GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO NO TRIBUNAL DE CONTAS DA UNIÃO - TCU[1]

Rafael Cancellier[2]

Resumo: Este artigo examina o processo de Gestão de Riscos de Segurança da Informação no âmbito do Tribunal de Contas da União (TCU). O objetivo principal é identificar de que forma esse processo foi implementado no TCU e se está aderente às normas nacionais e internacionais. A pesquisa, de caráter documental, amparou-se nos normativos internos editados pelo Tribunal para regulamentar seu Sistema de Gestão de Segurança da Informação (SGSI/TCU), nas normas internacionais ISO da família 27000 e nas normas editadas pelo Departamento de Segurança da Informação e Comunicações (DSIC) da Casa Militar da Presidência da República. Foi abordada, subsidiariamente, a metodologia prática adotada para a Gestão de Riscos de Segurança da Informação.

Palavras-chave: Segurança da Informação. Gestão de Riscos. Gestão de Riscos de Segurança da Informação. Tribunal de Contas da União (TCU).

[1] Artigo apresentado para conclusão do curso de pós-graduação em Gestão de Segurança da Informação da Universidade do Sul de Santa Catarina - Unisul, campus Unisul Virtual.

[2] Auditor Federal de Controle Externo do Tribunal de Contas da União. Contato: rafaelrc@tcu.gov.br.

1. INTRODUÇÃO

A administração pública tem como objetivo final prover serviços e bem-estar aos cidadãos, como educação, saúde, segurança e previdência, por meio de suas políticas públicas. Para que tais serviços sejam providos, a administração precisa conhecer quem são seus cidadãos, quais são seus problemas, qual é o orçamento disponível para aplicação nessas políticas, etc. Dessa forma, é razoável afirmar que a matéria prima da administração pública é a informação.

No caso do Tribunal de Contas da União (TCU), tal fato é evidente. O Tribunal não presta nenhum serviço físico ao cidadão, como emergência hospitalar ou policiamento comunitário. O produto do trabalho do TCU é informação. Informação sobre o andamento da gestão pública, sobre os gastos orçamentários e sobre a efetividade das políticas públicas implementadas pelo governo federal.

Nesse contexto, infere-se que proteger as informações das ameaças contra sua integridade, disponibilidade e confidencialidade é essencial para o trabalho do Tribunal. Esse processo de proteção é entendido como Segurança da Informação.

Assim, a segurança da informação visa preservar ativos de informação, levando em conta três objetivos fundamentais citados: confidencialidade (garantia de que o acesso à informação é restrito aos seus usuários legítimos); integridade (garantia da criação legítima e da consistência da informação ao longo do seu ciclo de vida: em especial, prevenção contra criação, alteração ou destruição não autorizada de dados e informações); e disponibilidade (garantia de que a informação e os ativos associados estejam disponíveis para os usuários legítimos de forma oportuna) (BEAL, 2005).

Para que a informação esteja efetivamente sob controle é importante conhecer quais de suas propriedades devem ser preservadas e protegidas e qual é seu ciclo de vida (SÊMOLA, 2014). Com o domínio desse conhecimento é possível definir o tratamento a ser dado à informação com base em critérios para aceitação de riscos compatíveis com os objetivos institucionais.

Conforma afirma Marcos Sêmola, é fundamental que todos tenhamos a consciência de que não existe segurança total, logo não há um nível definido de risco igual para todas as instituições (SÊMOLA, 2014). Assim, sempre será necessário avaliar o nível de segurança apropriado para cada momento vivido pela instituição e efetuar a adequada gestão dos riscos.

Especificamente em relação ao Tribunal de Contas da União, o processo de gestão de riscos de segurança da Informação encontra-se previsto na Política Corporativa de Segurança

da Informação do Tribunal (PCSI/TCU), consignada pela Portaria-TCU 210/2014. Esse normativo dispõe, em seu artigo 4º, que o Sistema de Gestão de Segurança da Informação do TCU (SGSI/TCU) é composto por seis processos, entre eles a gestão de riscos de segurança da informação.

O artigo teve como objetivo identificar de que forma foi implementado esse processo internamente ao TCU. A metodologia utilizada foi a pesquisa aplicada teórica, sem coleta de dados ou pesquisa de campo.

Os instrumentos utilizados foram as normas internacionais ISO27000, os normativos editados pelo Departamento de Segurança da Informação e Comunicações (DSIC) da Casa Militar da Presidência da República e pelo TCU, bem como a literatura existente no mercado nacional que trata de gestão de segurança da informação.

Foram também estudadas as análises de riscos de segurança da informação já efetuadas pela Diretoria de Segurança da Informação e Continuidade de Negócio do Tribunal, de forma a levantar o que já foi feito na prática.

Complementarmente, foi verificado o alinhamento do processo de gestão de riscos de segurança da informação já implantado no TCU com o disposto nos normativos supracitados.

2. A SEGURANÇA DA INFORMAÇÃO E A GESTÃO DE RISCOS

Conforme apresentado inicialmente, a informação é matéria-prima de grande parte das empresas e instituições atuais. Mesmo aquelas que não tem como objetivo finalístico a geração de novas informações, como por exemplo as indústrias ou as produtoras rurais, utilizam informações cotidianamente no gerenciamento dos processos ligados às suas atividades fim. Nesse ambiente, permeado pela circulação de informações, é essencial garantir sua confidencialidade, integridade e disponibilidade.

Complementarmente à utilização interna da informação, vivemos hoje em uma sociedade inserida em um mundo conectado à internet, que possibilitou a comunicação rápida e direta de dados, mas também aumentou a probabilidade de comprometimento da qualidade da informação.

Com a sociedade cada vez mais interligada, configura-se um cenário de alta complexidade e custo de proteção dos ativos de informação. Assim, de forma a proteger a informação em todo seu ciclo de vida, é de extrema importância para o alcance dos objetivos de segurança adotar um enfoque de gestão baseado nos riscos específicos de cada negócio. (BEAL, 2005).

Para Augusto Paes de Barros (CAPRINO, CABRAL, 2015), a gestão de risco é o objetivo máximo da segurança da informação, pois aplicamos medidas de segurança para evitar perdas, sejam elas relacionadas à confidencialidade, integridade ou disponibilidade. Como são eventos futuros, é necessário entender a chance e a dimensão de tais perdas. Em outras palavras, o risco.

Para o autor supracitado, gestão de risco é o processo por meio do qual tentamos conhecer os riscos aos quais estamos expostos e então decidir o que faremos com relação a eles. É possível tomar medidas para eliminá-los, reduzi-los ou até mesmo decidir aceita-los como parte de nossas atividades. A gestão de risco de segurança da informação visa aplicar técnicas para manter o risco ao qual a informação é exposta em um nível adequado, definido pela alta gestão.

3. A GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO NAS NORMAS ISO

A importância da gestão de riscos para a garantia da segurança da informação também se encontra disposta na família de normas ISO27000 que define os requisitos para um sistema de gestão de segurança da informação. Tais normas são publicadas pela International Organization for Standardization (ISO). Para a ISO, o núcleo do Sistema de Gestão de Segurança da Informação (SGSI) é um processo contínuo de gestão de risco, onde o ciclo PDCA (Plan Do Check Act) define fases de planejamento, execução, verificação e melhoria contínua (ABNT, ISO27001, 2006).

De forma resumida, a ISO/IEC 27001 define gestão de riscos como o conjunto de atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos. Geralmente inclui a análise/avaliação de riscos, o tratamento de riscos, a aceitação de riscos e a comunicação de riscos (ABNT, ISO27001, 2006).

A mesma norma dispõe que após definir uma política do SGSI é necessário, para o estabelecimento do Sistema: definir a abordagem de análise/avaliação de riscos da organização; identificar os riscos; analisar e avaliar os riscos; identificar e avaliar as opções para o tratamento de riscos e selecionar objetivos de controle e controles para o tratamento de riscos. Dessa forma, o processo de gestão de riscos de segurança da informação é essencial para a definição e planejamento do SGSI (ABNT, ISO27001, 2006).

Já a norma ISO/IEC 27005 fornece diretrizes e descreve um processo genérico para a gestão de riscos de segurança da informação de uma organização. O processo pode ser utilizado

tanto para o ciclo de melhoria contínua PDCA quanto de forma independente, como avaliações de risco em um projeto.

De acordo com essa norma ISO, o processo de gestão de risco começa com a definição do contexto. Em seguida é feita a análise/avaliação de riscos, em que os riscos são identificados, estimados e avaliados segundo critérios definidos no momento do estabelecimento do contexto. Ao final dessa fase, é realizada uma verificação para avaliar se a fase foi satisfatória ou não – caso não seja, o processo é repetido. Se a avaliação for considerada satisfatória passa-se ao tratamento do risco, etapa onde os riscos podem ser reduzidos, retidos, evitados ou transferidos (ABNT, ISO27005, 2008).

Após a etapa de tratamento dos riscos, é realizada a etapa de aceitação dos riscos residuais, que não serão tratados. A aceitação deve ser formalizada por autoridade competente da gestão da organização. Complementarmente, é essencial comunicar adequadamente o risco residual para a alta direção, de modo a garantir que este seja compreendido e aceito pelos responsáveis globais pela organização, ou, em caso de não-aceitação, para permitir que controles adicionais sejam escolhidos para diminuir o nível do risco remanescente (BEAL, 2005).

Por fim, de forma a garantir que os controles sejam implementados e os riscos mitigados, é necessário monitorar a execução do plano de tratamento de riscos.

Para a norma ISO/IEC 27005, o processo de gestão de riscos de segurança da informação, uma vez implementado, contribui para: identificação de riscos; análise e avaliação de riscos em função das consequências ao negócio e da probabilidade de sua ocorrência; comunicação e entendimento da probabilidade e das consequências destes riscos; estabelecimento da ordem prioritária para tratamento do risco; priorização das ações para reduzir a ocorrência dos riscos; envolvimento das partes interessadas quando as decisões de gestão de riscos são tomadas e mantidas informadas sobre a situação da gestão de riscos; eficácia do monitoramento do tratamento do risco; monitoramento e a análise crítica regular de riscos e do processo de gestão dos mesmos; coleta de informações de forma a melhorar a abordagem da gestão de riscos; e treinamento de gestores e pessoal a respeito dos riscos e das ações para mitiga-los.

4. A GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO NA ADMINISTRAÇÃO PÚBLICA

No âmbito da Administração Pública Federal (APF), o responsável por coordenar as atividades de segurança da informação é a Casa Militar da Presidência da República. Para essa

tarefa, conta com um Departamento exclusivo para orientar a implementação de ações de segurança da informação e definir normativos e requisitos metodológicos para essas ações, chamado Departamento de Segurança da Informação e Comunicações (DSIC).

Complementarmente ao DSIC, o governo federal também dispõe da Secretaria de Tecnologia da Informação (STI), vinculada ao Ministério do Planejamento, Desenvolvimento e Gestão. A STI é o órgão central do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) da Administração Pública Federal. É sua responsabilidade propor políticas e também planejar, coordenar e orientar normativamente as atividades de gestão dos recursos de TI, governo digital e segurança da informação no âmbito do sistema.

A Norma Complementar 02/IN01/DSIC/GSIPR, editada pelo DSIC, dispõe sobre a metodologia de gestão de segurança da informação a ser utilizada pelos órgãos da APF e baseia-se no ciclo PDCA (Plan-Do-Check-Act), referenciado pela ISO/IEC 27001. Dentro da fase de Planejamento (plan), deve ser definida uma metodologia de gestão de riscos que seja adequada ao escopo, limites e objetivos do órgão. Também nessa etapa devem ser definidos os riscos aceitáveis e os critérios para sua aceitação, considerando decisões superiores e o planejamento estratégico do órgão ou unidade (BRASIL, 2008).

Ainda na etapa de planejamento, conforme o normativo acima citado, deve-se identificar e analisar os riscos de segurança da informação, bem como as opções para o tratamento desses riscos (mitigá-los, evita-los, transferi-los ou aceita-los). Com essas informações definidas é necessário obter a ratificação da alta gestão (BRASIL, 2008).

As etapas de Do, Check e Act seguem o modelo previsto pela norma ISO/IEC 27001.

Adicionalmente, a Norma Complementar 04/IN01/DSIC/GSI/PR estabelece diretrizes para o processo de gestão de riscos de segurança da informação nos órgãos da Administração Pública Federal. Já em seu início, no item 2.2, ressalta a importância de que a gestão de riscos de segurança da informação esteja alinhada ao planejamento estratégico da organização. Ressalta também, como diretriz em seu item 5.2, que esse processo deve ser contínuo e aplicado na implementação e operação da Gestão de Segurança da Informação (BRASIL, 2013).

Para o DSIC, o processo de gestão de riscos de segurança da informação é composto pelas etapas de definições preliminares, análise/avaliação dos riscos, plano de tratamento dos riscos, aceitação dos riscos, implementação do plano de tratamento dos riscos, monitoração e análise crítica, melhoria do processo de gestão de riscos de segurança da informação e comunicação do risco. Nota-se que o processo proposto pelo DSIC é muito próximo ao proposto pela ISO/IEC 27005, já exposto anteriormente.

A STI, por sua vez, elaborou um manual compreensivo contendo uma Metodologia de Gestão de Riscos de Segurança da Informação, por meio de sua Fundação de Apoio à Capacitação em Tecnologia da Informação (Facti). A metodologia, em resumo, compreende os subprocessos: Estabelecer Contexto, Identificar Riscos, Estimar Riscos, Avaliar Riscos, Tratar Riscos, Comunicar Riscos e Monitorar Riscos (BRASIL, 2015).

A metodologia desenvolvida pela STI é mais detalhada que a do DSIC e demonstra como podem ser calculados quantitativamente os impactos dos riscos encontrados na análise de risco bem como o custo de implementação de cada controle.

5. A GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO NO TCU

5.1 NORMATIZAÇÃO

O Sistema de Gestão Segurança da Informação do TCU (SGSI/TCU) está contido em um Sistema de Gestão de Segurança Institucional que contempla, além do SGSI, o Sistema de Gestão de Segurança Física e Patrimonial do TCU (SGSF/TCU).

A Política de Segurança Institucional do TCU (PSI/TCU), que define o modelo de sistema acima citado, está disposta na Resolução-TCU 261/2014. Esse normativo dispõe que as dimensões da segurança institucional são: a segurança física e patrimonial; a segurança da informação; a continuidade de negócios; a segurança do trabalho e a gestão de riscos à segurança institucional (BRASIL, 2014). Ressalte-se que toda Resolução TCU deve ser aprovada pelo Plenário do Tribunal, garantido, dessa forma, pleno amparo do *board* da alta gestão a esses normativos.

Apesar da PSI/TCU ter sido editada no ano de 2014, até o momento não há norma que disponha sobre a gestão de riscos de segurança institucional, ou seja, contemplando de forma integrada os riscos de segurança da informação e segurança física e patrimonial.

Complementarmente, a PSI/TCU estabelece diretrizes para a edição da Política Corporativa de Segurança da Informação, e define que o SGSI/TCU é composto pelos processos de: classificação da informação; gestão de riscos de segurança da informação; gestão de incidentes em segurança da informação; controle de acesso à informação; segurança da informação em recursos humanos e conscientização em segurança da informação; e segurança em tecnologia da informação e comunicações (BRASIL, 2014).

Com base, portanto, nas diretrizes acima apresentadas, foi editada a Política Corporativa de Segurança da Informação do TCU (PCSI/TCU) e criado o Sistema de Gestão de Segurança da Informação do TCU (SGSI/TCU), consignados na Portaria-TCU 210/2014.

No Tribunal, as Portarias são editadas por seu Presidente, o que proporciona participação da alta gestão também nesses normativos, assim como as já citadas Resoluções.

A PCSI/TCU define com mais detalhes os processos do SGSI/TCU. Especificamente em relação à gestão de riscos de segurança da informação, a Portaria dispõe, em seu artigo 6º, que a gestão de riscos de segurança da informação tem por objetivo identificar os riscos que possam comprometer a confidencialidade, a integridade, a disponibilidade ou a autenticidade da informação, priorizando seu tratamento com base em critérios para aceitação de riscos compatíveis com os objetivos institucionais (BRASIL, 2014).

Observa-se que no TCU o tratamento dos riscos de segurança da informação deve ser priorizado conforme o nível de risco aceitável para os objetivos definidos pela alta gestão. Tal entendimento se coaduna com o disposto na Norma Complementar 02/IN01/DSIC/GSIPR que dispõe que no planejamento da gestão de riscos de segurança da informação sejam definidos os riscos aceitáveis e os critérios para sua aceitação, considerando decisões superiores e o planejamento estratégico do órgão ou unidade.

Apesar disso, em seu artigo 13, a PCSI/TCU determina que a definição de requisitos de segurança da informação necessários ao negócio é de responsabilidade do gestor da informação, devendo este basear-se em critérios de aceitação e tratamento de riscos inerentes aos processos de trabalho. O gestor da informação, para os fins previstos nesse normativo, corresponde a colegiado do TCU ou de sua Secretaria, autoridade do Tribunal ou dirigente de unidade responsável por informação em matéria de sua competência ou inerente a sua área de atuação (BRASIL, 2014).

Dessa forma, apesar do nível de risco aceitável ter que ser definido pela alta gestão, os requisitos de segurança da informação dos processos de trabalho do Tribunal serão definidos pelos gestores da informação. Observe-se que, no Tribunal, nem todos os gestores da informação são da alta administração (colegiados, autoridades ou secretários-gerais). É possível encontrar gestores da informação que são apenas os responsáveis técnicos por determinada base de dados ou conjunto de informações, estando longe, hierarquicamente, do Presidente ou do Plenário do Tribunal.

O impacto de tal modelo de gerenciamento de riscos se mostra no momento em que é necessário decidir se o risco deve ser tratado ou aceito, por exemplo. Cabe, conforme esse modelo, ao gestor da informação aceitar ou tratar determinado risco.

Outro normativo relevante para a gestão de riscos de segurança da informação no Tribunal é a Portaria-TCU 77/2015, que dispõe sobre o funcionamento do Comitê de Segurança Institucional (Cosin). O Comitê é órgão colegiado de natureza consultiva e caráter permanente

e tem por finalidade formular e conduzir diretrizes para o Sistema de Gestão de Segurança Institucional (SGSIN/TCU) e a Política de Segurança Institucional do TCU (PSI/TCU), analisar periodicamente sua efetividade, propor normas e mecanismos institucionais para melhoria contínua, bem como assessorar, em matérias correlatas, a Comissão de Coordenação Geral (CCG) e a Presidência do Tribunal (BRASIL, 2015).

A coordenação do Cosin observa rodízio anual entre o titular da Secretaria de Segurança e Serviços de Apoio (Sesap) e o da Secretaria de Planejamento, Governança e Gestão (Seplan) – esta última, responsável pela área de segurança da informação.

Nota-se que o Tribunal não possui um Comitê de Segurança da Informação, cabendo ao Cosin tratar desse assunto (considerando que a Política de Segurança da Informação está contida na Política de Segurança Institucional). A vantagem do modelo é a possibilidade de alinhamento entre as ações de segurança da informação e segurança física e patrimonial. A desvantagem é a disputa de espaço entre os assuntos.

Em resumo, essas são as normas que regem o processo de gestão de segurança da informação no TCU. Pelo exposto nota-se que a metodologia a ser utilizada não se encontra normatizada, cabendo ao setor responsável pela gestão do SGSI/TCU sua escolha.

Observa-se também a ausência de uma norma específica para a gestão de riscos em segurança da informação. Tal ausência é relevante pois ao servidor público só cabe agir dentro da disposição legal-normativa. Sem uma norma específica dispondo sobre o processo de gestão de riscos e definindo sua periodicidade, responsáveis, e, principalmente, a garantia de que seja cíclico e contínuo, sua implantação fica dependente da boa vontade e negociação política da administração.

5.2 ESTRUTURA ORGANIZACIONAL DA SEGURANÇA DA INFORMAÇÃO NO TCU

O Sistema de Gestão de Segurança da Informação do TCU é gerenciado e monitorado pela Diretoria de Segurança da Informação e Continuidade de Negócios (Disic), que faz parte da Secretaria de Planejamento, Governança e Gestão (Seplan), que por sua vez integra a Secretaria-Geral da Presidência (Segepres). Mais especificamente, o processo de gestão de riscos de segurança da informação é de responsabilidade dessa Diretoria.

A disposição organizacional da Disic permite que seu trabalho técnico sofra menos influência política, por estar no terceiro escalão hierárquico, mas dificulta que as demandas mais estratégicas (oriundas dos usuários dos sistemas de informação ou da própria Disic) alcancem de forma plena a alta gestão.

Complementarmente à essa Diretoria, a segurança da informação também é escopo do Serviço de Segurança em TI (Sesti). O Sesti é responsável pelo processo de segurança da informação em TI e comunicações, ou seja, pela definição e operação de ferramentas técnicas como antivírus, firewall, segurança na rede interna, AntiSpam e assim por diante. O Sesti integra a Secretaria de Infraestrutura de TI e não é subordinado à Disic. Apesar disso, as interações entre eles são constantes, sendo comum que trabalhos sejam realizados em conjunto, como a investigação de incidentes em segurança da informação ou a definição de normativos afetos à área.

5.3 METODOLOGIA DA GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

O processo de gestão de riscos de segurança da informação é de responsabilidade da Diretoria de Segurança da Informação e Continuidade de Negócios (Disic), conforme visto no item anterior. Também conforme exposto acima, não há no TCU definição normativa da metodologia a ser utilizada para esse processo. Dessa forma, coube à Disic não apenas implementá-la, mas também defini-la.

Ao escolher a metodologia a ser utilizada para a gestão de riscos de segurança da informação no TCU, a Disic considerou os seguintes critérios:

a) Vinculação da gestão de riscos de segurança da informação com a gestão de riscos corporativa: no caso do TCU ainda não há um processo formal de gestão de riscos corporativa, logo a metodologia a ser escolhida não depende de outras instâncias administrativas;

b) Definição do nível aceitável de risco pela alta gestão: a ausência de uma política de gestão de riscos corporativos implica em que não haja definição clara do nível de risco aceitável pela alta gestão. No caso específico do TCU, o nível de risco é definido pelos dirigentes de cada área técnica, obrigando a metodologia a ser flexível o suficiente para atender níveis diversos de tolerância ao risco;

c) Complexidade da metodologia em relação ao tamanho da equipe responsável: a Disic contava, à época da definição do processo, com 8 servidores da carreira de Auditoria do TCU para gerenciar todo o SGSI/TCU. Dessa forma, a metodologia de gestão de riscos não pode ser muito complexa de forma a não drenar em demasiado os parcos recursos humanos à disposição do setor;

d) Tempo de execução do processo de gestão de riscos bem como das análises de risco: é natural que todo setor que se empenhe em rever seus processos de trabalho de forma a melhorar sua gestão de riscos de segurança da informação espere resultados em curto prazo sem

comprometer toda sua equipe para essa atividade. Não é razoável esperar que um setor inteiro pare por semanas para realizar uma análise de risco em segurança da informação ou que o processo de gestão de riscos burocratize demais a rotina cotidiana. Dessa forma, a metodologia a ser adotada deve oferecer resultados práticos em um curto espaço de tempo, de forma a manter o comprometimento com o processo por parte do dirigente.

e) Custo do processo: a necessidade de contratação de consultorias ou mão-de-obra externas ao órgão pode inviabilizar o processo de gestão de riscos de segurança da informação, tornando-o caro demais.

Considerando os critérios acima citados, a metodologia escolhida foi a baseada no método FRAAP (*Facilitated Risk Analysis and Assessment Process* – Processo Facilitado de Análise e Avaliação de Risco). Esse modelo permite a utilização de mão-de-obra interna na gestão do processo e possibilita que uma análise de riscos em segurança da informação em determinado setor ou processo de trabalho seja realizada em questão de dias. Para Peltier, o desenvolvedor do método, esses fatores acarretam custo baixo e benefício alto, e aumentam o nível de aceitação por parte do resto da organização por não depender de uma consultoria externa e seus procedimentos genéricos (PELTIER, 2005).

Complementarmente, na ausência de uma definição corporativa de tolerância ao risco, o método FRAAP permite que, ao final de uma análise de riscos e com o Plano de Tratamento de Riscos (PTR) em mãos, o próprio gestor do setor ou do processo de trabalho defina quais riscos serão tratados e quais serão aceitos, aumentando o comprometimento dos envolvidos com a execução do Plano.

O método FRAAP é um método que envolve analisar um sistema, aplicação ou segmento de negócio por vez. Durante o trabalho, congrega no mesmo ambiente os gestores, que conhecem as necessidades gerenciais do negócio, e a equipe técnica, que está familiarizada com as potenciais vulnerabilidades dos processos de trabalho e possíveis controles para sua mitigação (PELTIER, 2000).

O modelo compreende reuniões que seguem uma organização pré-definida pela Disic e pelo gestor da área/processo de trabalho. Um membro da Disic permanece no apoio para garantir que os membros participantes se comuniquem efetivamente e mantenham aderência à agenda proposta.

Durante as reuniões, a equipe realiza sessões de *brainstorming* para identificar ameaças potenciais e vulnerabilidades no processo de trabalho em análise, e seus impactos negativos na confidencialidade, integridade e disponibilidade da informação. Em seguida, a

equipe analisa os efeitos desses impactos nas operações do negócio e realiza uma primeira classificação geral dos riscos por ordem de prioridade de tratamento.

Não são realizadas estimativas quantitativas de prejuízo estimado ou probabilidade de ocorrência das ameaças. As definições são amparadas com base no conhecimento geral da equipe das ameaças potenciais e vulnerabilidades, bem como em sua experiência de trabalho (PELTIER, 2000).

Após a identificação e categorização dos riscos, são discutidos possíveis controles que podem ser implementados para reduzi-los, com foco nos que possuam maior relação custo-benefício (PELTIER, 2000). No caso do TCU, utilizando-se de sua experiência no tratamento de incidentes de segurança da informação e em estudos na literatura específica, a Disic já leva às reuniões um conjunto prévio de controles que podem ser utilizados (ou já são por outros setores) de forma a iniciar e embasar as discussões.

O resultado final é um documento contendo riscos levantados e possíveis controles para mitigação. É o rascunho do Plano de Tratamento de Riscos. Esse documento é discutido e alterado em conjunto com o gestor da área/processo de trabalho em análise pois é ele que ficará responsável por sua implementação (em conjunto com as áreas que oferecem suporte às ações de mitigação dos riscos, como a TI ou logística). Nesse momento o gestor, em conjunto com a Disic, decide qual risco será tratado por qual controle, qual risco será aceito e qual pode ser transferido.

O monitoramento do Plano de Tratamento de Riscos é realizado semestralmente com o gestor responsável por sua implementação e as áreas de suporte de forma a levantar a situação do andamento das ações e identificar gargalos limitadores da plena aplicação dos controles definidos no PTR. Após o cumprimento de todo o Plano, o mesmo é arquivado e considera-se o processo de análise de riscos encerrado.

Nota-se que a metodologia permite uma rápida avaliação dos riscos em segurança da informação de determinada área ou processo de trabalho. Mas, por não ter vinculação com a alta gestão, pode levar à identificação e tratamento de riscos diversos àqueles considerados mais prioritários institucionalmente.

Apesar disso, observa-se a aderência dessa metodologia em grande parte àquela proposta pela ISO/IEC 27005 e pela Norma Complementar 04/IN01/DSIC/GSI/PR.

5.4 ANÁLISE DA APLICAÇÃO DA METODOLOGIA E DAS ANÁLISES DE RISCOS JÁ REALIZADAS

A Diretoria de Segurança da Informação e Continuidade de Negócios, em conjunto com as equipes dos setores analisados, já realizou 5 análises de riscos utilizando a metodologia FRAAP.

A primeira análise realizada foi na Secretaria de Controle Externo da Defesa Nacional e da Segurança Pública (SecexDefesa) em 2013. Por ser um setor que manipula uma grande quantidade de informações sensíveis e confidenciais, foi a primeira Secretaria do Tribunal a contar com o apoio da Disic para melhoria de seus processos de trabalho, considerando as premissas de garantir a confidencialidade, integridade e disponibilidade de suas informações.

O trabalho resultou na incorporação de mudanças e controles no processo de trabalho durante o ciclo de vida da informação que circula pela Secretaria e na conscientização de seus servidores da importância de manter esses controles ativos e permanentes.

Nos anos seguintes foram realizadas, em sequência, análises de riscos na Secretaria de Macroavaliação Governamental (Semag), na Diretoria de Gestão de Informações Estratégicas (DGI), na Secretaria de Fiscalização de Desestatização de Energia Elétrica e Comunicações (SefidEnergia) e na Secretaria Extraordinária de Operações Especiais em Infraestrutura (SeinfraOperações) – esta última em meados de 2016.

Os trabalhos na Semag e na DGI tiveram como foco o aumento do nível de proteção de suas bases de dados. Já os trabalhos na SefidEnergia e na SeinfraOperações tiveram o mesmo foco da SecexDefesa, ou seja, a melhoria do nível de proteção à informação durante seu ciclo de vida dentro da unidade. Em todos os casos os Planos de Tratamento de Riscos foram assumidos pelos gestores das áreas analisadas, ou seja, a decisão de tratar ou aceitar um risco ficou a seu critério.

Observa-se que as análises de risco são realizadas continuamente desde 2013. O resultado de cada análise tem sido utilizado para a mitigação dos riscos de segurança da informação, certamente, e também para: alimentar a base de dados da Disic em relação aos controles de mitigação de riscos que são viáveis e de baixo custo de implementação; orientar a atividade de conscientização em segurança da informação para todo o Tribunal, inclusive com a elaboração de treinamentos específicos; e, por fim, aperfeiçoar a metodologia de análise de risco para o atendimento de novas demandas.

Entretanto, apesar da continuidade na execução das análises de risco e da gestão dos riscos levantados, o alcance da atividade ainda é diminuto em relação à dimensão do Tribunal.

Somente na Secretaria-Geral de Controle Externo, responsável pelas auditorias e processos finalísticos do TCU, há mais de 30 unidades técnicas diferentes. E, em 3 anos, apenas 5 unidades foram analisadas.

Complementarmente, nota-se que o processo de gestão de riscos de segurança da informação resume-se à realização de análises de risco pontuais e com fim definido. Não é um processo cíclico nem contínuo, pois não há realimentação ou nova análise após o cumprimento do disposto nos planos de tratamento de risco. Nenhuma das unidades analisadas até o presente momento foi reavaliada.

Ademais, a ausência de uma norma que obrigue os gestores a analisar seus processos à luz da segurança da informação torna a atividade dependente das pessoas que ocupam os cargos de gestão. Se não for interesse da gestão atual (que no TCU dura 2 anos, considerando eleição e reeleição do Presidente) avançar para um Tribunal mais seguro, a área técnica não encontra amparo para realizar novas análises de risco e conquistar o comprometimento dos gestores das áreas técnicas.

Logo, fica evidente que não há um processo plenamente implantado de gestão de segurança da informação no TCU. Para que o processo seja plenamente implantado, faz-se necessário avançar nos seguintes aspectos:

a) Elaboração de norma específica que defina os parâmetros do processo de gestão de risco de segurança da informação, como periodicidade, agentes responsáveis, participação da alta gestão, formato do ciclo PDCA, entre outros. A falta de norma específica pode ser considerada o principal entrave à plena implementação do processo de gestão de riscos de segurança da informação;

b) Definição do apetite ao risco pela alta gestão. Sem essa definição, cada setor estabelece seu próprio nível aceitável de risco, impossibilitando uma gestão macro dos riscos de segurança da informação. Além disso, impossibilita também que a área técnica de segurança da informação (no caso do TCU, a Disic) aja sob parâmetros determinados pela alta gestão, descolando sua atuação do interesse da administração;

c) Alinhamento do processo de gestão de riscos de segurança da informação com o planejamento estratégico do Tribunal. Atualmente não há qualquer alinhamento nesse sentido, o que prejudica um alcance de longo prazo das ações de mitigação dos riscos de segurança da informação;

d) Aproximação hierárquica da área técnica de segurança da informação da alta administração. A atual localização organizacional da Disic não permite a interação entre a área técnica de segurança da informação e a alta gestão, dificultando o alinhamento entre o SGSI e

a expectativa dos dirigentes. Por conseguinte, não há amparo da alta gestão para a implementação plena do processo de gestão de riscos de segurança da informação;

e) Empoderamento do Comitê de Segurança Institucional. Nos moldes atuais do Cosin, as áreas técnicas gestoras do sistema de segurança institucional possuem completo poder sobre o planejamento e gestão das ações sob sua responsabilidade. Assim, cabe à Disic escolher quais ações de segurança da informação serão executadas em cada semestre. O Comitê age como mero ratificador do planejado pela Disic. Observa-se que nesse modelo as outras áreas do Tribunal não têm espaço para apresentar suas questões e dilemas relacionados à segurança da informação, e influenciar no planejamento das ações desse tema. Uma evolução do modelo seria trazer tal planejamento para o Cosin, permitindo a participação de mais áreas do TCU;

f) Nivelamento e conscientização gerencial de forma a sensibilizar a alta gestão para a necessidade de avanço na implantação do processo de gestão de riscos e das sugestão acima apontadas.

6. CONCLUSÕES

O presente artigo propôs-se a examinar a implementação do processo de gestão de riscos de segurança da informação (gestão de riscos de SI) no âmbito do Tribunal de Contas da União, identificando-se os normativos internacionais, nacionais e internos que amparam o processo, bem como a metodologia aplicada na prática cotidiana.

Ressalte-se, inicialmente, que em um mundo cada vez mais conectado e exposto às vulnerabilidades e ameaças à segurança da informação, a gestão de riscos de segurança da informação torna-se essencial para garantir níveis adequados de confidencialidade, integridade e disponibilidade. Tal fato é ainda mais relevante para instituições como o TCU, cujos insumo e produto são pura informação.

O processo de gestão de segurança da informação encontra-se positivado no Tribunal por meio de duas normas: a Resolução-TCU 261/2014, que dispõe sobre a Política de Segurança Institucional do Tribunal, e a Portaria-TCU 210/2014, que dispõe sobre a Política Corporativa de Segurança da Informação do TCU (PCSI/TCU).

Observou-se, pela leitura desses dois normativos, que não há intersecção entre as Políticas de Segurança Física e Patrimonial e de Segurança da Informação no Tribunal, configurando uma evidência de que a segurança da informação trabalha de forma separada dos demais processos administrativos da instituição.

A PCSI/TCU atribui à Diretoria de Segurança da Informação e Continuidade de Negócio (Disic) do Tribunal a responsabilidade pela gestão e monitoramento do Sistema de Gestão de Segurança da Informação (SGSI/TCU). Essa responsabilidade engloba o processo de gestão de riscos de segurança da informação.

Considerando que os normativos que positivaram o processo de gestão de riscos de SI não determinaram a metodologia a ser adotada, coube à Disic defini-la. A Diretoria optou pelo método FRAAP (*Facilitated Risk Analysis and Assessment Process*).

O boa viabilidade do método em termos de custo e tempo de execução permitiram à Disic realizar análises de risco de segurança da informação quase que anualmente. Entretanto, tais análises restringiram-se a levantar riscos de áreas e processos de trabalhos específicos, de setores específicos do Tribunal. Não houve uma análise de risco ampla, englobando os objetivos estratégicos da instituição.

Observa-se, também, que a aplicação da metodologia tem auxiliado o aperfeiçoamento dos controles de segurança da informação durante o ciclo de vida da informação nas áreas que a utilizaram. Mas não causaram mudança impactante na gestão como um todo do Tribunal.

Trata-se de evidente limitação do método, que não analisa a instituição como um todo, mas apenas um processo de trabalho por vez.

Complementarmente, foi possível concluir pelo exposto neste artigo que a definição do nível tolerável de risco aos processos de trabalho do Tribunal está nas mãos dos gestores de cada área, e não da alta gestão, como preceituam as normas ISO27000 e as Normas Complementares 02/IN01/DSIC/GSI/PR e 04/IN01/DSIC/GSI/PR. A própria PCSI/TCU preceitua que o tratamento dos riscos deve ser realizado com base em critérios compatíveis com os objetivos institucionais.

Assim, verificou-se que diferentes setores do Tribunal possuem diferentes níveis de tolerância ao risco, com mais ou menos controles de segurança da informação. E tais níveis não possuem qualquer aderência ao planejamento estratégico institucional, resumindo-se à percepção dos gestores de cada área.

Pelo exposto, conclui-se que o processo de gestão de riscos de segurança da informação no TCU encontra-se criado formalmente, com normas amparando-o e uma estrutura organizacional de sustentação (a própria Disic). Apesar disso, não há uma norma específica que estabeleça parâmetros para o processo e o mesmo não é cíclico nem contínuo. As análises de risco são realizadas somente nos setores que as demandam e quando demandam. Não há definição de um cronograma de análise de risco nem uma retroalimentação do processo. Trata-se de projetos específicos, com prazo definido de duração.

Tal situação decorre em grande parte devido ao desinteresse da alta administração em definir os níveis aceitáveis de risco para suas atividades mais importantes e em alocar o conjunto de recursos necessários para executar o processo de forma cíclica e contínua. Não é razoável supor que a Disic, atualmente com lotação de 5 servidores da carreira de auditoria do TCU, consiga gerir e controlar o SGSI/TCU sozinha e um processo permanente de gestão de riscos de segurança da informação.

Por fim, observa-se a falta de comunicação dos resultados encontrados à alta gestão do Tribunal, no caso a Presidência e o Plenário. Tal situação ocorre em parte porque a Disic encontra-se afastada hierarquicamente da alta gestão. E, ademais, ressalte-se novamente que não há interesse por parte da alta gestão em determinar o nível de tolerância ao risco. Essa ausência de comunicação entre a área técnica e a alta gestão não se coaduna com o disposto nas proposições dispostas na ISO/IEC 27005 e nas Normas Complementares 02/IN01/DSIC/GSIPR e 04/IN01/DSIC/GSI/PR.

De forma a contornar os obstáculos à plena implantação do processo de gestão de riscos de segurança da informação, sugere-se: a elaboração de norma específica que defina os

parâmetros do processo de gestão de riscos de segurança da informação; a definição do apetite ao risco pela alta gestão; o alinhamento do processo com o planejamento estratégico do TCU; a aproximação hierárquica da área técnica de segurança da informação com a alta administração; o empoderamento do Comitê de Segurança Institucional; e o nivelamento e conscientização gerencial para as questões apontadas.

Somente com o reforço do apoio institucional proporcionado pelas ações sugeridas é que poderá se implementar um processo de gestão de riscos de segurança da informação verdadeiramente completo, cíclico e contínuo, com visão de todo o Tribunal.

7. REFERÊNCIAS BIBLIOGRÁFICAS

ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos: ABNT NBR ISO/IEC 27001:2006. 1a. ed. Rio de Janeiro, 2006.

ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação: ABNT NBR ISO/IEC 27002:2005. 2a. ed. Rio de Janeiro, 2005.

ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. Tecnologia da informação - Técnicas de segurança - Gestão de riscos de segurança da informação - Requisitos: ABNT NBR ISO/IEC 27005:2008. 1a. ed. Rio de Janeiro, 2008.

BRASIL. Departamento de Segurança da Informação e Comunicações. Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC. Norma Complementar 02/IN01/DSIC/GSI/PR, de 13 de outubro de 2008. Disponível em: < http://dsic.planalto.gov.br/documentos/nc_2_metodologia.pdf>. Acesso em 03/04/2017.

BRASIL. Departamento de Segurança da Informação e Comunicações. Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC. Norma Complementar 04/IN01/DSIC/GSI/PR, de 15 de fevereiro de 2013. Disponível em: < http://dsic.planalto.gov.br/documentos/nc_04_grsic.pdf>. Acesso em 03/04/2017.

BRASIL. Secretaria de Tecnologia da Informação – STI/MP. Metodologia de Gestão de Riscos de Segurança da Informação, de maio de 2015. Disponível em: <https://www.governoeletronico.gov.br/documentos-e-arquivos/OE1-RM2-Julho.pdf/at_download/file>. Acesso em 04/04/2017.

BRASIL. Tribunal de Contas da União. Dispõe sobre a Política de Segurança Institucional (PSI/TCU) e o Sistema de Gestão de Segurança Institucional do Tribunal de Contas da União (SGSIN/TCU). Resolução-TCU nº 261, de 11 de junho de 2014. Disponível em: < http://www.tcu.gov.br/Consultas/Juris/Docs/judoc%5CResol%5C20140703%5CRES2014-261.doc>. Acesso em 03/04/2017.

BRASIL. Tribunal de Contas da União. Dispõe sobre a Política Corporativa de Segurança da Informação (PCSI/TCU) e sobre o Sistema de Gestão de Segurança da Informação do Tribunal de Contas da União (SGSI/TCU). Portaria-TCU nº 210, de 14 de agosto de 2014. Disponível em: <http://www.tcu.gov.br/Consultas/Juris/Docs/judoc/PORTN/20141023/PRT2014-210.doc>. Acesso em 03/04/2017.

BRASIL. Tribunal de Contas da União. Dispõe sobre o funcionamento do Comitê de Segurança Institucional (Cosin). Portaria-TCU nº 77, de 4 de fevereiro de 2015. Disponível em: < http://www.tcu.gov.br/Consultas/Juris/Docs/judoc%5CPORTN%5C20150623%5CPRT2015-77.doc>. Acesso em 20/04/2017.

SÊMOLA, Marcos. **Gestão da Segurança da Informação: uma visão executiva.** 2ª ed. – Rio de Janeiro: Elsevier, 2014.

CAPRINO, Willian Okuhara, CABRAL, Carlos. **Trilhas em Segurança da Informação: Caminhos e ideias para a proteção de dados.** 1ª ed – Rio de Janeiro: Brasport, 2015.

BEAL, Adriana. **Segurança da Informação – Princípios e Melhores Práticas para a Proteção dos Ativos de Informação nas Organizações**. 1ª ed – São Paulo: Atlas, 2005.

PELTIER, Thomas R. **Information Security Risk Analysis**. 2ª Ed – United States: Auerbach Publications, 2005.

PELTIER, Thomas R. **Facilitated Risk Analysis Process (FRAP)**. Artigo escrito para o periódico virtual IT Today (http://www.ittoday.info/). United States: 2000. Disponível em: < http://www.ittoday.info/AIMS/DSM/85-01-21.pdf >. Acesso em 10/04/2017.