Ministério do Planejamento, Orçamento e Gestão
Secretaria de Logística e Tecnologia da Informação
Departamento de Governo Eletrônico
www.governoeletronico.gov.br

gov.br
ePING

Padrões de Interoperabilidade de Governo Eletrônico

Respostas aos questionamentos encaminhados à Consulta Pública 2014

BRASIL

Item: Minuta do Documento de Referência da ePING 2015

Contribuição 1: Promover HTML 5 para adotado.

Justificativa: As especificações do padrão foram concluídas e o mesmo tornou-se recomendação do W3C a partir de 28 de outubro de 2014.

Responsável: Hudson Vinícius Mesquita

Resposta:

Caro Hudson,

Obrigado por contribuir no processo de aperfeiçoamento da versão 2015 do documento de referência da ePING.

Em atenção a sua contribuição, informamos que a mesma foi **aceita**.

Atenciosamente,

Coordenação da e-PING

Contribuição 2: Repensar, por completo, as razões de existir do ePING.

Justificativa: Antes de uma contribuição, esta é uma crítica à função geral do ePING. Uma dúvida que se levanta entre muitos que tomam conhecimento do ePING é a seguinte: para que serve, exatamente, o ePING? Quer dizer, quais são os problemas específicos a que ele visa a responder? É claro que há utilidade em se promover maior integração, ou interoperabilidade, entre sistemas; mas isso está dito de maneira demasiado abstrata. Quais integrações específicas, quais interoperabilidades, querem-se promover? Sem essa definição clara não se saberá se o ePING alcançou ou alcançará seus objetivos. Sem definição clara do problema, perde-se, ainda, o foco. O ePING hoje parece-me apenas uma lista de uma série de padrões os quais, em sua maioria, já estão consagrados. Não vejo necessidade de se ter um documento dizendo que os órgãos devem usar SMTP para correio, ou DNS para tradução de nomes de domínio, e assim por diante. Do jeito que está, estamos apenas repetindo as conclusões a que a comunidade (W3C etc.) já chegou faz tempos. Dito isso, sugeriria o foco em determinados problemas que, de fato, necessitem de padronização. Por exemplo, há muitos dados de outros órgãos aos quais um órgão poderia ter acesso; como se dá essa integração? Via serviço? Como publicá-lo? E assim por diante. Haveria de se estudarem, ainda, as causa que têm inviabilizado essa integração; é possível que, após estudos, cheguemos à conclusão de que o problema não é de falta de padrões, mas de falta de recursos, dificuldade técnica, dentre outros fatores. (Nesse caso, de nada adiantaria o estabelecimento de padrões). Tais estudos poderiam resultar em documentos de ?use cases?, ou de melhores práticas, os quais conteriam, acidentalmente, sugestões de padronização com base no sucesso que obtiveram em implementação real. Tais esforços resultariam em documento de orientação mais útil do que, apenas, o estabelecimento de padrões fora de contexto.

Responsável: Gustavo Henrique Maultasch de Oliveira

Resposta:

Caro Gustavo,

Obrigado por contribuir no processo de aperfeiçoamento da versão 2015 do documento de referência da ePING.

Em atenção a sua contribuição, informamos que a mesma foi **aceita**.

Entendemos que a definição de padrões de interoperabilidade por parte do governo foi importante para auxiliar os órgãos em aumentar sua maturidade nas contratações de TI ao longo dos últimos 10 anos. Por outro lado, é consenso dentro dos grupos da ePING que essa função já foi cumprida e encontra-se estável, e ao longo de 2014 foram definidas novas ações pela Comissão de Coordenação da ePING, visando auxiliar os órgãos no intercâmbio de dados e informações. Entre essas ações destacamos o desenvolvimento de um sítio para o governo eletrônico em 2015, onde teremos uma seção para interoperabilidade que conterá conteúdos sobre ferramentas, casos de uso, referências e modelos de implementação, padrões, entre outros, o que está bastante alinhado com suas sugestões.

Cabe destacar que o objetivo de um documento de padronização é justamente elicitar o óbvio, considerando os componentes aceitos pelo governo federal.

Atenciosamente,

Coordenação da e-PING

Contribuição 3: Em nome da IBM Brasil, gostaria de saudar a SLTI pela iniciativa em submeter à consulta pública as propostas de Padrões de Interoperabilidade de Governo Eletrônico ? ePING, para 2015. Neste momento, as contribuições da IBM Brasil dirigem-se mais à forma, do que ao conteúdo. Acreditamos que a janela de oportunidade aberta pelo governo para a discussão de temas fundamentais para a comunidade da segurança da informação ? como o padrão de correios eletrônicos e os critérios de auditoria de segurança ? mereça ter seu prazo consideravelmente estendido, de modo a possibilitar contribuições consistentes do setor. O fato de que tais propostas estejam vinculadas a um ato assinado pela Presidenta da República ? o Decreto 8135/2013 ? revela sua dimensão estratégica, de modo que discussões a elas relativas não possam se restringir a consultas públicas com prazos tão exíguos (35 dias). Diante disso, a IBM Brasil propõe: 1. O adiamento da consulta para o primeiro semestre de 2015. 2. Que a consulta pública seja precedida de um amplo debate com as empresas do setor e com a sociedade civil, inclusive para absorção de experiências internacionais referentes a padrões de interoperabilidade de governo eletrônico. Há 96 anos no Brasil, a IBM é um dos maiores empregadores da indústria de serviços de tecnologia, segue investindo na expansão de seus negócios, na formação de mão de obra e desempenha um importante papel no desenvolvimento de soluções inovadoras para endereçar os principais desafios tecnológicos da atualidade e das próximas décadas. Por oportuno, a IBM Brasil reafirma

seu compromisso em desenvolver globalmente serviços de tecnologia da informação cada vez mais eficientes e comprometidos com a segurança de seus clientes governamentais e privados. Agradecendo antecipadamente a atenção e a consideração pelas propostas apresentadas, coloco-me à disposição para esclarecimentos adicionais.
Respeitosamente, Fabio Rua Diretor de Relações Governamentais e Políticas Públicas IBM Brasil

Justificativa: Vide acima

Responsável: Fabio Assumpção Ribeiro de Lima Rua

Resposta:

Caro Fábio,

Obrigado por contribuir no processo de aperfeiçoamento da versão 2015 do documento de referência da ePING.

Em atenção a sua contribuição, informamos que a mesma **não foi aceita,** pois a consulta já foi prorrogada anteriormente e uma nova prorrogação impactaria na publicação da versão 2015 da ePING.

De qualquer forma, mesmo com o encerramento do processo de consulta pública, contribuições à ePING, inclusive para o padrão de correios eletrônicos e os critérios de auditoria de segurança, podem ser feitas através do e-mail eping@planejamento.gov.br a qualquer momento.

Atenciosamente,

Coordenação da e-PING

Contribuição 4: Verificar padrões GML 3.3, PDF/A e Daisy 3 na tabela 12 do Segmento 3, pois apresentam inconsistências.

Justificativa: 1) O padrão GML 3.3 foi incluído na tabela com o status "R" e já existe o padrão GML 2.0 ou superior com o status "A". 2) Não deixaram nenhuma opção de uso do PDF, pois o PDF/A foi colocado em transição (status "T"). 3)Foi incluído o padrão Daisy 3, porém o mesmo executa somente padrão de áudio MP3 e AAC, que exigem pagamento de royalties para implementações; o que não condiz com o conceito de padrão aberto.

Responsável: Ana Paula Pessoa Mello

Resposta:

Prezada Ana,

Obrigado por contribuir no processo de aperfeiçoamento da versão 2015 do documento de referência da ePING.

Em atenção a sua contribuição, informamos que a mesma foi **aceita.**

Quanto ao padrão GML, manteremos a versão “2.0 ou superior” como recomendado.

O status do padrão PDF/a foi erroneamente alterado de “Recomendado” para “em transição”. O mesmo será retornado para “Recomendado”, para os casos em que for necessário preservação digital de documentos, e o padrão PDF será recomendado para as demais situações.

Referente ao Daisy 3, o mesmo será retirado.

Atenciosamente,

Coordenação da e-PING

Contribuição 5: São Paulo, 12 de dezembro de 2014. A ILUSTRÍSSIMA SECRETÁRIA SENHORA LORENI FORESTI SECRETARIA DE LOGÍSTICA E TECNOLOGIA DA INFORMAÇÃO MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO Ref.: Consulta publica 144 ? e-PING 2015 Prezada Senhora Loreni Foresti, A Cisco cumprimenta e parabeniza esta Secretaria de Logística e Tecnologia da Informação, do Ministério do Planejamento Orçamento e Gestão pela respeitável inciativa de colocar em consulta pública a proposta de Padrões de Interoperabilidade de Governo Eletrônico ? ePING, versão 2015. Recebemos em alta estima e consideração esta consulta, de suma importância para toda sociedade. Presente no Brasil desde 1994, constituída sob as leis brasileiras, tendo operações de fabricação em Sorocaba, Estado de São Paulo, a Cisco é uma empresa multinacional fabricante de equipamentos de telecomunicações e soluções de rede, com particular destaque para a produção de roteadores, dentre outros equipamentos. Profundamente comprometida e envolvida nos objetivos do Governo brasileiro e com as finalidades de fortalecimento da indústria no setor de telecomunicações e no estímulo às atividades de pesquisa e desenvolvimento tecnológico nacional, a Cisco faz continuamente e de forma permanente investimentos significativos no país na área de tecnologia da informação, como se pode destacar a implementação de um Centro de Inovação no Rio de Janeiro dedicado à produção local de soluções verticais de tecnologia, e parcerias firmadas com universidades brasileiras, empresas e entidades para o desenvolvimento conjunto de inovações. Neste contexto de compromisso em contribuir para a indústria nacional no setor de telecomunicações, na criação de postos de trabalho qualificados, o que em suma contribui para o fortalecimento da indústria de telecomunicações, 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. A Cisco tem acompanhado e contribuído nas discussões em torno das políticas de tecnologia da informação no país e também em outras legislações, levando conhecimento e compartilhando experiências, e gostaria de aproveitar esta oportunidade para melhor contribuir com esta Secretaria com seu know-how adquirido em por conta de sua atuação em outras jurisdições. 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. Na certeza da vossa compreensão sobre a necessidade e importância deste pedido, subscrevemo-nos com protestos de estima e consideração. Atenciosamente, Giuseppe Marrara Diretor Cisco do Brasil Ltda

Justificativa: Vide justificativa no documento anexo.

Responsável: Giuseppe Sidrim Marrara

Resposta:

Caro Giuseppe,

Obrigado por contribuir no processo de aperfeiçoamento da versão 2015 do documento de referência da ePING.

Em atenção a sua contribuição, informamos que a mesma **não foi aceita**, pois a consulta já foi prorrogada anteriormente e uma nova prorrogação impactaria na publicação da versão 2015 da ePING.

De qualquer forma, mesmo com o encerramento do prazo de contribuições, considerações sobre a ePING, incluindo todos os documentos disponibilizados nesta Consulta Pública, podem ser feitas através do e-mail eping@planejamento.gov.br a qualquer momento.

Atenciosamente,

Coordenação da e-PING

Item: Padrão de Formação de Endereços de Correio Eletrônico de Caixas Postais Individuais

Contribuição 1: a) REGRA PADRÃO Onde se lê: O endereço de correio eletrônico deverá ser formado pelo primeiro prenome seguido de um PONTO (.) seguido do último sobrenome. Leia-se: A composição do endereço de correio eletrônico deverá obedecer à Regra Padrão devendo ser formada primeiro prenome seguido de um PONTO (.) seguido do último sobrenome. A Regra Padrão para criação de endereço de correio eletrônico destina-se a uniformizar a sua estrutura, para que o destinatário de uma mensagem possa ser identificado e localizado de maneira rápida, única e segura.

Justificativa: O tópico é sobre a Regra Padrão, então a nova redação dá ênfase a essa.

Responsável: RICARDO GAROFALO LOOS

Resposta:

Caro Ricardo,

Obrigado por contribuir no processo de aperfeiçoamento da versão 2015 do documento de referência da ePING.

Em atenção a sua contribuição, informamos que a mesma foi **aceita**.

Atenciosamente,

Coordenação da e-PING

Contribuição 2: b) EXCEÇÕES Onde se lê: A composição do endereço de correio eletrônico deverá obedecer à Regra Padrão de formação, destinada a uniformizar a sua estrutura, para que o destinatário de uma mensagem possa ser identificado e localizado de maneira rápida, única e segura. Contudo, nos casos definidos abaixo os usuários poderão solicitar, junto à área de TI do órgão, a utilização das Regras para Exceção para formação dos endereços. Leia-se: Os casos abaixo definidos constituem as Regras para Exceção, devendo os usuários solicitar junto à área de TI do órgão, a utilização das mesmas para formação do endereço eletrônico.

Justificativa: A parte da Regra Padrão foi transferida para aquele tópico.

Responsável: RICARDO GAROFALO LOOS

Resposta:

Caro Ricardo,

Obrigado por contribuir no processo de aperfeiçoamento da versão 2015 do documento de referência da ePING.

Em atenção a sua contribuição, informamos que a mesma foi **aceita**.

Atenciosamente,

Coordenação da e-PING

Contribuição 3: Inciso 2 Onde se lê: meio social Leia-se: meio social e de trabalho

Justificativa: Como o usuário é conhecido também no meio de trabalho (funcional)

Responsável: RICARDO GAROFALO LOOS

Comentários De forma resumida, as definições sobre meio social consideram a cultura em que um individuo foi criado e vive, e as pessoas e instituições com as quais ele interage. Minha preocupação quanto a distinção entre meio social e de trabalho é abrir espaço para contribuições que sugiram separar também os meios educacional, familiar, religioso ou qualquer outro ambiente que alguém queira destacar. De qualquer forma, se acharem por bem ser mais ponderado, sugiro a seguinte redação: "O usuário ser conhecido no seu meio social, inclusive profissional, pelo nome composto ou por outro sobrenome que não seja o definido pela regra padrão; ou"
Responsável: Hudson Vinícius Mesquita

Resposta:

Caro Ricardo,

Obrigado por contribuir no processo de aperfeiçoamento da versão 2015 do documento de referência da ePING.

Em atenção a sua contribuição, informamos que a mesma foi **aceita**.

O item passará a ter a seguinte redação: "O usuário ser conhecido no seu meio social, inclusive profissional, pelo nome composto ou por outro sobrenome que não seja o definido pela regra padrão; ou"

Atenciosamente,

Coordenação da e-PING

Contribuição 4: APRESENTAÇÃO Onde se lê: O objetivo desta publicação é definir o padrão a ser adotado na formação e criação de endereços de correio eletrônico (e-mails) dos órgãos da Administração Pública Federal direta, autárquica e fundacional, e os das demais organizações públicas que se utilizarem do serviço de mensageria do Governo Federal. Leia-se: O objetivo desta publicação é definir o padrão a ser adotado na formação e criação de endereços de correio eletrônico (e-mails) dos servidores, empregados, ocupantes de funções e contratados de órgãos da Administração Pública Federal direta, autárquica e fundacional, e os das demais organizações públicas que se

utilizarem do serviço de mensagens do Governo Federal

Justificativa: criação dos endereços é para os usuários e não dos órgãos. Conforme o Aurélio, não existe a palavra mensageria.

Responsável: RICARDO GAROFALO LOOS

Resposta:

Caro Ricardo,

Obrigado por contribuir no processo de aperfeiçoamento da versão 2015 do documento de referência da ePING.

Em atenção a sua contribuição, informamos que a mesma foi **aceita**.

Atenciosamente,

Coordenação da e-PING

Contribuição 5: Utilizar o mesmo exemplo dos documentos anteriores. "JOAQUIM JOSÉ DA SILVA XAVIER 2.2 Para efeito de formação do nome que vai aparecer no e-mail, o nome do usuário é decomposto em três partes: PRENOME (ou primeiro nome) JOAQUIM NOME(S) INTERMEDIÁRIO(S) JOSÉ DA SILVA SOBRENOME (ou último nome) XAVIER "

Justificativa: os exemplos utilizados no documento "CAIXAS POSTAIS INDIVIDUAIS FUNCIONAIS", creio que de 2001/2002 e republicado, creio que em 2011, são mais interessantes.

Responsável: Debora Botner Libman

Comentários Um NOME é FORMADO por PRENOME (simples ou composto) e por SOBRENOME (materno e paterno). Não existe nome intermediário. O nome Joaquim José da Silva Xavier é formado um prenome composto-Joaquim José e por dois sobrenomes-da Silva e Xavier
Responsável: RICARDO GAROFALO LOOS

Resposta:

Prezada Débora,

Obrigado por contribuir no processo de aperfeiçoamento da versão 2015 do documento de referência da e-PING.

Em atenção a sua contribuição, informamos que a mesma foi **rejeitada**.

O Código Civil Brasileiro, definido pela Lei Nº 10.406 de 10 de janeiro de 2002, estabelece

que o nome é compreendido apenas do prenome e sobrenome. Assim, o nome dito intermediário não está previsto legalmente. Portanto, na contribuição apresentada o prenome possui característica composta, ou seja, formado por dois nomes.

Atenciosamente,

Coordenação da e-PING

Contribuições enviadas pela Embratel para o e-mail eping@planejamento.gov.br

Contribuição 1)

Minuta do Documento de Referência da ePING 2015
Item: 6. Interconexão - Tabela 2 – Rede/Transporte
Texto do item: “Comutação por Label - Quando necessário, o tráfego de rede pode ser otimizado pelo uso do MPLS (RFC 3031), devendo este possuir, no mínimo, quatro classes de serviço.”

Contribuição: alterar o texto do item da seguinte forma:

Esclarecer que no caso de interconexão com a rede pública com comutação por label, não haverá troca de Label entre a rede privada do governo e a rede pública. Neste caso deve-se adotar interface NNI (Option A)entre a rede do governo e a rede pública.

Justificativa: Isolar os domínios de MPLS para evitar problemas de segurança, de gerenciamento de endereços IP e de sobrecarga de tabelas de labels que possam afetar ambas as redes.

Resposta à contribuição:
Em atenção a sua contribuição, informamos que a mesma foi **aceita**.

Contribuição 2)

Minuta do Documento de Referência da ePING 2015

Critérios de Auditoria de Segurança - Decreto 8.135/2013

Anexo B: Diretrizes para o planejamento, desenvolvimento, implantação e operação de serviços VoIP

Item B.3
Incluir Suporte a Tronco SIP para interconexão de PABX IP à PSTN.

Justificativa: A evolução tecnológica e a popularização dos PABX IP no mercado tende a reduzir os investimentos em acessos TDM para conexão à PSTN por parte das operadoras. Assim pode-se reduzir os gastos com Gateways de voz.

Resposta à contribuição:
Em atenção a sua contribuição, informamos que todas as contribuições relacionadas aos Decreto 8.135/2013 serão analisadas e respondidas por grupo de trabalho a ser instituído pelo Ministério do Planejamento no início de 2015.

Contribuição 3)

Minuta do Documento de Referência da ePING 2015
Item: 2.1. Políticas Gerais nas Dimensões. 2.1.1. Dimensão Técnica. Adoção de navegadores (browsers)
Texto do Item: "Como principal meio de acesso, todos os sistemas de informação de governo deverão ser acessíveis, preferencialmente, por meio de tecnologia baseada em browser. Outras interfaces são permitidas em situações específicas, como em rotinas de atualização e captação de dados onde não haja alternativa tecnológica disponível baseada em navegadores."

Contribuição: alterar o texto do item da seguinte forma:
Como meio de acesso, todos os sistemas de informação de governo deverão ser acessíveis, preferencialmente, por meio de tecnologia baseada em browser, quando esta tecnologia se mostrar a mais adequada, dentre as tecnologias disponíveis, ao nível de segurança requerido pelo serviço. Outras interfaces são permitidas em situações específicas, como em rotinas de atualização e captação de dados onde não haja alternativa tecnológica disponível baseada em navegadores.

Justificativa: Deve-se privilegiar a utilização de meio de acesso por meio de tecnologia que melhor se adeque ao nível de segurança requerido pelo serviço.

Resposta à contribuição:
Em atenção a sua contribuição, informamos que a mesma foi **aceita**.

Contribuição 4)

Minuta do Documento de Referência da ePING 2015
Item: 7. Segurança - Tabela 11 – Auditoria em programas e equipamentos
Texto do item: Serviços de tecnologia da informação, conforme definidos no art. 11 da Portaria Interministerial MP/MC/MD nº 141 de 02/05/2014 – **TELEBRÁS** - INSTRUÇÃO NORMATIVA – ANEXO DA CONTRATAÇÃO DE LINKS DE COMUNICAÇÃO.

Tabela Página 6

Item:

"Serviço de Rede de Comutação de Pacotes VPN/IP (MPLS)"
(...)
"Interfaces Padrão Ethernet"

Contribuição: alterar o texto da seguinte forma:
Interfaces Padrão Ethernet ou Padrão PDH europeu, com multiplexação TDM na taxas nas taxas de n x 2 Mbit/s (sendo "n" de 1 a 4) e interfaces Padrão SDH, nas taxas de 155 Mbit/s, 622 Mbit/s.

Justificativa: "Não limitar os padrões de atendimento para diferentes taxas de transmissão e recepção, sempre buscando maior isonomia e economicidade entre os fornecedores, bem como maior disponibilidade e eficiência na prestação dos serviços.

Resposta à contribuição:
Em atenção a sua contribuição, informamos que todas as contribuições relacionadas aos Decreto 8.135/2013 serão analisadas e respondidas por grupo de trabalho a ser instituído pelo Ministério do Planejamento no início de 2015.

Contribuição 5)

Minuta do Documento de Referência da ePING 2015

Item: 2. Politicas Gerais
Adoção Preferencial de Padrões Abertos
Texto do Item: "A ePING define que, sempre que possível, serão adotados padrões abertos nas especificações técnicas. Padrões proprietários são aceitos, de forma transitória, mantendo-se as perspectivas de substituição assim que houver condições de migração. Sem prejuízo dessas metas, serão respeitadas as situações em que haja necessidade de consideração de requisitos de segurança e integridade de informações."

Contribuição:
A ePING define que, sempre que possível, serão adotados padrões abertos nas especificações técnicas. Padrões proprietários são aceitos nas seguintes condições:

1) de forma transitória, mantendo se as perspectivas de substituição assim que houver condições de migração

2) quando da inexistência de padrão aberto, na qual poderão ser adotados padrões proprietários até que um padrão aberto esteja disponível.

Sem prejuízo dessas metas, serão respeitadas as situações em que haja necessidade de consideração de requisitos de segurança e integridade de informações.

Justificativa:
Evitar imposição de restrições para situações em que não existam padrões abertos ou que os padrões abertas não estejam num grau de maturidade satisfatório que possa incorrer em riscos para os órgãos do governo federal.

Resposta à contribuição:
Em atenção a sua contribuição, informamos que a mesma foi **aceita**.

Contribuição 6)

Critérios de Auditoria de Segurança - Decreto 8.135/2013

Item:
xiii) Especificação de informação sigilosa (informação de identificação que deve ser conhecida apenas pelo usuário autorizado
Componente 1: Verificação de informação sigilosa

Texto do Item: "O FSA deve prover mecanismos para verificar que informações sigilosas satisfaçam: [métrica de qualidade]."

Contribuição:
“O FSA deve prover mecanismos para verificar que informações sigilosas satisfaçam: [metrica de classificação da informação].”
Ou
“O FSA deve prover mecanismos para verificar que informacões sigilosas satisfaçam: [metrica de sigilo].”

Justificativa:
Métrica de qualidade não caracteriza necessidade de confidencialidade.

Resposta à contribuição:
Em atenção a sua contribuição, informamos que todas as contribuições relacionadas aos Decreto 8.135/2013 serão analisadas e respondidas por grupo de trabalho a ser instituído pelo Ministério do Planejamento no início de 2015.

Contribuição 7)

Critérios de Auditoria de Segurança - Decreto 8.135/2013

Item: 4.2.3. Análise de Segurança
2. Requisitos de Identificação, autenticação e autorização
Item 2.7

Texto do Item: “A solução deverá prover canal seguro de comunicação para autenticação, com utilização de HTTPS, seguindo regras do item Canal Seguro de Comunicação.”

Contribuição:
“A solução deverá prover canal seguro de comunicação para autenticação, com utilização de HTTPS, cujo certificado digital foi emitido por Autoridade Certificadora, seguindo regras do item Canal Seguro de Comunicação.”

Justificativa:
Evitar riscos de clone de sites ou ataques man-in-the-middle.

Resposta à contribuição:
Em atenção a sua contribuição, informamos que todas as contribuições relacionadas aos Decreto 8.135/2013 serão analisadas e respondidas por grupo de trabalho a ser instituído pelo Ministério do Planejamento no início de 2015.

Contribuição 8)

Minuta do Documento de Referência da ePING 2015
Item: Tabela 8 - Serviços de Rede:

Adicionar à tabela: Necessidade de monitoração 24 x 7

Justificativa: Instituições que lidam com informações confidenciais ou privativas de cidadãos devem estar preparadas para todo tipo de ataque cibernético. Tais ataques ocorrem não somente em horário comercial, mas sobretudo em horário fora do expediente normal, visto, em geral ser o momento de maior fragilidade das defesas. Esta fragilidade não deve ser permitida.

Adicionar à tabela: Necessidade de implementação de prevenção a intrusão:

Justificativa: Prevenção a intrusão é fundamental para inibir o acesso a dados confidenciais e privativos de cidadão, através da rede por parte de pessoas ou sistemas não autorizados;

Adicionar à tabela: Implementação de serviço de gestão de logs:

Justificativa: O armazenamento de logs é fundamental para permitir a forense computacional, método este necessário à identificação de ações ilícitas com dados confidenciais ou privativos de cidadãos. O armazenamento dos mesmos deve ser por período mínimo de 6 meses ou o requerido por lei.

Adicionar à tabela: Implementação de serviço de correlação de eventos de segurança:

Justificativa: Com a profissionalização dos atacantes e métodos cada vez mais avançados de ataque, identificar um intruso tem se tornado cada vez mais complexo. Para a identificação de ATP são necessárias ferramentas de correlação de logs em equipamentos de rede.

Resposta à contribuição:
Em atenção a sua contribuição, informamos que a mesma **não foi aceita.**
Em relação a defesa de perímetro da rede, entendemos que os Componentes descritos na Tabela 10 atendem as demandas para os temas apresentados, à exceção do monitoramento 24X7. Ocorre que a Norma Complementar nº 05/09 preve a criação de Equipes de Tratamento e Resposta a Incidentes de Segurança em Redes -ETIR, momento em que deve haver a definição da missão, a qual fornecerá a linha base para as atividades a serem desenvolvidas pela Equipe. Ou seja, se haverá atividades 24X7 é decisão de cada ETIR.

Contribuição 9)

Minuta do Documento de Referência da ePING 2015
Segurança: Adicionar nova tabela
Tabela YYY – Gestão de Segurança de end-point:

Adicionar à tabela: Implementação de serviço de anti-vírus
Justificativa: Vírus são a forma mais comum de ataque e devem proteger todos os equipamentos, tanto servidores como desktops e plataformas móveis, sendo monitorado 24 x 7

Adicionar à tabela: Serviço de monitoração de end-point:
Justificativa: Usar métodos para garantir que os servidores com informações privativas de cidadãos ou informações confidenciais sejam monitorados 24 x 7 identificando ATP (Advanced Threat Protection);

Resposta à contribuição:
Em atenção a sua contribuição, informamos que a mesma foi **parcialmente aceita**.
O Segmento 2 da ePING acolhe a proposta para estudos durante a próxima atualização, considerando que é necessário avaliar o impacto e aceitação entre interlocutores necessários no âmbito da Administração Pública.

Contribuição 10)

Minuta do Documento de Referência da ePING 2015
Segurança: Adicionar nova tabela
Tabela YYY – Politica de segurança da informação:

Adicionar à tabela: Política de segurança: A – Elaboração de política de segurança da informação obrigatório para todas as instituições que lidam com informações confidenciais ou privativas de cidadãos seguindo no mínimo os padrões especificados na ISO/IEC 27001.
Justificativa: Políticas de segurança da informação são base para a segurança e proteção de dados confidenciais e privativos de cidadãos.

Resposta à contribuição:
Em atenção a sua contribuição, informamos que a mesma **não foi aceita.**
O objetivo da ePING é elicitar padrões aceitos pela Administração Pública Federal, ou seja, um Componente que estabeleça um padrão é necessário para que se possa estudá-lo e avaliar a conveniência e oportunidade de incluí-lo na ePING. Em resumo, as normas que determinam a elaboração de política de segurança informação já existem e se houver alguma particularidade que deve se tornar padrão de governo, o Segmento de Segurança da ePING aguardará recebê-la para estudo durante o exercício de 2015.

Contribuição 11)

Anexo B3. Especificação de Requisitos específicos de Avaliação de Conformidade dos ativos.

Subitem: Estrutura de rede segura

Texto do Item: "Separar voz e dados em redes logicamente diferentes: Diferente sub-redes com blocos de endereços IP privados (RFC 1918) devem ser utilizados para separar o tráfego de voz e os dados, com servidores DHCP separados para cada rede, facilitando a incorporação do sistema de detecção de intrusos (IDS) e firewall de proteção."

Contribuição: alterar o texto do item para:
Nas redes locais (LAN), separar voz e dados em redes logicamente diferentes: Diferente sub-redes com blocos de endereços IP privados (RFC 1918) devem ser utilizados para separar o tráfego de voz e os dados, com servidores DHCP separados para cada rede, facilitando a incorporação do sistema de detecção de intrusos (IDS) e firewall de proteção.

Justificativa: Nosso entendimento é que as especificações deste parágrafo tratam da rede interna da instituição (LAN e WAN). Sendo este o entendimento correto, sugerimos alterar o texto do item de forma que se torne mais claro.

Resposta à contribuição:
Em atenção a sua contribuição, informamos que todas as contribuições relacionadas aos Decreto 8.135/2013 serão analisadas e respondidas por grupo de trabalho a ser instituído pelo Ministério do Planejamento no início de 2015.

Contribuição 12)

Critérios de Auditoria de Segurança - Decreto 8.135/2013

Item: 4.2.2. Mitigação, Análise de Risco e Auditabilidade

Texto do Item: "Nos casos em que não seja possível a auditabilidade plena ou que ela não seja viável, os órgãos deverão realizar planos de mitigação dos riscos relacionados com vazamentos de informações intencionais ou não. Recomenda-se nos casos em que não seja possível auditoria nos códigos dos softwares ou equipamentos, o monitoramento da comunicação de rede derivada dos produtos contratados. Esse monitoramento deverá ser realizado por ferramentas que possam ser auditadas plenamente, isto é, que permitam acesso completo ao código, bibliotecas e demais componentes da solução. Os custos decorrentes dessa etapa adicional de verificação de segurança deverão integrar a contratação e farão parte do contrato de firmado entre o órgão da APF e o fornecedor."

Contribuição: alterar o texto do item para:
Nos casos em que não seja possível a auditabilidade plena ou que ela não seja viável, os órgãos deverão realizar planos de mitigação dos riscos relacionados com vazamentos de informações intencionais ou não. Recomenda-se nos casos em que não seja possível auditoria nos códigos dos softwares ou equipamentos, o monitoramento da comunicação de rede derivada dos produtos contratados. Esse monitoramento deverá ser realizado por ferramentas que possam ser auditadas plenamente, isto é, que permitam acesso completo ao código, bibliotecas e demais componentes da solução. A análise dos dados gerados por estas ferramentas deverão ser analisados pelo órgão contratante. Os custos decorrentes dessa etapa adicional de verificação de segurança deverão integrar a contratação e farão parte do contrato de firmado entre o órgão da APF e o fornecedor.

Justificativa: A empresa contratada não consegue ter uma visão correta sobre o tráfego de cada cliente. Portanto, seria de responsabilidade de cada órgão a análise deste tráfego.

Resposta à contribuição:
Em atenção a sua contribuição, informamos que todas as contribuições relacionadas aos Decreto 8.135/2013 serão analisadas e respondidas por grupo de trabalho a ser instituído pelo Ministério do Planejamento no início de 2015.

Item: Critérios de Auditoria de Segurança - Decreto 8.135/2013

As pessoas jurídicas IBM, CISCO, BSA, ABES e BRASSCOM solicitaram prorrogação do prazo da consulta e foram informadas que o prazo terminaria no dia 12/12, mas contribuições poderiam ser enviadas em qualquer tempo para o e-mail eping@planejamento.gov.br.

As contribuições referentes aos Critérios de Auditoria de Segurança – Decreto 8.135/2013 serão analisadas e respondidas por grupo de trabalho a ser instituído pelo Ministério do Planejamento no início de 2015.