0100.034457/2013-12

Senado Federal
Secretaria Geral da Mesa
Secretaria de Comissões
Coordenação de Apoio às Comissões Especiais, Temporárias e Parlamentares de Inquérito

SENADO FEDERAL

12 DEZ 15 22

DIRETORIA ADJUNTA
PROTOCOLO ADMINISTRATIVO

ESP REC
000047

Ofício nº 069/2013 - CPIDAESP

Brasília, 11 de dezembro de 2013.

A Sua Senhoria o Senhor
Antônio Helder Rebouças
Diretor-Geral do Senado Federal

Assunto: **Requerimento de Informações**

Senhor Diretor-Geral,

Na qualidade de Presidente da *"Comissão Parlamentar de Inquérito, criada nos termos do Requerimento nº 811, de 2013, destinada a investigar a denúncia de existência de um sistema de espionagem estruturado pelo governo dos Estados Unidos"*, encaminho a Vossa Senhoria, para as providências devidas, o Requerimento n° 074 CPI-ESP, aprovado na 13ª Reunião deste colegiado realizada no dia 10 do corrente.

Atenciosamente,

Senadora Vanessa Grazziotin
Presidente

APROVADO EM 10/12/2013

SENADO FEDERAL
Gabinete da Senadora VANESSA GRAZZIOTIN

REQUERIMENTO Nº ,DE 2013.

CPI-ESP

Requerimento
Nº 074/13

Requeiro, baseada no Art. 264, § 2º, do Ato da Comissão Diretora nº14 de 2013, que o PRODASEN, através de sua equipe técnica, analise e emita parecer técnico sobre as informações enviadas pelos diversos órgãos e empresas públicas acerca da criptografia e sistemas de segurança de dados utilizados pelo governo federal, para subsidiar os trabalhos desta Comissão Parlamentar de Inquérito.

Sala das Comissões, de dezembro de 2013.

Senadora VANESSA GRAZZIOTIN

PCdoB/Amazonas

Subsecretaria de Apoio às Comissões Especiais e Parlamentares de Inquérito
Recebido em 06/12/2013
Às 15h03 horas
Rogério Faleiro Mavignier
Analista Legislativo
Mat. 256101

À (Ao) SEPROT

De ordem do Senhor Diretor-Geral

Para providências. Após, encaminhar ao Setor [illegible] Paraíba, para atendimento da solicitação à fl. 02.

Em, 12 / 12 / 2013

Sérgio Roberto Verch Harger
Subchefe de Gabinete da
Diretoria-Geral

SENADO FEDERAL

Secretaria de Tecnologia da Informação - Prodasen

Secretaria de Tecnologia da Informação - PRODASEN
Folha: 3
Rubrica

Despacho nº 449/2013 - PRDSTI/GBPRD
Processo nº 00200.027800/2013-44

Ref.: Requerimento de Informações nº 074/13.

Senhor Coordenador da COINTI,

A respeito da matéria em epígrafe, apresentamos a esta Coordenação o Requerimento nº 074/13 da Excelentíssima Senhora Senadora Vanessa Grazziotin, fl. 02, para que preste as informações pertinentes visando subsidiar os trabalhos da "*Comissão Parlamentar de Inquérito, criada nos termos do Requerimento nº 811, de 2013, destinada a investigar denúncia de existência de um sistema de espionagem estruturado pelo governo dos Estados Unidos*".

Secretaria de Tecnologia da Informação - Prodasen, 12 de dezembro de 2013.

João Jorge Squeff
Diretor-Adjunto do Prodasen


Secretaria de Tecnologia da Informação - PRODASEN
Página em Branco
Rubrica

PARECER TÉCNICO SOBRE AS INFORMAÇÕES ENVIADAS POR DIVERSOS ÓRGÃOS E EMPRESAS PÚBLICAS ACERCA DA CRIPTOGRAFIA E SISTEMAS DE SEGURANÇA DE DADOS UTILIZADOS PELO GOVERNO FEDERAL.

André Luiz Bandeira Molina

Flavio Henrique de Sousa Lima

Giuliano Macedo Arruda

Norman Pozo Molina Junior

Brasília, Fevereiro de 2014.

Sumário

SENADO FEDERAL
Secretaria de Tecnologia da Informação – Prodasen
Coordenação de Infraestrutura de Tecnologia da Informação - COINTI

Considerações Iniciais

Trata-se de solicitação de análise e emissão de parecer técnico sobre as informações enviadas por diversos órgãos e empresas públicas acerca da criptografia e sistemas de segurança de dados utilizados pelo governo federal, a fim de subsidiar os trabalhos da Comissão Parlamentar de Inquérito (CPI) destinada a investigar a denúncia de existência de um sistema de espionagem estruturado pelo governo dos Estados Unidos.

A solicitação encontra subsídio no Art. 264, § 2º, do Ato da comissão Diretora nº 14 de 2013, abaixo transcrito:

> *Art. 264. À Secretaria de Tecnologia da Informação – PRODASEN compete prover, por meio de recursos próprios ou de terceiros, serviços, soluções, suporte e infraestrutura de tecnologia da informação; gerir a tecnologia da informação do Senado Federal; implementar a estratégia de tecnologia da informação; propor inovações nos processos finalísticos e de apoio do Senado, com uso de tecnologia da informação; propor padrões, normas, métodos e processos para uso da tecnologia da informação e monitorar sua aplicação; integrar iniciativas de adoção de novas soluções de tecnologia da informação por outras unidades da Casa;* ***gerir a segurança da informação do Senado no âmbito da tecnologia da informação;*** *gerenciar os riscos operacionais do Senado com origem em tecnologia da informação;* ***e executar outras atividades correlatas.***
>
> *§ 2º Os órgãos subordinados à Secretaria de Tecnologia da Informação – PRODASEN têm as seguintes atribuições:*
>
> *II - Gabinete Administrativo, ao qual compete providenciar sobre o expediente do Prodasen, as audiências e a representação de seu titular; auxiliar e assessorar seu titular no desempenho de suas atividades; executar as tarefas de suporte administrativo vinculadas às atribuições do órgão; em parceria com demais áreas do Senado Federal, elaborar o Plano Anual de Capacitação dos servidores;* ***prestar assessoria e consultoria nas áreas de*** *planejamento, gestão, processos, projetos,* ***e segurança da informação;*** *exercer atividades de assessoramento e consultoria em questões de natureza jurídica administrativa relacionadas à tecnologia da informação; realizar estudos e preparar informações; apoiar a elaboração de normas técnicas e administrativas; apoiar o processo decisório dos titulares de órgãos administrativos do Prodasen; coordenar a elaboração e a execução da estratégia organizacional, no âmbito do Prodasen; coordenar programas de melhorias de processos organizacionais; propor normas técnicas; consolidar informações gerenciais; e executar outras atividades correlatas;* **(grifo nosso)**

Nesse sentido, foram analisados os documentos apresentados à CPI e disponibilizados no sítio http://www.senado.leg.br/atividade/comissoes/listaDocsCPI.asp?cc=1682&td=RE.

Desses documentos, 27 (vinte e sete) tratam de informações pertinentes aos temas criptografia e sistemas de segurança de dados, conforme lista abaixo:

Tabela 1 - Lista dos documentos encaminhados à CPI relacionados à criptografia e sistemas de segurança de dados utilizados pelo governo federal.

Nº	DATA RECEBIMENTO	REMETENTE	ORIGEM	DESCRIÇÃO	EM RESPOSTA
6	24/10/2013	General de Exército José Elito Carvalho Siqueira - Ministro de Estado do Gabinete de Segurança Institucional da Presidência da República	2191 24/10/2013	Presta informações sobre o CEPESC e sobre o uso de equipamentos criptográficos com o escopo de impedir o acesso indevido a informações estratégicas. Documentação contendo: 2 folha(s).	Of. 12/2013 (Req. 17/2013)
7	24/10/2013	General de Exército José Elito Carvalho Siqueira - Ministro de Estado do Gabinete de Segurança Institucional da Presidência da República	2192 24/10/2013	Presta informações sobre o CEPESC e sobre o uso de equipamentos criptográficos com o escopo de impedir o acesso indevido a informações estratégicas. Documentação contendo: 2 folha(s).	Of. 13/2013 (Req. 30/2013)
10	29/10/2013	Celso Amorim - Ministro de Estado da Defesa	12979 22/10/2013	Encaminha informações sobre a capacidade do Centro de Análises de Sistemas Navais - CASNAV de contribuir para minorar a dependência, por parte de organizações estratégicas do Governo Federal, de empresas estrangeiras do setor de sistemas de segurança computacionais. Documentação contendo: 3 folha(s).	Of. 11/2013 (Req. 16/2013)
14	13/11/2013	Edison Lobão - Ministro de | Ministerio de Minas e Energia	Aviso nº 242/2013/ GM-MME 12/11/2013	Encaminha o Memorando nº 317/2013 - SE-MME. acompanhado do Memorando nº 65/2013 - CGTI/SPOA- MME, ambos de 8 de novembro de 2013, contendo informações solicitadas. Documentação contendo: 4 folha(s).	Of. 61/2013 (Req. 68/2013)
15	14/11/2013	Jorge Fontes Hereda - Presidente da Caixa Econômica Federal	Of CAIXA 274/2013 14/11/2013	Encaminha informações referentes à Caixa Econômica Federal em resposta a questionamento desta CPI. Documentação contendo: 3 folha(s).	Of. 55/2013 (Req. 62/2013)
16	14/11/2013	Joaquim Barbosa	Ofício nº 342/GP 13/11/2013	Encaminha informações prestadas pela Secretaria de Tecnlogia da Informação do Supremo Tribunal Federal, em que foram repondidos os questionamentos constantes do Requerimento nº 056/13. Documentação contendo: 8 folha(s).	Of. 49/2013 (Req. 56/2013)
17	14/11/2013	Jorge Salles Camargo Neto	GAPRE - 413/13	Encaminha cópia do expediente JURIDICO/JAEIAOC 171/2013, o qual	Of. 46/2013 (Req. 53/2013)

SENADO FEDERAL

Secretaria de Tecnologia da Informação – Prodasen
Coordenação de Infraestrutura de Tecnologia da Informação - COINTI

			13/11/2013	contempla as informações providenciadas pela Gerência Executiva de Tecnologia da Informação e Comunicações (TIC) da Petrobras, bem como requer o tratamento sigiloso das referidas informações. Documentação contendo: 5 folha(s).	
18	14/11/2013	Dirceu Brás Aparecido Barbano - Diretor-Presidente da Agência Nacional de Vigilância Sanitária	1648/2013 14/11/2013	Fornece informações acerca das ações adotadas pela ANVISA para minorar a possibilidade de ataques virtuais/digitais às atividades do governo brasileiro. Documentação contendo: 2 folha(s).	Of. 52/2013 (Req. 59/2013)
19	13/11/2013	Paulo Gadelha - Presidente da Fundação Oswaldo Cruz	Ofício 453/2013-PR 04/11/2013	Encaminha informações acerca de criptografia e segurança da informação referentes a Fundação Oswaldo Cruz. Documentação contendo: 3 folha(s).	Of. 36/2013 (Req. 43/2013)
20	19/11/2013	ONS - Operador Nacional do Sistema Elétrico	CARTA ONS - 1397/100/2013 19/11/2013	Encaminha informações sobre as ações adotadas pelo Operador Nacional do Sistema Elétrico - ONS para minorar a possibilidade de ataques virtuais/digitais às atividades do governo brasileiro. Documentação contendo: 4 folha(s).	Of. 45/2013 (Req. 52/2013)
21	19/11/2013	Tito Cardoso de Oliveira Neto	CE-PR-1.00.360.13 19/11/2013	Encaminha informações da Eletrobras Eletronorte acerca de criptografia e segurança da informação. Documentação contendo: 1 folha(s).	Of. 42/2013 (Req. 49/2013)
22	19/11/2013	Adriano Meira Ricci	Diretoria de Gestão da Segurança 2013/0172 19/11/2013	Encaminha informações do Banco do Brasil acerca de criptografia e segurança da informação. Documentação contendo: 2 folha(s).	Of. 53/2013 (Req. 60/2013)
23	20/11/2013	Othon Luiz Pinheiro da Silva - Diretor Presidente da Eletrobras Eletronuclear	P 402/13 13/11/2013	Encaminha informações da Eletrobras Eletronuclear acerca de criptografia e segurança da informação. Documentação contendo: 2 folha(s).	Of. 40/2013 (Req. 47/2013)
24	21/11/2013	TSE - Tribunal Superior Eleitoral	OF.TST.GP nº 796/2013 20/11/2013	Encaminha informações sobre o sistema de criptografia e segurança da informação utilizados pelo TST. Documentação contendo: 2 folha(s).	Of. 51/2013 (Req. 58/2013)
25	21/11/2013	EMBRAPA - Empresa Brasileira de Pesquisa Agropecuária	C.PR.Nº 227/2013 20/11/2013	Encaminha informações sobre o sistema de criptografia e segurança da informação utilizados pela EMBRAPA. Documentação contendo: 2 folha(s).	Of. 53/2013 (Req. 60/2013)
28	22/11/2013	Wilson Roberto Trezza - Diretor-Geral da Agência Brasileira de Inteligência	252/ABIN/GSIPR 22/11/2013	Encaminha informações da ABIN sobre criptografia e segurança da informação. Documentação contendo: 1 folha(s).	Of. 38/2013 (Req. 45/2013)
29	22/11/2013	Adeilson Ribeiro Telles	0658/2013 PRESI 20/11/2013	Encaminha informações dos Correios sobre criptografia e segurança da informação. Documentação contendo: 2 folha(s).	Of. 60/2013 (Req. 67/2013)
30	26/11/2013	Flavio Decat de	DP.E.486.2	Encaminha informações da Eletrobras-Furnas	Of. 43/2013

		Moura - Diretor-Presidente da Eletrobras-Furnas	013 14/11/2013	referentes a criptografia e segurança da informação. Documentação contendo: 1 folha(s).	(Req. 50/2013)
32	26/11/2013	Marcos Aurélio Madureira da Silva - Diretor-Presidente da Companhia Hidro Elétrica do São Francisco	CE-PR-421/2013 21/11/2013	Encaminha informações da CHESF sobre criptografia e segurança da informação. Documentação contendo: 3 folha(s).	Of. 39/2013 (Req. 46/2013)
33	26/11/2013	Sérgio Gusmão Suchodolski	Ofício 866/2013 - BNDES GP 19/11/2013	Encaminha informações do BNDES sobre criptografia e segurança da informação. Documentação contendo: 3 folha(s).	Of. 59/2013 (Req. 66/2013)
34	03/12/2013	José Eduardo Cardozo - Ministro da Justiça	Aviso nº 1929-MJ 02/12/2013	Encaminha informações sobre ações da Polícia Federal para minorar a possibilidade de ataques virtuais/digitais às atividades do governo brasileiro. Documentação contendo: 3 folha(s).	Of. 62/2013 (Req. 69/2013) Of. 63/2013 (Req. 70/2013)
35	04/12/2013	Jorge Miguel Samek - Diretor da Itaipu Binacional	E/GB/0465 35 22/11/2013	Encaminha informações sobre criptografia e segurança da informação referentes a Itaipu Binacional. Documentação contendo: 2 folha(s).	Of. 44/2013 (Req. 51/2013)
37	04/12/2013	Felix Fischer - Presidente do Superior Tribunal de Justiça	Ofício 1261/GP	Encaminha informações sobre criptografia e segurança da informação referentes ao Superior Tribunal de Justiça. Documentação contendo: 7 folha(s).	Of. 50/2013 (Req. 57/2013)
38	09/12/2013	Antônio Helder Rebouças - Diretor-Geral do Senado Federal		Encaminha informações sobre segurança das comunicações referentes ao Senado Federal. Documentação contendo: 30 folha(s).	Of. 35/2013 (Req. 39/2013)
39	16/12/2013	Athayde Fontoura Filho	Ofício nº 5.268 GAB-DG 06/12/2013	Encaminha informações referentes a criptografia e segurança da informação do Tribunal Superior Eleitoral. Documentação contendo: 7 folha(s).	Of. 58/2013 (Req. 65/2013)
40	16/12/2013	Ademir Tardelli	Ofício nº 568/2013 PR/INPI 27/11/2013	Encaminha informações referentas a criptografia e segurança da informação do Instituto Nacional da Propriedade Industrial. Documentação contendo: 1 folha(s).	Of. 48/2013 (Req. 55/2013)
41	18/12/2013	Magda Chambriard - Diretora-Geral da Agência Nacional do Petróleo	Ofício 292/2013/ DG-ANP 09/12/2013	Encaminha informações sobre criptografia e segurança da informação referentes à Agência Nacional do Petróleo. Documentação contendo: 3 folha(s).	Of. 57/2013 (Req. 64/2013)

Os documentos analisados, em sua maioria, respondem aos requerimentos expedidos pela CPI solicitando as ações para minorar a possibilidade de ataques virtuais/digitais às atividades do governo brasileiro. As informações apresentadas tratam dos seguintes questionamentos:

1 – Criptografia:

a) Qual empresa desenvolveu o referido sistema?

SENADO FEDERAL
Secretaria de Tecnologia da Informação – Prodasen
Coordenação de Infraestrutura de Tecnologia da Informação - COINTI

b) Qual o sistema utilizado?

2 – Segurança da Informação:

a) Quais os dispositivos de segurança da informação utilizados?
b) Qual empresa ou as empresas que forneceram tais dispositivos?

Inicialmente observa-se que os questionamentos buscam, em essência, abordar somente o aspecto tecnológico empregado pelos órgãos e empresas públicas em suas ações para minorar a possibilidade de ataques virtuais/digitais, pois tratam somente das tecnologias e seus fabricantes, tanto para criptografia como para os dispositivos de segurança da informação.

Conforme a norma ABNT ISO 27002:2005, a segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos. Convém que isto seja feito em conjunto com outros processos de gestão do negócio.

Essa definição aponta que a segurança deve ser estabelecida por meio de pessoas, processos e tecnologias. Abordar somente a questão tecnológica não permite afirmar que possuir as soluções de segurança mais modernas e utilizar os algoritmos criptográficos mais robustos garanta um nível adequado de segurança, pois as pessoas ou os processos podem ser o elo mais fraco nesse trinômio.

Dessa forma, sem informações detalhadas sobre como as tecnologias apresentadas são efetivamente utilizadas, não é possível avaliar a eficácia dos sistemas de segurança implantados nos órgãos.

No Anexo I encontra-se uma breve contextualização sobre segurança da informação, inclusive seu cenário no setor público.

Padrões de mercado e algoritmos públicos

Com relação à criptografia observa-se a partir das respostas o uso maciço de protocolos baseados em padrões de mercado. A utilização dos protocolos HTTPS, SSL, TLS e IPSec indica que um nível adequado de segurança pode ser atingido por meio desses padrões, desde que se utilize suas últimas versões e que se saiba que tipo de proteção se deseja assegurar – confidencialidade e integridade. Todavia, a depender do tipo de informação que se deseja

proteger e o tipo de proteção, os algoritmos criptográficos que esses padrões utilizarão precisam ser cuidadosamente avaliados.

A escolha de algoritmos criptográficos padronizados pelo mercado e reconhecidamente fortes pela comunidade científica, como AES, 3-DES, RSA com chaves a partir de 2048 bits, SHA-256, SHA-512, ECC com chaves a partir de 224 bits, entre outros, permite garantir um nível mínimo de segurança em termos de confidencialidade e integridade. Vale destacar que esses algoritmos são abertos, além de exaustivamente testados pela comunidade científica em busca de falhas. Não se tem conhecimento de fragilidades que permitam a quebra desses algoritmos em tempo aceitável.

Outro aspecto relevante com relação à criptografia que foi observado nas respostas é a grande utilização de certificados e equipamentos padrão ICP-Brasil. A Infraestrutura de Chaves Públicas brasileira, ICP-Brasil (http://www.iti.gov.br/icp-brasil/), é um conjunto de técnicas, práticas e procedimentos que foram traçadas pelo seu Comitê Gestor com o objetivo de estabelecer os fundamentos técnicos e metodológicos de um sistema de certificação digital baseado em chave pública.

Os padrões de hardware, os algoritmos e parâmetros criptográficos a serem empregados em todos os processos realizados no âmbito da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) estão definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[1] (DOC ICP-01.01), atualmente em sua versão 2.3, de 06 de julho de 2012. Nele são estabelecidos tamanhos mínimos de chaves, opções de algoritmos aceitáveis, entre outras definições. Esses requisitos mínimos asseguram um nível adequado de segurança quando se utiliza essa infraestrutura de chaves públicas.

Com relação aos sistemas nos quais esses protocolos e algoritmos são utilizados, verifica-se principalmente:

a) Identificação, Autenticação e Autorização para acesso a sistemas;
b) Virtual Private Network (VPN): Utilizam os protocolos IPSec ou SSL para criar um canal seguro que garanta confidencialidade e/ou integridade à informação por meio dos algoritmos criptográficos apresentados, e eventualmente através de certificados ICP-Brasil;
c) Navegação segura (confidencialidade e integridade) por meio dos protocolos HTTPS, SSL e TLS utilizando os algoritmos criptográficos apresentados, e eventualmente certificados ICP-Brasil;
d) Criptografia para armazenamento de informações em bases de dados;
e) Criptografia de arquivos, discos e mídias.

[1] http://www.iti.gov.br/images/twiki/URL/pub/Certificacao/DocIcp/DOC-ICP-01.01_-_versao_2.3_PADROES_E_ALGORITIMOS_CRIPTOGRAFICOS_DA_ICP-BRASIL.pdf

f) Troca de e-mails seguros utilizando-se soluções proprietárias como Lotus Notes e Microsoft Exchange, que podem utilizar os algoritmos criptográficos supracitados.

Com relação à utilização do correio eletrônico, cabe destacar que adotar uma solução específica para troca de e-mails seguros só permite garantir a confidencialidade para os usuários que pertençam ao ambiente da solução em questão, mas usuários em sistemas distintos não terão seus e-mails criptografados automaticamente, a menos que eles utilizem algum mecanismo de criptografia adicional previamente acordado, a exemplo da criptografia de chave pública. Isso ocorre em virtude de o protocolo de troca de e-mails entre sistemas distintos – Simple Mail Transfer Protocol, SMTP – não prever confidencialidade na troca de mensagens, conforme RFC 5321[2].

Utilização de Algoritmos Frágeis

Observa-se que alguns órgãos fazem uso de algoritmos frágeis para os padrões atuais de criptografia, no caso o criptosistema DES, e os *hash* criptográficos SHA-1 e MD5. Grande parte dos atuais dispositivos de segurança ainda mantêm esses algoritmos disponíveis a fim de permitir compatibilidade com dispositivos mais antigos.

O criptosistema DES (Data Encryption Standard) foi o primeiro algoritmo criptográfico padronizado para o mercado, a partir de uma proposta do National Bureau of Standards (NBS), atual National Institute of Standards and Technology (NIST)[3], tendo vigorado como padrão entre 1977 e 1999, quando então o NIST recomendou o uso do 3DES, uma variante mais segura do DES. No último desafio de quebra do DES promovido pela empresa RSA, *DES Challenge III*, a mensagem secreta foi descoberta em 22 horas e 15 minutos, em 1999.

Com relação aos *hashs* criptográficos MD5 e SHA-1, a RFC 4270, datada de 2005, já recomendava o abandono desses algoritmos devido às fragilidades encontradas e que fosse utilizado o SHA-256. De fato, em 2008 um grupo de pesquisadores demonstrou a criação de um certificado digital forjado que utilizava o algoritmo MD5 para verificação da autenticidade. A partir de então o uso do MD5 em certificados digitais no mercado foi abandonado.

---

[2] RFC 5321 – A *Request for Comments* (RFC) é uma publicação do Internet Engeneering Task Force (IETF) com a finalidade de descrever os padrões que serão aplicados e utilizados na Internet. A RFC 5321 especifica o protocolo de transporte de e-mails.

[3] NIST (http://www.nist.gov/public_affairs/general_information.cfm) – Fundado em 1901, anteriormente conhecido como *The National Bureau of Standards*, o NIST é uma agência governamental não-regulatória do Departamento de Comércio dos Estados Unidos, cuja missão é promover a inovação e a competitividade industrial dos Estados Unidos, promovendo a metrologia, os padrões e a tecnologia de forma que ampliem a segurança econômica e melhorem a qualidade de vida.

A partir da documentação apresentada não se pode afirmar efetivamente que utilizar esses algoritmos seja inseguro, sem ter conhecimento do tipo de informação que está sendo protegida. Com base no conceito de esquema de criptografia computacionalmente seguro, descrito no Anexo I, pode ocorrer de as informações protegidas por esses algoritmos terem seu valor inferior ao custo de obtê-las, ou então de o tempo de vida dessas informações ser inferior ao tempo necessário para consegui-las.

Utilização de Algoritmo de Estado

Louva-se aqui a iniciativa do CEPESC de proporcionar soluções de segurança, baseadas em algoritmo criptográfico de Estado, voltadas para a segurança das comunicações de órgãos e entidades da Administração Pública Federal. Trata-se da utilização de um algoritmo criptográfico sigiloso, que é embutido em soluções de segurança nacionais.

Por outro lado, um importante princípio de Kerckhoffs[4] afirma que "O único segredo em um sistema criptográfico deve ser a chave. O algoritmo deve ser publicamente conhecido. Se a segurança for baseada em muitos segredos, haverá mais vulnerabilidades possíveis de se explorar." As motivações por trás desse princípio são várias. Técnicas de engenharia reversa podem ser utilizadas para se obter o funcionamento do algoritmo, ou ainda, há uma quantidade significativa de ataques com base em técnicas analíticas desenvolvidas e refinadas pela comunidade criptoanalítica ao longo de muitos anos, a exemplo da criptoanálise diferencial e criptoanálise linear.

Isso significa dizer que um algoritmo público, pelo fato de estar submetido à constante avaliação da comunidade acadêmica, tem sua robustez assegurada à medida que resiste às diversas tentativas de quebra, obrigando a segurança de seu uso residir na escolha de uma chave adequadamente escolhida.

Não se tem informações sobre quais foram os procedimentos de escolha, testes e validação do algoritmo criptográfico de Estado disponibilizado pelo CEPESC, o que impede qualquer afirmação a respeito de sua segurança.

O Decreto nº 7.845, de 14 de novembro de 2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento, determina em seus artigos 27, 28, 31, 38, 39 e 40 que os órgãos e entidades submetidos a essa legislação utilizem recursos de

[4] Kerckhoffs, A. (1883). La cryptographie militaire. Journal des Sciences Militaires, 9th Series, February, 161–191. Auguste Kerckhoffs afirmava que um sistema criptográfico deve ser seguro mesmo que tudo tudo sobre o sistema seja público, exceto a chave.

criptografia compatíveis com o grau de sigilo da informação, seja ela transmitida ou armazenada, e que seja utilizado recurso criptográfico baseado em algoritmo de Estado para a cifração e decifração de informação classificada em qualquer grau de sigilo.

Além disso, determina ainda a competência do Gabinete de Segurança Institucional da Presidência da República (GSI/PR) em estabelecer parâmetros e padrões para os recursos criptográficos baseados em algoritmo de Estado, ouvido o Comitê Gestor de Segurança da Informação previsto no art. 6º do Decreto no 3.505, de 13 de junho de 2000, definindo o prazo de um ano a contar da definição desses parâmetros e padrões para que os órgãos e entidades adotem os recursos criptográficos baseados em algoritmo de Estado.

Cumprindo seu papel, o GSI/PR elaborou a Instrução Normativa GSI/PR nº 3, de 06 de março de 2013, que dispõe sobre os parâmetros e padrões mínimos dos recursos criptográficos baseados em algoritmos de Estado para criptografia da informação classificada no âmbito do Poder Executivo Federal. Nela estabelece em seu artigo 4º que a cifração e decifração de informações classificadas, em qualquer grau de sigilo, devem utilizar recurso criptográfico baseado em algoritmo de Estado em conformidade com os padrões e parâmetros mínimos estabelecidos na NC 09/IN01/DSIC/GSI/PR (Revisão 01), de fevereiro de 2013.

Em seu artigo 5º define que o recurso criptográfico baseado em algoritmo de Estado deverá ser de desenvolvimento próprio ou por órgãos e entidades do Poder Executivo Federal, mediante acordo ou termo de cooperação, vedada a participação e contratação de empresas e profissionais externos, para tal finalidade.

Por outro lado, a partir das informações apresentadas à CPI, conclui-se que, na prática, a maior parte dos órgãos respondentes utiliza algoritmos criptográficos abertos e padronizados pelo mercado, a exemplo do 3DES, AES, SHA-256 e RSA. Entretanto, os requisitos mínimos de segurança para uso desses algoritmos na Administração Pública Federal (APF), a exemplo do tamanho mínimo da chave, não são normatizados, existindo apenas recomendações como as do e-Ping ou os padrões mínimos definidos pelo Instituto de Tecnologia da Informação (ITI), restritos à ICP-Brasil, conforme descrito no Anexo I.

Oportuno lembrar que em razão da independência entre os poderes, as normas de cunho essencialmente administrativo emanadas do Poder Executivo, sejam decretos, sejam instruções normativas, não são automaticamente aplicáveis aos outros Poderes, a não ser que as autoridades da Casa explicitamente as adotem. E serão aplicáveis, somente na extensão que o façam, conforme apontado no Parecer CON/NJU nº 120/2010, constante do Processo SIGAD 00200.006244/2010-20, que trata do Grupo de Trabalho para Propor Política de Segurança da Informação Corporativa – POSIC no âmbito do Senado Federal.

Dispositivos de Segurança Proprietários e Sistemas Abertos

Um dado relevante a partir das respostas indica que a maioria dos órgãos respondentes utiliza softwares e dispositivos de segurança fabricados por empresas privadas, a maior parte sediadas em outros países. Ainda que seus sistemas disponibilizem soluções de segurança públicas e padronizadas pelo mercado, a exemplo de protocolos de comunicação segura e algoritmos criptográficos, seus códigos não são abertos, impossibilitando uma validação pela comunidade, e a implementação pode ser frágil ou maliciosa.

Além disso, não há uma entidade nacional com a responsabilidade legal de auditar e atestar a confiabilidade desses softwares e dispositivos, buscando verificar se de fato implementam os protocolos e algoritmos padronizados pelo mercado sem que sejam inseridos *backdoors*[5], a exemplo do que o autor Simon Singh relata em seu livro "O Livro dos Códigos":

> *"Uma variação do cavalo de Tróia é um novo tipo de programa de cifragem que parece seguro, mas que na verdade contém uma "porta dos fundos". Isto é algo que permitirá que seus criadores decifrem as mensagens de todos que usarem aquele programa. Em 1998 um relatório feito por Waine Madsen revelou que uma empresa criptográfica suíça, a Crypto AG, tinha colocado portas dos fundos em alguns de seus produtos e dera ao governo norte-americano os detalhes de como explorar essas características. Como resultado disso, os Estados Unidos puderam ler as comunicações de vários países. Em 1991, os assassinos que mataram Shahpour Bakhtiar, o ex-primeiro-ministro iraniano no exílio, foram presos graças à interceptação e decifragem, pela "porta dos fundos", das mensagens iranianas cifradas com equipamentos da Crypto AG."*

Por outro lado, alguns órgãos citam a utilização de sistemas abertos ou livres, que disponibilizam o código fonte da solução de segurança. A utilização de sistemas abertos em detrimento de dispositivos proprietários não impede a ocorrência de *backdoors* ou ainda a simples existência de falhas de implementação que permitam a exploração de vulnerabilidades. O fato de serem sistemas abertos permite que sejam auditados pela comunidade ou meio acadêmico de forma mais objetiva, mas ainda assim não se garante que não existam tais ameaças.

A segurança da informação, em todos os casos, deve ser buscada por meio de proteções complementares, estratégia conhecida como "defesa em profundidade", a exemplo do que cita o Ofício da CAIXA, segundo a qual a proteção se dá por uma série de controles de

[5] *Backdoor* – Programa ou código malicioso que permite a um atacante ter acesso a um sistema sem que tenha que se submeter ao processo normal de autenticação.

segurança físicos, lógicos e em processos, com base em ambientes lógicos segregados e implantados através de camadas isoladas, por meio de tecnologias distintas, inclusive de fornecedores diferentes.

Um caminho possível para se atestar a confiabilidade dos softwares e dispositivos de segurança foi traçado por meio do Decreto nº 8.135, de 4 de novembro de 2013, que dispõe sobre as comunicações de dados da administração pública federal direta, autárquica e fundacional, e sobre a dispensa de licitação nas contratações que possam comprometer a segurança nacional. Em seu Art. 1º, § 3º, define que:

> *Os programas e equipamentos destinados às atividades de que trata o caput deverão ter características que permitam auditoria para fins de garantia da disponibilidade, integridade, confidencialidade e autenticidade das informações, na forma da regulamentação de que trata o § 5º.*

Não há ainda regulamentação detalhada a respeito dessa auditoria, mas é certo que ela permitirá assegurar que os softwares e dispositivos de segurança, ainda que fornecidos por empresas sediadas no exterior, possam ter sua confiabilidade atestada.

Auditorias de Sistemas de Segurança

Uma avaliação mais adequada acerca das ações para minorar a possibilidade de ataques virtuais/digitais às atividades do governo brasileiro só poderia ser obtida por meio de uma auditoria de tecnologia da informação, com abordagem específica de segurança da informação.

Nesse sentido, o Tribunal de Contas da União, por intermédio da sua Secretaria de Fiscalização de Tecnologia da Informação – SEFTI, que tem por finalidade fiscalizar a gestão e o uso de recursos de tecnologia da informação pela Administração Pública Federal (Resolução TCU nº 193/2006), realiza eventualmente esse tipo de auditoria por meio de Fiscalização Operacional e/ou de Conformidade. No Anexo I encontra-se um diagnóstico da Segurança da Informação no contexto do Setor Público Federal a partir de um levantamento realizado pelo TCU. Uma das recomendações emanadas a partir do levantamento foi no sentido de que os órgãos e entidades avaliados realizem Auditorias de TI, que permitam a avaliação regular da conformidade, da qualidade, da eficácia e da efetividade dos serviços prestados.

De maneira similar ao TCU, mas restrito ao Poder Executivo, a Controladoria-Geral da União (CGU) também realiza esse tipo de auditoria.

Ainda que TCU e CGU estejam aptas a realizar esse tipo de auditoria, a frequência e abrangência das auditorias são insuficientes para viabilizar uma avaliação das ações para minorar a possibilidade de ataques virtuais/digitais às atividades do governo brasileiro.

Por sua vez, em seu Ofício, a ABIN informa que disponibiliza programas de assessoria para segurança abrangendo avaliações de risco completas, que incluem identificação de vulnerabilidades nos sistemas de proteção e os conjuntos de recomendações associadas às respectivas medidas corretivas. Tais avaliações poderiam ser solicitadas para se obter um quadro mais detalhado da efetividade das ações do governo brasileiro.

Cabe citar como esse tipo de avaliação é feito no caso dos Estados Unidos. O *Department of Homeland Security* – DHS tem uma área denominada *Office of Audits* que realiza a auditoria de segurança da informação em todos os órgãos da administração federal americana. Isso foi regulado pelo ato *Federal Information Security Management Act of 2002* – FISMA[6]. Uma das determinações do ato é a realização anual de avaliação independente do programa de segurança da informação e práticas de cada agência para determinar a efetividade do programa e das práticas.

Os resultados e recomendações dessas auditorias são disponibilizados na Internet, inclusive quando da ocorrência de achados que indicam fragilidades nos programas de segurança da informação, como é o caso do relatório de auditoria do Departamento de Agricultura para o ano de 2012, disponível em www.usda.gov/oig/webdocs/50501-0003-12.pdf.

Considerações Finais

Observou-se, a partir dos questionamentos realizados, que a maioria dos órgãos respondentes abordou somente o aspecto tecnológico da segurança da informação, o que é insuficiente para se diagnosticar efetivamente se as ações para minorar a possibilidade de ataques virtuais/digitais às atividades do governo brasileiro são eficazes. A segurança da informação só é efetivamente conseguida quando pessoas, processos e tecnologia se harmonizam em um sistema de gerenciamento da segurança da informação.

Restrito ao aspecto da criptografia, os órgãos, em sua maioria, utilizam algoritmos e protocolos de criptografia abertos e definidos em padrões de mercado, o que não implica dizer que são inseguros. Pelo contrário, a maioria dos autores recomenda seu uso baseado na sua resistência comprovada a partir da constante avaliação em busca de quebra por parte do meio acadêmico. Por outro lado, por se tratarem de padrões de mercado, esses algoritmos e protocolos muitas vezes são mantidos em uso para fins de compatibilidade, ainda que a

[6] http://csrc.nist.gov/drivers/documents/FISMA-final.pdf

comunidade científica já tenha identificado falhas e recomendado o abandono, como foi o caso do MD5 e SHA-1.

Há ainda as determinações do Executivo no sentido de se utilizar algoritmo de estado para proteger as comunicações e informações classificadas. Ressalta-se que não é possível atestar a confiabilidade de tais algoritmos pelo fato de não estarem disponíveis informações a respeito de sua validação.

Com relação aos dispositivos de segurança, identifica-se o uso maciço de softwares e dispositivos de segurança fabricados por empresas privadas, a maior parte sediada em outros países, sem que haja uma entidade nacional que audite e ateste a confiabilidade desses softwares e dispositivos. Por outro lado, utilizar sistemas abertos ou livres não significa estar livre de uma implementação frágil ou maliciosa, que contenha falhas ou *backdoors*. A proteção, em todos esses casos, deve ser buscada por meio de proteções complementares.

Por fim, não se verifica a existência de auditorias de tecnologia da informação voltadas exclusivamente para segurança da informação com abrangência e periodicidade necessárias. Somente por meio de tais auditorias é possível se diagnosticar se as ações em curso pelo governo brasileiro são efetivas ou não.

André Luiz Bandeira Molina
Analista de Informática Legislativa

Flávio Henrique de Sousa Lima
Analista de Informática Legislativa

Giuliano Macedo Arruda
Analista de Informática Legislativa

Norman Pozo Molina Junior
Analista de Informática Legislativa

REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002:2005: Tecnologia da Informação – Técnicas de Segurança – Código de prática para a gestão da segurança da informação.** Rio de Janeiro. 2005. 120 p.

BASTOS, Angela; CAUBIT, Rosângela. **ISO 27001 e 27002: Gestão de Segurança da Informação – uma visão prática.** 1ª Ed. Porto Alegre, RS. Editora Zouk. 2009. 257 p.

BROCARDO, Marcelo Luiz; De Rolt, Carlos Roberto; Fernandes, Reinaldo. **Introdução à Certificação Digital. Da Criptografia ao Carimbo de Tempo.** 1ª Ed. BRy Tecnologia. [S.l., s.n.]. 2006. 79p.

COSTA, Celso José da; FIGUEIREDO, Luiz Manoel Silva de. **Curso de Criptografia Introdução à Criptografia.** Rio de Janeiro: UFF. Núcleo de Educação Assistida por Meios Interativos - NEAMI. 2009. 96 p.

COSTA, Celso José da; FIGUEIREDO, Luiz Manoel Silva de. **Curso de Criptografia Geral.** Rio de Janeiro: UFF. Núcleo de Educação Assistida por Meios Interativos - NEAMI. 2009. 192 p.

HANSCHE, Susan; BERTI, John; HARE, Chris. **Official (ISC)^2 Guide to the CISSP Exam. Auerbach Publications.** Boca Raton. 2003. 902 p.

MENEZES, Alfred J.; Oorschot, Paul C. van; Vanstone, Scott A. **HANDBOOK of APPLIED CRYPTOGRAPHY.** 5ª Impressão. 2001. 780 p. Disponível em http://www.cacr.math.uwaterloo.ca/hac/. Acessado em 06 de fevereiro de 2013.

SINGH, Simon. **O Livro dos Códigos.** 8ª Ed. Editora Record. 2010. 446 p.

STALLINGS, William. **Cryptography and Network Security Principles and Practice.** 5ª Ed. Prentice Hall. 2011. 900 p.

SENADO FEDERAL

Secretaria de Tecnologia da Informação – Prodasen
Coordenação de Infraestrutura de Tecnologia da Informação - COINTI

ANEXO I

Segurança da Informação

A segurança da informação é caracterizada pela aplicação adequada de dispositivos de proteção sobre um ativo ou um conjunto de ativos com o objetivo de preservar o valor que este possui para as organizações, buscando assegurar a confidencialidade, integridade e disponibilidade não só para sistemas ou aplicativos, mas principalmente para as informações armazenadas ou veiculadas.

Confidencialidade ou sigilo é a propriedade de proteção da informação de forma que apenas as pessoas, recursos e processos autorizados tenham acesso a determinada informação. **Integridade** é a propriedade de proteção da informação contra modificação ou destruição, acidental ou intencional. **Disponibilidade** é a propriedade de assegurar que a informação esteja acessível por usuários autorizados sempre que necessário.

Outras duas propriedades de proteção da informação são relevantes no contexto de segurança da informação: **autenticidade** é a propriedade que visa comprovar a origem e autoria de uma determinada informação ou transação; e **não-repúdio** ou irretratabilidade é a propriedade que garante que o emissor ou pessoa que executou determinada transação de forma eletrônica não poderá, posteriormente, negar sua autoria.

A segurança da informação é obtida a partir da implantação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos. Convém que isto seja feito em conjunto com outros processos de gestão do negócio.

A utilização de soluções de firewall, antivírus, VPN, detecção de intrusão, entre outras, causam a impressão de que existe um bom nível de segurança numa organização. Contudo, a segurança que pode ser alcançada unicamente por meios técnicos é limitada e deve ser apoiada por uma gestão e por procedimentos apropriados.

Não é rara a ocorrência de situações de burla a mecanismos de segurança nas organizações, tais como empréstimo de senhas pessoais, ou delegação de permissões de administrador sem real necessidade. Muitas vezes os usuários não sabem se estão realizando suas ações de acordo com os objetivos de segurança da informação da organização em virtude de não existir uma política documentada e amplamente divulgada. Quando não há regras claras de qual é o comportamento esperado dos usuários da informação em um ambiente, eles sempre serão o elo mais vulnerável.

Diariamente os sistemas de informação e redes de computadores são expostos a uma grande quantidade de ameaças à segurança da informação, que vão desde situações ligadas aos fenômenos da natureza, como raios e tempestades solares, até aquelas decorrentes dos ataques cibernéticos, como fraudes eletrônicas e espionagem.

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br)[7] disponibiliza em seu sítio, http://www.cert.br, um conjunto de estatísticas sobre notificações de incidentes de segurança a ele reportados. Tratam-se apenas dos incidentes efetivamente comunicados àquele Centro pelas organizações brasileiras.

É possível verificar a tendência de crescimento do número de incidentes reportados ao longo dos últimos anos - Figura 1. Dos tipos de incidentes reportados ao CERT.br entre julho e setembro de 2013, chama a atenção o alto percentual de incidentes relacionados à fraudes, que atinge 26,64% do total, sendo o segundo maior tipo de incidente – Figura 2.

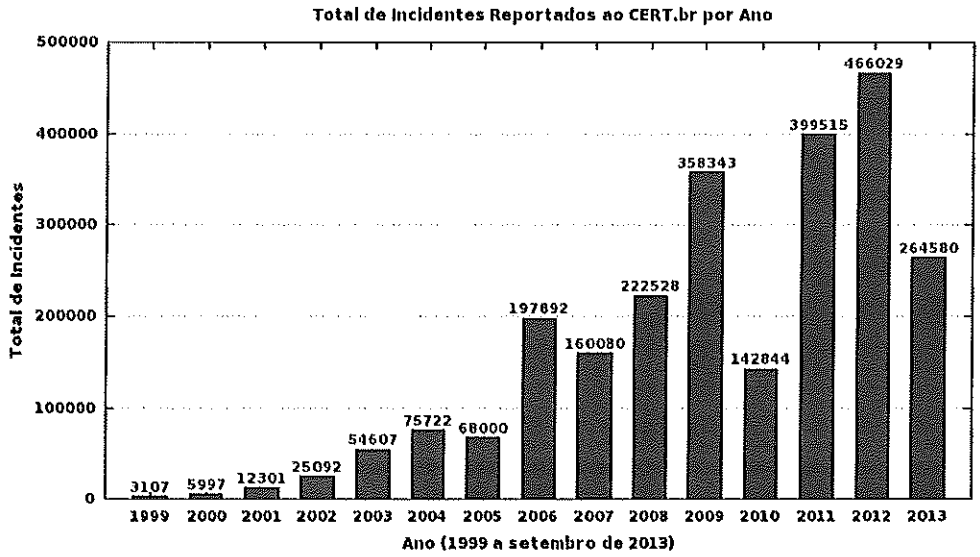

Figura 1 - Estatísticas de Incidentes em Redes Nacionais notificadas ao CERT.br, consolidadas até setembro de 2013 [Disponível em http://www.cert.br/stats/incidentes/].

[7] O CERT.br é o Grupo de Resposta a Incidentes de Segurança para a Internet brasileira, responsável por tratar incidentes de segurança em computadores que envolvam redes conectadas à Internet brasileira. Ele é mantido pelo NIC.br, do Comitê Gestor da Internet no Brasil. Atua como um ponto central para notificações de incidentes de segurança no Brasil, provendo a coordenação e o apoio no processo de resposta a incidentes e, quando necessário, colocando as partes envolvidas em contato.

SENADO FEDERAL
Secretaria de Tecnologia da Informação – Prodasen
Coordenação de Infraestrutura de Tecnologia da Informação - COINTI

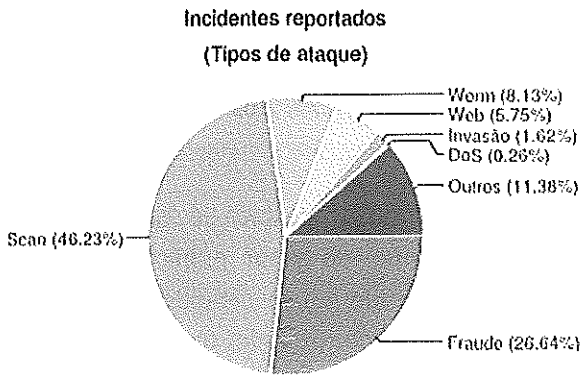

Figura 2 - Tipos de incidentes reportados ao CERT.br entre Julho a Setembro de 2013 [Disponível em http://www.cert.br/stats/incidentes/2013-jul-sep/tipos-ataque.html]

Um abrangente estudo[8] aponta como a segurança da informação está sendo tratada em diversos setores da economia, incluindo o setor público. Nesse estudo indica-se que apesar das manchetes apontarem para os casos de espionagem estrangeira, apenas 4% dos entrevistados relataram incidentes de segurança originados por nações estrangeiras. Segundo o estudo, os *hackers* constituem a maior ameaça para os entrevistados (Figura 3).

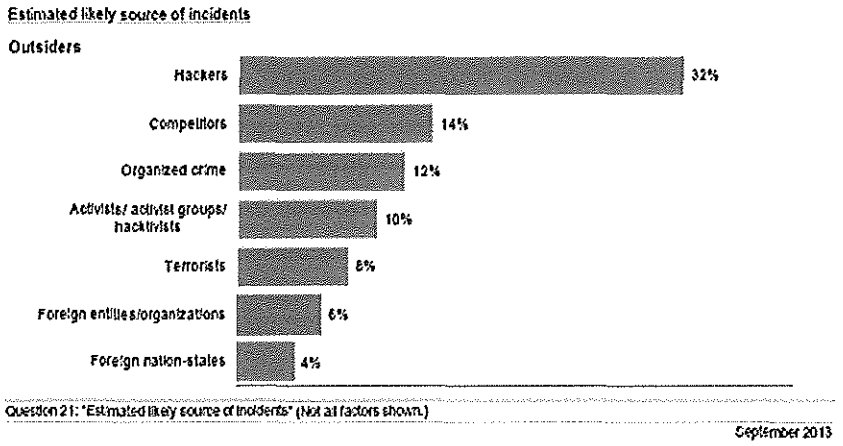

Figura 3 - Estatísticas sobre a origem provável dos incidentes de segurança. Hackers constituem a maior origem, com 32%, e casos relacionados a nações estrangeiras constituem apenas 4%. [Disponível em http://www.pwc.com/gx/en/consulting-services/information-security-survey/download.jhtml].

[8] O estudo "The Global State of Information Security® Survey 2014" dirigido pelas organizações PricewaterhouseCoopers (PwC), CIO Magazine e CSO Magazine, conduzido entre Fevereiro e Abril de 2013, representa a análise consolidada dos dados fornecidos por mais de 9,600 executivos, entre CEOs, CFOs, CIOs, CSOs, vice-presidentes e diretores de TI e segurança da informação. A América do Sul teve uma participação de 16% nas respostas, e o Brasil foi o país com maior participação (48%) nas respostas relacionadas a essa região. (http://www.pwc.com.br/pt/publicacoes/servicos/consultoria-negocios/pesquisa-global-seguranca-informacao-14.jhtml).

O estudo indica que os investimentos em segurança da informação em 2013 tiveram um acréscimo de 39% em relação a 2012. Além disso, para os doze meses subsequentes ao estudo, no caso da América do Sul, 65,77% dos respondentes afirmaram que haverá um aumento dos investimentos.

Dentre as diversas análises realizadas, destaca-se que, com base na percepção dos entrevistados, 74% dos respondentes do setor público afirmam que suas atividades de segurança são efetivas, e 54% consideram-se candidatos à liderança no que se refere a estratégias e práticas de segurança. Por outro lado, o número real de líderes cai para somente 16% quando se considera que para essa qualificação de liderança uma organização deve satisfazer quatro critérios principais: 1) possuir uma estratégia de segurança da informação abrangente; 2) possuir um CISO (Chief Information Security Officer: executivo sênior ou similar responsável pela segurança da informação) ou equivalente que se reporta à alta administração; 3) ter a efetividade da segurança do último ano medida e revisada; e 4) compreender exatamente quais os tipos de eventos de segurança ocorreram no último ano.

Essa última análise indica que pode existir uma percepção errônea da capacidade de segurança da informação por parte dos respondentes, o que pode ser extensível à grande maioria das organizações. De fato, medir a capacidade em segurança da informação é um processo que requer uma avaliação cuidadosa, e para que o resultado seja confiável recomenda-se a utilização de uma auditoria externa ou auditoria de terceira parte.

No caso do Setor Público Federal, o Tribunal de Contas da União executa esse tipo de auditoria. Merece especial atenção o Acórdão TCU 1603/2008 – Plenário, que apresenta resultados expressivos com relação a aspectos de governança de TI e gestão de segurança da informação no contexto do Setor Público Federal. Trata-se de resultado de uma pesquisa com 255 órgãos/entidades do Setor Público Federal com o objetivo de "coletar informações acerca dos processos de aquisição de bens e serviços de TI, de segurança da informação, de gestão de recursos humanos de TI, e das principais bases de dados e sistemas da Administração Pública Federal".

Consta no referido Acórdão que os recursos empregados pela Administração Federal na área de tecnologia da informação, segundo dados do Siafi de 2007, ultrapassam a soma de seis bilhões de reais por ano. Esse montante tem justificado uma atuação mais cuidadosa do Tribunal para com seus jurisdicionados, a fim de garantir a correta aplicação dos recursos empregados em tecnologia da informação.

Alguns resultados desse Acórdão demonstram que grande parte do Setor Público Federal não tratava adequadamente de temas importantes no contexto da Governança de TI e gestão de segurança da informação e comunicações, como pode ser verificado pelo conjunto de achados

consolidados na Tabela 2, que demonstra em percentuais o quantitativo de órgãos/entidades que não estão em conformidade com os requisitos listados.

Tabela 2 – Quadro resumo de alguns achados de auditoria do Acórdão TCU 1603/2008 – Plenário

Achado	Descrição
I	Ausência de planejamento estratégico institucional em vigor: 47%
II	Ausência de planejamento estratégico de TI. 59%
VIII	Ausência de política de segurança da informação em vigor: 64%
IX	Ausência de plano de continuidade de negócios em vigor: 88% A situação se agrava quando, adicionalmente, observa-se que, dentre os que possuem plano de continuidade de negócios em vigor, apenas 30% declararam tê-lo revisado em período inferior a um ano.
X	Ausência de classificação das informações: 80%
XIII	Ausência de área específica para gerência de incidentes: 76%

Dentre as recomendações emanadas pelo Tribunal para diversos órgãos, destacam-se as seguintes no contexto de segurança da informação:

> *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;*
>
> *9.1.8. Introduzam práticas voltadas à realização de Auditorias de TI, que permitam a avaliação regular da conformidade, da qualidade, da eficácia e da efetividade dos serviços prestados.*
>
> *9.2. recomendar ao Gabinete de Segurança Institucional da Presidência da República - GSI/PR que oriente os órgãos/entidades da Administração Pública Federal sobre a importância do gerenciamento da segurança da informação, promovendo, inclusive mediante orientação normativa, 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;*
>
> *9.3. recomendar à Controladoria-Geral da União - CGU que realize regularmente auditorias de TI e/ou promova ações para estimular a realização dessas auditorias nos órgãos/entidades da Administração Pública Federal;*

Dando sequência a essa avaliação, o Acórdão TCU 2.308/2010 - Plenário realizou levantamento destinado a verificar a evolução em relação à situação detectada no Acórdão anterior. No tocante à segurança da informação e comunicações, cabe reproduzir a conclusão:

> *75. Não se percebe melhora nos indicadores de segurança da informação em relação ao levantamento anterior, a despeito da recomendação emitida pelo TCU. A Administração, de forma geral, continua a desconhecer e a não proteger suas informações críticas adequadamente. Como não há avaliação de riscos, nem ao menos é possível estimar as suas consequências caso estes se materializem.*
>
> *76. Dessa forma, deve-se dar especial atenção a este aspecto no monitoramento das recomendações do Acórdão nº 1.603/2008-TCU-Plenário.*

Segundo o Acórdão, o significativo impacto da tecnologia da informação na administração pública federal decorre de seu papel crítico no apoio à execução de políticas, programas e projetos de governo, bem como do expressivo valor de recursos a ela alocados, que corresponderam a cerca de R$ 12,5 bilhões no orçamento da União de 2010. Verifica-se um aumento de aproximadamente 100% em relação ao levantamento realizado em 2007.

Também importante é o Acórdão TCU 2.471/2008 – Plenário, que foi realizado no âmbito do tema de maior significância "Terceirização na Administração Pública Federal", subtema "Terceirização em Tecnologia da Informação", mas que endereça diversas questões de segurança da informação e comunicações.

Neste Acórdão, dentre as recomendações, destacam-se no contexto de segurança da informação e comunicações:

> *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;*
>
> *9.6.2. Identifique boas práticas relacionadas à segurança da informação, difundindo-as na Administração Pública Federal;*

Conclui-se em relação à segurança da informação, que sendo a informação um dos principais insumos de qualquer organização, não basta a aplicação exclusiva controles técnicos/tecnológicos de segurança. Torna-se fundamental a existência de um mecanismo de gestão da segurança da informação que busque, além de garantir confidencialidade, integridade e disponibilidade, que as ações de segurança sejam coordenadas, eficientes e alinhadas aos objetivos organizacionais.

Criptografia

Criptografia é a ciência encarregada de esconder o significado de uma mensagem a fim de manter confidencialidade.

Cifragem consiste nos processos sistematizados de transformação da mensagem original (texto em claro) em uma mensagem ininteligível (texto cifrado). Decifragem consiste nos processos reversos aos da cifragem, a fim de tornar a mensagem inteligível.

A criptografia moderna, entendida como aquela que é utilizada nos sistemas computacionais atuais, pode ser dividida em dois tipos principais, Criptografia Simétrica e Criptografia Assimétrica.

A criptografia simétrica é uma forma de criptografia na qual uma única "chave secreta" é utilizada para o processo de cifragem e decifragem. Nesse caso, todos que possuem a chave secreta têm acesso à informação.

Um dos grandes problemas desse tipo de criptografia consiste da necessidade da troca da chave secreta por meio de um canal efetivamente seguro a fim de garantir que outros não tenham acesso a ela.

A criptografia assimétrica, também conhecida como criptografia de chave pública, consiste na utilização de um par de chaves matematicamente relacionadas, denominadas "chave privada" e "chave pública". Quando se utiliza uma dessas chaves para a cifragem, somente a outra chave pode decifrar, razão pela qual elas são matematicamente relacionadas.

A chave privada deve sempre ser mantida em segredo, o que não ocorre com a chave pública que pode ser distribuída sem restrições. Em virtude do conhecimento da chave privada ser restrito, o processo de cifragem com essa chave garante somente a autenticidade, pois qualquer um que possuir a chave pública poderá realizar a decifragem. Por outro lado, a cifragem com a chave pública garante a confidencialidade uma vez que somente quem possuir a chave privada poderá realizar a decifragem.

Há ainda os algoritmos criptográficos de integridade de dados, que tratam das funções hash criptográficas, as quais são utilizadas para a construção de códigos de autenticação de mensagens e assinaturas digitais.

Os sistemas computacionais modernos utilizam largamente os dois tipos principais de criptografia, aproveitando o que cada um oferece de melhor.

A utilização da criptografia assimétrica fez surgir a Infraestrutura de Chaves Públicas, que atua como um terceiro confiável para distribuir as chaves públicas por meio dos certificados digitais. No Brasil, a Infraestrutura de Chaves Públicas brasileira, ICP-Brasil

(http://www.iti.gov.br/icp-brasil/), é um conjunto de técnicas, práticas e procedimentos que foram traçadas pelo seu Comitê Gestor com o objetivo de estabelecer os fundamentos técnicos e metodológicos de um sistema de certificação digital baseado em chave pública. Ela surgiu da necessidade de regulamentar as atividades de certificação digital no Brasil e foi criada pela MP 2.200-2 de 24 de agosto de 2001.

Conforme citado em documento elaborado pelo ITI (http://www.iti.gov.br/certificacao-digital/o-que-e), na prática, o certificado digital ICP-Brasil funciona como uma identidade virtual que permite a identificação segura e inequívoca do autor de uma mensagem ou transação feita em meios eletrônicos, como a web. Esse documento eletrônico é gerado e assinado por uma terceira parte confiável, ou seja, uma Autoridade Certificadora (AC) que, seguindo regras estabelecidas pelo Comitê Gestor da ICP-Brasil, associa uma entidade (pessoa, processo, servidor) a um par de chaves criptográficas (chave pública e chave privada). Os certificados contêm os dados de seu titular conforme detalhado na Política de Segurança de cada Autoridade Certificadora.

Há dois tipos básicos de certificados, os de assinatura digital e os de sigilo. Os certificados de Assinatura Digital subdividem-se em A1, A2, A3, A4, T3 e T4, e são utilizados em aplicações como confirmação de identidade na Web, correio eletrônico, transações on-line, redes privadas virtuais, transações eletrônicas, informações eletrônicas, cifração de chaves de sessão e assinatura de documentos eletrônicos com verificação da integridade de suas informações.

Já os certificados de sigilo subdividem-se em S1, S2, S3, S4, e são utilizados em aplicações como cifração de documentos, bases de dados, mensagens e outras informações eletrônicas, com a finalidade de garantir o seu sigilo.

Os tipos de A1 a A4, T3 a T4, e de S1 a S4, indicados acima, definem escalas de requisitos de segurança, nas quais os tipos A1, S1 e T3 estão associados aos requisitos menos rigorosos e os tipos A4, S4 e T4 aos requisitos mais rigorosos.

No que se refere à escolha dos algoritmos criptográficos a serem utilizados, seja para transmitir ou armazenar uma informação, devem ser levadas em consideração as diferenças entre um **esquema de criptografia incondicionalmente seguro** e um **esquema de criptografia computacionalmente seguro.**

No primeiro, o texto cifrado não possui informações suficientes para determinar exclusivamente o texto claro correspondente, pois eles não guardam nenhuma relação previsível entre si. Para tanto, faz-se necessária a utilização de equipamentos que possuam geradores de números aleatórios reais, que são dispositivos encarregados de gerar sequências de números verdadeiramente aleatórias por meio de processos como mensuração do ruído térmico ou ruído atmosférico. Esses equipamentos têm alto custo, e a velocidade com que se

obtêm essas sequências depende exclusivamente do processo de mensuração, o que pode ser lento em determinados casos.

Já o esquema de criptografia computacionalmente seguro é aquele em que o custo para quebrar a cifra excede o valor da informação cifrada e/ou o tempo requerido para quebrar a cifra excede o tempo de vida da informação. Nesse caso, são utilizados equipamentos que contêm geradores de números pseudoaleatórios, desenvolvidos a partir de algoritmos computacionais.

De fato, optar por um determinado algoritmo criptográfico tem como premissa que antes disso se tenha uma avaliação da criticidade da informação a ser protegida. A escolha de um algoritmo fraco para os padrões computacionais atuais não implica em dizer que a informação estará desprotegida, pois seu valor pode ser menor que o custo para obtê-la, ou ainda, seu tempo de vida pode ser inferior ao tempo necessário para quebrar o algoritmo.

Essa avaliação requer uma análise e avaliação de riscos e um processo adequado de classificação da informação, o que exige um nível mínimo de maturidade em segurança da informação. Isso pode ser conquistado com uma gestão de segurança da informação eficaz, que garanta que os usuários estão conscientes de suas responsabilidades no tratamento da informação e que a informação seja classificada e analisada em termos de criticidade, para que os controles de segurança adequados sejam aplicados em maior ou menor grau de acordo com os requisitos de confidencialidade, disponibilidade e integridade.

Dispositivos de Segurança

Sistemas de segurança são os controles técnicos/tecnológicos destinados a garantir uma ou mais das propriedades de proteção da informação – confidencialidade, integridade, disponibilidade, autenticidade e não-repúdio.

De acordo com o tipo de proteção necessário, tais sistemas realizam, principalmente uma ou mais das seguintes atividades:

a) Controles de acesso, que podem ser aplicados de várias formas: diretivo, preventivo, corretivo, de recuperação, etc.;
b) Identificação, autenticação, autorização, contabilização de usuários;
c) Sigilo e garantia de integridade e autenticidade da informação e/ou das transações;
d) Monitoramento dos sistemas e recursos computacionais (identificação de ameaças, ataques).

A maioria das redes de computadores utiliza um conjunto mínimo de soluções de segurança que assegura proteção contra grande parte das ameaças. Abaixo segue uma lista com algumas das principais soluções disponíveis no mercado:

a) Firewall;
b) Antivírus;
c) Antispam;
d) Anti Distributed Denial of Service – Anti DDOS;
e) Security Information and Event Management - SIEM;
f) Virtual Private Network – VPN;
g) Intrusion Detection System – IDS / Intrusion Prevention System – IPS;
h) Softwares de controle de acesso à rede e autenticação de usuários;
i) Soluções de cópias de segurança (backup);
j) Hardware Security Module – HSM;
k) Data Loss Prevention – DLP;
l) Soluções de criptografia de arquivos e disco;

O estudo da PwC apresenta os principais dispositivos de proteção utilizados pelos respondentes do setor de Telecomunicações (Figura 4).

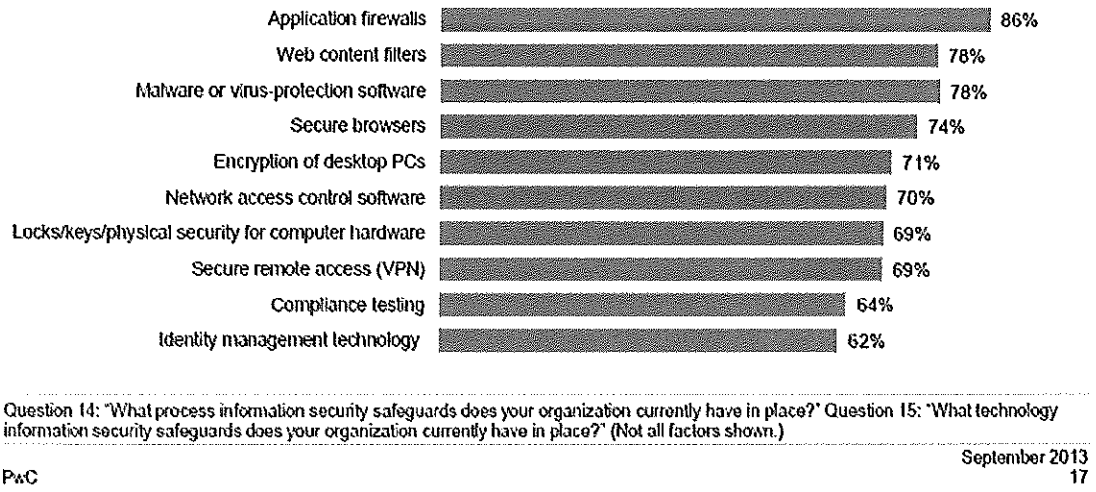

Figura 4 - Estatística de uso dos dispositivos de proteção tradicionalmente empregados como controles de segurança. [Disponível em http://www.pwc.com/gx/en/consulting-services/information-security-survey/download.jhtml].

A escolha de quais dispositivos de segurança implementar numa rede deve estar ligada a que proteções se deseja garantir e até que ponto é necessário assegurar proteção. Novamente, essa escolha requer uma análise e avaliação de riscos e um processo adequado de classificação da informação.

Optar por um conjunto mínimo de dispositivos de segurança que enderecem a maior parte das ameaças tem sido o caminho adotado por grande parte das organizações, cabendo avaliar, caso a caso, a adoção de soluções adicionais ou específicas para requisitos distintos de segurança.

Além disso, o governo brasileiro e as empresas de mercado têm colaborado na definição de requisitos mínimos de segurança para a maior parte das soluções. Como exemplo, os padrões de hardware, os algoritmos e parâmetros criptográficos a serem empregados em todos os processos realizados no âmbito da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) estão definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[9] (DOC ICP-01.01), atualmente em sua versão 2.3, de 06 de julho de 2012. Nele são estabelecidos tamanhos mínimos de chaves, opções de algoritmos aceitáveis, entre outras definições.

As várias soluções que estão sendo utilizadas para criptografia e segurança de dados no governo podem ser avaliadas quanto à adequação por meio da Arquitetura Padrão de Interoperabilidade de Governo Eletrônico – e-PING[10]. Este documento, desenvolvido e homologado pelo próprio governo brasileiro, inclui conjunto mínimo de premissas, políticas e especificações técnicas que regulamentam a utilização da TIC no governo federal, estabelecendo as condições de interação desenvolvido e homologado pelo próprio governo. Para os órgãos do Poder Executivo a adoção é obrigatória (Portaria SLTI/MP nº 5, de 14 de julho de 2005). Já para outras esferas e poderes a adoção dos padrões não pode ser imposta; dar-se-á de forma voluntária e sem qualquer ingerência. Cabe ressaltar que a e-PING não tem por objetivo recomendar ferramentas, mas sim tecnologias e padrões.

Apesar da arquitetura ePing ter a interoperabilidade como principal foco, ela inclui uma área de segurança, na qual são endereçados os tópicos de criptografia e segurança de dados.

Cada área teve seus componentes especificados, para os quais foram estabelecidos os respectivos padrões. Quanto à segurança, os componentes foram separados em sete tipos: comunicação de dados; correio eletrônico; criptografia; desenvolvimento de sistemas; serviços de rede; redes sem fio; e resposta a incidentes de segurança da informação. Além disso, cada componente pode estar em uma das cinco situações: adotado; recomendado; em transição; em estudo; e estudo futuro.

Os itens em questão devem seguir algumas políticas para fazer parte do documento. Umas das políticas gerais da segurança é que a interoperabilidade na prestação dos serviços de governo eletrônico deve considerar o nível de segurança requerido pelo serviço, com a máxima transparência. O e-Ping também inclui a referência a um conjunto de decretos e instruções normativas, aos quais os órgãos da APF devem recorrer. São eles: Decreto nº 3.505/2000; Decreto nº 7.845/2002; a Instrução Normativa nº 01/2008 – GSI/PR e suas Normas Complementares; a Instrução Normativa nº 02/2013 – GSI/PR; a Instrução Normativa nº 3/2013 – GSI/PR; e as normas NBR ISO/IEC 27001:2006 – sistemas de gestão de segurança da

[9] http://www.iti.gov.br/images/twiki/URL/pub/Certificacao/DocIcp/DOC-ICP-01.01_-_versao_2.3_PADROES_E_ALGORITIMOS_CRIPTOGRAFICOS_DA_ICP-BRASIL.pdf
[10] http://www.governoeletronico.gov.br/acoes-e-projetos/e-ping-padroes-de-interoperabilidade

informação; NBR ISO/IEC 27002:2005 – código de prática para a gestão da segurança da informação; NBR ISO/IEC 27003:2011 – diretrizes para implantação de um sistema de gestão da segurança da informação; NBR ISO/IEC 27004:2010 – medição; NBR ISO/IEC 27005:2008 - Gestão de riscos de segurança da informação NBR ISO/IEC 27011:2008 – diretrizes para gestão da segurança da informação para organizações de telecomunicações baseadas na ABNT NBR ISO/IEC 27002; e NBR 15999-1:2007 e 15999-2:2008 – gestão de continuidade de negócios. Com relação ao uso de criptografia e certificação digital, o e-Ping remete às técnicas, práticas e procedimentos definidos pela ICP-Brasil.

Considerando então os itens e essas políticas, dois estados podem ser considerados necessários: "adotados" (A) são aqueles que foram submetidos a um processo formal de homologação, e por isso são requisitos indispensáveis à segurança; os "recomendados" (R) são aqueles que ainda não foram submetidos ao processo formal de homologação, mas ainda assim, têm seu uso recomendado.

A seguir são apresentados os itens Adotados e Recomendados relacionados à comunicação de dados.

Componente	Especificação	SIT
Transferência de dados em redes inseguras	TLS – Transport Layer Security, RFC 5246 (atualizada pela RFC 5746 e RFC 5878). Caso seja necessário o protocolo TLS v1 pode emular o SSL v3.	R
Algoritmos para troca de chaves de sessão, durante o handshake	RSA, Diffie-Hellman RSA, Diffie-Hellman DSS, DHE_DSS, DHE_RSA;	R
Algoritmos para definição de chave de cifração	RC4, IDEA, 3DES e AES	R
Certificado Digital	X.509 v3 – ICP-Brasil, SASL - Simple Authentication and Security Layer, RFC 4422	R
Hipertexto e transferência de arquivos	RFC 2818 (atualizada pela RFC 5785)	R
Segurança de redes IPv4	IPSec Authentication Header RFC 4303 e RFC 4835 para autenticação de cabeçalho do IP. IKE – Internet Key Exchange, RFC 4306 (atualizada pela RFC5282 ESP – Encapsulating Security Payload, RFC 4303 Requisito para VPN – Virtual Private Network.	A
Segurança de redes IPv4 para protocolos de aplicação	O S/MIME v3, RFC 5751 deverá ser utilizado quando for apropriado para segurança de mensagens gerais de governo.	A
Segurança de redes IPv6 na camada de rede	O IPv6 definido na RFC 2460 (atualizada pela RFC 5095), RFC 5722 e RFC 5871 apresenta implementações de segurança nativas no protocolo. As especificações do IPv6 definiram dois mecanismos de segurança:	R

SENADO FEDERAL

Secretaria de Tecnologia da Informação – Prodasen
Coordenação de Infraestrutura de Tecnologia da Informação - COINTI

	a autenticação de cabeçalho AH (Authentication Header) RFC 4302 ou autenticação IP, e a segurança do encapsulamento IP, ESP (Encrypted Security Payload) RFC 4303.	

A seguir são apresentados os itens Adotados e Recomendados relacionados a Correio Eletrônico.

Componente	Especificação	SIT
Acesso a caixas postais	O acesso à caixa postal deverá ocorrer através do cliente do software de correio eletrônico utilizado, considerando as facilidades de segurança nativas do cliente. Quando não for possível utilizar o cliente específico ou for necessário acessar a caixa postal através de redes não seguras (por exemplo: Internet) deve-se utilizar HTTPS de acordo com os padrões de segurança de transporte descritos na RFC 2595 (atualizada pela RFC 4616), que trata da utilização do TLS com IMAP, POP3 e ACAP.	A
Conteúdo de e-mail	O S/MIME V3 deverá ser utilizado quando for apropriado para segurança de mensagens gerais de governo. Isso inclui RFC 5652, RFC 3370 (atualizada pela RFC 5754), RFC 2631, RFC 5750, RFC 5751 e RFC 5652.	A
Transporte de e-mail	Utilizar SPF (Sender Policy Framework) nos termos da RFC 4408, e reservar a porta 25, do protocolo SMTP, exclusivamente para transporte de mensagens entre MTAs; para comunicação entre MUAs e MTAs, utilizar a porta 587 (Submission), nos termos das RFCs 4409 e 5068	A
Identificação de e-mail	Utilizar DKIM (DomainKey Identified Mail) nos termos da RFC 4871 (atualizada pela RFC 5672).	R
Assinatura	Utilizar certificado padrão ICP-Brasil para assinatura de e-mail, quando exigido. Em conformidade com o disposto na Medida Provisória nº 2.200-2, de 24/08/2001 e Decreto nº 3.996 de 31/10/2001.	A

A seguir são apresentados os itens Adotados e Recomendados relacionados a Criptografia.

Componente	Especificação	SIT	Observações
Algoritmo de cifração	3DES ou AES	R	
Algoritmos para assinatura/hashing	SHA-256 ou SHA-512	R	
Algoritmo para transporte de chave criptográfica de conteúdo/sessão	RSA	A	
Algoritmos criptográficos baseados em curvas elípticas	ECDSA 256 e ECDSA 512 (RFC 5480). ECIES 256 e ECIES 512.	A	
Requisitos de segurança para módulos criptográficos	Homologação da ICP-Brasil NSH-2 e NSH-3; FIPS 140-1 e FIPS 140-2.	R	Ver Resolução nº 65, de 09/06/2009, do Comitê Gestor da Infra-estrutura de Chaves Públicas Brasileira – ICP-Brasil).

Certificado Digital da AC-raiz para Navegadores e Visualizadores de Arquivos	Devem ser aderentes aos padrões da ICP – Brasil.	R	Os certificados da AC-raiz devem ser instalados nos navegadores e visualizadores de arquivos conforme recomendado na IN nº 5/2009/ITI.

A seguir são apresentados os itens Adotados e Recomendados relacionados a Serviços de Rede.

Componente	Especificação	SIT	Observações
Diretório	LDAPv3 RFC 4510, RFC 4511, RFC 4512 e RFC 4513. LDAP v3 extensão para TLS RFC 4510, RFC 4511 e RFC 4513.	R	i) Portaria Normativa nº 2, de 3 de outubro de 2002 - Publicada no D.O. do dia 4 de outubro de 2002. Seção 1, página 85. ii) Consultar errata para RFC 4511 e RFC 4512.
DNSSEC	Resolução nº 7 de 29/07/2002 – Comitê Executivo do Governo Eletrônico Práticas de Segurança para Administradores de Redes Internet Centro de Estudos, Resposta e Tratamento a Incidentes – Tutorial DNSSEC - Versão 1.7.4 - ftp://ftp.registro.br/pub/doc/tutorial-dnssec.pdf	A	
Carimbo do tempo	RFC 3628 TSAs – Policy Requirements for Time-Stamping Authorities, Time-Stamp Protocol, RFC 3161 ETSI TS101861 (Time-Stamping Profile) (atualizada pela RFC 5816).	R	O serviço de carimbo do tempo deverá estar de acordo com as normas da ICP-Brasil. Consultar errata para RFC 3161.

A seguir são apresentados os itens Adotados e Recomendados relacionados a redes sem fio.

Componente	Especificação	SIT
LAN sem fio 802.11	Usar a especificação WPA2 (Wi-Fi Protect Access) com criptografia AES	R

A seguir são apresentados os itens Adotados e Recomendados relacionados à Resposta a Incidentes de Segurança da Informação.

Componente	Especificação	SIT
Preservação de registros	Guidelines for Evidence Collection and Archiving, RFC 3227.	R
Gerenciamento de incidentes em redes computacionais	Expectations for Computer Security Incident Response, RFC 2350. Criação de equipes de tratamento e resposta a incidentes em redes computacionais conforme Norma Complementar nº 05/09	A

SENADO FEDERAL

Secretaria de Tecnologia da Informação – Prodasen
Coordenação de Infraestrutura de Tecnologia da Informação - COINTI

	(http://dsic.planalto.gov.br/documentos/nc_05_etir.pdf). Diretrizes para gerenciamento de incidentes em redes computacionais nos órgãos e entidades da Administração Pública Federal conforme Norma Complementar nº 08/2010 (http://dsic.planalto.gov.br/documentos/nc_8_gestao_etir.pdf)	

Senado Federal
Prodasen

PARECER TÉCNICO SOBRE AS INFORMAÇÕES ENVIADAS POR DIVERSOS ÓRGÃOS E EMPRESAS PÚBLICAS ACERCA DA CRIPTOGRAFIA E SISTEMAS DE SEGURANÇA DE DADOS UTILIZADOS PELO GOVERNO FEDERAL

Fevereiro de 2014

Apresentação da Equipe

- André Luiz Bandeira Molina
  - Analista de Informática Legislativa - Coordenador de Infraestrutura de TI
  - Mestre em Telecomunicações pela Universidade de Brasília - UnB
  - Especialista em Criptografia pela Universidade Federal Fluminense - UFF
  - Engenheiro de Computação pelo Instituto Tecnológico de Aeronáutica - ITA
  - Certificado CCNA
- Flávio Henrique de Sousa Lima
  - Analista de Informática Legislativa - Coordenador do Escritório Corporativo de Governança e Gestão Estratégica do Senado Federal
  - Mestre em Ciência da Computação pela UNICAMP
  - MBA em Gestão Empresarial pela Fundação Dom Cabral
- Giuliano Macedo Arruda
  - Analista de Informática Legislativa - Chefe do Serviço de Suporte à Infraestrutura de Estações de Trabalho
  - Especialista em Segurança da Informação pela Universidade Metropolitana de Santos - UniMES
  - Engenheiro de Redes de Comunicação pela Universidade de Brasília - UnB
- Norman Pozo Molina Junior
  - Analista de Informática Legislativa - Chefe substituto do Serviço de Suporte à Infraestrutura de Rede
  - Bacharel em Ciência da Computação pela Universidade Federal do Paraná - UFPR
  - Certificado CCNA e CCAI

SENADO FEDERAL

Considerações Iniciais

- Solicitação de análise e emissão de parecer técnico sobre as informações enviadas por diversos órgãos e empresas públicas **acerca da criptografia e sistemas de segurança de dados utilizados pelo governo federal.**
- 27 documentos contendo informações pertinentes aos temas criptografia e sistemas de segurança de dados.
- Os requerimentos expedidos solicitam informações acerca das **ações para minorar a possibilidade de ataques virtuais/digitais às atividades do governo brasileiro.** A maioria das respostas endereça os seguintes questionamentos:

  1 – Criptografia:
  Qual empresa desenvolveu o referido sistema?
  Qual o sistema utilizado?

  2 – Segurança da Informação:
  Quais os dispositivos de segurança da informação utilizados?
  Qual empresa ou as empresas que forneceram tais dispositivos?

SENADO FEDERAL

Considerações Iniciais

- Os questionamentos buscam, em essência, abordar somente o aspecto tecnológico.
- A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e **funções de software e hardware** (ABNT ISO 27002:2005)
  - pessoas + processos + **tecnologia**

SENADO FEDERAL

Padrões de mercado e algoritmos públicos

- Uso maciço de protocolos baseados em padrões de mercado.
  - HTTPS, SSL, TLS e IPSec indica que um nível adequado de segurança pode ser atingido por meio desses padrões, desde que se utilize suas últimas versões e que se saiba que tipo de proteção se deseja assegurar
  - escolha de algoritmos criptográficos padronizados pelo mercado e reconhecidamente fortes pela comunidade científica
    - AES, 3-DES, RSA com chaves a partir de 2048 bits, SHA-256, SHA-512, ECC com chaves a partir de 224 bits
  - exaustivamente testados pela comunidade científica em busca de falhas
  - ICP-Brasil é muito utilizada
    - PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL (DOC ICP-01.01) - tamanhos mínimos de chaves, opções de algoritmos aceitáveis, entre outras definições. Utiliza padrões de mercado.

SENADO FEDERAL

Utilização de Algoritmos Frágeis

- Alguns órgãos fazem uso de algoritmos frágeis para os padrões atuais de criptografia.
- DES, SHA-1 e MD5.
- Grande parte dos atuais dispositivos de segurança ainda mantêm esses algoritmos disponíveis a fim de permitir compatibilidade com dispositivos mais antigos.
- Não se pode afirmar efetivamente que sua utilização seja insegura sem ter conhecimento do tipo de informação que está sendo protegida.
  - esquema de criptografia computacionalmente seguro: o custo para quebrar a cifra excede o valor da informação cifrada e/ou o tempo requerido para quebrar a cifra excede o tempo de vida da informação.

SENADO FEDERAL

Utilização de Algoritmos Frágeis

- DES – Data Encryption Standard
  - Utilizado como padrão americano entre 1977 e 1999
  - Ataques só por força bruta

Desafio	Grupo	Data	Duração
DES I	Rocke Verser	Julho de 1997	96 dias
DES II-1	Distributed.net	Fevereiro de 1998	41 dias
DES II-2	EFF (Deep Crack)	Julho de 1998	56 horas
DES III	EFF (Deep Crack e Distributed.net	Janeiro de 1999	22 horas e 15 minutos

SENADO FEDERAL

Utilização de Algoritmos Frágeis

- MD5 e SHA-1
  - RFC 4270 (2005), recomenda o abandono desses algoritmos devido às fragilidades encontradas e que fosse utilizado o SHA-256.
  - Em 2008: criado um certificado forjado para SSL, com assinatura válida utilizando MD5.
  - Em 2012, de acordo com a Microsoft, os autores do malware Flame utilizaram ataque sobre o MD5 para forjar um certificado de assinatura de código Windows.

SENADO FEDERAL

Utilização de Algoritmo de Estado

- CEPESC proporciona soluções de segurança, baseadas em algoritmo criptográfico de Estado, voltadas para a segurança das comunicações de órgãos e entidades da Administração Pública Federal.
  - Proteção ao sistema de comunicação e transferência eletrônica dos boletins de urna entre os TREs e o TSE.
  - Plataforma Criptográfica Portátil (PCP v2) – criptografia de arquivos, certificação digital e criptografia de sistema de arquivos.
- Princípio de Kerckhoffs: "O único segredo em um sistema criptográfico deve ser a chave. O algoritmo deve ser publicamente conhecido. Se a segurança for baseada em muitos segredos, haverá mais vulnerabilidades possíveis de se explorar."
  - engenharia reversa podem ser utilizadas para se obter o funcionamento do algoritmo
  - quantidade significativa de ataques com base em técnicas analíticas desenvolvidas e refinadas pela comunidade criptoanalítica. Ex: criptoanálise diferencial e criptoanálise linear.

SENADO FEDERAL

Utilização de Algoritmo de Estado

- Decreto nº 7.845, de 14 de novembro de 2012
  - Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento.
- Instrução Normativa GSI/PR nº 3, de 06 de março de 2013
  - Dispõe sobre os parâmetros e padrões mínimos dos recursos criptográficos baseados em algoritmos de Estado para criptografia da informação classificada no âmbito do Poder Executivo Federal.
- NC 09/IN01/DSIC/GSI/PR (Revisão 01), de fevereiro de 2013
  - Estabelece orientações específicas para o uso de recursos criptográficos em Segurança da Informação e Comunicações, nos órgãos ou entidades da Administração Pública Federal, direta e indireta.

SENADO FEDERAL

Utilização de Algoritmo de Estado

- Decreto nº 7.845, de 14 de novembro de 2012
  - Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento.
  - Classificação conforme Lei de Acesso à Informação: LEI Nº 12.527, DE 18 DE NOVEMBRO DE 2011.

> Art. 40. A cifração e a decifração de informação **classificada em qualquer grau de sigilo** deverão utilizar recurso criptográfico baseado em algoritmo de Estado.
>
> Parágrafo único. Compete ao Gabinete de Segurança Institucional da Presidência da República estabelecer parâmetros e padrões para os recursos criptográficos baseados em algoritmo de Estado, ouvido o Comitê Gestor de Segurança da Informação previsto no art. 6o do Decreto no 3.505, de 13 de junho de 2000.

SENADO FEDERAL

Utilização de Algoritmo de Estado

- Instrução Normativa GSI/PR nº 3, de 06 de março de 2013
  - Dispõe sobre os parâmetros e padrões mínimos dos recursos criptográficos baseados em algoritmos de Estado para criptografia da informação classificada no âmbito do Poder Executivo Federal.

> Art. 4º. A cifração e decifração de informações **classificadas, em qualquer grau de sigilo**, devem utilizar recurso criptográfico baseado em algoritmo de Estado em conformidade com os padrões e parâmetros mínimos estabelecidos na NC 09/IN01/DSIC/GSI/PR (Revisão 01), de fevereiro de 2013, reproduzidos no Anexo desta Instrução Normativa.
>
> Art. 5º. O recurso criptográfico baseado em algoritmo de Estado deverá ser de desenvolvimento próprio ou por órgãos e entidades do Poder Executivo Federal, mediante acordo ou termo de cooperação, vedada a participação e contratação de empresas e profissionais externos, para tal finalidade.

SENADO FEDERAL

Utilização de Algoritmo de Estado

- Na prática, a partir da documentação apresentada, a maior parte dos órgãos respondentes utiliza algoritmos criptográficos abertos e padronizados pelo mercado.
  - Os requisitos mínimos de segurança para uso desses algoritmos na Administração Pública Federal (APF), a exemplo do tamanho mínimo da chave, não são normatizados.
  - Existem apenas recomendações como as do e-Ping ou os padrões mínimos definidos pelo Instituto de Tecnologia da Informação (ITI), restritos à ICP-Brasil.

SENADO FEDERAL

Dispositivos de Segurança Proprietários e Sistemas Abertos

- A maioria dos órgãos respondentes utiliza softwares e dispositivos de segurança fabricados por empresas privadas, a maior parte sediadas em outros países.
  - Códigos não são abertos
  - Não há uma entidade nacional com a responsabilidade legal de auditar e atestar a confiabilidade desses softwares e dispositivos
  - Decreto nº 8.135, de 4 de novembro de 2013
    - Dispõe sobre as comunicações de dados da administração pública federal direta, autárquica e fundacional, e sobre a dispensa de licitação nas contratações que possam comprometer a segurança nacional.
    - Art. 1º, § 3º: Os programas e equipamentos destinados às atividades de que trata o caput deverão ter características que permitam auditoria para fins de garantia da disponibilidade, integridade, confidencialidade e autenticidade das informações, na forma da regulamentação de que trata o § 5º.

SENADO FEDERAL

Dispositivos de Segurança Proprietários e Sistemas Abertos

January 11, 2008

NSA Backdoors in Crypto AG Ciphering Machines

This story made the rounds in European newspapers about ten years ago -- mostly stories in German, if I remember -- but it wasn't covered much here in the U.S.

> For half a century, Crypto AG, a Swiss company located in Zug, has sold to more than 100 countries the encryption machines their officials rely upon to exchange their most sensitive economic, diplomatic and military messages. Crypto AG was founded in 1952 by the legendary (Russian born) Swedish cryptographer Boris Hagelin. During World War II, Hagelin sold 140,000 of his machine to the US Army.
>
> "In the meantime, the Crypto AG has built up long standing cooperative relations with customers in 130 countries," states a prospectus of the company. The home page of the company Web site says, "Crypto AG is the preferred top-security partner for civilian and military authorities worldwide. Security is our business and will always remain our business."

Dispositivos de Segurança Proprietários e Sistemas Abertos

Especialistas em criptografia classificam sistema RSA como falho

27/02/2012 Sem comentários Blog

Em estudo publicado em fevereiro e intitulado Ron was wrong, Whit is right, em que foram testadas milhões chaves públicas X.509 coletadas na web, especialistas em criptografia encontraram o que dizem ser uma frequência assustadoramente alta de chaves privadas RSA duplicadas. Segundo os especialistas, o módulo RSA de 1024 bits fornece a segurança de 99,8% na melhor das hipóteses. "As chaves privadas são acessíveis a qualquer pessoa que se dê ao trabalho de refazer o nosso trabalho."

NSA Paid a Huge Security Firm $10 Million to Keep Encryption Weak

Reuters reports that the NSA paid massive computer security firm RSA $10 million to promote a flawed encryption system so that the surveillance organization could wiggle its way around security. In other words, the NSA bribed the firm to leave the back door to computers all over the world open.

Dispositivos de Segurança Proprietários e Sistemas Abertos

- Sistemas abertos ou livres
  - Não impedem a ocorrência de *backdoors* ou ainda a simples existência de falhas de implementação que permitam a exploração de vulnerabilidades.
  - Auditados pela comunidade ou meio acadêmico de forma mais objetiva
- Solução: proteções complementares (defesa em profundidade)
  - Série de controles de segurança físicos, lógicos e em processos, com base em ambientes lógicos segregados e implantados através de camadas isoladas, por meio de tecnologias distintas, inclusive de fornecedores diferentes.

SENADO FEDERAL

Auditorias de Sistemas de Segurança

Auditorias governamentais:

- Tribunal de Contas da União, por intermédio da Secretaria de Fiscalização de Tecnologia da Informação - SEFTI
  - Fiscalização Operacional e/ou de Conformidade
  - Acórdão TCU 1603/2008 - Resultados expressivos com relação a aspectos de governança de TI e gestão de segurança da informação no contexto do Setor Público Federal
- Controladoria-Geral da União - CGU
  - Restrito ao Poder Executivo

SENADO FEDERAL

Auditorias de Sistemas de Segurança

- ABIN

6. Assim, dentro do escopo dessa proteção, a Agência Brasileira de Inteligência (ABIN), atendendo à sua atribuição legal, conforme o artigo 4º da lei 9.883/1999, desenvolve programas, que oferecem mecanismos preventivos e são direcionados a instituições nacionais detentoras de conhecimentos sensíveis.

7. Desse modo, os programas são implementados por meio de ações de sensibilização (palestras, oficinas, seminários) e de assessoria para a segurança, abrangendo desde o apoio na elaboração de normativos até avaliações de risco completas, as quais incluem identificação de vulnerabilidades nos sistemas de proteção e os conjuntos de recomendações associadas às respectivas medidas corretivas.

8. Os programas de proteção são ministrados sem ônus e destinam-se às instituições estratégicas nacionais interessadas. A adesão aos programas é realizada por meio de solicitação oficial ao Gabinete de Segurança Institucional (GSI).

Auditorias de Sistemas de Segurança

- Nos Estados Unidos
  - *Federal Information Security Management Act of 2002* - FISMA

TITLE III—INFORMATION SECURITY

SEC. 301. INFORMATION SECURITY.

(a) SHORT TITLE.—This title may be cited as the "Federal Information Security Management Act of 2002".

(b) INFORMATION SECURITY.—

(1) IN GENERAL.—Chapter 35 of title 44, United States Code, is amended by adding at the end the following new subchapter:

"SUBCHAPTER III—INFORMATION SECURITY

"§ 3541. Purposes

"The purposes of this subchapter are to—

"(1) provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets;

"(2) recognize the highly networked nature of the current Federal computing environment and provide effective governmentwide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian, national security, and law enforcement communities;

"(3) provide for development and maintenance of minimum controls required to protect Federal information and information systems;

Auditorias de Sistemas de Segurança

- Nos Estados Unidos
  - *Federal Information Security Management Act of 2002* – FISMA

''§ 3545. Annual independent evaluation
''(a) In General.–(1) Each year each agency shall have performed an independent evaluation of the information security program and practices of that agency to determine the effectiveness of such program and practices.
''(2) Each evaluation under this section shall include– ''(A) testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems;
''(B) an assessment (made on the basis of the results of the testing) of compliance with– ''(i) the requirements of this subchapter; and ''(ii) related information security policies, procedures, standards, and guidelines; and ''(C) separate presentations, as appropriate, regarding information security relating to national security systems.
''(b) Independent Auditor.–Subject to subsection (c)– ''(1) for each agency with an Inspector General appointed under the Inspector General Act of 1978, the annual evaluation required by this section shall be performed by the Inspector General or by an independent external auditor, as determined by the Inspector General of the agency; and ''(2) for each agency to which paragraph (1) does not apply,
the head of the agency shall engage an independent external auditor to perform the evaluation.

Auditorias de Sistemas de Segurança

- Nos Estados Unidos
  - Resultados e recomendações dessas auditorias são disponibilizados na Internet, inclusive quando da ocorrência de achados que indicam fragilidades nos programas de segurança da informação.

Findings and Recommendations

This report constitutes the Office of Inspector General's (OIG) independent evaluation of the Department of Agriculture's (USDA) Information Technology (IT) security program and practices, as required by the Federal Information Security Management Act (FISMA) of 2002, and is based on the questions provided by the Office of Management and Budget (OMB)/Department of Homeland Security (DHS). These questions are designed to assess the status of the Department's security posture during fiscal year (FY) 2012. The OMB/DHS framework requires OIG to audit processes, policies, and procedures that had already been implemented and documented, and were being monitored during FY 2012. While USDA's planned activities might improve its security posture in the future, we could not evaluate these initiatives as part of our FY 2012 FISMA review because they were not fully operational during the year. However, we did note that during FY 2012, the Office of the Chief Information Officer (OCIO) began a reorganization, appointed its first Chief Information Security Officer, and elevated the responsibility for policies to the executive level.

USDA has made improvements in its IT security over the last decade, but many longstanding weaknesses remain. In our FISMA audits for FYs 2009, 2010, and 2011, OIG made 43 recommendations for improving the overall security of USDA's systems. By the end of FY 2012, the Department had remediated and closed only 14 recommendations, leaving 29 to be addressed. OIG has reported on many of these remaining recommendations since 2001, when we first detailed material weaknesses in the design and effectiveness of USDA's overall IT security program. The findings in this report continue to be a material IT weakness for the Department.

Auditorias de Sistemas de Segurança

Dúvidas?

Folha nº 26
Processo
Rubrica

SENADO FEDERAL

Secretaria de Tecnologia da Informação – Prodasen
Coordenação de Infraestrutura de Tecnologia da Informação - COINTI

Despacho nº 007/2014 – PRDSTI/COINTI
Processo SIGAD nº 00200.027800/2013-44

SENADO FEDERAL
00100.011242/2014-12
COORD INFRAESTRUTURA TECNOL INF

Ref.: Requerimento de Informações nº 074/13.

Senhor Diretor do PRODASEN,

Conforme solicitado à folha 02, encaminho parecer técnico sobre as informações enviadas por diversos órgãos e empresas públicas acerca da criptografia e sistemas de segurança de dados utilizados pelo governo federal.

Segue, ainda, apresentação realizada em 11 de fevereiro aos senhores Gustavo Alves de Souza e Verner de Miranda Pereira, assessores legislativos do gabinete da Excelentíssima Senhora Senadora Vanessa Grazziotin, sobre os pontos principais do parecer técnico.

COINTI, 13 de fevereiro de 2014.

André Luiz Bandeira de Molina
Matrícula nº. 226029
Coordenador da COINTI

André Molina
Coordenador da COINTI

SENADO FEDERAL

Secretaria de Tecnologia da Informação – PRODASEN

Secretaria de Tecnologia da Informação - PRODASEN
Folha: 27
Rubrica

Despacho nº 018/2014-PRDSTI/GBPRD
Processo nº. 0200.027800/2013-44

Ref.: **Requerimento de informação. Solicitação de parecer técnico sobre as informações enviadas pelos diversos órgãos e empresas públicas acerca da criptografia e sistemas de segurança de dados utilizados pelo Governo Federal.**

Senhor Diretor-Geral,

Com meus cordiais cumprimentos, retorno o presente processo a Vossa Senhoria, com o parecer da equipe técnica do Prodasen, sobre as informações enviadas por diversos órgãos e empresas acerca da criptografia e sistemas de segurança de dados utilizados pelo Governo Federal e apresentação sobre os pontos principais do parecer técnico, às fls. 04/25.

Secretaria de Tecnologia da Informação-Prodasen, 13 de fevereiro de 2014.

Victor Guimarães Vieira
Diretor do Prodasen

SENADO FEDERAL
Diretoria-Geral

Diretoria Geral
Folha:
Rubrica

Processo nº 00200.027800/2013-44

Brasília, 14 de fevereiro de 2014.

Excelentíssima Senhora Senadora Vanessa Grazziotin,

Em atenção ao Ofício nº 069/2014 - CPIDAESP direcionado a esta Diretoria-Geral em 11 de dezembro de 2013, relativo ao Requerimento nº 074 CPI-ESP, encaminho os autos para conhecimento do parecer elaborado pela Secretaria de Tecnologia da Informação – PRODASEN (fls. 04/25).

Respeitosamente,

ANTÔNIO HELDER MEDEIROS REBOUÇAS
Diretor-Geral

U:\Dger\Assessoria Técnica\2014\DESPACHOS\GABINETES - sarahns