Interessado: Diretoria de Infraestrutura Tecnológica e Conectividade

Assunto: Resposta ao Questionamento - Empresa 03

ITEM 01 — Dimensionamento do NGFW Tipo "Small"

Aplica-se aos itens do LOTE 01 (Tipos 01, 02, 05, 06 e 13) e ao Item 34 do LOTE 02 (NGFW Tipo 02). Link real do cenário definido no TR: 500 a 600 Mbps (banda larga).

a) Throughput VPN IPSec — superdimensionamento de 5×
Item 1.2.17 (e equivalentes nos Tipos 02, 05, 06, 13 do LOTE 01 e Item 34 do LOTE 02)

"Deve possuir VPN com capacidade de, pelo menos, 06 (seis) Gbps de tráfego IPSec."
Considerando o Link real do cenário para esse modelo de NGFW definido no TR como 500 a 600 Mbps (banda larga).

O TR exige 6 Gbps de IPSec para um link real de 500–600 Mbps, cenário em que o gargalo efetivo de inspeção é o Threat Protection (1,2 Gbps), valor já corretamente dimensionado no item 1.2.15. Em NGFW + SD-WAN com inspeção ativa, todo o tráfego dos túneis IPSec passa obrigatoriamente pelo motor de Threat Protection; assim, o IPSec útil não pode exceder 1,2 Gbps. O valor de 6 Gbps reflete cenário sem inspeção (apenas criptografia em ASIC dedicado), e não tem função prática no cenário operacional exigido. O ajuste preserva ainda margem técnica de 2× sobre o link real.

Desta forma solicitamos que esse item seja alterado para: "Deve possuir VPN com capacidade de, pelo menos, 1,2 (um vírgula dois) Gbps de tráfego IPSec."

Nossa solicitação será acatada?

RESPOSTA

Não. Mantido conforme edital.

A capacidade IPSec e o throughput de Threat Protection representam métricas distintas, não havendo equivalência obrigatória entre esses parâmetros. O dimensionamento da solução não se limita exclusivamente à capacidade nominal dos enlaces WAN, considerando múltiplos túneis simultâneos, SD-WAN overlay, expansão futura do ambiente e preservação do desempenho da solução com as funcionalidades exigidas habilitadas. Adicionalmente, o Item 34 do Lote 02 não possui vinculação com o lote 01, Rede Governo, devendo ser utilizado em diferentes cenários e arquiteturas de rede, conforme as necessidades operacionais da Administração

b) Quantidade de interfaces RJ45 1GE

Item 1.2.22 (e equivalentes nos Tipos 02, 05, 06, 13 do LOTE 01 e Item 34 do LOTE 02)

“Deve possuir, pelo menos, 09 (nove) interfaces RJ45 1GE.”

Considerando o Link real do cenário para esse modelo de NGFW definido no TR como 500 a 600 Mbps (banda larga), e a topologia típica de unidade de pequeno porte (1 a 2 links WAN e 2 a 3 segmentos LAN).

Em unidades de pequeno porte, com 1 a 2 links WAN e 2 a 3 segmentos LAN, a exigência de 9 portas é tecnicamente excessiva. Seis portas atendem com folga ao cenário típico (WAN principal + WAN backup + LAN + DMZ + HA + porta de reserva), preservando a flexibilidade operacional sem inflar o custo. A exigência de 9 portas atua, na prática, como filtro de fabricantes, o que penaliza a competitividade sem benefício funcional.

Desta forma solicitamos que esse item seja alterado para: “Deve possuir, pelo menos, 06 (seis) interfaces RJ45 1GE.”

Nossa solicitação será acatada?

RESPOSTA

Não. Mantido conforme edital.

O dimensionamento da quantidade de interfaces não se limita exclusivamente ao cenário nominal de enlaces WAN, considerando também segmentação de rede, expansão operacional, múltiplas zonas de segurança, alta disponibilidade e demais requisitos de conectividade da solução. Adicionalmente, o Item 34 do Lote 02 não possui vinculação com o lote 01, Rede Governo, devendo ser utilizado em diferentes cenários e arquiteturas de rede, conforme as necessidades operacionais da Administração

ITEM 02 — Dimensionamento do NGFW Tipo “MEDIO”

Aplica-se ao Item 03 do LOTE 01 (Tipo 03). Link real do cenário definido no TR: até 1 Gbps.

a) Throughput VPN IPSec — superdimensionamento de 13×
Item 3.2.17

“Deve possuir VPN com capacidade de, pelo menos, 33 (trinta e três) Gbps de tráfego IPSec.”

Considerando o Link real do cenário para esse modelo de NGFW definido no TR como até 1 Gbps.

O TR exige 33 Gbps de IPSec para um link real de 1 Gbps, valor 33× superior ao link de WAN e 13× superior ao Threat Protection (2,5 Gbps), que é o limite real da cadeia de inspeção. Em NGFW + SD-WAN com inspeção ativa, o IPSec útil não pode exceder o Threat Protection. O valor de 33 Gbps reflete cenário sem inspeção (apenas criptografia em ASIC dedicado), e não tem função prática no cenário operacional exigido. A sugestão alinha o IPSec ao Threat (2,5 Gbps), preservando margem técnica de 2,5× sobre o link real.

Desta forma solicitamos que esse item seja alterado para: “Deve possuir VPN com capacidade de, pelo menos, 2,5 (dois vírgula cinco) Gbps de tráfego IPSec.”

Nossa solicitação será acatada?

RESPOSTA

Não. Mantido conforme edital.

A capacidade IPSec e o throughput de Threat Protection representam métricas distintas, não havendo equivalência obrigatória entre esses parâmetros. O dimensionamento da solução não se limita exclusivamente à capacidade nominal dos enlaces WAN, considerando múltiplos túneis simultâneos, SD-WAN overlay, expansão futura do ambiente e preservação do desempenho da solução com as funcionalidades exigidas habilitadas.

b) Inspeção SSL Throughput

Item 3.2.16 “Deve possuir Inspeção SSL Throughput com capacidade mínima de processamento de 3 (três) Gbps.”

Considerando o Link real do cenário para esse modelo de NGFW definido no TR como até 1 Gbps.

A Inspeção SSL é uma das funcionalidades habilitadas no motor de Threat Protection. Como o gargalo real do equipamento é o Threat (2,5 Gbps) e o link máximo é de 1 Gbps, exigir 3 Gbps de Inspeção SSL é incoerente com o restante do dimensionamento, pois sugere capacidade superior ao próprio gargalo da cadeia.
O ajuste para 2,3 Gbps mantém margem técnica adequada (2,3× sobre o link real) e elimina a inconsistência interna do TR.

Desta forma solicitamos que esse item seja alterado para: “Deve possuir Inspeção SSL Throughput com capacidade mínima de processamento de 2,3 (dois vírgula três) Gbps.”

Nossa solicitação será acatada?

RESPOSTA

Não. Mantido conforme edital.

Os indicadores de SSL Inspection Throughput e Threat Protection Throughput representam métricas técnicas distintas, conforme metodologias e arquiteturas adotadas por cada fabricante, não havendo equivalência obrigatória entre esses parâmetros. O dimensionamento da solução não se limita exclusivamente à capacidade nominal dos enlaces WAN, considerando também escalabilidade, tráfego lateral e preservação do desempenho da solução com as funcionalidades avançadas exigidas habilitadas.

c) Composição de interfaces (RJ45 1GE, SFP 1GE e SFP+ 10GE)

Item 3.2.22, 3.2.23 e 3.2.24 (alteração consolidada)

“3.2.22. Deve possuir, pelo menos, 10 (dez) interfaces RJ45 1GE. 3.2.23. Deve possuir, pelo menos, 04 (quatro) interfaces SFP+ 10GE. 3.2.24. Deve possuir, pelo menos, 06 (seis) interfaces SFP 1GE.” (texto conforme retificação — redução do 3.2.22 de 12 para 10 portas RJ45, mas mantidos 4× SFP+ 10GE e 6× SFP 1GE.)

Considerando o Link real do cenário para esse modelo de NGFW definido no TR como até 1 Gbps.

A retificação reduziu o item 3.2.22 de 12 para 10 portas RJ45 1GE, mas manteve a exigência de 4× SFP+ 10GE (item 3.2.23) e de 6× SFP 1GE (item 3.2.24). Para um link real de 1 Gbps, exigir 4× SFP+ 10GE no appliance permanece tecnicamente injustificável: nenhuma porta de 10 Gbps será utilizada durante a vigência contratual, ocupando custo de hardware sem benefício funcional. As 6 interfaces SFP 1GE pressupõem entrega óptica direta no appliance, cenário pouco frequente em links de banda larga (a maioria dos ISPs entrega via ONT com saída RJ45 1GE). A exigência atual atua como filtro de fabricantes, restringindo a competição. A composição sugerida (8× RJ45 + 2× SFP para redundância) atende plenamente ao cenário operacional, com flexibilidade para entrega via fibra quando necessário.

Desta forma solicitamos que esse item seja alterado para: “3.2.22. Deve possuir, pelo menos, 08 (oito) interfaces RJ45 1GE. 3.2.23. Deve possuir, pelo menos, 02 (duas) interfaces SFP 1GE para redundância (suprimida a exigência de SFP+ 10GE). 3.2.24. Suprimido.”

Nossa solicitação será acatada?

RESPOSTA

Não. Mantido conforme edital.

O dimensionamento das interfaces não se limita exclusivamente à capacidade nominal dos enlaces WAN, considerando também tráfego lateral, segmentação interna, alta disponibilidade, uplinks LAN/core, agregação de enlaces, crescimento operacional e demais cenários de utilização da solução. Adicionalmente, a exigência de interfaces 10GE visa evitar dependência excessiva de agregação de múltiplas interfaces 1GE para atendimento simultâneo das possíveis demandas de conectividade e segurança

ITEM 03 — Dimensionamento do NGFW Tipo "LARGE"

Aplica-se aos itens do LOTE 01 (Tipos 04, 14, 15 e 16) e ao Item 36 do LOTE 02 (NGFW Tipo 03). Link real do cenário definido no TR: até 2,1 Gbps agregado (dois links WAN).

a) Throughput de IPS — alinhamento ao Threat Protection
Item 4.2.14 (e equivalente no Item 36 do LOTE 02)

"Deve possuir IPS com capacidade mínima de processamento de 5 (cinco) Gbps."

Considerando o Link real do cenário para esse modelo de NGFW definido no TR como até 2,1 Gbps agregado (dois links WAN).

O IPS exigido (5 Gbps) é maior que o Threat Protection (2,5 Gbps), o que é tecnicamente incoerente: o IPS é um dos componentes do motor de Threat Protection. Quando todas as funções de inspeção estão habilitadas (cenário operacional real), o limite efetivo do IPS é igual ao do Threat Protection. O alinhamento em 2,5 Gbps elimina a inconsistência interna do TR e preserva margem técnica adequada (>2× sobre o link agregado de 2,1 Gbps).

Registra-se que a retificação incluiu, neste item, a cláusula "Para efeitos de comprovação pode também ser considerado o throughput de Threat Protection". Tal cláusula constitui flexibilidade exclusivamente documental (aplicável a fabricantes cujo datasheet não publica o IPS isoladamente) e não reduz o valor numérico de 5 Gbps exigido, razão pela qual a incongruência técnica entre IPS (5 Gbps) e Threat Protection (2,5 Gbps) permanece e o questionamento é mantido.

Desta forma solicitamos que esse item seja alterado para: "Deve possuir IPS com capacidade mínima de processamento de 2,5 (dois vírgula cinco) Gbps."

Nossa solicitação será acatada?

RESPOSTA

Não. Mantido conforme edital

O IPS e o Threat Protection representam métricas distintas, conforme metodologias e arquiteturas adotadas por cada fabricante, não havendo equivalência obrigatória entre esses parâmetros. O dimensionamento da solução não se limita exclusivamente à capacidade nominal dos enlaces WAN, considerando escalabilidade, tráfego lateral e preservação do desempenho da solução sob carga. Adicionalmente, o Item 36 do Lote 02 não possui vinculação com o lote 01, Rede Governo, devendo ser utilizado em diferentes cenários e arquiteturas de rede, conforme as necessidades operacionais da Administração

b) Throughput VPN IPSec — superdimensionamento de 13×
Item 4.2.17 (e equivalente no Item 36 do LOTE 02)

"Deve possuir VPN com capacidade de, pelo menos, 33 (trinta e três) Gbps de tráfego IPSec."

Considerando o Link real do cenário para esse modelo de NGFW definido no TR como até 2,1 Gbps agregado (dois links WAN).

O IPSec útil é limitado pelo Threat Protection (2,5 Gbps), gargalo efetivo da cadeia de inspeção em NGFW + SD-WAN com inspeção ativa. Exigir 33 Gbps de IPSec para um cenário com link agregado de 2,1 Gbps é 13× superdimensionado. O valor de 33 Gbps reflete cenário sem inspeção (apenas criptografia em ASIC dedicado), e

não tem função prática no cenário operacional exigido. O ajuste para 2,5 Gbps mantém margem técnica adequada e preserva o cenário operacional pretendido.

Desta forma solicitamos que esse item seja alterado para: “Deve possuir VPN com capacidade de, pelo menos, 2,5 (dois vírgula cinco) Gbps de tráfego IPSec.”

Nossa solicitação será acatada?

RESPOSTA

Não. Mantido conforme edital.

A capacidade VPN IPSec e o throughput de Threat Protection representam métricas distintas, não havendo equivalência obrigatória entre esses parâmetros. O dimensionamento da solução não se limita exclusivamente à capacidade nominal dos enlaces WAN, considerando múltiplos túneis simultâneos, SD-WAN overlay, expansão futura do ambiente e preservação do desempenho da solução com as funcionalidades exigidas habilitadas.

Adicionalmente, o Item 36 do Lote 02 não possui vinculação com o lote 01, Rede Governo, devendo ser utilizado em diferentes cenários e arquiteturas de rede, conforme as necessidades operacionais da Administração.

c) Composição de interfaces (RJ45 1GE, SFP 1GE e SFP+ 10GE)

Item 4.2.22, 4.2.23 e 4.2.24 (alteração consolidada — e equivalentes no Item 36 do LOTE 02)

“4.2.22. Deve possuir, pelo menos, 10 (dez) interfaces RJ45 1GE. 4.2.23. Deve possuir, pelo menos, 04 (quatro) interfaces SFP+ 10GE. 4.2.24. Deve possuir, pelo menos, 06 (seis) interfaces SFP 1GE.” (texto conforme retificação — o item 4.2.22 foi reduzido de 12 para 10 portas RJ45, atendendo parcialmente o solicitado; permanecem, entretanto, 4× SFP+ 10GE e 6× SFP 1GE.)

Considerando o Link real do cenário para esse modelo de NGFW definido no TR como até 2,1 Gbps agregado (dois links WAN).

A retificação reduziu o item 4.2.22 de 12 para 10 portas RJ45 1GE, atendendo parcialmente o pleito, mas manteve a exigência de 4× SFP+ 10GE (item 4.2.23) e de 6× SFP 1GE (item 4.2.24). Para tráfego agregado máximo de 2,1 Gbps (dois links de 1 Gbps em SD-WAN), as 4 portas SFP+ 10GE não têm justificativa técnica: ficariam permanentemente ociosas. As 6 portas SFP 1GE pressupõem entrega óptica direta, cenário raro em banda larga. A composição sugerida (10× RJ45 + 2× SFP para HA/LACP) atende plenamente ao cenário, com folga de portas para LAN, DMZ, segmentação interna e alta disponibilidade, eliminando a barreira artificial de fabricantes imposta pela exigência de 10GE.

Desta forma solicitamos que esse item seja alterado para: “4.2.22. Deve possuir, pelo menos, 10 (dez) interfaces RJ45 1GE. 4.2.23. Deve possuir, pelo menos, 02 (duas) interfaces SFP 1GE para HA/LACP (suprimida a exigência de SFP+ 10GE). 4.2.24. Suprimido.”

Nossa solicitação será acatada?

RESPOSTA

Não. Mantido conforme edital.

O dimensionamento da quantidade de interfaces não se limita exclusivamente ao cenário nominal de enlaces WAN, considerando também segmentação de rede, expansão operacional, múltiplas zonas de segurança, alta disponibilidade e demais requisitos de conectividade da solução. Adicionalmente, o Item 36 do Lote 02 não possui vinculação com o lote 01, Rede Governo, devendo ser utilizado em diferentes cenários e arquiteturas de rede, conforme as necessidades operacionais da Administração.

ITEM 04 — Dimensionamento do NGFW Tipo I (Data Center)

Aplica-se ao Item 13 do LOTE 02 (Solução de Segurança de Rede NGFW — Tipo I, appliance físico de Data Center, maior porte). A topologia adotada no projeto utiliza segurança descentralizada, com inspeção NGFW + Threat Protection completa em cada unidade governamental (perfis Small, Medium e Large). Nesse modelo, o NGFW de Data Center deixa de exercer função de “inspeção massiva de tráfego de saída” e passa a desempenhar três funções principais: (i) terminação de túneis IPSec/SD-WAN das unidades; (ii) proteção e segmentação interna dos serviços do DC; e (iii) inspeção de tráfego norte-sul de aplicações expostas. O dimensionamento do DC deve refletir essa função, evitando sobrecapacidade sem ganho real e, simultaneamente, garantindo capacidade de expansão futura.

a) Throughput de IPS
Item 38.13.1 (renumerado na retificação; anteriormente 38.14)

“Deve possuir IPS com capacidade mínima de processamento de 40 (quarenta) Gbps.”
Considerando que a arquitetura adotada é descentralizada, com inspeção IPS principal já ocorrendo na borda de cada unidade governamental, e que o NGFW de DC tem função de proteção de serviços e segmentação interna.
O valor de 40 Gbps de IPS é superdimensionado para uma arquitetura descentralizada onde a inspeção IPS principal já ocorre na borda de cada unidade. O ajuste para 30 Gbps mantém capacidade robusta para a função desempenhada pelo DC (proteção de serviços e segmentação interna), elimina sobrecapacidade desnecessária e amplia a competitividade entre fabricantes. Registra-se que a retificação incluiu, neste item (renumerado para 38.13.1), a cláusula “Para efeitos de comprovação pode também ser considerado o throughput de Threat Protection”. Tal cláusula constitui flexibilidade exclusivamente documental e não reduz o valor numérico de 40 Gbps exigido, razão pela qual o questionamento é mantido.

Desta forma solicitamos que esse item seja alterado para: “Deve possuir IPS com capacidade mínima de processamento de 30 (trinta) Gbps.”

Nossa solicitação será acatada?

RESPOSTA

Não. Mantido conforme edital.

O Item 13 do Lote 02 refere-se à “Solução de Segurança de Rede NGFW TIPO I” , integrante do conjunto de “soluções de segurança da informação e cibersegurança” do Lote 02 , não possuindo vinculação técnica ou operacional com os cenários de conectividade do Lote 01 – Rede Governo V.

b) Threat Protection Throughput
Item 38.14 (renumerado na retificação; anteriormente 38.15)

“Proteção contra ameaças avançadas (Threat Protection) com capacidade mínima de processamento de 30 (trinta) Gbps.”

Considerando que a arquitetura adotada é descentralizada, com inspeção principal já ocorrendo nas pontas, e que o NGFW de DC executa Threat Protection essencialmente para tráfego norte-sul, leste-oeste e tráfego que atravesse a borda do DC.

O valor de 30 Gbps de Threat Protection é superdimensionado para uma arquitetura descentralizada, onde a inspeção principal já ocorre nas pontas. No DC, o Threat Protection é exigido essencialmente para: (i) tráfego norte-sul (aplicações expostas), (ii) inspeção de tráfego entre segmentos internos (leste-oeste) e (iii) inspeção de tráfego que atravesse a borda do DC. Para esse perfil de uso, 20 Gbps representam capacidade adequada com margem técnica robusta, sem sobrecapacidade que infla o custo do appliance.

Desta forma solicitamos que esse item seja alterado para: “Proteção contra ameaças avançadas (Threat Protection) com capacidade mínima de processamento de 20 (vinte) Gbps.”

Nossa solicitação será acatada?

RESPOSTA

Não. Mantido conforme edital.

O Item 13 do Lote 02 refere-se à “Solução de Segurança de Rede NGFW TIPO I” , integrante do conjunto de “soluções de segurança da informação e cibersegurança” do Lote 02 , não possuindo vinculação técnica ou operacional com os cenários de conectividade do Lote 01 – Rede Governo V.

c) Throughput VPN IPSec — alinhamento ao Threat Protection
Item 38.16 (renumerado na retificação; anteriormente 38.17)

“Deve possuir VPN com capacidade de, pelo menos, 50 (cinquenta) Gbps de tráfego IPSec.”

Considerando que o NGFW de DC é o concentrador de túneis IPSec das unidades, mas todo o tráfego que entra pelos túneis passa, em seguida, pelo motor de Threat Protection.

O DC é o concentrador de túneis IPSec das unidades, mas todo o tráfego que entra pelos túneis passa, em seguida, pelo motor de Threat Protection (que será 20 Gbps na sugestão do item 10.b). Portanto, o IPSec útil não pode exceder, na prática operacional, o limite do Threat Protection. O valor de 50 Gbps reflete cenário sem inspeção (apenas criptografia em ASIC dedicado), e não tem função prática no cenário operacional exigido. A sugestão de 30 Gbps preserva folga sobre o Threat Protection ajustado e atende plenamente à função de concentração de túneis.

Desta forma solicitamos que esse item seja alterado para: “Deve possuir VPN com capacidade de, pelo menos, 30 (trinta) Gbps de tráfego IPSec.”

Nossa solicitação será acatada?

RESPOSTA

Não. Mantido conforme edital.

O Item 13 do Lote 02 refere-se à “Solução de Segurança de Rede NGFW TIPO I” , integrante do conjunto de “soluções de segurança da informação e cibersegurança” do Lote 02 , não possuindo vinculação técnica ou operacional com os cenários de conectividade do Lote 01 – Rede Governo V.

d) Inclusão de interfaces de alta velocidade (40GE/100GE) para expansão
Item 38.21, 38.22, 38.23, 38.24 (inclusão de novo subitem para interfaces QSFP; itens renumerados na retificação)

“38.21. Deve possuir, pelo menos, 10 (dez) interfaces RJ45 1GE. 38.22. Deve possuir, pelo menos, 4 (quatro) interfaces SFP28 25GE. 38.23. Deve possuir, pelo menos, 4 (quatro) interfaces SFP+ 10GE. 38.24. Deve possuir, pelo menos, 1 (uma) interface RJ45 2.5GE.” (texto conforme retificação)

Considerando que o NGFW de DC é o concentrador da rede e deve estar dimensionado para expansão futura ao longo da vigência contratual e suas eventuais renovações.

Em redes governamentais, o NGFW do Data Center é o concentrador da rede e deve estar dimensionado para expansão futura ao longo da vigência contratual (12 meses + renovações). A inclusão de 2 interfaces de alta velocidade (QSFP+ 40GE ou QSFP28 100GE) garante capacidade de evolução do backbone do DC e do uplink para core/spine sem necessidade de troca de hardware. A inclusão é especialmente relevante em cenários de crescimento de tráfego intra-DC e de adoção de aplicações de governo digital. Esse ajuste agrega valor técnico sem onerar excessivamente o custo, uma vez que praticamente todos os modelos de NGFW de DC do mercado já oferecem essa interface em série ou via slot de expansão. Cabe ressaltar, ainda, que o próprio Edital retificado já contempla 2× QSFP28 100GE em outro perfil de NGFW (item 21.6.1.1.15), o que demonstra a factibilidade técnica e a aderência da inclusão ora pleiteada ao padrão já adotado pela PRODEB.

Desta forma solicitamos que esse item seja alterado para: “Inclusão do item 38.24-A: Deve possuir, pelo menos, 02 (duas) interfaces QSFP+ 40GE ou QSFP28 100GE. (Os itens 38.21, 38.22, 38.23 e 38.24 permanecem inalterados.)”

Nossa solicitação será acatada?

RESPOSTA

Não. Mantido conforme edital.

O Item 13 do Lote 02 refere-se à “Solução de Segurança de Rede NGFW TIPO I” , integrante do conjunto de “soluções de segurança da informação e cibersegurança” do Lote 02 , não possuindo vinculação técnica ou operacional com os cenários de conectividade do Lote 01 – Rede Governo V.

Documento assinado eletronicamente por **Elmo dos Santos Sales**, **Assessor Especial**, em 26/05/2026, às 16:03, conforme horário oficial de Brasília, com fundamento no art. 13º, Incisos I e II, do Decreto nº 15.805, de 30 de dezembro de 2014.

A autenticidade deste documento pode ser conferida no site https://seibahia.ba.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **00141056474** e o código CRC **0EC3B5F6**.

Referência: Processo nº 065.10933.2026.0003946-61 SEI nº 00141056474