Implantação da segurança na gestão da informação na administração pública: um estudo de caso no Tribunal de Contas do Estado do Amazonas

Angelo Eduardo Nunan
Tribunal de Contas do Estado do Amazonas (TCE-AM)

Mário José de Moraes Costa Filho
Tribunal de Contas do Estado do Amazonas (TCE-AM)

Adriana Almeida Lima
Universidade do Estado do Amazonas (UEA)

A partir de uma visão moderna da gestão contemporânea, os órgãos da administração pública têm assumido uma nova postura na busca pela prestação de serviços de excelência à sociedade. Nesse contexto, a informação passou a exercer um papel preponderante e estratégico na tomada de decisões. Isso promoveu a necessidade de protegê-la de forma estruturada e adequada. Considerando a aplicação prática da pesquisa científica, este trabalho tem por objetivo analisar a implantação da segurança na gestão da informação no âmbito da administração pública e divulgar como o conhecimento pode ser aplicado em benefício do setor. A pesquisa apresenta um estudo de caso sobre a implantação da segurança da informação no âmbito do TCE-AM. Dentre os resultados alcançados, destaca-se a elevação do nível de proteção dos ativos, aumento da resiliência dos serviços e processos de trabalho e o fortalecimento dos controles internos e da imagem organizacional.

Palavras-chave: gestão pública, segurança da informação, gestão estratégica

[Artigo recebido em 19 de abril de 2014. Aprovado em 18 de maio de 2015]

Seguridad de la información como un factor en la gestión de información estratégica en la administración pública

Desde un punto de vista moderno de la gestión contemporánea, organismos de la administración pública han adoptado un nuevo enfoque en la búsqueda de brindar servicios de excelencia a la sociedad. En este contexto, la información comenzó a ejercer un papel importante y estratégico en la toma de decisiones. Esto promovió la necesidad de protegerla de una manera estructurada y adecuada. Considerando la aplicación práctica de la investigación científica, el presente trabajo tiene como objetivo examinar la implantación de seguridad en el manejo de la información dentro de la administración pública y revelar cómo se puede aplicar el conocimiento para el beneficio del sector. La investigación presenta un estudio de caso sobre el despliegue de seguridad de la información en el TCE-AM. Entre los logros, existe un alto nivel de protección de activos, el aumento de la capacidad de recuperación de los servicios y procesos de trabajo y el fortalecimiento de los controles internos y la imagen de la organización.

Palabras clave: gestión pública, seguridad de la información, dirección estratégica

Information security as strategic factor in the information management in public administration

From a modern vision of contemporary management, the public administration have taken a new approach in the quest to provide excellent services to society. In this context, information began to play an important and strategic role in decision-making. This endorsed the need to protect it in an appropriate structure. Considering the practical application of scientific research, this paper aims to examine the security deployment in the information management within the public administration and disclose how knowledge can be applied for the benefit of the sector. The research presents a case study on information security deployment in the TCE-AM. Among the results, there was a high level of protection to actives, increase of the resilience of services and work processes and the strengthening of internal controls and organizational image.

Keywords: public administration, security of information, strategic management

Introdução

As constantes mudanças políticas e tecnológicas vivenciadas em tempos de globalização impuseram ao setor público a necessidade de assumir uma nova postura de comportamento na sua gestão e uma abordagem contemporânea e moderna para alcançar as suas metas finalísticas. Isso conduziu muitas organizações públicas a repensarem sobre os fatores estratégicos essenciais e determinantes para alcançar a excelência na prestação de seus serviços e garantir a sua credibilidade junto à sociedade.

Nesse ambiente, caracterizado pela necessidade de partilha e elicitação de conhecimento, de identificação de oportunidades, de capacidade para inovações e de melhoria contínua da qualidade, a informação passou a exercer um papel preponderante.

Assim, a informação consolidou-se como um dos ativos mais importantes para as organizações, agregando valor diferencial às tomadas de decisões e norteando as ações mais ajustadas e aderentes ao alcance dos resultados esperados pela administração.

Ao longo do seu ciclo de vida, a informação é produzida, processada, transmitida, armazenada, apresentada ou descartada por diversos recursos e ativos físicos, tecnológicos e humanos.

Com a dependência cada vez maior da informação, por parte das organizações, esse ativo passou a demandar um conjunto de políticas, mecanismos e controles de segurança sobre todo o seu ciclo de vida, de forma a permitir que a mesma possa ser empregada de maneira oportuna, precisa e segura pelo gestor e por toda a organização na consecução e garantia de seus processos de trabalho e de seu poder de decisão.

Este trabalho tem por objetivo analisar a prática da segurança na gestão da informação no âmbito do setor público e divulgar como o conhecimento pode ser aplicado em benefício dos sistemas sociais em geral, em especial na administração pública, de forma a garantir a manutenção de seus processos de trabalho, melhoria contínua dos serviços prestados à sociedade e a qualidade da tomada de decisões.

O tema é desenvolvido a partir da apresentação do referencial teórico sobre segurança da informação. Apresenta-se uma breve descrição da metodologia aplicada e em seguida faz-se uma análise acerca do atual cenário relativo à adoção de práticas de segurança da informação no âmbito do setor público e da sua importância na administração pública. Por fim, é apresentado um estudo de caso sobre a implantação de controles de segurança da informação e os resultados parciais alcançados no âmbito do Tribunal de Contas do Estado do Amazonas.

Referencial teórico

Segurança da informação

Para compreender melhor a segurança é preciso entender os aspectos que envolvem a informação e a sua importância para a sobrevivência e sucesso das organizações.

Conforme destaca Sianes (2005), a informação é uma série de dados organizados de um modo significativo, analisados e processados, que pressupõe soluções ou novos insumos para o processo de tomada de decisão, estando associado à utilidade que ela apresenta em determinado contexto.

Essa informação, contudo, pode ter significado, forma e valor diferente, dependendo do seu estado e momento de uso, ou seja, é preciso considerar o seu ciclo de vida para protegê-la em diversas fases de sua existência.

Segundo Sêmola (2003), o ciclo de vida da informação é composto e identificado por momentos distintos durante a sua vida útil. Esse ciclo é definido em quatro momentos: **(i) manuseio:** momento em que a informação é criada e manipulada, seja sob a forma física ou eletrônica; **(ii) armazenamento:** momento em que há o armazenamento propriamente dito da informação, seja em papel, arquivo físico, banco de dados ou qualquer outro tipo de mídia; **(iii) transporte:** momento em que a informação é transportada, seja em papel, mídia ou por meio remoto em uma rede de computadores; **(iv) descarte:** momento em que a informação é descartada, seja na forma física ou eletrônica.

Entender o ciclo de vida da informação é de suma importância para a sua segurança, pois durante esse ciclo existem condições que, de alguma forma, a colocam em uma situação vulnerável, podendo comprometer ativos e processos de trabalho da organização. Conforme Sêmola (2003), as condições que afetam a informação são: **(i) ameaças**: agentes ou condições que podem causar incidentes que comprometam as informações e seus ativos por meio da exploração de vulnerabilidades e que tragam prejuízos à confidencialidade, integridade e disponibilidade da informação; **(ii) vulnerabilidades:** fragilidades existentes ou associadas a ativos que processam informações e que, se explorados, podem comprometer a segurança da informação; **(iii) riscos:** probabilidades de ameaças explorarem vulnerabilidades, provocando perdas ou danos aos ativos e às informações.

Para neutralizar ou mitigar essa tríade (ameaça-vulnerabilidade-risco) é preciso estabelecer formas estruturadas de proteção que garantam a segurança da informação durante todo o seu ciclo de vida e nas diversas camadas ou aspectos em que a mesma é processada ou tratada.

Assim, Ramos (2006) define segurança da informação como a proteção aos ativos da informação, ou seja, aqueles que produzem, processam, transmitem ou armazenam informações. Essa proteção é alcançada a partir de um conjunto de instrumentos que englobam políticas, processos, procedimentos, estruturas organizacionais, *softwares* e *hardware*, em conjunto com outros processos da gestão da informação. Isso visa garantir os fundamentos básicos que norteiam o processo de proteção, que são estabelecidos como: **(i) confidencialidade:** refere-se a garantir que apenas as pessoas as quais devam ter conhecimento legitimamente sobre um assunto terão acesso ao mesmo; **(ii) integridade:** refere-se a proteger as informações contra alterações em seu estado original, sejam intencionais ou acidentais; **(iii) disponibilidade:** refere-se a garantir que a informação possa ser acessada por aqueles que dela necessitam, no momento em que precisam.

O comprometimento desses princípios envolve, de acordo com Sêmola (2003), outros conceitos importantes: **(i) incidente de segurança:** evento decorrente da exploração de uma vulnerabilidade. O incidente pode ser considerado como uma ação indesejada ou inesperada com alto potencial de comprometimento dos princípios da segurança da informação: confidencialidade, integridade e disponibilidade; **(ii) impacto:** é a mensuração quantitativa ou qualitativa acerca dos prejuízos que advém de um incidente de segurança. Dessa forma, qualquer incidente que afete a informação, necessariamente, afetará também a pelo menos um desses princípios.

Assim, por exemplo, caso os dados de um processo sigiloso sejam acessados por agentes não autorizados, seja em sua forma física ou digital, a confidencialidade será afetada, podendo comprometer a credibilidade de todo o sistema administrativo operacional e os preceitos da segurança, como fator de estratégia na administração. Em outro exemplo, caso um sistema de apoio à decisão apresente problemas ou falhas que inviabilizem o seu uso em um momento oportuno e decisivo para o gestor, o princípio da disponibilidade será afetado e poderá comprometer a tomada da melhor decisão para a administração. Por fim, se algum dado armazenado em uma mídia ou transmitido de forma digital é corrompido ou alterado de forma ilegítima, o princípio da integridade será afetado.

Conforme o grau de impacto do incidente, a organização poderá ter prejuízos financeiros ou de imagem, além do comprometimento dos seus processos de trabalho.

Diante da complexidade e demanda de investimentos em segurança, é necessário adotar estratégias que priorizem essas atividades segundo o seu grau de criticidade, valor e importância para a organização.

Para otimizar a aplicação desses recursos em função dos ativos a serem protegidos, Ramos (2006) propõe estratégias de proteção para o balanceamento

entre a necessidade de proteção e as vulnerabilidades e ameaças sobre esses ativos, quais sejam:

(i) privilégio mínimo (*least privilege*): refere-se a uma não exposição a risco desnecessário. Segundo esse enfoque, o acesso do usuário deve ser restrito às suas reais necessidades para o desempenho de suas funções;

(ii) defesa em profundidade (*defense in depth*): refere-se à aplicação de defesas distintas, de controles complementares como redundância, para que, no caso de falha ou violação de um, haja outro controle. Assim, o sistema como um todo não se torna vulnerável, por estar restrito a somente um único controle. Afinal, em segurança nada é infalível;

(iii) elo mais fraco (*weakest link*): refere-se ao princípio de que o elo mais fraco de uma corrente define a resistência do sistema, pois o invasor precisará apenas de uma falha para alcançar o seu objetivo;

(iv) ponto de estrangulamento (*choke point*): refere-se a adotar medidas de segurança estratégicas em um mesmo ponto de controle em que passem todos os usuários;

(v) segurança pela obscuridade (*security throught obscurity*): refere-se à estratégia de que quanto menos informações um agente tiver a respeito do ambiente alvo, maior será a sua dificuldade em invadi-lo, porém, é preciso combinar outros controles para que seja eficaz;

(vi) simplicidade (*simplicity*): refere-se à estratégia de avaliar a complexidade do sistema a ser protegido, pois quanto mais complexo um sistema, maior será a dificuldade em torná-lo seguro.

Para gerir e garantir a segurança desses dados, de forma processual, sistemática e criteriosa, considerando todas essas premissas, adota-se um sistema de gestão de segurança da informação (SGSI), em que são implantados e geridos os requisitos e boas práticas de segurança recomendados em normas de padronização nacionais e internacionais.

Sistema de gestão de segurança da informação (SGSI)

A norma da Associação Brasileira de Normas Técnicas (ABNT), ABNT NBR-ISO/IEC 27001:2006 (Associação Brasileira de Normas Técnicas, 2006) tem por propósito prover um modelo de sistema de gestão da segurança da informação (SGSI) independentemente do tipo, tamanho ou natureza da organização. Esse sistema é definido pela mesma norma como um sistema de gestão global baseado em uma abordagem de riscos do negócio com o objetivo de implantar e gerir a segurança da informação. Esse sistema inclui a estrutura organizacional, as políticas

de segurança, os planejamentos, a definição de responsabilidades, a adoção e gestão de processos, procedimentos, recursos e ativos da organização (Associação Brasileira de Normas Técnicas, 2006, p.3).

De acordo com a norma ABNT NBR-ISO/IEC 27001:2006 (Associação Brasileira de Normas Técnicas, 2006), o SGSI é um sistema baseado em processos estruturados no modelo PDCA (*plan-do-check-act*): **(i) *plan* (planejar):** fase de planejamento e estabelecimento do SGSI. Nessa fase são estabelecidos o escopo, os limites do sistema, os objetivos, as políticas, os processos e procedimentos que serão tratados pelo SGSI; **(ii) *do* (fazer):** fase de implementação e operação do SGSI; **(iii) *check* (checar):** fase em que ocorre a avaliação do SGSI. Avalia-se a conformidade com o que foi planejado; **(iv) *act* (atuar):** fase em que são realizados os ajustes demandados pelo processo de auditoria interna. Essa fase visa à melhoria contínua do sistema. O PDCA é um processo cíclico.

Para implantar o SGSI, a organização precisa estar alinhada às recomendações da norma ABNT NBR-ISO/IEC 27002:2005 (Associação Brasileira de Normas Técnicas, 2005), que estabelece o código de prática para a gestão da segurança da informação.

A norma possui 133 controles de segurança distribuídos sob a perspectiva de 11 domínios, descritos a seguir: **(i) política de segurança:** conjunto de diretrizes, normas, procedimentos e instruções que se destinam a definir a proteção adequada aos ativos, de forma alinhada aos objetivos da organização. De acordo com Beal (2005, p.43), "a elaboração de uma política de segurança da informação representa um passo fundamental no estabelecimento de um sistema de gestão de segurança de informação eficaz"; **(ii) organização da segurança:** esse domínio prevê a definição de controles voltados para o estabelecimento da estrutura de gerenciamento e coordenação da implantação e manutenção da segurança da informação; **(iii) classificação de bens e controles:** define controles para gestão dos ativos, ou seja, a sua identificação, inventário e gestão; **(iv) segurança em recursos humanos:** define controles para disciplinar os processos de admissão e desligamento de pessoal, delimitação de perfil de acesso à informação, treinamentos e processo disciplinar; **(v) segurança física e do meio ambiente:** define controles para definição de perímetros, controle de acessos físicos e proteção de equipamentos e estrutura organizacional; **(vi) gestão das operações e comunicações:** define controles para garantir a operação segura dos recursos de tecnologia da informação; **(vii) controle de acesso:** define controles para disciplinar o acesso à informação; **(viii) aquisição, desenvolvimento e manutenção de sistemas de informação:** define controles para garantir a conformidade dos sistemas de informações com as boas práticas de segurança e requisitos do negócio; **(ix) gestão de incidentes de segurança:** define controles para garantir a comunicação rápida e

tratamento de incidentes de segurança; **(x) gestão da continuidade dos negócios:** define controles para melhorar a resiliência da organização diante de paralisações de processos de trabalho; e, por fim, **(xi) conformidade:** define controles para garantir a conformidade com os requisitos legais, tributários, estatutários, regulamentares, contratuais e de segurança.

Alinhada à gestão da segurança da informação, a norma ABNT ISO/IEC 27005:2008 (Associação Brasileira de Normas Técnicas, 2008) apresenta as diretrizes para o gerenciamento dos riscos de segurança da informação. A análise de riscos é uma atividade essencial dentro do processo de gestão de riscos de segurança da informação e tem por objetivo reduzir os riscos a um nível aceitável para a organização.

Segundo Sêmola (2003), a análise de riscos é fundamental no estabelecimento da situação de segurança da informação da organização. A ABNT ISO/IEC 27005:2008 (Associação Brasileira de Normas Técnicas, 2008) recomenda que essa atividade deva considerar: **(i)** a política de segurança da informação estabelecida; **(ii)** o planejamento estratégico da organização; **(iii)** a estrutura organizacional e seus processos de trabalho; **(iv)** os ativos da organização; **(v)** os requisitos legais e contratuais; **(vi)** a localização geográfica e o ambiente sociocultural em que está inserida a organização; e **(vii)** a interação e comunicação com o ambiente externo.

O alinhamento entre os conceitos de segurança da informação, estratégias e as recomendações contidas nas principais normas técnicas adotadas no mercado converge para uma sinergia fundamental na gestão da segurança da informação.

Metodologia

Este trabalho caracterizou-se como uma pesquisa descritiva e exploratória. Utiliza-se a pesquisa bibliográfica e um estudo de caso em um órgão de controle da administração pública estadual do Estado do Amazonas. A técnica de observação utilizada no estudo de caso foi a de participante natural, uma vez que os pesquisadores trabalham no órgão e participam diretamente do processo de implantação estudado.

De acordo com a Associação Nacional de Pós-Graduação e Pesquisa em Administração – Anpad (Associação Nacional de Pós-Graduação e Pesquisa em Administração, 2010), divulgar como o conhecimento pode ser aplicado em benefício dos sistemas sociais, em geral, é avaliado positivamente, considerando o interesse da pesquisa científica e a sua aplicação prática para os gestores de organizações em geral.

A coleta dos dados ocorreu em duas fases: **(i)** pesquisa bibliográfica que teve por objetivo apresentar o referencial teórico sobre segurança da informação e identificar o atual cenário de implantação da segurança da informação na administração pública; **(ii)** análise das ações e documentações procedidas na implantação da segurança da informação no Tribunal de Contas do Estado do Amazonas.

A implantação da segurança da informação, apresentada no estudo de caso, foi realizada com base no sistema de gestão de segurança da informação (SGSI), sustentado no modelo PDCA (*plan-do-check-act*), que mantém o processo de gestão da segurança da informação de forma estruturada e cíclica. Esses modelos são amplamente adotados pelo mercado e preconizados na Norma ABNT NBR-ISO/IEC 27001:2006 (Associação Brasileira de Normas Técnicas, 2006), versão normativa em vigor à época da implantação do projeto.

Implantação da segurança como estratégia na gestão da informação na administração pública

Sacconi (1998) define estratégia como o conhecimento necessário para a realização de desígnios hábeis que determinam uma posição privilegiada para a organização. Araújo e Easton (1996) avaliam a estratégia como um posicionamento consistente derivado da combinação de diversos elementos nas relações internas e externas da organização. Dentre os diversos elementos, Kodama (1994) destaca a importância dos dados e informações para o estabelecimento de estratégias.

Nesse contexto, a estratégia pode ser posicionada e definida como a realização de um plano hábil que depende de um conjunto de dados, que, ao ser transformado em informação útil, é usado pelo gestor, segundo o seu conhecimento, a sua habilidade e perspicácia administrativa em uma análise ponderada entre as relações internas e externas à organização na tomada de decisões.

Ao compreender o próprio conceito de estratégia, é possível observar de imediato que a informação exerce um papel determinante na tomada de decisões do gestor. Por inferência, garantir os princípios básicos que norteiam o seu processo de proteção é um fator estratégico importante na gestão da informação que é usada pela organização, pois dispô-la de forma correta e no momento oportuno permite a tomada de decisões de forma ágil e efetiva, favorecendo que a organização potencialize o sucesso no alcance de suas metas e de uma posição de destaque ou de excelência em seu campo de atuação.

Gimenez (Gimenez; Pelisson; Kruger; Hayashi, 1999, p.69) afirma que a gestão estratégica das informações é fundamental para as organizações, pois "possibilita tomadas de decisão que sustentam outros processos de gestão e outros processos

estratégicos". Segundo Laureano e Moraes (2005), é necessário valorizar o uso de sistemas de segurança como estratégia para a gestão da informação e dos dados organizacionais.

Cenário atual de implantação da segurança da informação no setor público

De uma forma geral, sob o ponto de vista científico, a segurança da informação é uma área do conhecimento que ainda apresenta muitas lacunas, inclusive de estudos específicos sob a ótica do setor público (Nobre; Ramos; Nascimento, 2010).

Nobre, Ramos e Nascimento (2010) realizaram um estudo com 80 gestores públicos estaduais do Programa Nacional de Apoio à Modernização da Gestão e do Planejamento dos Estados e Distrito Federal (Pnage) em todo o Brasil, com exceção do estado de Goiás, e evidenciaram, em um dos indicadores avaliados, que a intenção comportamental de utilização de práticas avançadas de segurança da informação por parte dos gestores foi de 54,4%, desde que os mesmos tivessem o acesso às normas de segurança. Isso demonstra um nível de aceitabilidade razoável.

Entretanto, a mesma pesquisa apresenta resultados preocupantes em que demonstra que a segurança da informação ainda não é uma prática amplamente difundida, considerando o escopo da pesquisa. Entre os resultados, verificou-se que 43,1% dos gestores realizam cópias de segurança (*backup*) com intervalos de mais de um mês, e 21,5% nunca realizaram tal procedimento. O fato é que, no setor público, o estabelecimento de práticas de segurança da informação ainda apresenta baixo nível de maturidade.

Atento à importância da segurança da informação no âmbito das organizações públicas e das consequências decorrentes de sua ausência ou deficiência, o Tribunal de Contas da União (TCU) passou a realizar, desde o ano de 2007, levantamentos na área de governança de tecnologia da informação em que, entre outros indicadores, afere o percentual de implantação de práticas de segurança da informação em órgãos da administração pública federal (Tribunal de Contas da União, 2010).

Essa avaliação se apresenta como de suma importância, principalmente no sentido de se visualizar o cenário atual e de se proceder a orientações para que as organizações exerçam um papel proativo, de forma a melhorar a eficiência e seu poder de decisão, a qualidade do serviço prestado e a sua credibilidade junto à sociedade, evitando, ainda, o desperdício de recursos públicos em ações corretivas ou no emprego inadequado de ferramentas, técnicas ou de soluções de segurança, na tentativa de garantir a integridade, confidencialidade e disponibilidade da informação.

Conforme consta do sumário executivo do TCU, "a área de segurança da informação continua a chamar a atenção pelos altos índices de não conformidades" (Tribunal de Contas da União, 2010, p.07). O resultado da pesquisa destaca que as organizações públicas avaliadas não tratam seus riscos, principalmente por não

os conhecerem, o que inviabiliza estimar suas consequências, caso esses riscos se materializem. Certamente, isso pode afetar todo o processo de gestão da informação da organização e seu processo estratégico e decisório.

Para ressaltar a importância estratégica da segurança da informação para as organizações públicas, o TCU, após o primeiro levantamento realizado em 2007, emitiu uma recomendação registrada no item 9.1.3 do Acórdão nº 1.603/2008-TCU-Plenário, com a seguinte redação:

> 9.1.3 orientem sobre a importância do gerenciamento da segurança da informação, promovendo, inclusive mediante normatização, ações que visem estabelecer e/ou aperfeiçoar a gestão da continuidade do negócio, a gestão de mudanças, a gestão de capacidade, a classificação da informação, a gerência de incidentes, a análise de riscos de TI, a área específica para gerenciamento da segurança da informação, a política de segurança da informação e os procedimentos de controle de acesso; [...]. (Tribunal de Contas da União, 2010, p. 18).

Após a recomendação, o TCU divulgou o comparativo entre os resultados dos levantamentos do ano de 2007 e 2010, em que apresenta um quadro preocupante em relação à implantação da segurança nos 315 órgãos avaliados. A Tabela 1 demonstra a evolução dos indicadores de segurança da informação em órgãos da administração pública federal.

A análise dos indicadores demonstrados na Tabela 1 sinaliza que não houve avanço significativo na adoção de práticas de segurança da informação na administração pública federal. A redução verificada em alguns itens corresponde, segundo o TCU, a uma melhor compreensão dos órgãos sobre os itens questionados e um maior rigor na avaliação realizada em 2010. Entretanto, conforme destaca o próprio TCU, "a Administração, de forma geral, continua a desconhecer e a não proteger suas informações críticas adequadamente" (Tribunal de Contas da União, 2010, p.20).

Tabela 1 – Evolução dos indicadores de segurança da informação em órgãos avaliados pelo TCU

INDICADOR	ANO	
	2007	2010
Possui área de segurança da informação	38%	42%
Há política de segurança da informação	37%	37%
Faz análise de riscos	26%	16%
Há gestão de incidentes de segurança da informação	26%	24%
Classifica a informação	22%	12%
Há gestão de capacidade	16%	7%
Há gestão de mudanças	12%	19%
Tem plano de continuidade do negócio	13%	3%

Fonte: TCU (2010).

Seguindo essa mesma abordagem, o Tribunal de Contas do Estado do Amazonas (TCE-AM) realizou uma pesquisa pioneira, no ano de 2013, acerca da governança em tecnologia da informação no Estado do Amazonas, que foi conduzida pela Diretoria de Controle Externo de Tecnologia da Informação (Diati).

A análise do indicador descrito na Tabela 2 demonstra que o cenário, no âmbito da administração pública estadual no Estado do Amazonas, não é diferente da esfera administrativa federal. Os resultados são tecnicamente idênticos, demonstrando que o nível de maturidade da administração pública em geral, no que tange à adoção de práticas de segurança da informação, ainda é baixo e precisa ser aperfeiçoado.

Tabela 2 – Indicador geral acerca da gestão da segurança da informação em órgãos da administração pública estadual avaliados pelo TCE-AM

Indicador: Possui gestão na área de segurança da informação?			**ANO**
			2013
Administração pública estadual	Órgãos consultados	Órgãos respondentes	Resultado (SIM)
Administração direta	79	61	**27 (44,26%)**
Administração indireta	35	30	**16 (53,3%)**
Total	114	91	**43 (47,25%)**

Fonte: TCE-AM (2013).

Na mesma pesquisa, foram avaliados os órgãos que realizaram treinamento em segurança da informação. O resultado foi de apenas sete órgãos, o que equivale a 16,27% entre aqueles que declararam realizar a gestão da segurança da informação. Esse indicador pode traduzir um importante fator de risco, tendo em vista que a falta de capacitação dos servidores públicos na área de segurança pode resultar no tratamento inadequado dos riscos organizacionais, podendo comprometer, assim, os processos de trabalho, serviços e a qualidade da tomada de decisões por parte da alta administração.

Apesar dos resultados serem preocupantes, é possível perceber que já existe uma mobilização por parte dos órgãos de controle no sentido de avaliar, orientar e conduzir mudanças necessárias ao atual cenário do setor público em relação à gestão das informações organizacionais, demonstrando claramente a sua importância para a administração pública.

Estudo de caso da implantação da segurança da informação no Tribunal de Contas do Estado do Amazonas

O presente estudo de caso foi realizado no âmbito do Tribunal de Contas do Estado do Amazonas, a partir dos resultados das pesquisas estabelecidas pelo

TCU, das normativas da ABNT e das boas práticas de segurança já estabelecidas no setor privado. A partir desse referencial, consolidou-se a compreensão sobre a importância da implantação de práticas estruturadas de segurança para a gestão das informações organizacionais, bem como da necessidade de se estabelecer ações junto aos órgãos jurisdicionados do estado.

A primeira ação foi desenvolver a política de segurança da organização. De acordo com a NBR ISO/IEC 27001 (Associação Brasileira de Normas Técnicas, 2006), a política de segurança da informação (PSI) é o documento que contém as diretrizes da instituição quanto ao tratamento da segurança da informação. A sua formalização é considerada o primeiro passo para a implantação de um sistema de gestão da segurança da informação. A PSI tem o propósito de regular como deve ser gerenciada e protegida a informação e os recursos e usuários que com ela interagem durante todo o seu ciclo de vida, fornecendo orientação e apoio às ações de gestão de segurança.

O ponto de partida foi a realização de uma análise de ambiente, de forma a possibilitar a compreensão sistêmica do estado atual da organização em relação à segurança da informação. Para isso, foram aplicadas técnicas de entrevista junto aos gestores das áreas mais críticas envolvidas na gestão da informação, como, por exemplo, a área de tecnologia da informação, recursos humanos e segurança patrimonial. Essa fase considerou as premissas e abordagens descritas na Seção 2.

As entrevistas foram compostas de um conjunto de perguntas direcionadas de forma estratégica e indireta para os gestores e para mais dois servidores públicos de nível operacional de cada setor pertencente às áreas supracitadas. A técnica empregada seguiu um padrão semiestruturado, o que permitiu o acompanhamento das respostas, e, quando oportuno, eram efetuadas novas perguntas relacionadas, que não faziam parte da bateria inicial de questionamentos. Isso permitiu, conforme recomendam Hair e outros (2005), a descoberta de informações adicionais.

Basicamente, o questionário teve por finalidade obter as respostas para as seguintes questões básicas: **(i)** o que deve ser protegido; **(ii)** quais ameaças mais prováveis e quais deverão ser neutralizadas ou mitigadas; **(iii)** quais as principais vulnerabilidades; **(iv)** qual a probabilidade de ocorrência de um incidente de segurança (risco); **(v)** qual a importância de cada recurso; **(vi)** qual o grau de proteção desejado; **(vii)** quais os mecanismos de proteção existentes; **(viii)** quanto tempo, recursos humanos e financeiros são necessários para atingir os objetivos de segurança desejados; **(ix)** quais as expectativas dos usuários em relação à segurança das informações; **(x)** quais as consequências para a instituição se os recursos e sistemas forem paralisados parcial ou totalmente e as informações forem violadas ou roubadas.

Com base no cruzamento e avaliação das respostas e em uma análise de riscos preliminar estabelecida para o escopo definido pela equipe, foi possível identificar um baixo nível de maturidade em relação à adoção de práticas estruturadas de segurança da informação, o que motivou e norteou a implantação da segurança da informação no âmbito da organização.

A partir desse ponto foi realizado um estudo bibliográfico criterioso sobre a legislação vigente e normas de segurança da ABNT com o objetivo de produzir a política de segurança da informação da organização em consonância com as boas práticas e de forma alinhada aos objetivos da organização e prioridades identificadas na análise de riscos preliminar.

Após a avaliação de uma comissão de legislação e assessoria jurídica, a PSI proposta foi aprovada pela alta direção. Foram estabelecidos nesse documento os padrões, os controles, as responsabilidades e os critérios para o manuseio, armazenamento, transporte e descarte das informações, dentro do nível de segurança estabelecido para a organização. As dimensões tratadas pela PSI abrangeram os pontos de controle das normas de padronizações NBR ISO/IEC 27001 (Associação Brasileira de Normas Técnicas, 2006) e NBR ISO/IEC 27002 (Associação Brasileira de Normas Técnicas, 2005). A PSI da organização estabeleceu os seguintes objetivos:

- prover a orientação e apoio para a segurança da informação e ativos da organização, em conformidade com os requisitos do negócio, com a análise de riscos e com as leis, normas e regulamentações vigentes, de forma a assegurar a confidencialidade, integridade, disponibilidade, autenticidade e legalidade da informação;
- regular a classificação da informação e de áreas físicas que mereçam tratamento especial quanto ao sigilo e criticidade, com adoção de níveis adequados de proteção, sigilo e controle de acesso físico e lógico;
- 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 Federal;
- assegurar o acesso à informação, resguardado o sigilo da fonte, quando necessário ao exercício profissional, nos termos previstos na Constituição Federal;
- sistematizar e regular o uso adequado de mecanismos de segurança que inibam e previnam o acesso físico e lógico não autorizado, danos e interferências em instalações e informações;
- criar, desenvolver e manter, no âmbito da organização, a conscientização e a mentalidade de segurança da informação, bem como a importância das informações processadas e dos seus riscos e vulnerabilidades;

- alertar e conscientizar as organizações parceiras, prestadoras de serviços e jurisdicionados sobre a importância das informações processadas e sobre os seus riscos e vulnerabilidades;
- estabelecer responsabilidades do usuário sobre a informação da qual é detentor, sobre suas senhas e uso dos sistemas de computação e serviços de rede de computadores, extensivas aos prestadores de serviços, observados os termos contratuais;
- manter a segurança na divulgação e troca de informações por meios convencionais e eletrônicos, internamente à organização e com entidades externas, estabelecendo medidas preventivas, orientações e treinamentos, incluindo-se os aspectos relativos às ameaças da engenharia social;
- sistematizar processos e medidas que protejam os processos críticos e minimizem os impactos em casos de falhas ou desastres significativos, assegurando a sua retomada em tempo hábil.

O gerenciamento da segurança tem por objetivo manter os ativos da informação em nível de risco controlado. Para implantar a PSI e gerenciar a segurança no âmbito da organização, foi aprovada a formação de um comitê gestor de segurança da informação (CGSI), constituído por um presidente, que faz parte da alta direção; um coordenador, que faz parte do corpo técnico, com conhecimentos na área de segurança da informação; e por cinco membros, representantes das principais áreas definidas pelo comitê: **(i)** segurança em recursos humanos e sensibilização; **(ii)** segurança física e do meio ambiente; **(iii)** segurança tecnológica em infraestrutura de redes de computadores; **(iv)** segurança tecnológica em sistemas de banco de dados; e **(v)** segurança tecnológica em desenvolvimento de *software*.

O CGSI se compõe, ainda, como membros representativos, dos chefes de todas as unidades organizacionais, com o objetivo de fornecer o retorno das ações de segurança implantadas e propiciar um amplo debate sobre o tema em reuniões ordinárias.

A estratégia de implantação do projeto adotou a proposta de Sêmola (2003), em que a gestão da segurança da informação segue uma abordagem baseada em camadas. Dessa forma, o CGSI definiu três camadas: física, humana e tecnológica.

Camada física: são tratados todos os aspectos da segurança patrimonial e de ambientes de compartimentalização de ativos críticos que produzem, processam e armazenam informações sensíveis, como, por exemplo, as salas de telecomunicações e datacenter. As ações visam atender a teoria do perímetro, em que são estabelecidas segmentações de ambientes físicos com recursos, ferramentas e barreiras de proteção em níveis de controle de acesso classificados em três níveis de criticidade. Nessa camada, são tratados também controles de inteligência e contrainteligência, necessários à proteção do ambiente físico, no que tange ao aspecto de vazamento de informações por meio de recursos multimídia não autorizados.

Camada humana: nessa camada são estabelecidos e gerenciados controles diretamente voltados para os colaboradores da organização e prestadores de serviço. O objetivo é divulgar a PSI da organização e estabelecer uma cultura de boas práticas com ações e eventos de conscientização, educação e treinamento em segurança da informação. Nessa camada, são gerenciadas também as credenciais de acesso físico aos ambientes de proteção e acesso lógico aos recursos de tecnologia da informação (TI). Para ratificar o compromisso dos usuários com a PSI, foi estabelecida a assinatura de dois termos de compromisso: Termo de Uso dos Sistemas de Informações e Termo de Responsabilidade e Sigilo da Informação.

Camada tecnológica: nessa camada, são estabelecidos e gerenciados controles sobre todos os recursos de TI. Com a dependência cada vez maior desses ativos, essa camada passou a ser a mais crítica e a mais sensível para os processos de trabalho da organização e níveis de decisão. As ações nessa camada envolvem as três principais atividades da área de TI: infraestrutura de rede/ambiente computacional, sistemas de banco de dados e desenvolvimento e gerenciamento de *software*.

As atividades do CGSI nas diversas áreas têm como pré-requisito básico a realização de análise de riscos dos ativos. Isso se faz necessário para que todos os ativos considerados relevantes sejam identificados, mapeados e analisados. O escopo pode contemplar partes específicas ou um cenário complexo da organização.

Para simplificar essa atividade, de forma a gerar ações rápidas, é produzido um documento denominado Análise de Riscos Simplificada (ARS), com os pontos de checagem recomendados pela NBR ISO/IEC 27005 (Associação Brasileira de Normas Técnicas, 2008) e em consonância com os requisitos e práticas das normas NBR ISO/IEC 27001 (Associação Brasileira de Normas Técnicas, 2006) e NBR ISO/IEC 27002 (Associação Brasileira de Normas Técnicas, 2005). As ARSs são realizadas para ativos individualmente e posteriormente são consolidadas em um mapeamento de maior dimensão em que são analisadas as dependências entre os ativos e tratados os riscos de forma holística.

Considerando a complexidade na gestão da segurança, a implantação dos controles norteados na PSI é realizada de forma gradual, de acordo com a disponibilidade técnica, recursos humanos, tecnológicos e financeiros. As ações são priorizadas em virtude de seu grau de relevância, criticidade, impacto e em função da disponibilidade dos recursos envolvidos. A Tabela 3 apresenta o percentual de progresso da implantação de cada ponto geral de controle de segurança, correspondente às sessões da norma NBR ISO/IEC 27002 (Associação Brasileira de Normas Técnicas, 2005) e a situação da segurança da informação antes da aprovação da PSI e efetiva organização e ação do CGSI.

Cabe ressaltar que esses valores refletem apenas o percentual de ações necessárias que foram avaliadas e/ou executadas, sejam elas a validação de

controles já implantados, a implantação de novos controles ou a melhoria daqueles já existentes em cada ponto geral de controle, que integram um conjunto de pontos específicos de controles secundários.

Pode-se observar, na Tabela 3, que ainda existem muitos desafios a serem vencidos, entretanto, a organização tem avançado significativamente nessa área e se insere em uma posição diferenciada em relação à grande parte das organizações públicas avaliadas pelo TCU, visto o baixo percentual de órgãos que efetivamente implantaram controles de segurança da informação.

A Tabela 3 apresenta o percentual de ações realizadas pelo CGSI e a situação da segurança antes da aprovação da PSI. Os processos existentes que apresentaram inconformidades importantes em relação aos pontos de controle especificados na norma ABNT NBR ISO/IEC 27002:2005 (Associação Brasileira de Normas Técnicas, 2005) foram definidos na Tabela 3 como "deficiente". Após a implantação da segurança da informação, esses processos passaram a ser tratados e/ou aperfeiçoados.

Tabela 3 – Implantação da segurança da informação no TCE-AM

Pontos gerais de controle (Sessões da ABNT NBR ISO/IEC 27002:2005)	Implantação da segurança da informação		
	Situação antes da aprovação da PSI	Situação após a aprovação da PSI	
	(Abril/2011)	(Abril/2014)	Progresso
Política de segurança da informação	Inexistente	Implantado	99%
Organização da segurança da informação	Inexistente	Implantado	99%
Processo de admissão e desligamento de pessoal	Deficiente	Implantado	80%
Controle de acesso a sistemas e serviços de rede	Deficiente	Implantado	80%
Conscientização, educação e treinamento em S.I	Inexistente	Implantado	70%
Segurança física e do meio ambiente	Deficiente	Implantado	50%
Segurança de mídias e do meio ambiente	Deficiente	Implantado	50%
Gerenciamento das operações, com. e suporte	Deficiente	Implantado	50%
Gestão e segurança dos ativos tecnológicos	Deficiente	Implantado	40%
Segurança arquivos sist. e proc. desenv. e suporte	Deficiente	Implantado	40%
Gestão da continuidade dos negócios	Inexistente	Implantado	40%
Gestão de incidentes de segurança da informação	Inexistente	Implantado	40%
Gestão e análise de riscos	Inexistente	Implantado	40%
Classificação da informação	Inexistente	Implantado	30%
Segurança na tramitação da informação	Inexistente	Implantado	30%
Gestão de contratos	Deficiente	Implantado	30%
Auditoria interna em segurança da informação	Inexistente	Inexistente	0%

Fonte: Elaboração própria.

Resultados parciais da implantação da segurança da informação no TCE-AM

Apesar da gestão da segurança da informação estar em fase de implantação, já se podem perceber os resultados parciais com as ações implantadas até o momento. A análise foi baseada sob o aspecto qualitativo. Dentre elas destacam-se:

Valorização da imagem da organização: a aprovação da Política de Segurança da Informação aumentou a visibilidade e credibilidade junto à sociedade e aos outros órgãos públicos de controle, no que tange à segurança. A adoção da PSI organizacional foi destacada em um portal nacional dos tribunais de contas estaduais e em um programa de entrevista de grande popularidade na TV aberta do Estado do Amazonas. Além disso, o órgão recebeu o contato e registrou visitas técnicas de outros órgãos públicos interessados na adoção e implantação da PSI.

Mudança de comportamento do usuário: já se percebe uma mudança significativa na postura e nas ações proativas de segurança do usuário. As orientações e monitoramento do CGSI, divulgados em palestras e difundidos por mensagens na intranet da organização, além da assinatura dos termos de compromisso do usuário com a PSI da organização reafirmaram a sua conduta responsável no uso dos sistemas e sigilo da informação.

Implantação ou melhoria de controles de segurança: as ações de análise de riscos e a implantação de controles têm permitido aumentar o nível de segurança nas camadas física, humana e tecnológica, garantindo processos de trabalho mais seguros e eficientes. O CGSI, por exemplo, executa periodicamente a análise de riscos, testes de penetração e ações corretivas em recursos da rede local, sistemas corporativos e portais eletrônicos, de forma a mitigar as principais ameaças de ataques cibernéticos.

Prevenção contra paralisações ou interrupções de serviço: a implantação de controles de contingência, *backup* e ações preventivas de segurança tem promovido a redução no tempo de paralisações de serviços essenciais, como, por exemplo, a contratação de *links* de *internet* com rotas de saída/entrada contingenciadas, aquisição de sistemas de suprimento de energia adicionais, implantação de planos de manutenção preventiva para equipamentos críticos, implantação de planos de recuperação etc.

Considerações finais

A globalização aumentou o grau de incertezas e riscos para todas as organizações. Nesse contexto, a informação correta, de qualidade e em momento oportuno passou a ser essencial no processo decisório e sobrevivência das instituições.

Para garantir maior eficiência nesse processo, as empresas tornaram-se mais dependentes da informação e dos recursos que a manipulam. Esses ativos se transformaram em elementos praticamente inseparáveis das atividades estratégicas, gerenciais e produtivas da organização, passando a constituir um dos principais pontos de investimentos e modernização das organizações contemporâneas. Contudo, o ambiente corporativo e a gestão da informação se tornaram altamente complexos e as instituições passaram a ficar expostas a uma gama maior de riscos.

Dessa forma, as práticas de segurança da informação passaram a ocupar uma posição estratégica na gestão da informação e na garantia da continuidade dos processos de trabalho e serviços mantidos e fornecidos em diversos ativos capazes de produzir, processar e manter a informação, de forma a garantir a sua disponibilidade em momento oportuno para que o gestor possa tomar a decisão adequada.

Entretanto, as pesquisas demonstram que, no âmbito da administração pública, o setor ainda apresenta um baixo nível de maturidade em relação à implantação da segurança da informação. A partir dessa análise, consolidou-se a compreensão sobre a importância estratégica de se estabelecer práticas estruturadas de segurança para a gestão da informação organizacional no âmbito do órgão público amazonense e a sua implantação efetiva.

Este trabalho destaca a importância da segurança na gestão da informação e apresenta um estudo de caso que reflete as ações do órgão amazonense na área de segurança da informação. Verifica-se, em pequeno prazo, que os resultados parciais são positivos e convergem para a diminuição de custos, fortalecimento dos controles internos, valorização da imagem organizacional e para o cumprimento das metas estratégicas em uma melhor relação custo-benefício.

Além disso, esses resultados permitiram fortalecer uma visão moderna que almeja uma melhor qualidade no atendimento à sociedade, não só por parte do órgão, mas também por seus jurisdicionados. Dessa forma, seguindo a mesma abordagem do TCU, o TCE-AM realizou uma pesquisa regional pioneira, acerca da governança de TI, para avaliar o estado atual da administração pública estadual amazonense.

Sob o aspecto concernente à gestão da segurança da informação, os resultados demonstram a mesma deficiência detectada na administração pública federal, o que aponta para a necessidade de atuação do órgão em ações de auditoria nessa área, visando à melhoria ou à implantação de boas práticas de segurança da informação junto aos demais órgãos jurisdicionados.

Por fim, o estudo revela a importância da implantação da segurança na gestão da informação no setor público, representando, dessa forma, uma vertente importante de mobilização que deve ser conduzida e difundida para o aprimoramento da gestão pública.

Referências bibliográficas

Associação Brasileira de Normas Técnicas (ABNT). *ABNT NBR ISO/IEC27002. Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação*. Rio de Janeiro: ABNT, 2005.

Associação Brasileira de Normas Técnicas (ABNT). *ABNT NBR ISO/IEC27001. Tecnologia da Informação - Técnicas de Segurança - Sistemas de Gestão de Segurança da Informação – Requisitos*. Rio de Janeiro: ABNT, 2006.

Associação Brasileira de Normas Técnicas (ABNT). *ABNT NBRISO/IEC27005. Tecnologia da Informação - Técnicas de segurança - Gestão de riscos de segurança da informação*. Rio de Janeiro: ABNT, 2008.

Associação Nacional de Pós-Graduação e Pesquisa em Administração (Anpad). *Boas Práticas da Publicação Científica:* um manual para autores, revisores, editores e integrantes de Corpos Editoriais. Rio de Janeiro: Anpad, 2010. Disponível em: http://www.anpad.org.br/diversos/boas_praticas.pdf. Acessado em 25 de março de 2013.

Araújo, Luis; Easton, Geoff. Strategy: where is the pattern*? Sage Publication*, California, v. 3, n. 3, p. 361-383, 1996.

Beal, Adriana. *Segurança da informação:* princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2005.

Gimenez, Fernando A. P.; Pelisson, C.; Krüger, E. G. S.; Hayashi, Paulo. Estratégia em pequenas empresas*:* uma aplicação do modelo de Miles e Snow*. Revista de Administração contemporânea,* Curitiba, v. 2, n. 3, p. 53-74, 1999.

Hair, Joseph F.; Babin, Berry; Money, Arthur; Samouel, Philip. *Fundamentos de métodos de pesquisa em Administração*. Porto Alegre: Bookman, 2005.

Kodama, Fumio. *Emerging patterns of innovation:* sources of Japan's technological edge*.* Boston: Harvard Business School Press, 1994.

Laureano, Marcos A. P.; Moraes, Paulo. E. S. Segurança como estratégia de gestão da informação. *Revista Economia & Tecnologia*, Curitiba, v. 8, n. 3, p. 38-44, 2005. ISSN 1415-451X.

Nobre, Anna C. S; Ramos, A. S. M; Nascimento, T. C. *Fatores que influenciam a aceitação de práticas avançadas de gestão de segurança da informação:* um estudo com gestores públicos estaduais no Brasil*.* Rio de Janeiro: XXXIV Anpad, 2010.

Ramos, Anderson. *Security Officer:* guia oficial para formação de gestores em segurança da informação*.* Porto Alegre: Zouk, 2006.

Sacconi, Luis A. *Dicionário da língua portuguesa*. São Paulo: Atual, 2010.

Sêmola, Marcos. *Gestão da segurança da informação:* visão executiva da segurança da informação aplicada ao Security Officer*.* São Paulo: Campus, 2003.

Sianes, Marta. Gestão estratégica da informação e inteligência competitiva. São Paulo: Saraiva, 2005.

Tribunal de Contas do Estado do Amazonas (TCE-AM). *Levantamento da governança de tecnologia da informação na administração pública no Estado do*

Amazonas. Manaus: Diretoria de Controle Externo de Tecnologia da Informação – DIATI/Tribunal de Contas do Estado do Amazonas, 2013.

Tribunal de Contas da União (TCU). *Levantamento da governança de tecnologia da informação na administração pública* federal. Sumário Executivo. Brasília: TCU, 2010.

Angelo Eduardo Nunan

Diretor de Controle Externo de Tecnologia da Informação e Coordenador do Comitê Gestor de Segurança da Informação do Tribunal de Contas do Estado do Amazonas. Mestre em Ciência da Computação pela Universidade Federal do Amazonas e especialista em Gestão Pública pela Universidade do Estado do Amazonas.
Contato: eduardonunan@gmail.com

Mário José de Moraes Costa Filho

Auditor de Contas Públicas Estadual do Tribunal de Contas do Estado do Amazonas. Bacharel em Direito e em Processamento de Dados pela Universidade Federal do Amazonas.
Contato: mario.filho@tce.am.gov.br

Adriana Almeida Lima

Mestre em Direito Ambiental pela Universidade do estado do Amazonas (UEA), advogada e professora da Universidade do Estado do Amazonas (UEA).
Contato: a.almeida.lima@uol.com.br

RSP