**CONSULTA PÚBLICA 144**

**Proposta de Padrões de Interoperabilidade de Governo Eletrônico - ePING, versão 2015**

**Órgão Responsável:** Secretaria de Logística e Tecnologia da Informação/MP

**Item:** Critérios de Auditoria de Segurança - Decreto º 8.135, de 4 de novembro de 2013

**CONTRUBUIÇÃO 1: Giuseppe Sidrim Marrara da Cisco**

A Cisco acredita que a implementação de políticas industriais restritivas pode afastar os investimentos estrangeiros no desenvolvimento e produção nacional de equipamentos e de produtos de rede no Brasil, podendo trazer consequências negativas não previstas para todo o ecossistema de contratações. Assim, em uma breve análise dos documentos levados à consulta pública, vislumbra-se a complexidade e os diversos aspectos técnicos que necessitam de análises mais profundas e apuradas, considerando também a extrema importância para sociedade e para setor de TI no país, de tal sorte que a Cisco acredita que o prazo para manifestações se mostra deveras insuficiente para as contribuições e análises que se fazem necessárias. Os assuntos apresentados em consulta necessitam de um diálogo amplo e aberto sobre os temas contidos nos diversos documentos trazidos ao debate. Um prazo maior permitiria uma melhor análise de todo o material por pessoal técnico qualificado, como também possibilitaria uma correta avaliação das densas diretrizes apresentadas. Desta forma, acreditando em um amplo diálogo, sempre característica desta Ilustre Secretaria, a Cisco solicita uma extensão de prazo de 90 dias para apresentação de seus comentários e contribuições.

**RESPOSTA**

A Consulta não será prorrogada, mas os documentos estarão em contínua evolução, podendo receber proposta a qualquer momento e cada publicação será precedida de consulta pública.

**CONTRIBUIÇÃO 2: Victor Jardim da BSA | The Software Alliance1 e *Information Technology Industry Council* (ITI)**

Vimos por meio dessa requerer, respeitosamente, uma oportunidade para discutir as propostas atuais em uma reunião presencial com o governo, no início de 2015. Nesse mote, tomamos a liberdade de recomendar ao Governo Brasileiro, com o devido respeito, que postergue a finalização das diretrizes de implementação ao menos até que tenha a oportunidade de conduzir consultas técnicas com os representantes da indústria afetados. Apesar de não podermos oferecer comentários técnicos abrangentes neste documento, conforme mencionado acima, propomos uma reunião presencial para termos uma discussão substancial sobre os objetivos e os aspectos técnicos dos documentos. Destacamos abaixo algumas preocupações gerais relativas à abordagem proposta. Desvio em relação aos padrões globais: No documento “Conjunto de Características, Critérios e Medidas para Auditorias de Segurança da Informação

em Programas e Equipamentos, Versão 01 de Julho de 2014", a seção 4.2 (Avaliação de Riscos de Segurança), parece nos que se reafirmam muitos aspectos dos padrões globais para a garantia de produtos. No entanto, o documento parece propor uma série de ajustes nacionais a padrões globais. O desvio em relação aos padrões globais na implementação nacional poderá gerar consequências negativas. Em primeiro lugar, ele elevará os custos para o governo, já que os fornecedores de TIC deverão criar conjuntos de produtos novos e diferenciados para atender aos padrões locais, eliminando a economia de escala na produção, que permite que governos obtenham produtos da maior qualidade a preços baixos. Em segundo lugar, os padrões nacionais danificariam a competitividade global de empresas locais de pequeno e médio porte. Forçadas a criar produtos em conformidade com padrões nacionais para conquistar contratos no Brasil, as empresas locais se tornariam incapazes de competir globalmente. Foco em auditorias: A abordagem do Brasil parece concentrar-se na auditoria de programas e equipamentos. Mesmo que auditorias possam oferecer certos benefícios dentro de um contexto mais amplo de segurança da informação, estamos preocupados com o foco restrito e exclusivo em auditorias de software e equipamentos para a segurança das comunicações do Brasil. Tal abordagem supõe que o risco é gerado apenas no equipamento a ser adquirido, e ignora alguns dos mais importantes indicadores de risco digital em uma organização, especificamente o papel crucial da missão ou do programa, e do uso pretendido dos bens e serviços adquiridos para o apoio à missão ou o programa. A adoção de tal abordagem poderia deixar o governo brasileiro vulnerável a uma variedade de riscos de segurança digital decorrentes de pessoas e processos, assim como a forma como o governo usa um determinado item de tecnologia. Para atingir as metas de cibersegurança aprimorada nos dados e sistemas de comunicação, sugerimos um foco em gestão de risco de cibersegurança, e não simplesmente na auditoria de equipamentos. Foco no exame da propriedade intelectual (IP) de produtos de TIC: O foco na obtenção propriedade intelectual de fornecedores, como documentos, modelos, diagramas e código-fonte, também terá um impacto negativo. Muitos fornecedores globais, muitos dos quais produzem as tecnologias de ponta em segurança que o governo brasileiro busca, provavelmente não participarão de licitações que exijam que se entregue ou disponibilize propriedade intelectual, como código-fonte ou outras informações de projeto. Isto privaria o governo brasileiro de algumas das tecnologias de ponta das quais poderia precisar para proteger seus sistemas. Descrições prescritivas sobre o que a tecnologia deve fazer: Alguns dos documentos contêm detalhes extensivos sobre as funções técnicas, características e capacidades de produtos a serem licitados. Enquanto políticas de licitação devem especificar certos objetivos de segurança, as decisões relativas à maneira pela qual tais objetivos são atendidos (tal como quais tecnologias serão usadas, ou quais funções específicas cada tecnologia deverá ter) deveriam ser deixadas a cargo do fornecedor que deseja vender à entidade governamental, ou, no caso de especificações funcionais, ser abordadas em contratos individuais.

**RESPOSTA**

Sobre desvio dos padrões globais: Contribuição não procede já que foi uma preocupação, desde o inicio dos

trabalhos, de não “inventarmos” nada. A única diretriz que pode causar estranhamento ao mercado é que já no inicio dos trabalhos acordamos que só seriam referenciadas mais fortemente normas de padrão brasileiro (NBRs). As normas internacionais 15408, série 27.000 e mesmo normas nacionais de outros países foram usadas, livremente adaptadas(copiadas), serviram de inspiração e referencia informal, mas o grupo não tem e não teve intenção de adaptar de maneira forçada nenhuma norma internacional que não tenha NBR aprovada e publicada. Quanto ao “Foco no exame da propriedade intelectual (IP) de produtos de TIC: O foco na obtenção propriedade intelectual de fornecedores, como documentos, modelos, diagramas e código-fonte”: A Administração Pública Federal Direta, Autárquica e Fundacional Operam (ou demandam a operação de) sistemas, produtos e serviços de TIC com diferentes níveis de criticidade e importância para o cumprimento de suas missões, diferentes níveis de serviço, diferentes impactos para a continuidade de suas operações, lidando com informações de diferentes níveis de classificação de sigilo, dentre muitas variáveis.
Os documentos ora em consulta, considerando a complexidade acima citada, preveem os diferentes perfis de missão de futuras especificações de contratação e especificações de auditoria e lidam com tal complexidade ao determinar níveis de criticidade desses perfis de missão, controles e componentes funcionais a serem especificados para auditoria, contratação e operação dos serviços previstos no Decreto 8135/2013, inspirado-se para isso em padrões nacionais e internacionais de Segurança da Informação, de gestão da segurança da informação, de auditoria. Além disso, está publicado ainda um cronograma da adoção desses componentes.

Dessa forma, o documento prevê uma série de condições em que diferentes níveis de auditoria e, portanto, diferentes níveis de acesso as tecnologias envolvidas serão especificados para a contratação, operação ou auditoria desses serviços, caso a caso.

Assim como em outros casos da atuação de organizações de governo, de normatização e padronização, de metrologia, de agências, etc, não há intenção de ferir Propriedade Intelectual e são seguidos mecanismos de compartilhamento de códigos-fonte e afins com o devido tratamento de confidencialidade.

Para alguns casos especificados de acordo com os documentos ora em Consulta, será necessário, inevitável e indispensável acesso a maiores partes das tecnologias e documentações dos serviços, mais uma vez, caso a caso.

O documento prevê também casos em que tais acessos serão facilitados, por exemplo, quando houver o uso de tecnologias livres.

**CONTRIBUIÇÃO 3: Anselmo Gentile da ABES - Associação Brasileira das Empresas de Software**

Consideramos que o prazo oferecido para as manifestações, mesmo considerando a prorrogação concedida pela SLTI, foi exíguo para apresentar uma análise no nível de detalhamento que o tema exige. Propomos a montagem de um grupo de trabalho composto por representantes da indústria e do governo.

1) Orientações Técnicas Extrapolam o Escopo do Decreto: Ocorre, entretanto, que as orientações apresentadas nos documentos oferecidos à consulta pública vão muito além deste escopo, abrangendo temas como a computação em nuvem de forma generalizada e apresentando apêndices detalhados para questões que ultrapassam o âmbito do "serviço de correio eletrônico e funcionalidades complementares".

2) Aderência a Padrões Internacionais Para que o Governo Brasileiro possa implementar o disposto no Decreto nº 8135/13 e nas portarias complementares, seria essencial a aderência a padrões técnicos internacionais. Embora esteja claro que os documentos tenham sido baseados na norma ISO / IEC 14508 (*Common Criteria for Information Technology Security Evaluation*), não está claro se outras normas internacionais também foram consideradas na elaboração do documento.

3) Prover um Mapa dos Padrões e Controles Utilizados No texto dos documentos apresentados, não é possível identificar quais componentes são baseados em quais padrões e seus respectivos controles associados, bem como se existem novos requisitos técnicos criados que não podem ser remetidos a nenhum padrão internacional.

4) Foco restrito em auditoria. A adoção dessa abordagem, com foco restrito em auditoria, pode deixar o Governo Brasileiro vulnerável a uma miríade de riscos cibernéticos que podem originar-se de pessoas, de processos, e de como as agências públicas utilizam certos elementos tecnológicos. Sugerimos a ampliação do foco para a gestão de riscos cibernéticos, e não exclusivamente na auditoria de equipamentos.

5) Suporte à Neutralidade de Tecnologia É de suma importância para todos os governos apoiar a neutralidade tecnológica nas suas aquisições, e como citado anteriormente, a adoção de padrões internacionais. Apesar do software de código fonte aberto exercer papel fundamental na indústria, as orientações apresentadas devem suportar a neutralidade tecnológica e não sugerir nenhum tipo de preferência a modelos de desenvolvimento específicos, posto que os critérios de segurança apresentados serão o crivo maior para justificar a adoção ou não de qualquer solução. A primazia na adoção de software público ou de código fonte aberto não basta para assegurar atendimento com maior eficiência dos requisitos de garantia e segurança, nem são suficientes para reduzir os investimentos que o Governo fará no atendimento dos resultados almejados pelo Decreto.

6) Acesso ao Código Fonte dos Programas Utilizados Muitos fornecedores de soluções possuem restrições à liberação dos códigos fontes de seus programas e eventualmente podem deixar de participar de processos licitatórios caso este requisito tenha peso significativo na determinação dos níveis de segurança exigidos pelo contratante.

7) Computação em Nuvem Embora, sem dúvida, a computação em nuvem esteja fora do âmbito do Decreto nº 8135/13, foram detectados diversos destaques nas orientações apresentadas que atingem os serviços disponibilizados por essa plataforma. Antes que os documentos da consulta pública sejam finalizados, é importante considerar os impactos no requerimento de que toda a plataforma de nuvem utilizada pelo

governo brasileiro seja privada. Sugerimos também que a sessão de computação em nuvem seja atrelada especificamente ao teor do Decreto nº 8135, como consta em seu escopo: “comunicações de dados da administração pública federal direta, autárquica e fundacional”.

8) Descrições prescritivas sobre o que a tecnologia deve fazer Alguns dos documentos contem detalhes completos sobre as técnicas, funções e características dos produtos a serem adquiridos. Embora seja aceitável para as políticas de contratação especificar os objetivos de segurança, as decisões a respeito de como atingir esses objetivos (quais tecnologias utilizar ou quais funções implementar) deveriam ser delegadas ao fornecedor.

9) Exemplo: análise técnica sobre utilização do *Common Criteria* como consta nos documentos da consulta pública A despeito do pouco tempo disponibilizado para analisar tecnicamente todos os assuntos apresentados nos documentos que compõe a consulta pública, gostaríamos de oferecer um exemplo técnico para demonstrar porque consideramos importante estabelecer uma agenda de reuniões para melhor debater este e outros aspectos relevantes e essenciais desta consulta. Melhorar as referências ao *Common Criteria* (ISO / IEC 15408): a abordagem descrita nas orientações poderia ser uma base para o descrever os requisitos funcionais e de garantia da segurança para os produtos e serviços de TI abrangidos pelo Decreto Presidencial. Este é apenas um exemplo de uma área muito técnica em que as orientações atuais não refletem algo facilmente implementável atualmente.

**RESPOSTA**

**Resposta ao preâmbulo da contribuição**

Ver resposta da CONTRIBUIÇÃO 1

**Resposta ao item 1) Orientações Técnicas Extrapolam o Escopo do Decreto**

Afirmamos tratar-se de considerações e recomendações quanto à responsabilidade para realização de auditorias de software e hardware no paradigma de computação em nuvem nos diferentes modelos de serviço quando contratada por órgão da APF no escopo dos serviços constantes do Decreto º 8.135/2013. As particularidades deste tipo de tecnologia impõem a necessidade de considerações especiais de segurança para os recursos e serviços do Decreto º 8.135/2013, quando oferecidos na forma de computação em nuvem. Assim entendemos que não foi extrapolado o escopo do Decreto. Entretanto, para evitar uma interpretação equivocada do documento, vamos fazer a revisão do texto para que fique claro que as recomendações estão restritas aos serviços de correio eletrônico, compartilhamento e sincronização de arquivos, mensageria instantânea, conferência (teleconferência, telepresença e *webconferência*) e comunicação de voz sobre protocolo de internet (VoIP), quando prestados no modelo de computação em nuvem.

**Resposta ao item 2) Aderência a Padrões Internacionais**

As especificações técnicas de segurança relatadas neste documento são baseadas parcialmente em uma norma internacional, referência em se tratando de segurança em tecnologia da informação, a ISO/IEC 15408 (*Information technology — Security techniques — Evaluation criteria for IT security*). Esta norma foi desenvolvida pelo comitê técnico ISO/IEC em colaboração com o projeto conhecido como "*Common Criteria*". A ISO/IEC 15408 foi selecionada como base devido ao seu caráter genérico, isto é, por ser potencialmente aplicável à avaliação de segurança de qualquer produto TIC, e também pela sua ampla aceitação na indústria e academia. As normas internacionais 15408, série 27.000 e mesmo normas nacionais de outros países foram usadas livremente adaptadas e serviram de inspiração e referencia informal, mas o grupo não tem e não teve intenção de adaptar de maneira forçada nenhuma norma internacional que não tenha NBR aprovada e publicada.

**Resposta ao item 3) Prover um Mapa dos Padrões e Controles Utilizados**

No momento não é possível prover tal ferramenta. Entretanto, acreditamos que com a evolução dos trabalhos por parte dos GTs formados no âmbito da e-PING, este "Mapa" seja desenhado.

**Resposta ao item 4) Foco restrito em auditoria.**

Uma adequada Gestão de Riscos é imprescindível para um trabalho satisfatório no tocante à Gestão de Segurança da Informação. Impende destacar, porém, que o trabalho submetido a comentários públicos tinha como o foco definir características que permitissem auditoria, em programas e equipamentos, para fins de garantia da disponibilidade, integridade, confidencialidade e autenticidade, consoante o que disciplina o Decreto nº 8.135/2013, e a Portaria Interministerial nº 141, de 2 de maio de 2014.

**Resposta ao item 5) Suporte à Neutralidade de Tecnologia**

O Governo Federal vem adotando uma política de favorecimento e incentivo ao uso e desenvolvimento do software livre no Brasil. Isso não significa, entretanto, uma proibição ao uso de soluções proprietárias. Nesse sentido, o Decreto nº 8.135/2013, e a Portaria Interministerial nº 141, de 2 de maio de 2014, não trazem inovação, apenas respeitam diretrizes anteriormente definidas.

O grupo de trabalho tem se empenhado para garantir a neutralidade de tecnologia, buscando padrões reconhecidos que adotam essa pratica. Nenhuma tecnologia terá privilegio em detrimento de outra. Todo o esforço se pauta a estabelecer regras claras para a Administração Pública, proporcionando maior transparência, qualidade e interoperabilidade, com foco nas características e segurança dispostos no Decreto.

**Resposta ao item 6) Acesso ao Código Fonte dos Programas Utilizados**

A Administração Pública, na condição de contratante/demandante, deve direcionar a especificação dos requisitos de suas soluções tecnológicas de forma a viabilizar tecnicamente o seu negócio visando a eficiência, eficácia, segurança e economicidade dos serviços públicos a serem prestados utilizando-se as

soluções contratadas. Da mesma forma, é importante que a participação dos fornecedores de soluções tecnológicas nos processos licitatórios seja cada vez maior. Assim sendo, entendimentos são necessários no sentido de minimizar estas restrições por parte dos fornecedores, quando estas forem essenciais para garantir a segurança da informação e a conformidade com o Decreto nº 8.135/13 (dependendo do nível de criticidade e da profundidade da auditoria).

**Resposta ao item 7) Computação em nuvem**

Apesar de o documento explicitar que a seção de nuvem foi colocada apenas para a divisão de responsabilidades na auditoria de programas no caso de diferentes configurações de serviços de nuvem, vamos revisar para deixar isto mais claro, retirando qualquer referencia a serviços não incluídos no Decreto º 8.135/2013.

**Resposta ao item 8) Descrições prescritivas sobre o que a tecnologia deve fazer**

O conjunto de características, critérios, condições mínimas e medidas para auditoria de segurança da informação em programas e equipamentos apresentados no documento estão abertos a discussão e revisão. A exigência ou não de um componente implementado pode ser especificado em cada compra/licitação por parte do órgão contratante, observando sempre a adequação destes requisitos a suas necessidades de negócio e ao disposto no Decreto nº 8.135/2013.

**Resposta o item 9) Exemplo: análise técnica sobre utilização do *Common Criteria* como consta nos documentos da consulta pública**

O modelo de trabalho adotado pelos Grupos de Trabalho (GT) vinculados à Coordenação de Padrões de Interoperabilidade de Governo Eletrônico (e-PING) prevê a possibilidade de participação de diferentes atores. É importante salientar que os trabalhos realizados, e posteriormente submetidos à consulta pública, constituem-se versão inicial, que serão devidamente refinados, consideradas as contribuições recebidas durante a consulta pública, bem como, as que serão recebidas na Audiência Pública, que ocorrerá (na data provável de 12/03/15). Cabe salientar, que os documentos estarão em contínua evolução, podendo receber propostas de alteração a qualquer momento, e que cada publicação será precedida de consulta pública. Portanto, os canais de comunicação entre as partes interessadas não foram e nem devem ser interrompidos. A participação e atuação em rede, de fato, podem contribuir para a resolução de demandas complexas.

**CONTRIBUIÇÃO 4: Brasscom - Associação Brasileira de Empresas de Tecnologia da Informação e Comunicação**

Se faz necessário um tempo mais dilatado para uma análise detalhada e a concepção de contribuições relevantes. não observamos, nos documentos apresentados, nenhum indício de aproximação com órgãos

certificadores e auditores mundialmente reconhecidos, como foi, por nós, sugerido em correspondências anteriores. O Brasil corre o risco de se isolar técnica, operacional e economicamente em um setor marcadamente globalizado. Respeitosamente solicitamos:

I.Que seja postergada a publicação de novas medidas infralegais sobre o tema, de modo a dar ensejo a um amplo debate com o setor de TIC.

II.Que a Brasscom seja formalmente convidada a participar dos grupos de trabalho relevantes ao processo, na qualidade de representante setorial, nos moldes em que já o faz em diversas outras instâncias.

III.Que seja agendada uma reunião ministerial para que apresentemos uma perspectiva ampliada sobre o tema, concebida com aporte e apoio dos nossos Associados, dentre os quais estão as maiores empresas do Brasil e do mundo.

**RESPOSTA**

I) A Consulta não será prorrogada, mas os documentos estarão em contínua evolução, podendo receber proposta a qualquer momento e cada publicação será precedida de consulta pública.

II) Não procede a contribuição já que as definições serão feitas apenas no âmbito do governo, podendo outros interessados participar pelo envio de propostas a qualquer momento e em especial nas consultas públicas.

III) Uma audiência pública será agendada para uma discussão presencial sobre temas relevantes ao Decreto nº 8.135/2013.