



PRESIDÊNCIA DA REPÚBLICA
Secretaria-Geral

OFÍCIO Nº 766/2022/SG/PR/SG/PR

Brasília, na data da assinatura.

A Sua Excelência o Senhor
Deputado Luciano Bivar
Primeiro-Secretário
Câmara dos Deputados – Edifício Principal
70160-900 Brasília/DF

Assunto: Requerimento de Informação nº 710/2022.

Senhor Primeiro-Secretário,

Cumprimentando-o, faço referência ao **Ofício 1ªSec/RI/E/nº 999**, de 14 de dezembro de 2022, que remete o **Requerimento de Informação nº 710/2022**, de autoria do Deputado Marcelo Calero, para encaminhar manifestação desta Pasta, consubstanciada na **Nota Informativa nº 2/2022/CGINT/DITEC/SA** (3829144), expedida pela Coordenação-Geral de Infraestrutura Tecnológica da Diretoria de Tecnologia da Secretaria Especial de Administração, bem como na **Nota SAJ nº 112/2022/SAINST/SAJ/SG/PR** (3838670), exarada pela Subchefia para Assuntos Jurídicos.

Por oportuno, ao passo em que renovo os votos de estima e consideração, coloco esta Secretaria-Geral à disposição para esclarecimentos que ainda se façam necessários.

Atenciosamente,

LUIZ EDUARDO RAMOS
Ministro de Estado Chefe da Secretaria-Geral
da Presidência da República



Documento assinado eletronicamente por **Luiz Eduardo Ramos Baptista Pereira**, Ministro de Estado Chefe da Secretaria-Geral da Presidência da República, em 29/12/2022, às 15:43, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade do documento pode ser conferida informando o código verificador **3844110** e o código CRC **605F41CD** no site:

https://super.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0

Referência: Caso responda este Ofício, indicar expressamente o Processo nº 00133.001079/2022-02

SUPER nº 3844110

Palácio do Planalto - 4º andar sala 402 — Telefone: (61)3411-1447

CEP 70150-900 Brasília/DF - <https://www.gov.br/planalto/pt-br>

PRESIDÊNCIA DA REPÚBLICA
Secretaria-Geral
Secretaria Especial de Administração
Diretoria de Tecnologia
Coordenação-Geral de Infraestrutura Tecnológica

Nota Informativa nº 2/2022/CGINT/DITEC/SA

Assunto: **Requerimento de Informação nº 710/2022 - Deputado Marcelo Calero.**

Ref.: 00133.001079/2022-02

Ao Diretor de Tecnologia,

1. A presente Nota Informativa tem como intuito apresentar subsídios à Secretaria-Geral da Presidência da República, tendo em vista a solicitação contida no Ofício 1ªSec/RI/E/nº 999 (3810340), de 14/12/2022, da Primeira-Secretaria da Câmara dos Deputados, que envia, entre outros, o Requerimento de Informação nº 710/2022 (3810344), de 11/11/2022, de autoria do Deputado Marcelo Calero, por meio do qual são solicitadas informações sobre suposta contaminação por vírus e formatação de computadores no Palácio do Planalto.

2. Neste sentido, com base nos documentos supra aludidos, a nota em pauta tem o condão de prover informações bastantes sobre o incidente cibernético que acometeu a rede computacional da Presidência da República em 1º de novembro de 2022.

3. De antemão, impende destacar que a terminologia “servidor” será utilizada no corpo deste documento para se referir ao “tipo de computador responsável por prover algum serviço de rede” e não se deve confundir com a pessoa do “servidor público”, o qual será referenciado nesta Nota como “usuário”.

4. Em sendo, assim, passa-se a elucidar os questionamentos elencados no Requerimento de Informação nº 710/2022 (3810344), de 11/11/2022, cujas respostas, estarão a seguir ordenadas:

4.1. A Secretaria-Geral da Presidência da República confirma a informação de computadores do Palácio do Planalto foram formatados após suspeita de contaminação por vírus?

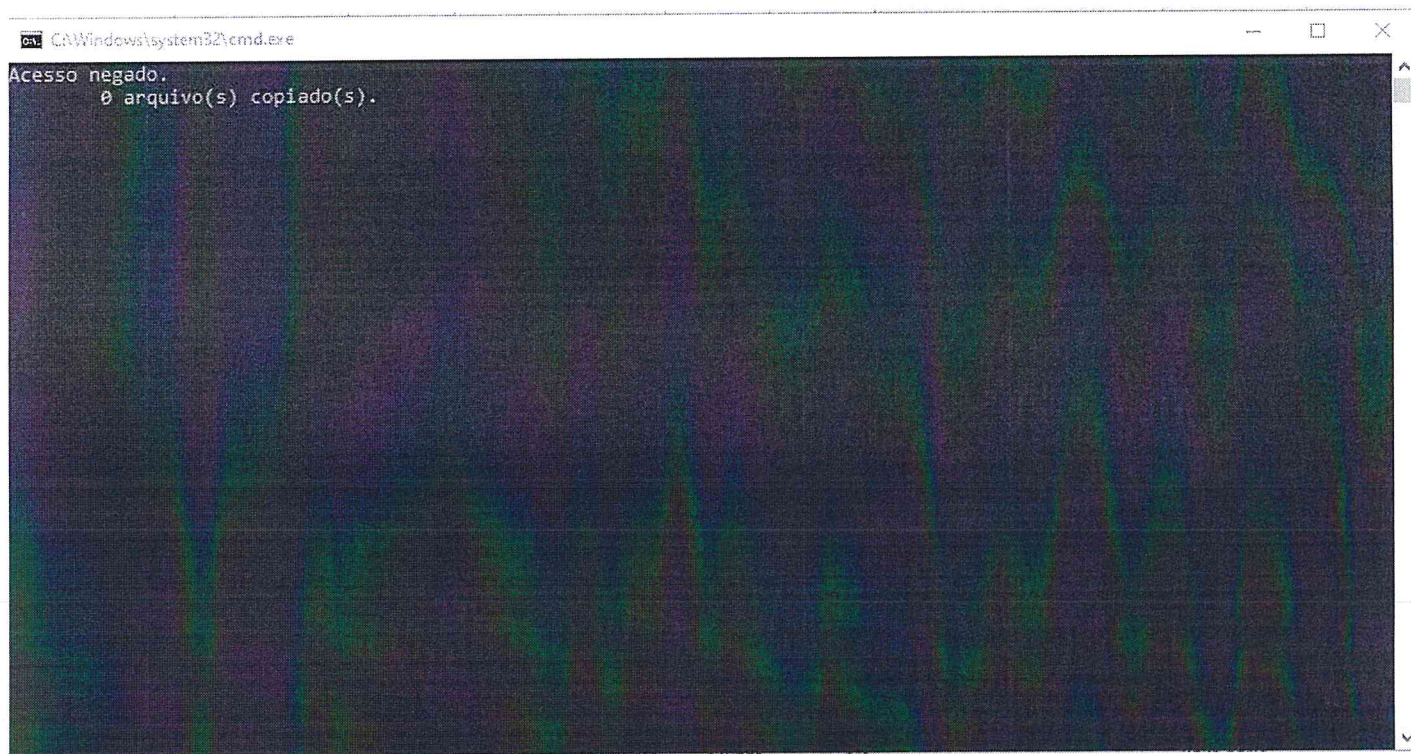
4.1.1. Na data de 01 de novembro de 2022, a Equipe de Tratamento de Incidentes em Rede da Presidência da República (ETIR-PR) detectou, por volta das 7h30, a ocorrência de incidente cibernético, gerado por meio de malware do tipo Ransomware, variante do Ransomware TeslaCrypt, tendo neutralizado suas ações por volta das 10h30 da mesma data.

4.1.2. Por ação do malware, foi identificada a criptografia de alguns arquivos do Sistema Operacional de computadores de usuários e de arquivos hospedados no servidor de arquivos. Os dados do servidor de arquivos que, porventura, foram corrompidos/criptografados foram recuperados por meio da restauração de backup, não havendo perda de dados institucionais, nem pagamento de resgate por parte da Presidência da República.

4.1.3. De outro turno, para casos em que houve corrompimento/criptografia dos arquivos do sistema operacional, **não foi dada orientação para formatação dos equipamentos**. As máquinas afetadas precisaram ser reinstaladas, mediante solicitação (Ordem de Serviço) dos usuários à Central de Atendimento a Usuários, pois o corrompimento/criptografia inviabilizava o seu uso. Ressalta-se, entretanto, que o **processo de reparo foi precedido de backup dos dados locais dos computadores**, tendo estes sido restaurados nos computadores, após o término do processo de reinstalação. **Não foram utilizadas ferramentas de formatação física (zerofill) nos discos rígidos.**

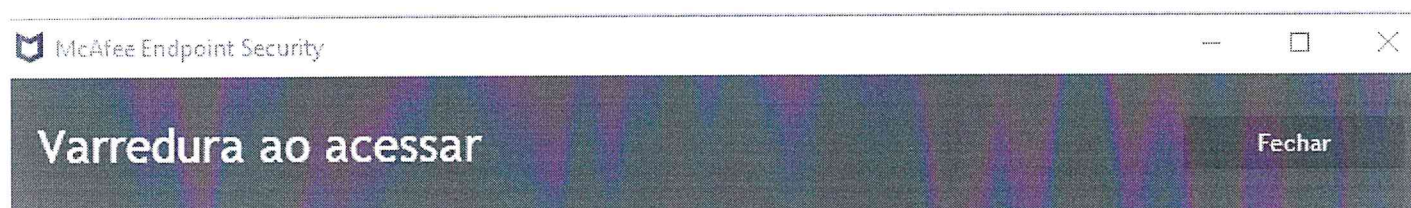
4.2. Quando ocorreu o ataque e quando este foi detectado?

4.2.1. Na data do dia 01 de novembro do ano corrente, às 07 horas e 30 minutos, foi identificada em algumas estações de trabalho da rede computacional da Presidência da República uma janela do prompt de comando com a informação de restrição na tentativa de cópia de um arquivo, logo após o login do usuário em seu computador, conforme Imagem_01.



Imagem_01

4.2.2. Em seguida, foi exibida notificação da solução de AntiVírus (McAfee), a qual reportou a detecção de uma ameaça. A imagem 02 exemplifica a detecção ocorrida em um dos computadores.



O McAfee Endpoint Security detectou uma ameaça.

1 Detecções

[Limpar](#)[Excluir](#)[Remover entrada](#)

Data	Nome da detecção	Tipo	Arquivo	Ação realizada
1/11/2022 8:27 AM	Suspect-ER!EDC87DA8...	Cavalo de Troia	...	Excluir

Imagem_02**4.3. Qual vírus de computador foi detectado, como se deu a contaminação e como se deu a atuação do vírus?**

4.3.1. Tão logo as primeiras ocorrências foram detectadas, a Equipe de Tratamento de Incidentes em Rede da Presidência da República (ETIR-PR) iniciou, de pronto, sua atuação.

4.3.2. Inicialmente, procedeu-se à análise dos eventos reportados na gerência da solução de antivírus. Ao perceber a ocorrência do mesmo evento em outros computadores da rede, desencadeou-se, então, a análise do comportamento dos computadores afetados, fazendo uso da aplicação Process Monitor, com a qual foi possível identificar o artefato que estava sendo copiado para a pasta c:\windows dos computadores. O artefato utilizava a nomenclatura SVCHOSTS.exe.

4.3.3. De imediato, foi levantado o hash (assinatura) do artefato, assim como sua análise por meio de serviços de segurança. O hash do malware foi, então, cadastrado na base de reputação da solução de segurança, garantindo a sua detecção como malicioso em todas as ferramentas do ecossistema McAfee, bem como a submissão no serviço online Virustotal, que analisa arquivos e URLs e que possibilita a identificação de conteúdo malicioso detectável por antivírus e scanners de websites.

4.3.4. No entanto, foi verificado que mesmo sendo excluído pela solução de Antivírus, o arquivo voltava a aparecer minutos depois no mesmo local. Utilizando-se da ferramenta McAfee Active Response (MAR), foi possível identificar o processo executando o arquivo help.bat, a partir do compartilhamento sysvol do servidor de autenticação, o qual copiava outro arquivo help.exe, no mesmo local, para c:\windows dos computadores, renomeando para SVCHOSTS.exe.

4.3.5. Assim sendo, ambos os arquivos, help.bat e help.exe, são alheios aos scripts regularmente utilizados na rede da Presidência da República. Além da cópia do help.exe, era realizada a execução do arquivo svchosts.exe, bem como a alteração de duas chaves no registro, que direcionavam os comandos do sistema operacional TASKHOST.exe e TASKHOSTW.exe para a execução do help.bat, o que fazia o sistema operacional se comportar com limitações.

4.3.6. Adicionalmente, cumpre salientar que, pelo comportamento de cópia persistente, passou-se a suspeita de utilização de GPO (Objeto de Política de Grupo) para realização dessa cópia. Portanto, foi feita uma verificação das datas de alteração das GPO, constatando-se que a Diretiva de Grupo "Default Domain Policy" havia sido alterada para a distribuição do malware. Cabe observar que os arquivos das GPO também ficam no compartilhamento sysvol. Por conseguinte, foram realizadas as ações para interromper a execução da GPO, tendo sido feita a restauração da versão anterior dessa GPO.

4.3.7. Tendo em vista que o compartilhamento sysvol é de escrita permitida apenas para usuários com privilégio administrativo, a suspeita inicial foi de que houvesse ocorrido o comprometimento de alguma credencial com privilégio administrativo, por phishing. Por tal razão, foi realizada rapidamente a remoção de todas as contas do grupo Domain Admins, deixando apenas as contas de sistema necessárias ao seu funcionamento.

4.3.8. As ações do malware foram neutralizadas por volta das 10h30 da mesma data. Todo o trabalho realizado foi documentado em relatório técnico confeccionado pela ETIR-PR e compartilhado com o CTIR Gov e os Gestores de Segurança da Informação da Presidência da República.

4.3.9. Após análises realizadas pela ETIR-PR, verificou-se que o artefato utilizado é um malware do tipo ransomware, amplamente utilizado na tentativa de sequestro de dados, por meio de criptografia de arquivos, sendo uma variante do Ransomware TeslaCrypt.

4.3.10. Detalhes do *malware*:

- Assinaturas:

- **MD5:** edc87da8654e966bee0e5c9b92ed67cb
- **SHA-1:** db99fc79a64873bef25998681392ac9be2c1c99c
- **SHA-256:** 9990388776daa57d2b06488f9e2209e35ef738fd0be1253be4c22a3ab7c3e1e2
- **Vhash:** 015076655d155515555az4f!z
- **Authentihash:** 34805da1acd162d128173a1aa1f9a0746b48aeea879bde70d23faac14c16602f
- **Imphash:** 9ee213cc92019de3ab89fab1fe03397f

- **Rich PE header hash:** d330f9d90128efd0450b405f020b36f0
- **SSDEEP:** 3072:hkEX9cOsQDqXX+nJZ0pVfdjHHO50gpy2RHawPZtOzR:tK6DqozABnO5jtyF
- **TLSH:** T1A0F37C5BB7A520F8E5779239C8525606F772783213349B6F03A4077A5F233A09E3EB61
- **Dados da compilação:**
 - **File type:** Win32 EXE
 - **Magic:** PE32+ executable for MS Windows (console) Mono/.Net assembly
 - **TrID:** Win64 Executable (generic) (48.7%) Win16 NE executable (generic) (23.3%) OS/2 Executable (generic) (9.3%) Generic Win/DOS Executable (9.2%) DOS Executable Generic (9.2%)
 - **DetectItEasy:** PE64 Compiler: Microsoft Visual C/C++ Linker: Microsoft Linker (14.28, Visual Studio 2019 16.8 or 16.9*) [Console64,console]
 - **File size:** 160.50 KB (164352 bytes)
- **Dados sobre o resgate:**
 - **Btc Address:** bc1qakuel0s4nyge9rxjylsqdxnn9nvyhc2z6k27gz
 - **email:** fishA001@protonmail.com
- **Análise:** <https://www.hybrid-analysis.com>
 - **URL resultado:** <https://www.hybrid-analysis.com/sample/9990388776daa57d2b06488f9e2209e35ef738fd0be1253be4c22a3ab7c3e1e2?environmentId=160>
 - **Ransomware:** Detected indicator that file is ransomware
 - **Spyware:** Accesses potentially sensitive information from local browsers, Hooks API calls
 - **Persistence:** Installs hooks/patches the running process
 - **Fingerprint:** Contains ability to retrieve information about the current system, Queries process information
 - **Evasive:** Contains ability to adjust token privileges, Contains ability to check if a debugger is running, Contains ability to detect virtual environment (API), Input file contains API references not part of its Import Address Table (IAT)

4.3.11. Logo, a partir de dados históricos do serviço online Virustotal, a ETIR- ETIR-PR percebeu que a Presidência da República foi o primeiro órgão a reportar o aludido malware. Até a presente data, desde a submissão realizada pela ETIR-PR, 47 fornecedores de segurança e 1 sandbox sinalizaram este arquivo como malicioso.

- Creation Time: 2022-11-03 09:27:57 UTC
- First Submission: 2022-11-01 11:45:05 UTC
- Last Submission: 2022-11-29 06:58:17 UTC
- Last Analysis: 2022-11-11 00:12:12 UTC

4.3.12. Na data da infecção, a solução de antivírus encontrava-se atualizada e reconheceu o malware como possível ameaça. O hash do malware foi cadastrado pela ETIR-PR na base de reputação da solução de segurança para garantir a sua detecção como malicioso em todas as ferramentas do ecossistema McAfee.

4.4. Houve perda de dados em função do ataque? Quais dados foram perdidos?

4.4.1. No que tange aos dados eventualmente corrompidos/criptografados pelo malware, frise-se, por necessário, que foram recuperados por meio da restauração de backup, não havendo perda de dados institucionais ou mesmo pagamento de resgate por parte da Presidência da República.

4.4.2. Outrossim, importa enfatizar que **não foi detectado vazamento, tampouco o comprometimento de sistemas hospedados na rede da Presidência da República.**

4.4.3. A título de informação, desde o evento do incidente na Rede-PR, todas as informações sob a guarda do Centro de Dados da Presidência da República, solicitadas por Unidades da Presidência da República, Órgãos da Administração Pública Federal e pela Equipe de Transição de Governo, têm sido, de pronto, disponibilizadas.

4.5. Há backup dos dados violados e/ou apagados? Se sim, foi possível recuperar os dados?

4.5.1. Os arquivos institucionais ficam armazenados em servidor de arquivos no Centro de Dados da Presidência da República e a política de segurança prevê o backup regular desses dados. A restauração de backup é feita mediante solicitação dos usuários à Central de Atendimento a Usuários.

4.5.2. Ressalte-se, por necessário, que todos os dados eventualmente corrompidos/criptografados pelo *malware* foram recuperados por meio da restauração de *backup*, não havendo perda de dados institucionais ou mesmo pagamento de resgate por parte da Presidência da República.

4.6. **Quantos computadores foram afetados pelo vírus?**

4.6.1. O número de computadores de usuários tratados por meio de abertura de ordens de serviço registradas na Central de Atendimento a Usuários foi de 192 (cento e noventa e dois), o que corresponde, aproximadamente, a 5% (cinco por cento) do parque computacional da Presidência da República.

4.7. **Quantos computadores foram formatados? Solicita-se discriminar por órgão e entidade da Administração Pública.**

4.7.1. Relativamente aos computadores dos usuários, a equipe ETIR-PR atuou na tentativa de correção do Registro Windows alterado pelo *malware*, com o objetivo de restabelecer o funcionamento do sistema operacional. Tal medida foi efetiva para os computadores afetados que não tiveram arquivos do sistema operacional criptografados, tendo a correção sido realizada via GPO, desfazendo as alterações realizadas pelo *malware*.

4.7.2. De outro turno, para os casos em que houve corrompimento/criptografia dos arquivos do sistema operacional, o uso da máquina ficou inviabilizado. Sendo assim, mediante solicitação dos usuários à Central de Atendimento a Usuários, realizou-se a reinstalação do sistema operacional.

4.7.3. Destaca-se que o procedimento de reinstalação das máquinas foi precedido de *backup* dos arquivos dos usuários, tendo sido restaurados nos computadores, após o término do processo de reinstalação. Cabe salientar que os procedimentos de recuperação dos computadores afetados entraram na rotina de atendimento ao usuário, ***não tendo sido dada orientação para formatação dos equipamentos, nem mesmo para a utilização de ferramentas de formatação física (zerofill/wipe) dos discos rígidos.***

4.7.4. Neste contexto, os discos utilizados para realização dos *backups* encontram-se preservados no Laboratório da Coordenação de Informática da Diretoria de Tecnologia da Presidência da República. Este procedimento foi realizado por técnicos da Coordenação-Geral de Atendimento a Usuários e Telecomunicações da Diretoria de Tecnologia da Presidência da República.

4.7.5. Todos os computadores afetados são da Presidência da República, da qual fazem parte seus Órgãos Essenciais (<https://www.gov.br/planalto/pt-br/conheca-a-presidencia/orgaos-da-presidencia-da-republica/orgaos-essenciais>).

4.8. **Quais órgãos e entidades da Administração Pública foram afetados pelo vírus?**

4.8.1. Os impactos do incidente cibernético aqui relatado e já tratado atingiu tão somente a rede computacional da Presidência da República, da qual fazem parte seus Órgãos Essenciais.

EDSON FLORIANO SOUSA JUNIOR

Gestor de Segurança da Informação em Meios Tecnológicos

BRUNO PEREIRA PONTES

Coordenador-Geral de Infraestrutura Tecnológica



Documento assinado eletronicamente por **Edson Floriano de Sousa Júnior, Coordenador(a)**, em 22/12/2022, às 12:16, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.



Documento assinado eletronicamente por **Bruno Pereira Pontes, Coordenador(a)-Geral**, em 22/12/2022, às 13:17, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

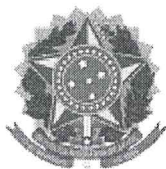


A autenticidade do documento pode ser conferida informando o código verificador **3829144** e o código CRC **B9F5EB4E** no site:

https://super.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0

Referência: Processo nº 00133.001079/2022-02

SUPER nº 3829144



PRESIDÊNCIA DA REPÚBLICA
SECRETARIA-GERAL
SUBCHEFIA PARA ASSUNTOS JURÍDICOS

Nota SAJ nº 112 / 2022 / SAAINST/SAJ/SG/PR

CÂMARA DOS DEPUTADOS - CD

Interessado:

Ref: Requerimento de Informação nº 710/2022

Anexo: -----

Assunto: Solicita ao Ministro de Estado Chefe da Secretaria-Geral da Presidência da República informações acerca da formatação de computadores do Palácio do Planalto

Processo : 00133.001079/2022-02

Senhor Subchefe,

I - RELATÓRIO

1. Trata-se do Ofício 1ªSec/RI/E/nº 999, de 14 de dezembro de 2022, expedido pela Mesa da Câmara dos Deputados ao Ministro de Estado Chefe da Secretaria-Geral da Presidência da República, que encaminha o Requerimento de Informação de nº 710, de 2022, de autoria do Deputado Federal Marcelo Calero, que solicita informações acerca da formatação de computadores do Palácio do Planalto, mais precisamente o que segue:

1. A Secretaria-Geral da Presidência da República confirma a informação de computadores do Palácio do Planalto foram formatados após suspeita de contaminação por vírus?
2. Quando ocorreu o ataque e quando este foi detectado?
3. Qual vírus de computador foi detectado, como se deu a contaminação e como se deu a atuação do vírus?
4. Houve perda de dados em função do ataque? Quais dados foram perdidos?
5. Há backup dos dados violados e/ou apagados? Se sim, foi possível recuperar os dados?
6. Quantos computadores foram afetados pelo vírus?
7. Quantos computadores foram formatados? Solicita-se discriminar por órgão e entidade da Administração Pública.
8. Quais órgãos e entidades da Administração Pública foram afetados pelo vírus?

2. O feito foi recebido na Secretaria-Geral da Presidência da República em 14.12.2022, sendo encaminhado à Secretaria Especial de Administração (SA/SG/PR) e a esta Subchefia para Assuntos Jurídicos (SAJ/SG/PR) para manifestação.

3. É o que basta relatar.

II – ANÁLISE JURÍDICA

4. De acordo com a Constituição Federal, compete aos Ministros de Estado exercer a orientação, coordenação e supervisão dos órgãos e entidades da administração federal na área de sua competência (art. 87, parágrafo único, inciso I). Os Ministros de Estado, ademais, podem ser convocados, pelas Comissões do Congresso Nacional, para *prestar informações sobre assuntos inerentes a suas atribuições* (art. 58, §2º, inciso III). No mesmo sentido, o art. 50, §2º, destaca que as Mesas da Câmara dos Deputados e do Senado Federal poderão encaminhar pedidos escritos de informações aos Ministros de Estado.

5. Por sua vez, o artigo 50 da Constituição Federal e os artigos 115 e 116 do Regimento Interno da Câmara dos Deputados, ao regulamentarem o Requerimento de Informação a Ministro de Estado, estabelecem que:

Constituição Federal

Art. 50. A Câmara dos Deputados e o Senado Federal, ou qualquer de suas Comissões, poderão convocar Ministro de Estado ou quaisquer titulares de órgãos diretamente subordinados à Presidência da República para prestarem, pessoalmente, informações sobre assunto previamente determinado, importando crime de responsabilidade a ausência sem justificativa adequada.

(...)

§ 2º - As Mesas da Câmara dos Deputados e do Senado Federal poderão encaminhar pedidos escritos de informações a Ministros de Estado ou a qualquer das pessoas referidas no caput deste artigo, importando em crime de responsabilidade a recusa, ou o não - atendimento, no prazo de trinta dias, bem como a prestação de informações falsas.

Regimento Interno da Câmara dos Deputados

Art. 115. Serão escritos e despachados no prazo de cinco sessões, pelo Presidente, ouvida a Mesa, e publicados com a respectiva decisão no Diário da Câmara dos Deputados, os requerimentos que solicitem:

I - informação a Ministro de Estado;

(...)

Art. 116. Os pedidos escritos de informação a Ministro de Estado, importando crime de responsabilidade a recusa ou o não-atendimento no prazo de trinta dias, bem como a prestação de informações falsas, serão encaminhados pelo Primeiro-Secretário da Câmara, observadas as seguintes regras:

I - apresentado requerimento de informação, se esta chegar espontaneamente à Câmara ou já tiver sido prestada em resposta a pedido anterior, dela será entregue cópia ao Deputado interessado, caso não tenha sido publicada no Diário da Câmara dos Deputados, considerando-se, em consequência, prejudicada a proposição;

II - os requerimentos de informação somente poderão referir-se a ato ou fato, na área de competência do Ministério, incluídos os órgãos ou entidades da administração pública indireta sob sua supervisão:

a) relacionado com matéria legislativa em trâmite, ou qualquer assunto submetido à apreciação do Congresso Nacional, de suas Casas ou Comissões;

b) sujeito à fiscalização e ao controle do Congresso Nacional, de suas Casas ou Comissões;

c) pertinente às atribuições do Congresso Nacional;

III - não cabem, em requerimento de informação, providências a tomar, consulta, sugestão, conselho ou interrogação sobre propósitos da autoridade a que se dirige;

(destaque nosso)

6. Dito isso, convém destacar as atribuições da Secretaria-Geral da Presidência da República, bem como sua estrutura, nos termos da **Lei 13.844, de 18 de junho de 2019**, *in verbis*:

Seção IV

Da Secretaria-Geral da Presidência da República

Art. 7º À Secretaria-Geral da Presidência da República compete assistir diretamente o Presidente da República no desempenho de suas atribuições, especialmente:

- I - na supervisão e na execução das atividades administrativas da Presidência da República e, supletivamente, da Vice-Presidência da República;
- II - no acompanhamento da ação governamental e do resultado da gestão dos administradores, no âmbito dos órgãos integrantes da Presidência da República e da Vice-Presidência da República, além de outros órgãos determinados em legislação específica, por intermédio da fiscalização contábil, financeira, orçamentária, operacional e patrimonial;
- III - no planejamento nacional estratégico e de modernização do Estado;
- IV - na orientação das escolhas e das políticas públicas estratégicas de modernização do Estado, de economicidade, de simplificação, de eficiência e de excelência de gestão do País, consideradas a situação atual e as possibilidades para o futuro;
- V - na elaboração de subsídios para a preparação de ações de governo;
- VI - na definição, na coordenação, no monitoramento, na avaliação e na supervisão das ações dos programas de modernização do Estado necessárias à sua execução; (Redação dada pela Lei nº 13.901, de 2019).
- VII - na implementação de políticas e ações destinadas à ampliação das oportunidades de investimento, de cooperações, de parcerias e de outros instrumentos destinados à modernização do Estado; (Redação dada pela Lei nº 13.901, de 2019).
- VIII - na verificação prévia da constitucionalidade e da legalidade dos atos presidenciais; (Incluído pela Lei nº 13.901, de 2019).
- IX - na coordenação do processo de sanção e veto de projetos de lei enviados pelo Congresso Nacional; (Incluído pela Lei nº 13.901, de 2019).
- X - na elaboração de mensagens do Poder Executivo federal ao Congresso Nacional; (Incluído pela Lei nº 13.901, de 2019).
- XI - na preparação dos atos a serem submetidos ao Presidente da República; e (Incluído pela Lei nº 13.901, de 2019).
- XII - na publicação e preservação dos atos oficiais. (Incluído pela Lei nº 13.901, de 2019).

Art. 8º A Secretaria-Geral da Presidência da República tem como estrutura básica:

- I - o Gabinete;
 - II - a Secretaria Executiva;
 - III - a Secretaria Especial de Modernização do Estado, com até 3 (três) Secretarias;
 - IV - a Secretaria Especial de Assuntos Estratégicos, com até 2 (duas) Secretarias;
 - V - (revogado); (Redação dada pela Lei nº 13.901, de 2019).
 - VI - (revogado); (Redação dada pela Lei nº 13.901, de 2019).
 - VII - a Secretaria Especial de Administração;** (Incluído pela Lei nº 13.901, de 2019).
 - VIII - a Subchefia para Assuntos Jurídicos; (Incluído pela Lei nº 13.901, de 2019).
 - IX - 1 (uma) Secretaria; e (Incluído pela Lei nº 13.901, de 2019).
 - X - a Imprensa Nacional. (Incluído pela Lei nº 13.901, de 2019).
- Parágrafo único. (Revogado). (Redação dada pela Lei nº 13.901, de 2019).
- (destaque nosso)

7. De acordo com o **Decreto 11.144, de 21 de julho de 2022**, que aprova a estrutura regimental da Secretaria-Geral da Presidência da República, cabe salientar as atribuições da Secretaria Especial de Administração e de sua Diretoria de Tecnologia, *litteris*:

Art. 13. À **Secretaria Especial de Administração** compete, no âmbito dos órgãos integrantes da estrutura organizacional da Presidência da República e supletivamente da Vice-Presidência da

República, ressalvadas as hipóteses previstas em legislação específica:

I - planejar, coordenar, supervisionar, dirigir e controlar as atividades administrativas da Presidência da República e exercer a função de órgão setorial do:

- a) Sistema de Pessoal Civil da Administração Federal - Sipec;
- b) Sistema de Administração dos Recursos de Tecnologia da Informação - Sisp;
- c) Sistema de Serviços Gerais - Sisg;
- d) Sistema de Planejamento e de Orçamento Federal;
- e) Sistema de Contabilidade Federal;
- f) Sistema de Administração Financeira Federal - Siafi;
- g) Sistema de Organização e Inovação Institucional do Governo Federal - Siorg; e
- h) Sistema de Gestão de Documentos de Arquivo - Siga;

II - articular-se com os órgãos centrais dos sistemas de que trata o inciso I e informar e orientar os órgãos da Presidência da República quanto ao cumprimento das normas estabelecidas;

III - planejar, coordenar e supervisionar as atividades de administração patrimonial e de suprimento, de telecomunicações e de publicação dos atos oficiais da Presidência da República e da Vice-Presidência da República;

IV - planejar, coordenar, supervisionar e controlar as atividades de articulação com a Autoridade Certificadora Raiz da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, no âmbito dos órgãos integrantes da estrutura da Presidência da República e com os agentes públicos indicados pela Secretaria-Geral da Presidência da República, quanto à expedição de documentos eletrônicos;

V - gerir a reserva técnica de Gratificações de Exercício de Cargo em Confiança nos órgãos da Presidência da República e de Gratificação de Representação da Presidência da República;

VI - supervisionar e coordenar as atividades de relações públicas na Presidência da República;

VII - elaborar manuais, normas e procedimentos regulamentares aplicáveis às atividades de sua competência;

VIII - firmar contratos, convênios, acordos de cooperação, ajustes ou outros instrumentos congêneres, no âmbito de suas competências; e

IX - gerir os imóveis funcionais da Presidência da República.

(...)

Art. 17. À Diretoria de Tecnologia compete:

I - planejar, executar, coordenar e supervisionar as atividades relacionadas com:

- a) a política, as diretrizes e a administração de recursos de tecnologia da informação, de telecomunicações e de eletrônica;
- b) o desenvolvimento, a contratação e a manutenção de soluções de tecnologia;
- c) a especificação de recursos, a implementação, a disseminação e o incentivo ao uso de soluções de tecnologia;
- d) a orientação e o suporte aos usuários na instalação, na configuração e no uso de equipamentos e na utilização de sistemas, aplicativos e serviços na área de tecnologia;
- e) a operação e a manutenção ininterrupta das centrais de comunicações, de atendimento, de informações e de Private Automatic Branch Exchange - PABX, no âmbito da Presidência da República e da Vice-Presidência da República; e
- f) as diretrizes e a administração de recursos de tecnologia da informação para segurança da informação em meios tecnológicos;

II - planejar, executar, coordenar e controlar as atividades da Autoridade Certificadora da Presidência da República, em articulação com a Autoridade Certificadora Raiz da ICP-Brasil;

III - promover a segurança das comunicações no âmbito da Presidência da República; e

IV - planejar e executar, em articulação com o Gabinete de Segurança Institucional da Presidência da República, as atividades técnicas de apoio de telecomunicações, de eletrônica, de rádio operação, de telefonia e de segurança eletrônica ao Presidente da República, incluídas aquelas relacionadas com viagens, deslocamentos e eventos dos quais ele participe.

(destaque nosso)

8. Já no que diz respeito ao objeto deste processo, a Diretoria de Tecnologia, por sua Coordenação-Geral de Infraestrutura Tecnológica (CGINT), manifestou-se por meio da **Nota Informativa nº**

2/2022/CGINT/DITEC/SA (doc SEI 3829144), respondendo aos questionamentos de nº 1 a 8, de ordem técnica, encaminhados pelo i. Deputado.

9. Dessa forma, esta Subchefia entende que a solicitação de informações em epígrafe encontra-se atendida pela **Nota Informativa nº 2/2022/CGINT/DITEC/SA**, *supra*, que, sugere-se, deve ser encaminhada ao Requerente, juntamente com esta Nota SAJ, no prazo legal.

III - CONCLUSÃO

10. Sendo esta a manifestação jurídica com relação às indagações encaminhadas por meio do Requerimento de Informação de nº 710, de 2022, sugere-se que, uma vez aprovada, seja remetida à Chefia de Gabinete do Ministro de Estado Chefe da Secretaria Geral, em resposta ao Despacho de 14/12/2022.

À consideração superior.

Brasília, 26 de dezembro de 2022.

BETINA GÜNTHER SILVA

Coordenadora-Geral de Atos Internacionais e Informações

Subchefia para Assuntos Jurídicos

Secretaria-Geral da Presidência da República

De Acordo.

RONALD FERREIRA SERRA

Subchefe Adjunto

Subchefia para Assuntos Jurídicos

Secretaria-Geral da Presidência da República



Documento assinado eletronicamente por **Betina Gunther Silva, Assessor**, em 27/12/2022, às 10:36, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.



Documento assinado eletronicamente por **Ronald Ferreira Serra, Subchefe Adjunto**, em 27/12/2022, às 10:41, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade do documento pode ser conferida informando o código verificador **3838670** e o código CRC **51D1DE69** no site:

https://super.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0

Referência: Processo nº 00133.001079/2022-02

SUPER nº 3838670