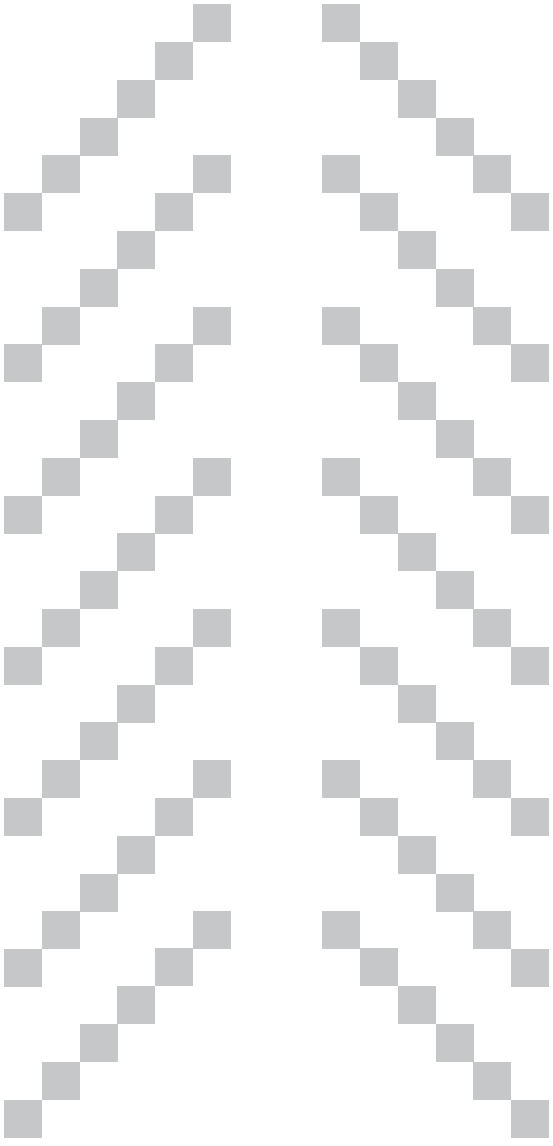
Segurança da informação no TCU: cumprindo as próprias recomendações

Cláudia Augusto Dias e
Felício Ribas Torres



Cláudia Augusto Dias é servidora do Tribunal de Contas da União. Graduada em Engenharia Elétrica, mestre e PhD em Ciência da Informação pela Universidade de Brasília (UnB).
Felício Ribas Torres é servidor do Tribunal de Contas da União. Graduado em Ciências Econômicas, especialista em Tecnologia da Informação, mestre em Administração pela Universidade de Brasília (UnB) e pós-graduado em Finanças e em Planejamento e Orçamento Público.

1 INTRODUÇÃO

O negócio das organizações modernas, públicas ou privadas, é sustentado pela gestão da informação. A informação, como ativo organizacional importante, assim como os ambientes e os meios utilizados para o seu tratamento, devem ser mantidos em segurança. Nesse contexto, a adoção de práticas de segurança da informação deixa de ser uma opção e passa a ser mandatória, como ação essencial à sobrevivência das organizações.

Entende-se por práticas de segurança da informação o conjunto de procedimentos e ferramentas que visa assegurar os princípios da confidencialidade, disponibilidade e integridade da informação não só sob aspectos físicos (instalações, equipamentos e infra-estrutura) e tecnológicos (sistemas, bases de dados e demais recursos de tecnologia da informação), mas também organizacionais (pessoas e processos de trabalho) (FONTES, 2008; SÊMOLA, 2003).

O Tribunal de Contas da União (TCU) é uma organização que lida essencialmente com informações para auxiliar o Congresso Nacional no exercício do controle externo da Administração Pública – Constituição Federal de 1988, artigos 70 e 71 (BRASIL, 1988). Tal controle exercido externamente à estrutura do Poder controlador, segundo Wurman (2005, p. 11), visa "a preservação e o equilíbrio das instituições políticas democráticas do País".

O trabalho desenvolvido pelo TCU, entregue ao Congresso Nacional e à sociedade por meio de acórdãos, despachos, instruções e decisões normativas, baseia-se em informações recebidas das unidades jurisdicionadas, da imprensa e da sociedade de modo geral, mediante fiscalizações, prestações e tomadas de contas, denúncias, entre outros mecanismos. Em síntese, o insumo e o produto do trabalho do TCU são, em última instância, informação.

Ciente disso, o TCU, no exercício de sua função pedagógica e orientadora, vem realizando ações para apoiar a adoção de boas práticas em segurança da informação nos órgãos da Administração Pública Federal e demais entes jurisdicionados. Dentre essas ações destacam-se:

a) a elaboração da cartilha "Boas Práticas em Segurança da Informação", publicada em 2003 e revisada em 2007, com o objetivo de despertar a atenção para a segurança da informação nas organizações governamentais e de fornecer importante fonte de consulta para o aperfeiçoamento da Administração Pública nessa área;

b) a instituição da Secretaria de Fiscalização de Tecnologia da Informação (Sefti), em 2006, para incrementar e aperfeiçoar as atividades de auditoria desenvolvidas pelo corpo técnico do Tribunal. Um dos focos de trabalho dessa secretaria é a verificação da conformidade e do desempenho das ações governamentais em segurança da informação; e

c) a expedição de acórdãos que recomendam e/ou determinam a adoção de boas práticas em segurança da informação.

Essas ações, por outro lado, geram para o TCU, sob o prisma da legitimidade, a necessidade de se tornar referência no que concerne à adoção de práticas de segurança da informação. Suchman (1995, p.4) define legitimidade como:

> [...] uma percepção generalizada ou suposição de que as ações de uma entidade são desejadas, próprias ou apropriadas dentro de algum sistema de normas, valores, crenças e definições socialmente construídas.

Pfeffer e Salancik (1978) destacam que a legitimidade é um *status* conferido pela sociedade a uma determinada organização, após avaliar a utilidade de suas atividades e endossá-las.

A coerência entre discurso e prática é uma das formas pelas quais a legitimidade é alcançada pelas organizações (MORGAN, 1996). De acordo com a tipologia apresentada por Suchman (1995), essa legitimidade é denominada legitimidade moral. É nesse sentido que o TCU tem buscado ser exemplo para seus jurisdicionados no envide de esforços para cumprir internamente as recomendações presentes em suas decisões.

2 O DISCURSO DIRECIONANDO A PRÁTICA

Conhecer bem seu discurso é o primeiro passo a ser dado por uma organização que busca alcançar legitimidade moral (ORLANDI, 1999). O passo seguinte é direcionar suas ações para o mesmo sentido. Assim, o olhar sobre as recomendações constantes em seus acórdãos é requisito essencial para que o TCU conduza suas iniciativas em segurança da informação.

Embora o tema segurança da informação esteja presente nos acórdãos do TCU há anos, a inclusão de recomendações com esse foco passou a ser mais frequente a partir de 2003, não por coincidência o ano da elaboração da primeira versão da cartilha "Boas Práticas em Segurança da Informação", citada anteriormente.

Tomando, então, o ano de 2003 como ponto de partida e agosto de 2009 como fim, um breve levantamento[1] revela a existência de 50 acórdãos que tratam o tema segurança da informação. Com maior detalhamento, percebe-se que cerca de 90 por cento desses acórdãos recomendam a realização de pelo menos uma das seguintes ações: a) elaboração ou revisão de política de segurança da informação; b) adoção de estrutura organizacional específica para tratar a segurança da informação; c) normatização da classificação das informações; d) implantação de controle de acesso; e e) implantação da gestão da continuidade do negócio.

Vale destacar que o Tribunal tem utilizado como referência, em suas recomendações sobre segurança da informação, a NBR ISO/IEC 17799:2005[2]. Isso ocorre em razão do reconhecimento da excelência técnica da Associação Brasileira de Normas Técnicas (ABNT), entidade responsável pela elaboração da norma, e do fato de que a equivalente versão internacional, ISO/IEC 17799, é amplamente reconhecida e utilizada, para o mesmo fim, por Entidades Fiscalizadoras Superiores e órgãos de governo em todo o mundo.

Dentre os acórdãos exarados pelo TCU, merecem destaque os Acórdãos nº 1.603 – Plenário, de 13 de agosto de 2008, e nº 2.471 – Plenário, de 5 de novembro de 2008, nos quais esta Corte de Contas inova e, demonstrando o intuito de ser referência para seus jurisdicionados, recomenda a si mesma, por meio das Secretarias Gerais da Presidência e de Administração, a adoção de medidas para o gerenciamento da segurança da informação.

Acórdão nº 1.603/2008-PL

> 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;
>
> 9.6 recomendar à Secretaria-Geral da Presidência – Segepres e à Secretaria-Geral de Administração – Segedam que adotem, no âmbito deste Tribunal, as providências contidas no item 9.1; (BRASIL, 2008c, grifo nosso)

Acórdão nº 2.471/2008-PL

> 9.6.1 crie procedimentos para elaboração de Políticas de Segurança da Informação, Políticas de Controle de Acesso, Políticas de Cópias de Segurança, Análises de Riscos e Planos de Continuidade do Negócio. Referidas políticas, planos e análises deverão ser implementadas nos entes sob sua jurisdição por meio de orientação normativa;
>
> 9.16 recomendar, com fulcro no art. 43, I, da Lei nº 8.443/92, à Secretaria-Geral da Presidência do Tribunal de Contas da União, que adote as providências contidas nos itens "9.4.", "9.6", "9.8" e "9.10" acima no âmbito do TCU; (BRASIL, 2008f, grifo nosso)

Diante disso, fica claro o discurso organizacional do TCU e, por coerência, também o caminho a ser trilhado, visto que os acórdãos citados *in verbis* delineiam as ações a serem realizadas. Nesse ponto, a organização venceu a etapa do "conhecer" o discurso e, indo além, definiu alvos a serem alcançados. Restava, portanto, o "praticar".

Vale destacar que antes mesmo da edição dos acórdãos citados, diversas iniciativas de segurança da informação já estavam presentes no Tribunal. Além das ações orientadoras de controle externo, o Tribunal já havia disciplinado internamente aspectos referentes a esse tema, tais como procedimentos para salvaguarda de documentos de natureza sigilosa; acesso, circulação e permanência de pessoas e veículos nos edifícios do Tribunal; política de segurança da informação; critérios para cadastramento de informações nas bases corporativas de dados; procedimentos e ações de gestão documental; competências e designação de unidades gestoras de soluções de tecnologia da informação (TI) e critérios para acesso à internet por meio da rede TCU.

Além disso, dentre as ações realizadas com foco interno, destaca-se o diagnóstico de maturidade e aderência de processos de segurança da informação frente à norma NBR ISO/IEC 17799:20053, concluído em julho de 2008. Resultaram desse diagnóstico recomendações para a melhoria da segurança da informação no Tribunal, como a criação de área estratégica de coordenação da segurança da informação e a revisão da política de segurança da informação vigente à época.

3 ESTRATÉGIA DE IMPLANTAÇÃO DE SEGURANÇA DA INFORMAÇÃO NO TCU

O alcance dos objetivos almejados depende, e muito, da estratégia adotada, isto é, da definição de um curso a ser seguido pela organização (KOTLER, 1975; ANSOFF, 1993). Assim, de posse da lista de ações a serem realizadas, o TCU precisou definir prioridades e direcionar recursos e esforços para realizá-las.

Mais do que isso, o TCU precisou deixar clara a importância que o tema segurança da informação tem internamente. Para isso, o comprometimento e o envolvimento da alta administração foram fundamentais. Ainda em 2007, a participação da alta

administração começara a ficar evidente por meio da designação do Ministro Augusto Sherman Cavalcanti para a coordenação estratégica na definição de políticas e diretrizes relativas à área de tecnologia da informação no Tribunal. Com a estratégia definida e o forte apoio da alta administração, a busca por cumprir as recomendações direcionadas ao próprio Tribunal teve início.

3.1 DEFINIÇÃO DE ESTRUTURA ESPECÍFICA

As boas práticas em segurança da informação (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2005; BRASIL, 2007a; DIAS, 2000) recomendam que exista, na estrutura da organização, uma área responsável pela segurança de informações ativamente apoiada pela alta direção. Essa área deve iniciar o processo de elaboração da política de segurança da informação, coordenar sua implantação, aprovação e revisão, e cuidar da divulgação e aplicação correta da política, de forma que todos, funcionários, fornecedores e clientes, entendam suas responsabilidades com relação à segurança de informações na organização.

Seguindo essa recomendação, a política corporativa de segurança da informação do TCU (PCSI/TCU), aprovada pela Resolução – TCU nº 217, de 15 de outubro de 2008 (BRASIL, 2008e), estabelece que esse papel seja desempenhado pela Secretaria-Geral da Presidência (Segepres), por meio da Assessoria de Segurança da Informação e Governança de Tecnologia da Informação (Assig), e pelo Comitê de Segurança da Informação (CSI).

A Assig, unidade especializada de assessoramento instituída pela Segepres em abril de 2008 (BRASIL, 2008b), tem como atribuições coordenar e acompanhar a implementação da PCSI/TCU e normas complementares, homologar processos de trabalho e procedimentos operacionais necessários, monitorar e avaliar periodicamente as práticas de segurança da informação adotadas pelo Tribunal.

O CSI, por sua vez, órgão colegiado de natureza consultiva instituído pela PCSI/TCU, tem por finalidade formular e conduzir diretrizes para a política de segurança da informação do Tribunal, analisar periodicamente sua efetividade, propor normas e mecanismos institucionais para melhoria contínua e assessorar, em matérias correlatas, a Comissão de Coordenação Geral (CCG) e a Presidência do Tribunal.

Tal comitê é composto por dois representantes de cada Secretaria-Geral, além de um representante da Secretaria de Infraestrutura de TI (Setic) e do titular da Assig, que o preside. A composição heterogênea e representativa de interesses e setores diversos do Tribunal atende às boas práticas de segurança da informação (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2005; PINHEIRO, 2009), propicia ampla discussão e confere legitimidade às propostas submetidas por esse comitê às instâncias superiores.

3.2 REVISÃO DA POLÍTICA CORPORATIVA DE SEGURANÇA DA INFORMAÇÃO

O diagnóstico de maturidade e aderência de processos de segurança da informação frente à norma NBR ISO/IEC 17799:2005 e a recomendação da NBR ISO/IEC 27002:2005 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2005), substituta da norma anterior, de que a política de segurança da informação seja analisada criticamente a intervalos planejados ou quando mudanças significativas ocorrerem, motivaram a atualização da PCSI/TCU.

A formalização, a atualização e a divulgação da PCSI/TCU também vão ao encontro de decisões do Tribunal, em especial os acórdãos nº 1.603/2008-PL (BRASIL, 2008c) e nº 2.471/2008-PL (BRASIL, 2008f), para que os entes fiscalizados elaborem, formalizem, divulguem e mantenham atualizadas políticas de segurança da informação norteadoras da gestão da segurança da informação nessas entidades.

O trabalho de revisão iniciou-se com análise da Assig sobre o conteúdo do relatório do diagnóstico. Tal relatório apontou que a política de segurança da informação vigente à época apresentava limitadores, tais como abordagem excessivamente tecnológica, indo de encontro ao conceito de que segurança da informação não engloba apenas tecnologias, mas também processos e pessoas no âmbito organizacional; não atribuição de responsabilidades sobre a segurança da informação, o que dificulta a implementação das ações decorrentes da política; inclusão de temas específicos que deveriam estar contidos em normas complementares, a exemplo do disciplinamento do uso do correio eletrônico no Tribunal.

Após a análise do relatório e de sugestões coletadas em reuniões com unidades do TCU envolvidas com o tema, a Assig elaborou minuta da PCSI/TCU, a qual foi aprovada pela Resolução – TCU nº 217/2008 (BRASIL, 2008e). As diretrizes estabelecidas nessa resolução determinam as linhas mestras a serem seguidas por todos para que seja assegurada a segurança das informações produzidas e custodiadas pelo Tribunal.

Em relação ao disciplinamento anterior, destacam-se na PCSI/TCU a atribuição de competência à Segepres, por meio da Assig, para coordenar e acompanhar a implementação da política e de suas normas complementares; instituição do CSI; definição e atribuição de responsabilidades para gestores e custodiantes de informação, dirigentes e chefias de unidades no Tribunal; e exclusão do tema correio eletrônico, tratado em norma específica.

Na PCSI/TCU, como um conjunto de princípios, objetivos e diretrizes que norteiam a gestão de segurança de informações no Tribunal, constam tópicos comuns em políticas de segurança da informação, recomendados pela norma da ABNT (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2005), tais como: definição e objetivos de segurança da informação, responsabilidades gerais na gestão de segurança da informação, menção às normas e procedimentos complementares que apóiam a política, consequências de violações das normas estabelecidas na política, necessidade de treinamento e educação em segurança da informação, entre outros assuntos.

Com o objetivo de tornar mais claro o conteúdo dessa política a todos os envolvidos – servidores, unidades do Tribunal, prestadores de serviço terceirizado, estagiários ou quaisquer outros colaboradores do Tribunal que tenham acesso, de forma autorizada, a informações produzidas ou custodiadas pelo Tribunal, foram elaborados a cartilha "Segurança da informação no TCU: política corporativa comentada" e o *folder* "Política Corporativa de Segurança da Informação do TCU".

3.3 EDIÇÃO DE NORMATIVOS COMPLEMENTARES

Como toda política, a PCSI/TCU se concentra em princípios e diretrizes. É o principal de muitos outros documentos, como por exemplo, os comentados a seguir, com informações cada vez mais detalhadas sobre procedimentos e padrões de segurança da informação a serem aplicados em determinadas circunstâncias.

3.3.1 CLASSIFICAÇÃO DE INFORMAÇÕES

Após a aprovação da PCSI/TCU, o CSI, em sua prerrogativa de propor normas e mecanismos institucionais para melhoria contínua em segurança da informação e em atendimento ao Acórdão –

TCU nº 1.603/2008-PL (BRASIL, 2008c), aprovou e submeteu à CCG minuta de normativo sobre classificação das informações produzidas ou custodiadas pelo Tribunal.

A regulamentação da classificação das informações no TCU merece destaque por permear o desenvolvimento das atividades do Tribunal e por se constituir em instrumento estruturante para que a gestão da informação seja efetuada adequadamente nos processos de trabalho corporativos. Tal regulamentação não só atende ao referido acórdão, mas também promove a instituição de mecanismo fundamental à implantação sustentável do processo eletrônico na Casa e propicia a implementação de requisitos de segurança que favoreçam o intercâmbio de informações entre o TCU, seus jurisdicionados, órgãos e entidades partícipes da rede de controle e de demais acordos de cooperação.

3.3.2 CONTROLE DE ACESSO

Impelidos pelas discussões sobre segurança da informação na revisão da PCSI/TCU, foram aprovados pelo Tribunal, ainda antes da publicação da política revisada, procedimentos e regras para concessão de perfil de acesso a soluções de tecnologia da informação para profissionais de empresas contratadas e estagiários, condicionada a assinatura de termo de responsabilidade no uso de recursos de tecnologia da informação. Como complemento, a Assig editou nota técnica sobre o processo de concessão e revogação de perfis do sistema de gerência de acesso a soluções de tecnologia da informação do Tribunal, com recomendações para formalizar a política de controle de acesso a partir dos processos de trabalho já adotados, incluindo a definição conjunta de responsabilidades, procedimentos e prazos por gestores de soluções de TI e Setic.

3.4 GERÊNCIA DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Seguindo a boa prática de instruir os usuários a notificarem qualquer observação ou suspeita de fragilidade em segurança da informação e de estabelecer canal apropriado para registro dessa notificação (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2005), a PCSI/TCU atribuiu a usuários internos e colaboradores do TCU a responsabilidade de reportar à Assig os incidentes de segurança da informação de que tenham conhecimento. A Assig é, portanto, o principal canal de comunicação para registro de notificações de incidentes de segurança da informação.

Os usuários que, por desconhecimento ou dúvida quanto à caracterização de um fato como incidente de segurança da informação, entram em contato com a Ouvidoria ou a Central de Atendimento do Usuário da Setic, também têm sua notificação registrada, sem necessidade de um novo contato com a Assig. Essas unidades atuam, portanto, como canais alternativos para registro de notificações de incidentes.

Após o registro, as informações coletadas com os usuários são encaminhadas à unidade competente para análise do incidente e identificação de suas causas, relato da solução adotada, implementação de medidas para prevenir sua recorrência, etc. Dependendo da gravidade do incidente, a Assig é imediatamente comunicada para que seja possível a tomada de ação corretiva em tempo hábil.

Atendendo ao Acórdão nº 1.603/2008-PL quanto à gestão de incidentes, a Assig, à qual compete coordenar e acompanhar a implementação da PCSI/TCU e normas complementares, assim como monitorar e avaliar periodicamente as práticas de segurança da informação adotadas pelo Tribunal, também é responsável pela análise e pelo controle consolidado dos incidentes de segurança da informação registrados.

3.5 Uma ação leva a outra

Na caminhada em busca de cumprir as próprias recomendações, além daquelas descritas nos acórdãos nº 1.603/2008-PL (BRASIL, 2008c) e nº 2.471/2008-PL (BRASIL, 2008f), a realização de outras ações se mostrou necessária para complementar os esforços de praticar, de fato, segurança da informação no TCU.

Em termos estruturais, o Tribunal criou, na Setic, o Serviço de Segurança em TI ao qual compete promover e acompanhar, no âmbito dessa secretaria, a implementação de ações para segurança da informação em consonância com a PCSI/TCU; coordenar a gestão de processos de trabalho,

métodos e ferramentas para gestão da continuidade, incidentes de segurança da informação e tratamento de riscos relacionados aos serviços e soluções de TI, entre outras competências.

Em termos normativos, além da minuta sobre classificação das informações produzidas ou custodiadas pelo Tribunal (item 3.3.1), foram aprovadas pelo CSI e submetidas à CCG minutas sobre uso do serviço de correio eletrônico e uso da rede de computadores, de dispositivos portáteis e de demais recursos de TI. Ainda se encontram em discussão no âmbito do CSI minutas de normativos que regulamentam procedimentos para cópia de segurança e instalação de *softwares* em estações de trabalho.

Além disso, a Assig elaborou modelo de termo de sigilo e responsabilidade para assinatura por parte de estagiários e demais colaboradores quando da autorização para acesso a informações não públicas, e tem divulgado ao público interno orientações de segurança para a realização de trabalho fora das dependências do TCU e o uso de fragmentadoras para descarte de documentos em meio físico. Vale destacar, ainda, o programa de conscientização (item 3.5.1) e a elaboração de notas técnicas sobre segurança na emissão de certidões e sobre controle de acesso lógico, em especial no que tange à concessão e revogação de perfis do sistema de gerência de acesso a soluções de TI do Tribunal (item 3.3.2).

3.5.1 PROGRAMA DE CONSCIENTIZAÇÃO

Com o objetivo de manter o corpo técnico do TCU capacitado nas práticas de segurança da informação e consciente da importância desse tema para a instituição, a Assig instituiu um programa para conscientização de servidores e autoridades do TCU sobre segurança da informação. Tal programa não tem a pretensão de cobrir necessidades técnicas especiais em segurança da informação em função de atribuição no TCU, como é o caso das unidades Assig, Sefti, Setic e Serviço de Segurança (Segur), por exemplo. Seu foco é a difusão de conceitos básicos, práticas gerais e hábitos de trabalho fundados na preocupação com a segurança da informação.

O programa de conscientização, como atividade contínua, é composto de ações periódicas, como a divulgação, na comunidade "Segurança da Informação" no portal corporativo e em coluna quinzenal no informativo interno do Tribunal (União), de políticas e normas internas, dicas, orientações e notícias de iniciativas no TCU ligadas à segurança da informação. O contato direto com servidores e autoridades, em visitas às unidades para discutir problemas, sanar dúvidas e captar diferentes percepções sobre segurança da informação, também faz parte do programa.

No programa, há ainda a instituição, com previsão anual, do "Dia da Segurança da Informação no TCU", com palestras de convidados internos

e externos, e atividades lúdicas e educacionais. A primeira edição desse evento interno, em 29 de outubro de 2009, contou com a participação de palestrantes da Sefti e da Petrobras, além de apresentação teatral e premiação aos vencedores de *quiz* sobre segurança da informação.

4 PLANOS PARA O FUTURO

Embora diversas ações tenham sido realizadas no âmbito do Tribunal, ainda existem desafios a serem encarados. Dentre eles, estão previstos para o próximo ano a implantação da gestão da continuidade de negócio (GCN), a revisão de normativos e a implementação de controle de acesso físico compatível com as necessidades da organização.

A gestão da continuidade de negócios tem por objetivo "não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos, e assegurar a sua retomada em tempo hábil, se for o caso" (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2005). Como a interrupção das atividades do negócio de uma organização pode acarretar problemas legais, financeiros ou de imagem, a relevância da GCN está cada vez mais evidente, tanto para organizações privadas como públicas.

Para viabilizar a implantação da GCN no TCU, a estratégia desenhada pela Assig e aprovada pelo CSI parte de cooperação com outras organizações da Administração Pública que já tenham passado por essa experiência. A ideia é obter o máximo de informações e absorver métodos e procedimentos para identificação dos processos críticos do TCU durante análise de impacto no negócio (*Business Impact Analysis* – BIA).

No que concerne ao controle de acesso físico, vale registrar que o TCU possui normatização interna sobre o tema desde 1995. No entanto, sua última atualização ocorreu em 2000, abordando itens como o acesso de veículos à garagem do Tribunal e a identificação pessoal de servidores, colaboradores e visitantes.

A atualização periódica desse normativo é necessária para que seja compatível com a necessidade organizacional de minimizar os riscos inerentes ao tema. Dessa forma, à semelhança do que foi feito acerca do controle de acesso lógico, é mister que o acesso às dependências do TCU seja avaliado sob a ótica da segurança da informação.

5 CONSIDERAÇÕES FINAIS

Diante do exposto, pode-se dizer que o TCU tem trilhado o caminho correto para o alcance de legitimidade moral perante seus jurisdicionados. As ações e atividades relatadas de forma sintética neste artigo vão ao encontro do discurso presente nas orientações e nos acórdãos expedidos pelo Tribunal.

Especificamente quanto aos acórdãos nº 1.603/2008-PL (BRASIL, 2008c) e nº 2.471/2008-PL (BRASIL, 2008f), todas as recomendações ali contidas ou já foram realizadas ou se encontram em andamento no TCU. Vale esclarecer que as ações de gerência de mudanças e gerência de capacidade citadas nos acórdãos, embora estejam relacionadas com o tema segurança da informação, possuem foco na gestão de serviços de TI. Por essa razão, tais assuntos não foram abordados de forma direta neste artigo, mesmo que a implementação dessas recomendações esteja em andamento no TCU, amparada no conjunto de boas práticas ITIL[4].

Não obstante os passos dados para cumprir as próprias recomendações e, assim, ser referência para os jurisdicionados, muitos desafios ainda precisam ser enfrentados pelo Tribunal. Mesmo em relação às ações já realizadas, o trabalho permanece, visto que é necessário revisitar os assuntos periodicamente, para manter ações e normativos atualizados frente às necessidades da organização.

Em se tratando de segurança da informação, conjugar verbos no pretérito não parece ser o mais adequado. É uma atividade contínua, e a estratégia para o sucesso pressupõe alargar as fronteiras sem descuidar do espaço já conquistado. É preciso elaborar normativos e políticas, definir e implantar estrutura e controles adequados. Mas, ao realizar cada uma dessas ações, não se pode declarar o trabalho como de todo realizado. É preciso avaliar riscos continuamente e, a partir dos resultados encontrados, atualizar cada uma das ações citadas.

É por essa razão que o gerúndio foi utilizado no título deste artigo. No esforço para ser exemplo aos jurisdicionados e para alinhar discurso e prática, o TCU está "cumprindo" as próprias recomendações. E deve se esforçar cada vez mais para isso, sob pena de perder legitimidade para recomendar a adoção de práticas de segurança da informação. Assim, o TCU deve ser perseverante e diligente, de modo a consolidar as ações já realizadas, concluir aquelas em andamento e construir cultura de segurança da informação em toda a organização.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *NBR ISO/IEC 27002* : Tecnologia da informação: técnicas de segurança : código de prática para a gestão da segurança da informação. Rio de Janeiro, 2005.

ANSOFF, H. Igor. *Implantando a administração estratégica*. São Paulo: Atlas, 1993.

BRASIL. Constituição (1988). *Constituição da República Federativa do Brasil*. Brasília: Senado Federal, 1988.

_____. Tribunal de Contas da União. Resolução nº 91, de 25 de junho de 1997. Aprova procedimentos a serem observados para salvaguarda dos documentos, assuntos e processos de natureza sigilosa, a serem submetidos à apreciação e ao julgamento do Tribunal de Contas da União e dá outras providências *Diário Oficial da União*, Brasília, DF, 30 jun. 1997.

_____. _____. Resolução nº 126, de 3 de novembro de 1999. Dispõe sobre a Política de Segurança de Informações do Tribunal de Contas da União (PSI/TCU). *Boletim do Tribunal de Contas da União*, Brasília, DF, ano 32, nº 66, p. 2386-2389, 8 nov. 1999.

_____. _____. Portaria nº 39, de 18 de fevereiro de 2000. Dispõe sobre acesso, circulação e permanência de pessoas e veículos nos edifícios do Tribunal. *Boletim do Tribunal de Contas da União*, Brasília, DF, ano 33, n. 10, p. 4, 9 mar. 2000.

_____. _____. Portaria nº 211, de 28 de junho de 2001. Define critérios para cadastramento de informações nas bases corporativas de dados do TCU. *Boletim do Tribunal de Contas da União*, Brasília, DF, ano 34, n. 48, p. 1-2, 9 jul. 2001.

_____. _____. Portaria nº 108, de 6 de maio de 2005. Dispõe sobre procedimentos e ações de Gestão Documental no TCU. *Boletim do Tribunal de Contas da União*, Brasília, DF, ano 38, n. 10, 21 mar. 2005.

_____. _____. Portaria nº 105, de 29 de maio de 2006. Dispõe sobre competências e designação das unidades gestoras de soluções de tecnologia da informação do Tribunal de Contas da União. Disponível em: < http://www.tcu.gov.br/Consultas/Juris/Docs/judoc/PORTN/20090206/PRT2006-105.doc>. Acesso em: ago. 2009.

_____. _____. Portaria nº 169, de 31 de julho de 2006. Estabelece critérios para acesso à internet por meio da rede de computadores do TCU. *Boletim do Tribunal de Contas da União*, Brasília, DF, ano 39, n. 29, p. 2-4, 7 ago. 2006.

_____. _____. *Boas práticas em segurança da informação*. 2. ed. Brasília: TCU, 2007.

_____. _____. Portaria nº 138, de 2 de maio de 2007. Designa o Auditor Augusto Sherman Cavalcanti para a coordenação estratégica relativa à área de tecnologia da informação no âmbito do Tribunal de Contas da União. *Boletim do Tribunal de Contas da União*, Brasília, DF, ano 40, n. 16, p. 3-4, 7 maio 2007.

_____._____. *Segurança da informação no TCU*: política corporativa comentada. Brasília: TCU, Assig, 2008.

_____. _____. Portaria – Segepres nº 2, de 2 de abril de 2008. Dispõe sobre as competências, estrutura, lotação e alocação de funções de confiança da Secretaria-Geral da Presidência. Disponível em:< http://portal2.tcu.gov.br/portal/page/portal/TCU/unidades/segepres/atos_segepres/segepres/2008/Portaria_Segepres-n%C2%BA%202-08.doc>. Acesso em: ago. 2009.

_____. _____. Acórdão nº 1.603 – Plenário, de 13 de agosto de 2008. Ministro Relator Guilherme Palmeira. Disponível em:< http://contas.tcu.gov.br/portaltextual/MostraDocumento?qn=3&doc=1&dpp=20&p=0>. Acesso em: ago. 2009.

_____. _____. Portaria nº 202, de 8 de setembro de 2008. Dispõe sobre a concessão de perfil de acesso a soluções de tecnologia da informação para profissionais de empresas contratadas e estagiários, no âmbito do Tribunal de Contas da União. *Boletim do Tribunal de Contas da União*, Brasília, DF, ano 41, n. 35, p. 4-7, 15 de setembro de 2008.

_____. _____. Resolução – TCU nº 217, de 15 de outubro de 2008. Dispõe sobre a Política Corporativa de Segurança da Informação do Tribunal de Contas da União (PCSI/TCU). *Boletim do Tribunal de Contas da União*, Brasília, DF, ano 41, n. 41, p. 1-5, 28 out. 2008.

_____. _____. Acórdão nº 2.471 – Plenário, de 5 de novembro de 2008. Ministro Relator Benjamin Zymler. Disponível em:< http://contas.tcu.gov.br/portaltextual/MostraDocumento?qn=1&doc=1&dpp=20&p=0>. Acesso em: ago. 2009.

_____. _____. Portaria nº 277, de 18 de novembro de 2008. Dispõe sobre o Comitê de Segurança da Informação no âmbito do Tribunal de Contas da União. *Boletim do Tribunal de Contas da União*, Brasília, DF, ano 41, n. 45, p. 23-24, 24 nov. 2008.

_____. _____. *Política corporativa de segurança da informação do TCU*. Brasília: TCU, Assig, [2009]. Folder.

DIAS, Cláudia. *Segurança e auditoria da tecnologia da informação*. Rio de Janeiro: Axcel Books do Brasil, 2000.

FONTES, Edison. *Praticando a segurança da informação*. Rio de Janeiro: Brasport, 2008.

KOTLER, Philip. *Administração de marketing*. São Paulo: Atlas, 1975.

MORGAN, Gareth. *Imagens da organização*. São Paulo: Atlas, 1996.

ORLANDI, Eni. *Análise de discurso:* princípios e procedimentos. 2. ed. Campinas: Pontes, 1999.

PFEFFER, Jeffrey & SALANCIK, Gerald R. *The external control of organizations*: a resource dependence perspective. New York: Harpes & Row, 1978.

PINHEIRO, Patrícia. *Direito digital*. 3. ed. rev., atual. e ampl. São Paulo: Saraiva, 2009.

SÊMOLA, Marcos. *Gestão da segurança da informação*: uma visão executiva. Rio de Janeiro: Campus, 2003.

SUCHMAN, Mark C. Managing legitimacy: strategic and institutional approaches. *Academy Management Review*, v.20, n.3, p. 571-560, jul. 1995.

WURMAN, Samy. *Controle externo*. 2. ed. Brasília, 2005.

NOTAS

1 Pesquisa realizada em 30/9/2009 no Portal TCU, por meio das ferramentas Jurisprudência Sistematizada e Pesquisa de Acórdãos.

2 Atualizada para a NBR ISO/IEC 27002:2007

3 Atualizada para a NBR ISO/IEC 27002:2005

4 *Information Technology Infrastructure Library*