00001.003590/2013-45

ESP REC
000007

PRESIDÊNCIA DA REPÚBLICA
GABINETE DE SEGURANÇA INSTITUCIONAL
Palácio do Planalto – 2º Andar – sala 215
70150-900 – Brasília-DF
(61) 3411-1117 – gsipr@presidencia.gov.br

Ofício nº 2192/GSIPR/CH

Brasília, 24 de outubro de 2013.

A Sua Excelência a Senhora
Senadora VANESSA GRAZZIOTIN
Presidente da Comissão Parlamentar de Inquérito
Senado Federal
70.160-900 - Brasília - DF

Assunto: **Requerimento de Informação nº 030, de 2013.**

Senhora Presidente,

Em resposta ao Ofício nº 013/2013-CPIDAESP, de 25 de setembro de 2013, que encaminhou cópia do Requerimento de Informação nº 030/13, levo ao conhecimento de Vossa Excelência o seguinte:

1. O CEPESC foi criado em 1982 com o objetivo de sanar a flagrante deficiência do Brasil em salvaguardar o sigilo das transmissões oficiais e, desde essa época, vem pesquisando e desenvolvendo soluções, baseadas em algoritmo criptográfico de Estado, voltadas para a segurança das comunicações de órgãos e entidades da Administração Pública Federal – APF.

2. Além do Poder Executivo, o CEPESC vem, desde 1996, fornecendo solução de proteção ao sistema de comunicação e transferência eletrônica dos boletins de urna entre os Tribunais Regionais Eleitorais – TREs e o Tribunal Superior Eleitoral – TSE.

3. Atualmente, o CEPESC dispõe dispositivos criptográficos, baseados em algoritmo criptográfico de Estado, que implementam soluções para a segurança de dados, voz e imagem, todas elas. Os dispositivos criptográficos são:

a) Telefone Seguro Governamental (TSG-NML) – telefonia fixa;

b) Plataforma Criptográfica Portátil (PCP v2) – criptografia de arquivos, certificação digital e criptografia de sistema de arquivos;

c) Plataforma Criptográfica de Alto Desempenho (PCAD) – estabelecimentos de redes virtuais privadas com criptografia baseada em algoritmo criptográfico de Estado.

4. É importante destacar, porém, que no caso em tela, o uso de equipamentos criptográficos, em si, pode não constituir uma solução completa ao impedimento de acesso indevido aos conhecimentos estratégicos nacionais e seus desdobramentos.

Inclusive, mesmo que uma instituição possua sistemas de segurança, e, se considerados como falhos, informações poderão ser acessadas, remotamente ou não, por meio de diversas técnicas invasivas, antes mesmo que o conteúdo de um documento seja criptografado para ser transmitido.

5. Para que se chegue a uma solução eficaz, se faz premente a adoção de sistemas de proteção, necessários às instituições, visando à implementação de medidas de segurança corporativa/orgânica voltadas para a proteção na gestão de pessoas, de documentos, de áreas e de sistemas de informação.

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).

Atenciosamente,

José Elito C. Siqueira

JOSÉ ELITO CARVALHO SIQUEIRA
Ministro de Estado Chefe do Gabinete de Segurança Institucional
da Presidência da República

Subsecretaria de Apoio às Comissões
Especiais e Parlamentares de Inquérito
Recebido em, 24 / 10 / 2013
Às 15h20 horas.
Keny Cristina R. Martins
Keny Cristina R. Martins
Analista Legislativo
Mat 221664