idgnoticia.2007-08-21.5177662036/> Acesso em: 13 out. 2010.

INTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO. Resolução nº 39, de 18 de abril de 2006. Aprova a versão 2.0 da Política de Segurança da ICP-Brasil. Diário Oficial da União, Poder Executivo, Brasília, DF, 24 abr. 2006.

LAUREANO, Marcos Aurelio Pchek. Gestão de Segurança da Informação. Disponível em: <http://www.scribd.com/doc/20723105/apostila-versao-20> Acesso em: 27 set. 2010.

MORESI, Eduardo Amadeu Dutra. Delineando o valor do sistema de informação de uma organização. Ciência da Informação, Brasília, vol. 29, n. 1, p. 14-24, jan/abr. 2000. Disponível em: <http://www.scielo.br/pdf/ci/v29n1/v29n1a2.pdf> Acesso em: 13 out. 2010.

ROUSSEAU, Jean-Yves; COUTURE, Carol. Os fundamentos da disciplina arquivística. Trad. de Magda Bigotte de Figueiredo. Lisboa: Publicações Dom Quixote, 1998.

SANTOS, Vanderlei Batista dos; INNARELLI, Humberto Celeste; SOUSA, Renato Tarciso Barbosa de (org.). Arquivística: temas contemporâneos: classificação, preservação digital, gestão do conhecimento. 2ª ed. Distrito Federal: SENAC, 2008.

SANTOS, Vanderlei Batista dos. Gestão de documentos eletrônicos: uma visão arquivística. 2 ed. rev. e aum. Brasília: ABARQ, 2005.

SILVA FILHO, Antonio Mendes da. Segurança da informação: sobre a necessidade de proteção de sistemas de informações. Revista Espaço Acadêmico, n. 42, Nov. 2004. Disponível em: <http://www.espacoacademico.com.br/042/42amsf.htm> Acesso em: 27 set. 2010.

TONINI, Regina S. S. Custo na gestão da informação. In: ENCONTRO NACIONAL DE ENSINO E PESQUISA EM INFORMAÇÃO, 7, 2007, Salvador. Anais eletrônicos... Salvador: UFBA, 2007. Disponível em: <http://www.cinform.ufba.br/7cinform/soac/papers/adicionais/ReginaTonini1.pdf> Acesso em: 13 out. 2010.

Dados da autora

Sandra Buth Zanon

Possui graduação em Arquivologia pela Universidade Federal de Santa Maria – UFSM (2002). É professora, conteudista e tutora da Academia Nacional de Polícia na área de Ciências da Informação. Tem experiência na área de Ciências da Informação, com ênfase em Gestão de Documentos.

sandrazanon@gmail.com

Recebido – Received : 2014-05-31

Aceitado – Accepted : 2014-09-30