ESP REC
000029

CORREIOS

Ofício 0658 /2013-PRESI

Brasília, 20 de novembro de 2013.

A Sua Excelência a Senhora
Senadora **VANESSA GRAZZIOTIN**
Senado Federal
Praça dos Três Poderes, Anexo II, Ala Alexandre Costa, sala 15 - Subsolo
70165-900 Brasília/DF

Assunto: **Requerimento de Informações**

Referência: **Processo 53101.007714/2013-08**

Senhora Senadora,

1. Em atenção à solicitação formulada por meio do Ofício 60/2013-CPIDAESP, versando sobre o Requerimento nº 67 CPI-ESP, encaminhamos a V. Exª. cópia do Memorando 760/2013-GESI/DETIC, por meio do qual a Vice-Presidência de Tecnologia e Infraestrutura desta Empresa apresenta a manifestação técnica sobre a matéria.

Respeitosamente,

ADEILSON RIBEIRO TELLES
Chefe de Gabinete

Subsecretaria de Apoio às Comissões Especiais e Parlamentares de Inquérito
Recebido em 22/11/13
Às 15:35
Reinilson Prado
Secretário
Matr. 228130

Anexo: o citado

NOSSA MISSÃO: Fornecer soluções acessíveis e confiáveis para conectar pessoas, instituições e negócios, no Brasil e no mundo.

SENADO FEDERAL
Fls. nº 01
SSCEPI

CORREIOS

ECT
Fls: 07
R:

MEM.760/2013 - GESI/DETIC

Brasília, 14 de novembro de 2013.

Ao Chefe do GAPRE.

Assunto: Requerimento de Informações 811/2013 – Destinada a investigar a denúncia de existência de um sistema de espionagem estruturado pelo governo dos Estados Unidos.

Ref.: CI/PRESI – 02888/2013

1) Em atendimento a CI/PRESI – 02888/2013 e em resposta ao requerimento nº. 67 CPI-ESP, seguem as informações conforme solicitado:

I. Criptografia:

a) Qual empresa desenvolveu o referido sistema?
b) Qual o sistema utilizado?

Solução	Finalidade	Fornecedor
VPN	Criptografar os túneis rede privada virtual	Não há fornecedor. A criptografia utilizada é IPsec com 3DES/SHA1 e AES128/SHA1
FTPS/SFTP	Criptografar a transferência de arquivos	Não há fornecedor a criptografia utilizada é SSL e SSH
HTTPS	Criptografar tráfego relacionado à Internet pelo sistema de informação utilizando certificado digital padrão ICP-Brasil	Não há fornecedor. A criptografia é SSL. Fornecedor do certificado digital - CERTSIGN

Atualmente, os Correios não utilizam nenhum sistema de criptografia em seus sistemas ou em base de dados.

II. Segurança da Informação:

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

Solução	Finalidade	Fabricante/Fornecedor
Firewall - FortiGate	Controle de acesso lógico	Fortinet (www.fortinet.com/) / NCT (www.nct.com.br)
IPS - Proventia	Prevenção de ataques cibernéticos	IBM (www.ibm.com) / Mahvla (www.mahvla.com.br)
Filtro de conteúdo WEB – FortiGate (Web Filtering)	Filtragem de tráfego relacionado à Internet	Fortinet (www.fortinet.com/) / NCT (www.nct.com.br)
Ferramenta de segurança para email – Symantec Message Gateway	Filtro antiSPAM	Symantec (www.symantec.com) / NCT (www.nct.com.br)

SENADO FEDERAL
Fls. nº 02
SSCEPI

CORREIOS

ECT
Fls: 07
R:

Solução	Finalidade	Fabricante/Fornecedor
Concentrador VPN - FortiGate	Estabelecimento de túneis VPN	Fortinet (www.fortinet.com/) / NCT (www.nct.com.br)
Proxy – ISA Server 2006	Controlar as conexões de acordo com o interesse de tráfego e realizar cache de acesso à internet	Microsoft (www.microsoft.com)
Antivírus - Simantec Endpoint Protection	Antivírus/Antimaware	Symantec (www.symantec.com) / NCT (www.nct.com.br)
Roteador 3845	Acesso a rede corporativa dos Correios	CISCO (www.cisco.com) / British Telecommuhications (www.globalservices.bt.com/br/pt/home)
Roteador 7401	Acesso a Internet dos Correios	CISCO (www.cisco.com) / EMBRATEL (www.embratel.com.br)
Switch 2960	Acesso a Internet	CISCO (www.cisco.com)
Switch 7910	Rede Data Center - Correios	3COM / NCT (www.nect.com.br)
Switch 4800	Rede Data Center - Correios	3COM / NCT (www.nect.com.br)

Notas

1. **Advanced *Encryption Standard* (AES)** – Padrão de Criptografia Avançada . Tem um tamanho de bloco fixo em 128 bits e uma chave com tamanho de 128, 192 ou 256 bits.
2. **FTPS** – Abreviação de FTP/SSL. É um nome usado para indicar que o software FTP proporciona uma transferência de arquivos segura. Envolve o uso de um protocolo FTP SSL/TLS de criptografia no controle de canais FTP.
3. ***Intrusion Detection System* (IDS)** – Sistema de detecção de intrusão
4. ***Secure Hash Algorithm* (SHA)** - *Secure Hash Algorithm* está relacionado com as funções criptográficas. A função mais usada nesta família, a SHA-1, é usada numa grande variedade de aplicações e protocolos de segurança.
5. ***Secure Shell* (SSH)** – Serviço de emulação de terminal, semelhante ao serviço Telnet, porém utiliza criptografia na transmissão dos dados.
6. ***Secure Socket Layer* (SSL)** – Padrão de comunicação utilizado para permitir a transferência segura de informações através da Internet.
7. ***SSH File Transfer Protocol* (SFTP)** – Protocolo de transferência de arquivos e de manipulação funcional.
8. ***Triple Data Encryption Standard* (3DES)** – Padrão de criptografia baseado em outro algoritmo de criptografia simétrica, o DES, desenvolvido pela IBM em1974 e adotado como padrão em 1977. O 3DES usa 3 chaves de 64 bits.
9. ***Virtual Private Network* (VPN)** – Infraestrutura de segurança que permite interligar várias redes e usuários remotos através de um meio público (como a Internet), de forma que toda a comunicação seja criptografada.

Atenciosamente,

Fabiana de Assunção Cruvinel Nascimento
Chefe do DETIC

Fabiana de A. Cruvinel Nascimento
Chefe do DETIC
Mat. 8.012.650-2

CCR/ffss