00133.001080/2022-29

PRESIDÊNCIA DA REPÚBLICA
Secretaria-Geral

OFÍCIO Nº 767/2022/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 726/2022.

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 766/2022**, de autoria da da Comissão de Fiscalização Financeira e Controle, para encaminhar manifestação desta Pasta, consubstanciada na **Nota Informativa nº 3/2022/CGINT/DITEC/SA** (3830848), expedida pela Coordenação-Geral de Infraestrutura Tecnológica da Diretoria de Tecnologia da Secretaria Especial de Administração, bem como na **Nota SAJ nº 113/2022/SAAINST/SAJ/SG/PR** (3838710), 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 15:45, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Referência: Caso responda este Ofício, indicar expressamente o Processo nº 00133.001080/2022-29 SUPER nº 3844537

Palácio do Planalto - 4º andar sala 402 — Telefone: (61)3411-1447
CEP 70150-900 Brasília/DF - https://www.gov.br/planalto/pt-br

00133.001080/2022-29

PRESIDÊNCIA DA REPÚBLICA
Secretaria-Geral
Secretaria Especial de Administração
Diretoria de Tecnologia

Nota Informativa nº 3/2022/GAB/DITEC/SA

Assunto: **Requerimento de Informação nº 726/2022 - Comissão de Fiscalização Financeira e Controle.**

Ref.: 00133.001080/2022-29

1. A presente Nota Informativa tem como intuito apresentar subsídios à Secretaria Executiva da Secretaria-Geral da Presidência da República, tendo em vista a solicitação contida no Despacho SE/SG/PR (3810492), Ofício 1ªSec/RI/E/nº 999 (3810376), de 14/12/2022, da Primeira-Secretaria da Câmara dos Deputados, que envia, entre outros, o Requerimento de Informação nº 726/2022 (3810377), de 30/11/2022, de autoria da Comissão de Fiscalização Financeira e Controle da Câmara dos Deputados, por meio do qual são solicitadas informações sobre "a notícia de que os computadores do Planalto foram apagados por suposta ameaça".

2. Neste sentido, com base nos documentos supra aludidos, a nota em pauta tem o condão de elucidar o pedido exarado pela Comissão de Fiscalização Financeira e Controle da Câmara dos Deputados, face à representação de autoria da Comissão de Fiscalização Financeira e Controle da Câmara dos Deputados, que concerne ao 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. DA DETECÇÃO DA AMEAÇA

4.1. Preliminarmente, insta ressaltar que, na data do dia primeiro 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, logo após o login do usuário em seu computador, uma janela do prompt de comando com a informação de restrição na tentativa de cópia de um arquivo, conforme Imagem_01.

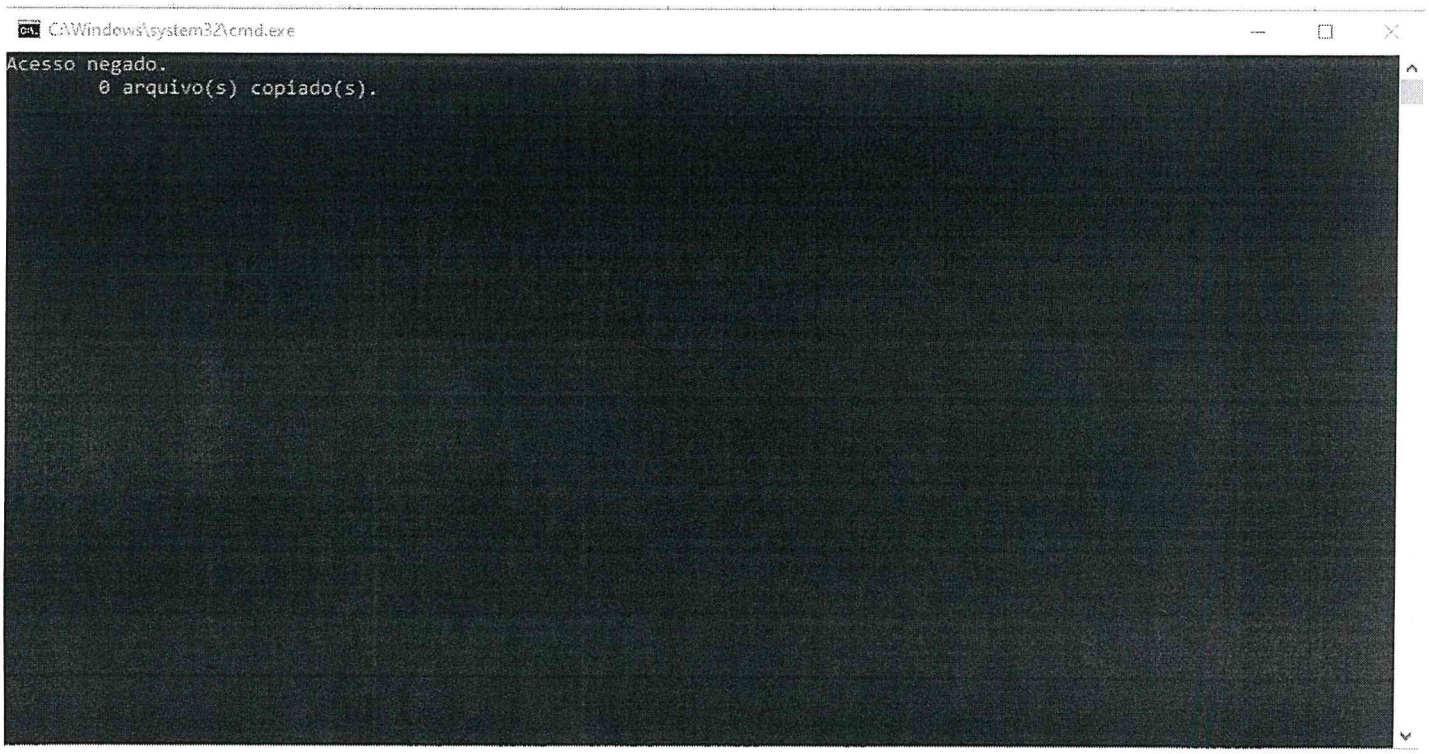

Imagem_01

4.2. 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.

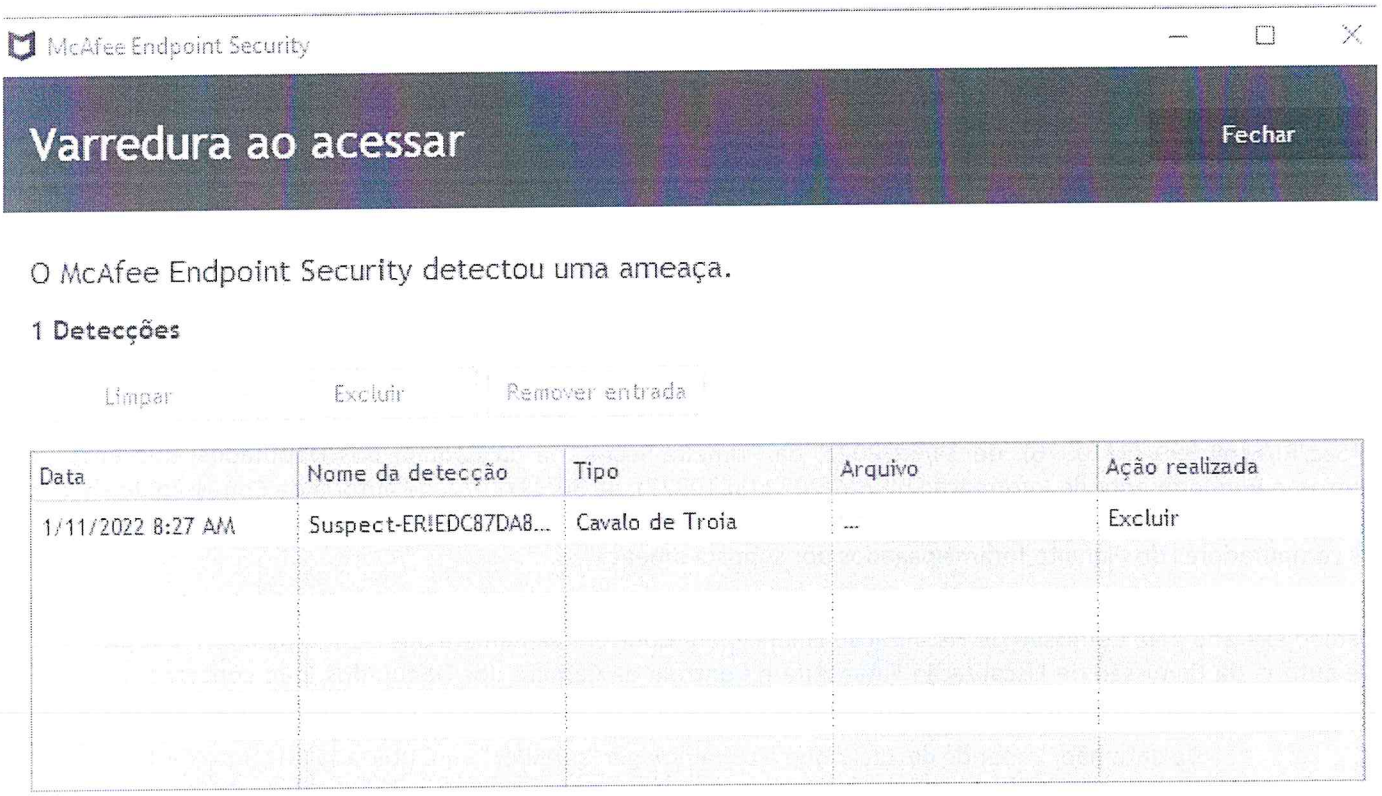

Imagem_02

5. **DO TRATAMENTO DO INCIDENTE**

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

5.2. 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.

5.3. 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.

5.4. 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.

5.5. 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.

5.6. 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.

5.7. 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.

5.8. Isto posto, após análises mais detalhadas dos logs e eventos relacionados ao incidente e de um melhor entendimento do malware utilizado, passou-se a suspeitar de que tenha ocorrido a exploração de alguma vulnerabilidade do Active Directory ou o comprometimento de alguma credencial comum e posterior escalonamento de privilégio para obter permissão de escrita no compartilhamento do servidor de autenticação (sysvol).

5.9. Não obstante o emprego de ferramentas de segurança disponíveis e o exercício de todo o conhecimento técnico-científico, a ETIR-PR não logrou sucesso na conclusão da autoria do incidente. Por oportuno, informa-se que os computadores virtuais dos servidores afetados, bem como os artefatos utilizados na ocorrência, encontram-se preservados para análise e/ou perícia.

5.10. Todo o trabalho realizado foi documentado em relatório técnico confeccionado pela ETIR-PR e compartilhado com o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo - CTIR Gov e os Gestores de Segurança da Informação da Presidência da República.

6. DO MALWARE

6.1. Após análises realizadas pela ETIR-PR, verificou-se que o artefato utilizado tratava-se de 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.

6.2. Detalhes do malware:

6.2.1. 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

6.2.2. 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)

6.2.3. Dados sobre o resgate:

- Btc Address: bc1qakuel0s4nyge9rxjylsqdxnn9nvyhc2z6k27gz
- email: fishA001@protonmail.com

6.2.4. 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)

6.3. 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 (quarenta e sete) fornecedores de segurança e 1 (um) 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

6.4. 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.

7. DOS IMPACTOS CAUSADOS PELO MALWARE

7.1. Impende destacar que, ainda no dia do incidente, foi realizada uma avaliação dos equipamentos e de eventuais dados que foram afetados.

7.2. Dessa forma, por ação do malware, foi identificada a ocorrência de corrompimento/criptografia de arquivos do sistema operacional de alguns servidores e de computadores de usuários, bem como de alguns arquivos hospedados no servidor de arquivos.

7.3. **Todos os arquivos do servidor de arquivos pontualmente comprometidos foram recuperados por meio de restauração de *backup*.**

7.4. Quanto aos servidores afetados, eles foram reinstalados, restaurando os backups existentes. Como medida preventiva, em que pese encontrarem-se atualizados, todos os servidores que atuam como Controlador de Domínio, mesmo não tendo sido afetados, foram refeitos (novas máquinas virtuais). Todas as configurações e usuários foram preservados. As máquinas virtuais dos servidores substituídos foram preservadas para fins de auditoria.

7.5. 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.

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

7.7. Destaca-se que a reinstalação das máquinas é procedimento rotineiro nestes casos e foi precedido de backup dos arquivos dos usuários, os quais foram restaurados nos respectivos computadores após o término do processo de reinstalação. Cabe ressaltar 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.**

7.8. 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 Unidade.

7.9. Por fim, cumpre observar que o número de computadores de usuários tratados corresponde, aproximadamente, a 5% (cinco por cento) do parque computacional da Presidência da República.

8. DA PRESERVAÇÃO DOS DADOS INSTITUCIONAIS

8.1. No que tange aos dados eventualmente corrompidos/criptografados pelo *malware*, frise-se, por necessário, que foram recuperados por meio da restauração de *backup*, não tendo ocorrido perda de qualquer dado institucional ou mesmo pagamento de resgate por parte da Presidência da República.

8.2. Outrossim, importa enfatizar que **não foi detectado vazamento, tampouco o comprometimento de sistemas hospedados na rede da Presidência da República**. Os servidores de rede afetados foram recriados (novas máquinas), com acesso às mesmas bases de dados, as quais não sofreram qualquer comprometimento, destacando que as máquinas virtuais dos servidores substituídos foram preservadas para análise/auditoria posterior.

8.3. 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.**

9. DOS RECURSOS DE PREVENÇÃO E TRATAMENTO DE INCIDENTES CIBERNÉTICOS

9.1. No que concerne ao tópico em pauta, a Equipe de Tratamento de Incidentes em Rede da Presidência da República (ETIR-PR), em conformidade com a Norma Complementar nº 5/IN01/DSIC/GSIPR, foi instituída pela Portaria nº 97/SA/SE/SG/PR, de 11 de setembro de 2014, alterada pela Portaria nº 66/SA/SE/SG/PR, de 25 de maio de 2018. Seus agentes responsáveis foram designados pela Portaria nº 65/SA/SE/SG/PR, de 25 de maio de 2018.

9.2. Dessa forma, a ETIR-PR é composta pelos seguintes agentes:

- Agente Responsável Titular;
- Agente Responsável Substituto;
- Integrantes técnicos.

9.3. Complementarmente, convém esclarecer que, na estrutura organizacional da Secretaria-Geral da Presidência da República, a ETIR-PR está subordinada à Coordenação-Geral de Infraestrutura Tecnológica da Diretoria de Tecnologia da Secretaria Especial de Administração.

9.4. No tocante aos recursos de defesa, salienta-se que a rede computacional da Presidência da República é protegida por soluções de segurança como firewalls, antivírus (Solução McAfee Endpoint Security versão 10.7), antispam e IPS. O tratamento de incidentes como o reportado faz parte da rotina de sua ETIR, que, com o apoio de ferramentas de segurança, tem sido historicamente efetivo na defesa das ameaças e ataques que recebe diuturnamente.

10. DOS COMUNICADOS SOBRE O INCIDENTE

10.1. Em referência ao item em comento, a ETIR-PR comunicou o incidente cibernético ao CTIR Gov (3815349), aos Gestores de Segurança da Informação da Presidência da República (3815361) e ao público interno do órgão (3815374) no primeiro dia útil após o incidente, tão logo se configuraram informações suficientes para o relato.

10.2. Vale ressaltar que, desde a data do incidente, a ETIR-PR, em conjunto com a Coordenação de Segurança e Administração de Serviços da Coordenação-Geral de Infraestrutura Tecnológica e com a Coordenação-Geral de Atendimento a Usuários da Diretoria de Tecnologia dedicaram-se, sobremaneira, ao trabalho de garantir o restabelecimento pleno e seguro do ambiente computacional da Presidência da República, visando a continuidade da prestação dos serviços consoante suas competências regimentais estabelecidas.

10.3. Em paralelo, as mesmas equipes se dedicaram ao esforço de reunir todos os elementos considerados necessários para subsidiar o mérito de possível solicitação de apoio de recursos periciais para colaborarem na investigação do ilícito cibernético.

10.4. Neste sentido, um comunicado foi enviado ao Núcleo de Repressão a Crimes de Alta Tecnologia da Divisão de Repressão a Crimes Cibernéticos (NUCAT/DRCC) do Departamento de Polícia Federal para, de forma colaborativa, participar na elucidação do evento em pauta.

10.5. Todas as ações implementadas até presente data foram documentadas pela ETIR-PR e compartilhadas com o CTIR Gov e os Gestores de Segurança da Informação da Presidência da República.

11. DOS NORMATIVOS

11.1. No respeitante aos normativos que regulam a matéria sob exame, a Equipe de Tratamento de Incidentes em Rede da Presidência da República (ETIR-PR), em conformidade com a Norma Complementar nº 5/IN01/DSIC/GSIPR, foi instituída pela Portaria nº 97/SA/SE/SG/PR, de 11 de setembro de 2014, alterada pela Portaria nº 66/SA/SE/SG/PR, de 25 de maio de 2018. Seus agentes responsáveis foram designados pela Portaria nº 65/SA/SE/SG/PR, de 25 de maio de 2018.

11.2. Há de se mencionar, também, a Resolução nº 4/CGD/PR, de 05 de junho de 2020, que institui a Política de Segurança da Informação em Meios Tecnológicos da Presidência da República – POSITEC/PR, estabelece que a

Diretoria de Tecnologia deverá manter Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR, com a responsabilidade de receber, analisar e responder notificações e atividades relacionadas a incidentes de segurança em redes de computadores. A mesma resolução institui a figura do Gestor de Segurança da Informação em Meios Tecnológicos, cujo titular e substituto estão nomeados pela Portaria nº 1/DITEC/SA/SG/PR, de 19 de janeiro de 2022.

11.3. Adicionalmente, cita-se a Norma Complementar nº 8/IN01/DSIC/GSIPR, que estabelece as diretrizes para gerenciamento de incidentes computacionais nos órgãos e entidades da Administração Pública Federal, a qual dispõe em seu item 8, Disposições Gerais, os aspectos e procedimentos mínimos a serem observados pela ETIR; e Norma Complementar nº 21 /IN01/DSIC/GSIPR, estabelece as diretrizes para o registro de eventos, coleta e preservação de evidências de incidentes de segurança em redes nos órgãos e entidades da Administração Pública Federal, direta e indireta.

11.4. **As legislações supracitadas foram seguidas no tratamento do incidente cibernético em comento.**

11.5. Links dos normativos:

- Portaria nº 97/SA/SE/SG/PR, de 11 de setembro de 2014: https://www.in.gov.br/web/dou/-/portaria-n-97-de-11-de-setembro-de-2014-30164094
- Resolução nº 4/CGD/PR, de 05 de junho de 2020: http://www4.planalto.gov.br/cgd/assuntos/politica-de-seguranca-da-informacao-em-meios-tecnologicos-da-pr/positec-resolucao-no-04-de-05-de-junho-de-2020.pdf
- Norma Complementar nº 8/IN01/DSIC/GSIPR: https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=17/08/2009&jornal=1&pagina=8&totalArquivos=108
- Norma Complementar nº 8/IN01/DSIC/GSIPR: https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=24/08/2010&jornal=1&pagina=1&totalArquivos=144
- Norma Complementar nº 21 /IN01/DSIC/GSIPR: https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=10/10/2014&jornal=1&pagina=5&totalArquivos=224

12. DAS PROVIDÊNCIAS PÓS INCIDENTE CIBERNÉTICO

12.1. Considerando a forma como se deu o incidente, bem como o tipo de malware utilizado, foram adotadas as seguintes providências pela ETIR-PR e pela equipe de Infraestrutura Tecnológica da Diretoria de Tecnologia:

12.1.1. Revogação de todas as credenciais com privilégios administrativos e criação de novas contas;

12.1.2. Apresentação do incidente ocorrido, seu tratamento e providências decorrentes aos membros do Subcomitê de Segurança da Informação do Comitê de Governança Digital da Presidência da República, em reunião extraordinária;

12.1.3. Aprimoramento da política de gestão de credenciais com privilégios de administração das estações de trabalho; e

12.1.4. Solicitação ao Núcleo de Repressão a Crimes de Alta Tecnologia da Divisão de Repressão a Crimes Cibernéticos - NUCAT/DRCC) do Departamento de Polícia Federal para, de forma colaborativa, participar na elucidação do incidente.

13. Por fim, diante de todo o exposto, a Diretoria de Tecnologia da Presidência da República se coloca à disposição para os esclarecimentos complementares julgados ainda necessários.

Brasília, *na data da assinatura.*

Atenciosamente,

EDSON FLORIANO SOUSA JUNIOR
Gestor de Segurança da Informação em Meios Tecnológicos

BRUNO PEREIRA PONTES
Coordenador-Geral de Infraestrutura Tecnológica

De acordo. Encaminhe-se à Secretaria Especial de Administração para providências decorrentes.

CARLOS AUGUSTO PISSUTTI
Diretor de Tecnologia

Documento assinado eletronicamente por **Edson Floriano de Sousa Júnior**, **Coordenador(a)**, em 23/12/2022, às 10:56, 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 23/12/2022, às 11:06, 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 **Carlos Augusto Pissutti**, **Diretor(a)**, em 23/12/2022, às 11:09, 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 **3830848** e o código CRC **888FC884** no site:
https://super.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0

PRESIDÊNCIA DA REPÚBLICA

SECRETARIA-GERAL

SUBCHEFIA PARA ASSUNTOS JURÍDICOS

Nota SAJ nº 113 / 2022 / SAAINST/SAJ/SG/PR

CÂMARA DOS DEPUTADOS - CD

Interessado:

Ref: Requerimento de Informação nº 726/2022

Anexo: ----------

Assunto: Solicita ao Ministro de Estado Chefe da Secretaria-Geral da Presidência da República informações sobre a notícia de que os computadores do Planalto foram apagados por suposta "ameaça"

Processo : 00133.001080/2022-29

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 726, de 2022, de autoria da Comissão de Fiscalização Financeira e Controle, que solicita informações sobre a notícia de que os computadores do Planalto foram apagados por suposta "ameaça". Destaca-se que a solicitação decorre da aprovação do Requerimento nº 125/2022, de autoria do Deputado Leo de Brito, aprovado pelo plenário da Comissão, em reunião extraordinária do dia 23/11/2022.

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 justificação 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 conseqüência, 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 manifestou-se por meio da **Nota Informativa nº 3/2022/GAB/DITEC/SA** (doc SEI 3830848), respondendo aos questionamentos de ordem técnica, encaminhados pela Comissão.

9. Dessa forma, esta Subchefia entende que a solicitação de informações em epígrafe encontra-se atendida pela **Nota Informativa nº 3/2022/GAB/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 726, 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 28/12/2022, às 15:46, 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 28/12/2022, às 17:05, 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 **3838710** e o código CRC **CC75A433** no site: https://super.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0