



PRESIDÊNCIA DA REPÚBLICA
COORDENAÇÃO DE LICITAÇÕES

Decisão nº 78/2025/COLIT/COLIC/DILOG/SA/SE/CC/PR

Brasília, 11 de dezembro de 2025.

Assunto: Decisão de Recurso

Referência: Pregão nº 90037/2025 – Objeto: Aquisição de storages visando a atualização tecnológica de solução de armazenamento de dados, incluindo software, serviços de instalação, configuração, migração de dados, garantia e suporte técnico para a Presidência da República.

Processo: 00094.000081/2024-21

Trata-se de recurso interposto pela empresa COMPWIRE INFORMÁTICA LTDA (7201139), inscrita no CNPJ sob o nº 01.181.242/0003-53, contra a decisão do Pregoeiro que recusou sua proposta e contra a decisão que aceitou a proposta da empresa SERVIX INFORMATICA LTDA no âmbito do Pregão, na forma eletrônica, nº 90037/2025.

As razões de recurso foram interpostas tempestivamente e encontram-se disponíveis no sítio www.gov.br/compras.

DOS FATOS

1. Aos 30 dias de outubro do ano de 2025, foi aberta sessão da licitação instaurada pela Secretaria de Administração, com vistas à escolha da proposta mais vantajosa para aquisição de storages visando a atualização tecnológica de solução de armazenamento de dados, incluindo software, serviços de instalação, configuração, migração de dados, garantia e suporte técnico para a Presidência da República.
2. Em cumprimento aos procedimentos licitatórios, no dia 30 de outubro, foi realizada a convocação da empresa COMPWIRE INFORMÁTICA LTDA, primeira classificada após a fase de lances, para o envio da proposta de preços ajustada ao último lance, por meio do anexo do Sistema de Compras do Governo Federal, conforme estabelecido no edital.
3. Após, foram juntadas ao processo a proposta e a documentação de habilitação enviadas, na forma prevista do subitem 6 e 8 do edital, as quais foram submetidas à área técnica demandante para análise.
4. Na ocasião, a área técnica solicitou diligência, nos termos do documento (7126124). Por sua vez, a empresa COMPWIRE INFORMÁTICA LTDA apresentou sua resposta, conforme Documento de diligência (7133459).
5. Após nova análise da equipe técnica, considerando as informações apresentadas em diligência, conforme Despacho (7135730), a empresa COMPWIRE INFORMÁTICA LTDA teve proposta rejeitada, em razão do descumprimento dos itens 2.1.80.8, 2.2.81.8, 2.1.81 e 2.2.82 do Termo de Referência, além de não comprovar plenamente os itens 2.1.3, 2.2.3, 2.1.5, 2.2.5, 2.1.51, 2.2.50, 2.1.68.2, 2.2.69.2, 2.1.69, 2.2.70, 2.1.77 e 2.2.78.
6. Em seguida, na ordem de classificação, foi convocada a empresa SERVIX INFORMATICA LTDA, para envio da proposta e documentação de habilitação, conforme documento (7157922, 7157952, 7157993).
7. Na ocasião, a área técnica solicitou diligência, nos termos do Despacho (7162748). Em sua resposta, a empresa SERVIX INFORMATICA LTDA apresentou o Documento de diligência SERVIX (7171605).
8. Considerando a documentação apresentada em diligência, a área técnica manifestou-se favorável quanto à aceitação da proposta e da qualificação técnica da empresa SERVIX INFORMATICA LTDA, de acordo com o Despacho COCED/CGINT/DITEC/SA/SE/CC/PR (7172473). Diante disso, a empresa SERVIX INFORMATICA LTDA teve sua proposta aceita e, na sequência, foi habilitada.
9. Em momento oportuno, foi registrado pela empresa COMPWIRE INFORMÁTICA LTDA a intenção de recorrer.

DO RECURSO

10. Em sua peça recursal, a Recorrente COMPWIRE INFORMÁTICA LTDA (7201139), consigna o seguinte pedido:

(...)

REQUERIMENTOS:

Ante todo o exposto, respeitosamente e ante a fundamentação supra, requer-se que seja dado provimento ao presente Recurso Administrativo, a fim de seja reformada a r. decisão que desclassificou a COMPWIRE do processo de contratação regido pelo Edital Pregão Eletrônico nº 90037/2025-AS, bem como a r. decisão que habilitou e declarou a empresa SERVIX INFORMATICA LTDA como provisoriamente vencedora do Pregão em questão.

DAS CONTRARRAZÕES DO RECURSO

11. A empresa Recorrida SERVIX INFORMATICA LTDA, apresentou suas contrarrazões, com o seguinte pedido:

DA BREVE SÍNTESE DOS FATOS

(...)

Diante do exposto, a empresa SERVIX INFORMATICA LTDA., requer que:

- a) Seja a presente contrarrazão recebida, processada e julgada pela autoridade competente;
- b) Seja mantida a decisão de que desclassificou a licitante COMPWIRE INFORMÁTICA LTDA.;
- c) Seja mantida a decisão que aceitou e habilitou a proposta vencedora, apresentada pela empresa SERVIX INFORMATICA LTDA., com sua adjudicação e homologação de vencedora do certame;
- d) O encaminhamento da presente CONTRARRAZÃO para instância superior, na remota hipótese de ser julgado improcedente, o que se admite apenas como argumentação, para que então se proceda à reforma da decisão.

DA ANÁLISE

12. Quanto ao recurso interposto pela empresa COMPWIRE INFORMÁTICA LTDA, considerando que as razões apresentadas pela recorrente são eminentemente técnicas, as quais recaem sobre as exigências contidas no Termo de Referência que é de responsabilidade exclusiva da área demandante, a qual detém conhecimento técnico do objeto por ela especificado, os autos foram remetidos à área técnica demandante para análise da peça recursal, conforme Despacho COLIT/COLIC/DILOG/SA (7201155), que emitiu a Nota técnica (7203024), transcrita abaixo:

ANÁLISE TÉCNICA QUANTO AO RECURSO INTERPOSTO PELA LICITANTE COMPWIRE

1. A empresa COMPWIRE apresentou RECURSO contra a análise encaminhada à CPL por meio do Despacho (Doc 7135730) onde foi concluída que a proposta técnica apresentada pela referida empresa encontra-se em desacordo com as exigências do edital do Pregão.

2. Cabe ressaltar que a COMPWIRE, além não concordar com sua desclassificação, apresentou RAZÕES para discordar da classificação da empresa SERVIX.

3. A seguir são apresentados os principais pontos das RAZÕES da empresa Recorrente COMPWIRE, as CONTRARRAZÕES da empresa Recorrida SERVIX e o parecer da área técnica da Presidência da República - PR referentes ao Recurso Administrativo da COMPWIRE.

4. RAZÕES COMPWIRE:

5. A seguir as razões apresentadas pela Recorrente em relação aos itens “2.1.3”, “2.1.5”, “2.2.3” e “2.2.5” do Termo de Referência.

“II.1. ATENDIMENTO AOS ITENS “2.1.3”, “2.1.5”, “2.2.3” E “2.2.5” – SOLUÇÃO QUE NÃO POSSUI END-OF-LIFE DEFINIDA E DIZ RESPEITO À FAMÍLIA MAIS RECENTE DISPONÍVEL PARA COMERCIALIZAÇÃO:”

“16. Nos termos da análise técnica, a proposta da COMPWIRE supostamente deixou de atender os Itens “2.1.3”, “2.1.5”, “2.2.3” E “2.2.5”, que assim dispõe:

“2.1.3. O equipamento deverá pertencer a família mais recente disponível para atendimento aos requisitos deste termo, não sendo aceitos equipamentos que possuam “end of sale” e “end of support” anunciados até a data de abertura do edital.

2.1.5. No momento da apresentação das propostas, o equipamento ofertado deverá ser o mais recente disponível no portfólio do fabricante e ter sido lançado em um prazo não superior a 24 meses.

2.2.3. O equipamento deverá pertencer a família mais recente disponível para atendimento aos requisitos deste termo, não sendo aceitos equipamentos que possuam “end of sale” e “end of support” anunciados até a data de abertura do edital.

2.2.5. No momento da apresentação das propostas, o equipamento ofertado deverá ser o mais recente disponível no portfólio do fabricante e ter sido lançado em um prazo não superior a 24 meses.”

17. Nos termos da análise técnica, supostamente fora apresentado pela COMPWIRE o documento oficial e público de EOM (end of marketing) de versão já descontinuada dos produtos Huawei, OceanStor V5, assim disponível:

(...)

18. Ocorre que a análise técnica parte de premissa equivocada. Isso porque está explícito por **todos** os documentos comprobatórios que a solução proposta possui linha de armazenamento nomeada como *OceanStor Capacity Flash* na sua versão 6.x, firmware 6.1.8, não possuindo End-of-Life definido, conclusão esta que é reforçada por meio de declaração oficial da fornecedora da solução para o presente processo de contratação:

(...)

19. A análise técnica alegou suposta incoerência da Recorrente ao afirmar que a Huawei já teria anunciado a nova geração da linha *OceanStor Dorado* (“*New-Gen Dorado*”).

20. Todavia, trata-se apenas de um anúncio global, referente ao *roadmap* internacional do fabricante, não havendo, até o presente momento, liberação para comercialização dessa linha no Brasil pela própria Huawei.

21. Logo, a alegação não se sustenta, pois se refere a um produto indisponível no mercado nacional, sendo que o atendimento aos Itens “2.1.3”, “2.1.5”, “2.2.3” e “2.2.5” é corroborado pela própria fornecedora, como acima colacionado e também apresentado junto à proposta.

22. Ademais, a linha OceanStor Dorado não pertence à mesma família de produtos ofertada no presente certame. A Recorrente apresentou a solução *OceanStor Capacity Flash*, cuja arquitetura, catálogo técnico, ciclo de vida e posicionamento comercial **são totalmente distintos e independentes da linha OceanStor Dorado**.

23. Assim, o anúncio global de um produto de outra família, com características, público-alvo e especificações diferentes, não guarda qualquer relação com o modelo efetivamente ofertado na licitação.

24. Para fins de esclarecimento, o portfólio de armazenamento primário da Huawei é atualmente composto por quatro linhas distintas:

(i) *OceanStor Dorado V6* (linha all-flash atual de alta performance);

(ii) *OceanStor Capacity Flash* (linha all-flash atual de alta capacidade — produto ofertado neste certame);

(iii) *OceanStor Pacific* (storage distribuído de objetos/arquivos);

(iv) *OceanStor Hybrid* (família híbrida SAS/NL-SAS).

25. Dessa forma, reafirma-se que o modelo OceanStor 5510 Capacity Flash representa sim a última geração disponível e oficialmente comercializada pela HUAWEI no Brasil dentro de sua respectiva linha de produtos, bem como o pleno atendimento da solução da Recorrente aos Itens “2.1.3”, “2.1.5”, “2.2.3” e “2.2.5”.

6. CONTRARRAZÕES SERVIX

6.1 A seguir as contrarrazões apresentadas pela Recorrida em relação aos itens “2.1.3”, “2.1.5”, “2.2.3” E “2.2.5” do Termo de Referência.

“a) Do não atendimento aos itens 2.1.3, 2.1.5, 2.2.3 e 2.2.5.

Ao que dispõe a exigência constante no Termo de Referência, os itens 2.1.3, 2.1.5, 2.2.3 e 2.2.5 demandam que as licitantes ofertem equipamentos novos, não possuam restrição de comercialização, anúncio de fim de suporte e não possuam tempo superior à 24 (vinte e quatro) meses de lançamento.

(...)

Em suas alegações, a licitante afirma que a análise da D. Comissão é equivocada, uma vez que apresenta documentos de outros equipamentos, os quais seriam o objeto da entrega. Apenas de que para o cumprimento da exigência, apresentou o documento que corroborou em sua desclassificação.

A licitante, mesmo após a diligência, não apresentou em nenhum momento a data de lançamento nem documentação oficial que comprove o atendimento aos requisitos. No recurso, novamente limitou-se apenas a informar que existem diferentes linhas de produtos e a versão de firmware utilizada.

A licitante apresentou apenas uma carta como “comprovação”, mesmo sendo ratificado no item 2.6 do edital que tal tipo de documento não é válido para comprovação, sendo aceitas apenas cópias de manuais, datasheets ou páginas oficiais do fabricante publicadas na Internet.

Item 2.6.:

“a) Tabela de itens visando facilitar a conferência das funcionalidades exigidas neste Termo. Nela deverá haver referência a manuais, “data-sheet” ou páginas do fabricante publicadas na Internet que comprove a funcionalidade exigida em cada item das especificações técnicas. Esta tabela de comprovação e seus anexos (cópia de manuais, “data-sheet” ou páginas do fabricante publicadas na Internet) deverão ser encaminhados, no prazo estabelecido no edital para envio da proposta, à Comissão Permanente de Licitação – CPL, utilizando-se de arquivo, preferencialmente, em formato PDF (protegido para somente leitura) via correio eletrônico, para o endereço cpl@planalto.gov.br”

Desta forma, resta clara que a apresentação de documentos diversos foi deliberada, para que se aproveitasse de uma possível confusão da D. Comissão, o que não ocorreu. Ou haveria outra razão para que a documentação apresentada à Presidência não pode ser considerada, qual devemos considerar? A falta de fornecimento desta data específica impede a validação do cumprimento deste critério. Tal omissão coloca em dúvida a atualização e a modernidade da solução proposta pela Compwire.

Em comparação, a Servix deixou claro essa exigência, garantindo que a tecnologia ofertada está atualizada e acompanha os avanços mais recentes do mercado, o que é crucial para a eficácia e eficiência da infraestrutura tecnológica da Presidência da República.

Não havendo qualquer irregularidade ao ato, deve ser mantida a desclassificação da licitante.”

7. PARECER TÉCNICO

7.1 O End of Marketing (EOM) apresentado em: <https://support.huawei.com/enterprise/en/bulletins-product/ENEWS2000013060> não é apenas da versão descontinuada dos produtos Huawei OceanStor V5, pois também cita a versão posterior da solução, mencionada no documento como produto de substituição à V5, e identificada pela ausência do sufixo V5. Além disso, a indisponibilidade de um produto de família mais recente no mercado nacional não configura atendimento aos itens do termo de referência. Tendo a fabricante abrangência internacional, a disponibilidade e o suporte do equipamento devem ser avaliadas na devida escala global de atuação, em concordância com o item 2.1.4 do Termo de Referência:

2.1.4. O equipamento deverá ser ofertado em todos os mercados globais que o fabricante possui representatividade, ou seja, não serão aceitos equipamentos ou versões de equipamentos criados especificamente para atendimento a um mercado, edital ou cliente. Isso é válido também para os softwares do equipamento, incluindo o firmware.

7.2 Por fim, não se verifica distinção e independência entre as soluções OceanStor Capacity Flash e OceanStor Dorado para a finalidade dos itens 2.1.3 e 2.1.5, a começar pelo segmento da solução (OceanStor, distinta de outras soluções de armazenamento como OceanCyber, OceanDisk, e FusionCube, por exemplo), seguida de seu versionamento (ambas coincidiram como geração V5 e versão 6.x, sendo a nova geração V7 uma sequência direta desse versionamento), além da nomenclatura de seus produtos (códigos entre 5000 e 6000), e o fato de ambas serem ofertadas como linhas All-Flash, requisito necessário para a consideração do produto como item 1 desse certame, independente de distinções relativas a performance ou capacidade.

8. RAZÕES COMPWIRE:

8.1 A seguir as razões apresentadas pela Recorrente em relação aos itens “2.1.80” e “2.2.81” do Termo de Referência.

“II.II. ATENDIMENTO AOS ITENS “2.1.80” E “2.2.81” – NÃO CONFORMIDADE DA SOLUÇÃO OFERTADA E COMPATIBILIDADE COM FIPS 140-2:

“26. Nos termos da análise técnica, a proposta da COMPWIRE supostamente deixou de atender os Itens “2.1.80” E “2.2.81”, que assim dispõe:”

“2.1.80. O sistema deverá possuir software para criptografia dos dados com as funcionalidades:

2.1.80.1. Possuir tecnologia nativa para criptografia dos dados armazenados no sistema, utilizando algoritmo AES-256 ou superior.

2.1.80.2. A funcionalidade deverá ser totalmente nativa ao sistema, sem necessidade de hardware ou software externo, para a gerência da(s) chave(s) de criptografia, ou qualquer outra rotina proveniente da funcionalidade de cifragem dos dados, caso haja necessidade a proponente deve considerar o servidor e a licença necessária para tal funcionalidade.

2.1.80.3. A funcionalidade deverá estar licenciada para a capacidade máxima total suportada pelo sistema definido neste termo.

2.1.80.4. Permitir a coexistência de dados cifrados e não cifrados no mesmo sistema.

2.1.80.5. Permitir a ativação e o desligamento da funcionalidade, em nível de LUN ou volume a qualquer tempo ou “Storage Pool”.

2.1.80.6. Suportar a funcionalidade de criptografia seja implementada para as áreas NAS (CIFS e NFS) e SAN (FC e ISCSI).

2.1.80.7. Possuir conformidade com FIPS 140-2. Federal Information Processing Standard (FIPS) Publication 140 é um padrão que define requisitos mínimos de segurança para módulos criptográficos em produtos e sistemas.

2.1.80.8. A comprovação da conformidade com a FIPS 140-2, serão validadas em: <https://csrc.nist.gov/>”

27. Como comprovado na diligência pelo documento “*OceanStor Capacity Flash Storage 6.1.8 Security Technical White Paper.pdf*”, página 34:

“3 Security Certification All Huawei OceanStor storage systems have obtained the PCI-DSS and CC EAL 3+ security certification. Self-encrypting SSDs have obtained the FIPS certification.”

[Em tradução livre]:

“3 Certificação de segurança

Todos os sistemas de armazenamento OceanStor da Huawei obtiveram a certificação de segurança PCI-DSS e CC EAL 3+. SSDs de criptografia automática obtiveram a certificação FIPS.”

28. Adicionalmente, no documento “OceanStor 6.1.x & V700R001 Disk Encryption User Guide.pdf”, páginas 1 e 5:

• *Complying with the Federal Information Processing Standard (FIPS) 140-*

2, *OceanStor self-encrypting NVMe SSDs effectively improve data processing efficiency and enhance data security protection capabilities.*

1.2.2 Encryption Using the Data Encryption Function “Data is encrypted and decrypted by the built-in encryption module during data reads and writes. The encryption module supports AES-256. The algorithm used by the key manager must match that of the encryption module.”

[Em tradução livre]:

• Em conformidade com o Federal Information Processing Standard (FIPS) 140-2, os SSDs NVMe de criptografia automática OceanStor melhoraram efetivamente a eficiência do processamento de dados e aprimoram as capacidades de proteção de segurança dos dados.

1.2.2 Criptografia Usando a função de criptografia de dados “Os dados são criptografados e descriptografados pelo módulo de criptografia integrado durante as leituras e gravações de dados. O módulo de criptografia suporta AES-256. O algoritmo usado pelo gerenciador de chaves deve corresponder ao do módulo de criptografia.”

29. Referidos trechos comprovam que os discos SED (Self-Encrypting Drives) utilizados pela solução **são compatíveis com FIPS 140-2** e que a criptografia é **realizada nativamente no hardware, por módulo dedicado e com suporte a AES-256**, conforme exigido.

30. É possível perceber que a HUAWEI busca manter conformidade com os principais padrões internacionais de segurança, adotando módulos de criptografia baseados em AES256 e implementando controles alinhados às diretrizes do FIPS 140-2.

31. A documentação oficial da fabricante confirma que os SSDs auto criptografados utilizados na solução seguem esse padrão e realizam a proteção dos dados diretamente no hardware, garantindo maior segurança e desempenho.

32. Dessa forma, ao contrário da análise técnica, a solução proposta atende às diretrizes técnicas de criptografia solicitadas no Edital e Termo de Referência no Item “2.1.80” e seguintes, conforme comprovado nos documentos apresentados em resposta à diligência.”

9. CONTRARRAZÕES SERVIX

9.1 A seguir as contrarrazões apresentadas pela Recorrida em relação aos ITENS “2.1.80” e “2.2.81” do Termo de Referência.

“b) Do não atendimento aos itens 2.1.80 e 2.2.81.

COMPATIBILIDADE COM FIPS 140-2:

Na resposta ao diligenciado, a licitante admite que os padrões de segurança adotados estão desatualizados e novamente reafirma que o FIPS está vinculado com discos auto criptografados.

“É possível perceber que a Huawei busca manter conformidade com os principais padrões internacionais de segurança, adotando módulos de criptografia baseados em AES-256 e implementando controles alinhados às diretrizes do FIPS 140-2.

A documentação oficial da fabricante confirma que os SSDs auto criptografados utilizados na solução seguem esse padrão e realizam a proteção dos dados diretamente no hardware, garantindo maior segurança e desempenho. Dessa forma, a solução atende às diretrizes técnicas de criptografia solicitadas no edital, conforme demonstrado nos documentos apresentados.

As sanções americanas contra as empresas chinesas dificultam a atualização dos certificados da Huawei no site da NIST (National Institute of Standards and Technology), mas de acordo com a documentação apresentada, está claro que a solução atende plenamente às diretrizes solicitadas.”

E também em sua peça recursal.

“29. Referidos trechos comprovam que os discos SED (Self-Encrypting Drives) utilizados pela solução são compatíveis com FIPS 140-2 e que a criptografia é realizada nativamente no hardware, por módulo dedicado e com suporte a AES-256, conforme exigido.”

Ou seja, mesmo que a solução ofertada possua discos auto criptografados (com a criptografia nativa ao hardware), em momento algum, a LICITANTE afirmou que o disco ofertado seria da linha SED, ou seja, talvez em discos auto criptografados eles possuam FIPS (apesar de não possuir documentação atual) mas eles não ofereceram esse tipo de disco em sua proposta.

Vale ressaltar que a importância dessa certificação é garantir que os módulos de criptografia atendem aos rigorosos padrões de segurança. Aceitar discos SED (Self-Encrypting Drives) sem a devida certificação FIPS prejudica a isonomia do processo, pois outros concorrentes, incluindo a Servix, incluíram em suas propostas tecnologias certificadas e, portanto, incorreram em custos adicionais para atender a tais requisitos. Isso reflete um compromisso com a integridade e a segurança que são essenciais para a infraestrutura de TIC da Presidência da República.

Além disso, nem em documentação, nem em diligência e nem em recurso, foi comprovado o item “2.1.80.5. Permitir a ativação e o desligamento da funcionalidade, em nível de LUN ou volume a qualquer tempo ou “Storage Pool””, que a Compwire convenientemente não mencionou.”

10. PARECER TÉCNICO:

10.1 Como analisado e respondido em diligência, a Recorrente não comprovou a conformidade em fonte oficial da entidade certificadora (NIST), como exige o Termo de referência.

10.2 Durante a fase da diligência, a LICITANTE reconhece que não atende esta exigência do Termo de Referência referente aos itens 2.1.80.8 e 2.2.81.8, e conforme contrarrazões da Recorrida, “em momento algum, a LICITANTE afirmou que o disco ofertado seria da linha SED, ou seja, talvez em discos auto criptografados eles possuam FIPS (apesar de não possuir documentação atual) mas eles não ofereceram esse tipo de disco em sua proposta.”

10.3 Conforme a Recorrida ressaltou: “(...) nem em documentação, nem em diligência e nem em recurso, foi comprovado o item “2.1.80.5. Permitir a ativação e o desligamento da funcionalidade, em nível de LUN ou volume a qualquer tempo ou “Storage Pool”.”

11. RAZÕES COMPWIRE:

11.1 A seguir as razões apresentadas pela Recorrente em relação aos itens “2.1.81” e “2.2.82” do Termo de Referência.

“II.III. ATENDIMENTO AO ITENS “2.1.81 E 2.2.82 – CONFORMIDADE E ATENDIMENTO DA SOLUÇÃO PROPOSTA COM AUTENTICADOR OAUTH 2.0:

33. Nos termos da análise técnica, a proposta da COMPWIRE supostamente deixou de atender os Itens “2.1.80” E “2.2.81”, que assim dispõe:

“2.1.81. Possuir integração com o framework Open Authorization (OAuth 2.0).

2.1.82. Possuir a funcionalidade WORM (Write Once Read Many), garantindo a imutabilidade dos dados armazenados através dos protocolos CIFS/SMB e NFS, de forma que não sejam apagados ou modificados durante um período de tempo especificado pelo administrador da solução, com retenção em nível de arquivo.

2.1.82.1. Possuir a certificação SEC Rule 17a-4 e um relógio interno à prova de adulteração, a fim de que um administrador mal-intencionado não consiga adiantar o relógio do sistema e, artificialmente, fazer com que o período de retenção expire mais cedo.

2.2.82. Possuir integração com o framework Open Authorization (OAuth 2.0).”

34. A partir da documentação comprovada, “OceanStor Capacity Flash Storage 6.1.8 Security Technical White Paper.pdf”, página 28 e 29, verifica-se que o storage Huawei utiliza das seguintes formas de autenticação:

(i) Autenticação local via SSH por usuário e senha ou chave pública;

(ii) Autenticação multifator para acesso Web (senha + OTP);

(iii) Autenticação de domínio via LDAP/LDAPS integrado ao Active Directory;

(iv) Autorização via RADIUS com OTP para usuários de domínio e CAS-SSO (Single sign-on).

35. Principalmente com a autenticação via RADIUS (iv), é possível estabelecer que o OceanStor Capacity Flash da Huawei contemple o uso dos principais autenticadores do mercado, como Microsoft Authenticator, RSA SecurID, FreeOTP e outros.

36. Usando de exemplo o Microsoft Authenticator, este funciona justamente como um provedor de OTP vinculado às contas de domínio do Active Directory/Azure AD. Quando o storage realiza a autenticação via RADIUS, o servidor RADIUS pode estar integrado ao AD e habilitado para exigir o segundo fator de autenticação, sendo o Microsoft Authenticator um método completamente compatível e amplamente utilizado para emissão de OTP nesse cenário.

37. Os mecanismos adotados na solução são compatíveis com os modelos de autenticação e controle de acesso amplamente utilizados no setor de armazenamento corporativo, baseados em integração com Active Directory, uso de RADIUS com OTP, autenticação multifator (MFA) e Single Sign-On (SSO). Esses métodos representam o padrão predominante nas grandes fabricantes de storage, por permitirem autenticação centralizada, verificação de identidade segura e integração com aplicações já presentes nas infraestruturas corporativas.

38. Dessa forma, o OceanStor Capacity Flash oferece suporte completo aos principais métodos consolidados de autenticação do mercado — LDAP/LDAPS, RADIUS/OTP, MFA e SSO — garantindo aderência às práticas atuais de segurança e habilitando o uso dos mais difundidos autenticadores corporativos, tais como Microsoft Authenticator, RSA SecurID, FreeOTP, entre outros, atendendo integralmente ao disposto nos Itens “2.1.80” E “2.2.81”.

”

12. CONTRARRAZÕES SERVIX

12.1 A seguir as contrarrazões apresentadas pela Recorrida em relação aos itens “2.1.81” e “2.2.82” do Termo de Referência.

“Em diligência, a licitante não apresentou documentação que comprove o atendimento ao item, afirmou de forma equivocada que apenas a NetApp atende ao requisito e, ainda, admitiu que não o atende, conforme declarado:

“A maioria dos fabricantes de storage do mercado (Huawei, Dell, IBM, HPE, Lenovo, entre outros) utiliza autenticação robusta baseada em LDAP, LDAPS, RADIUS/OTP e SSO, sem o uso de OAuth 2.0. Assim, a solução ofertada atende todos os demais mecanismos modernos de autenticação e segurança exigidos no mercado como MFA, SSO, LDAP/LDAPS e RADIUS. OAuth ainda é um framework novo na integração dentro dos storages primários, que traz suas vantagens na automação. Apesar da NetApp ter sido inovadora na implementação desse framework aos seus storages, é a única que utiliza a tecnologia para validação de tokens e autorização de servidores.”

No recurso, a licitante altera seu discurso, passando a afirmar que oferece suporte completo aos principais métodos consolidados de autenticação, embora continue sem atender ao item explicitamente solicitado pela Presidência.

Caso o requisito em questão representasse qualquer impossibilidade técnica, a licitante deveria ter questionado no momento dedicado a isso. Entretanto, não o fez, deixando evidente a intenção de induzir a Presidência ao erro.

Por fim, a Servix cumpriu rigorosamente esse critério, demonstrando que sua solução está pronta para integração com as arquiteturas de autenticação e autorização estabelecidas pelo órgão, garantindo maior coesão e produtividade na gestão dos sistemas.”

“c) Da correta desclassificação.

Conforme exposto, apesar da licitante ter mudado o discurso diversas vezes, ficou claro, conforme já constatado pela Presidência, que a licitante não atende plenamente aos itens solicitados, e ainda, itens referentes à segurança dos dados.

A segurança de dados é um pilar essencial para qualquer instituição que busca proteger suas operações, e principalmente, sua imagem. Em um cenário de ameaças digitais cada vez mais sofisticadas, garantir a integridade e a confidencialidade das informações não é apenas uma obrigação técnica, mas uma necessidade estratégica. A adoção de mecanismos conhecidos, renomados e reconhecidos internacionalmente de autenticação e criptografia reduz riscos, previne incidentes e assegura que decisões e serviços sejam prestados com responsabilidade e credibilidade.

Investir em segurança da informação, portanto, é investir na continuidade, na transparência e na resiliência da Presidência. Assim, a diferença de apenas 2% entre a oferta da Compwire representa o investimento necessário para adequar o ambiente a políticas amplamente reconhecidas e comprovadamente eficazes no mercado.

13. PARECER TÉCNICO:

13.1 A Recorrente cita principalmente a compatibilidade do produto com autenticadores OTP (Microsoft Authenticator, RSA SecurID e FreeOTP), que são formas de autenticação multifator (MFA), ou seja, uma solução distinta e independente do framework OAuth 2.0 exigido pelo Termo de Referência.

13.2 A área técnica mantém seu parecer apresentado na análise da diligência que a Recorrente não cumpriu esta exigência do Termo de Referência.

14. RAZÕES COMPLEMENTARES COMPWIRE

“II.IV. PLENO ATENDIMENTO DA SOLUÇÃO PROPOSTA PELA RECORRENTE EM FACE DAS ESPECIFICAÇÕES EXIGIDAS PELO EDITAL E TERMO DE REFERÊNCIA – DESCLASSIFICAÇÃO IRREGULAR QUE DEIXA DE VISLUMBRAR A PROPOSTA MAIS VANTAJOSA PARA A ADMINISTRAÇÃO PÚBLICA:

39. Como demonstrado, em que pese a análise exarada pela equipe técnica em sede de diligências, a solução proposta pela COMPWIRE atende integralmente a todas as exigências e especificações do Edital e Termo de Referência.

40. Assim, cumpre ressaltar que a r. decisão desclassificou a Recorrente não apenas deixou de vislumbrar o pleno atendimento das exigências pela solução, mas também a obtenção de proposta mais vantajosa.

41. Frisa-se que a obtenção de maior vantajosidade se trata de um princípio no curso do processo de contratação, por meio da economicidade:

“Art. 5º Na aplicação desta Lei, serão observados os princípios da legalidade, da impessoalidade, da moralidade, da publicidade, da eficiência, do interesse público, da probidade administrativa, da igualdade, do planejamento, da transparência, da eficácia, da segregação de funções, da motivação, da vinculação ao edital, do julgamento objetivo, da segurança jurídica, da razoabilidade, da competitividade, da proporcionalidade, da celeridade, da economicidade e do desenvolvimento nacional sustentável, assim como as disposições do Decreto-Lei nº 4.657, de 4 de setembro de 1942 (Lei de Introdução às Normas do Direito Brasileiro).

42. O vantajosidade é ainda um dos objetivos buscados no processo licitatório, nos termos do art. 11, inc. I, da Lei nº 14.133/21:

“Art. 11. O processo licitatório tem por objetivos:

I - assegurar a seleção da proposta apta a gerar o resultado de contratação mais vantajoso para a Administração Pública, inclusive no que se refere ao ciclo de vida do objeto;

43. A necessidade da obtenção da maior vantajosidade possível no valor a ser dispendido pela Administração Pública em uma contratação é de extrema relevância, conforme pontua MARÇAL JUSTEN FILHO:

“Existe um dever de a Administração adotar a escolha mais vantajosa para a exploração dos recursos econômicos de sua titularidade. Como regra, a licitação visa a obter a solução contratual economicamente mais vantajosa para a Administração. [...]”

Quando a Administração desembolsa um montante de recursos para uma contratação determinada, o referido montante não poderá ser utilizado para promover outras atividades. Por isso, existe o dever de a Administração desembolsar o menor valor possível para obter uma prestação inclusive porque isso lhe assegurará a possibilidade de satisfazer outras necessidades com os recursos remanescentes. O Estado dispõe de recursos limitados para custeio de suas atividades e realização de investimento. Portanto, a vantagem para o Estado se configura com a solução que assegure os maiores benefícios para a aplicação de seus recursos econômico-financeiros. O Estado tem o dever de realizar a melhor contratação sob o ponto de vista da economicidade. Isso significa que a contratação comporta avaliação como modalidade de relação custo-benefício.

A economicidade é o resultado da comparação entre encargos assumidos pelo Estado e direitos a ele atribuídos, em virtude da contratação administrativa. Quanto mais desproporcional em favor do Estado o resultado dessa relação, tanto melhor atendido estará o princípio da economicidade. A economicidade exige que o Estado desembolse o mínimo e obtenha o máximo e o melhor. Em princípio, a economicidade se retrata no menor preço pago pelo Estado ou no maior lance por ele recebido, conforme a natureza da contratação.”

44. É incontestável, assim, a necessidade da reforma da r. decisão que desclassificou

COMPWIRE do processo de contratação regido pelo Edital Pregão Eletrônico nº 90037/2025-AS, ante o integral atendimento de sua proposta às exigências e especificações do Edital e Termo de Referência. Para além de visar a regularidade da condução do certame, a revisão da desclassificação também trará para a Administração Pública maior vantajosidade econômica.

45. Neste ponto, e conforme será exposto adiante, a reclassificação da COMPWIRE ganha contornos mais relevantes quando verificado que o Pregão Eletrônico nº 90037/2025-AS habilitou e declarou como vencedora licitante que, de fato, deixou de atender às exigências Editalícias, e que possui, inclusive, proposta economicamente menos vantajosa para a Contratante.”

15. PARECER TÉCNICO

15.1 De acordo com a LEI Nº 14.133, DE 1º DE ABRIL DE 2021, Lei de Licitações e Contratos Administrativos, Art. 34. “o julgamento por menor preço ou maior desconto e, quando couber, por técnica e preço considerará o menor dispêndio para a Administração, atendidos os parâmetros mínimos de qualidade definidos no edital de licitação.”

16. RAZÕES COMPWIRE QUANTO A CONFORMIDADE DA SERVIX:

“III. DO NÃO ATENDIMENTO DOS REQUISITOS TÉCNICOS EXIGIDOS NO EDITAL E SEUS ANEXOS PELA RECORRIDA SERVIX INFORMÁTICA LTDA.:

46. A Recorrida apresenta comprovações falhas e inconclusivas que carecem de fundamentação técnica sólida, caracterizando esforço para dissimular a não conformidade com as exigências editalícias.

47. As alegações ora apresentadas pela Recorrente demonstram, de forma técnica e fundamentada, que a solução ofertada pela Recorrida não atende plenamente às especificações previstas no Edital. Nos subtópicos

seguintes serão expostos, de maneira objetiva e detalhada, os pontos de descumprimento identificados, comprovando-se tecnicamente a inaptidão da proposta apresentada pela SERVIX INFORMÁTICA LTDA, que merece ser desclassificada do Pregão Eletrônico nº 90037/2025-AS."

16.1 A seguir as razões apresentadas pela Recorrente em relação aos itens "2.1.1" e "2.2.1" do Termo de Referência.

"III.II. NÃO ATENDIMENTO DA SOLUÇÃO DA RECORRIDA AOS ITENS "2.1.1" E "2.2.1":

48. O Edital estabelece no Item 2.1.1 (ao que tange o Storage Tipo 1 – AFFC80) e 2.2.1 (ao que tange o Storage Tipo 2 – FAS50):

"2.1.1. O equipamento de armazenamento de dados deve ser constituído de, no mínimo, 02 (duas) controladoras de discos, operando na modalidade de cluster sem ponto único de falha, de modo a implementar total e plena disponibilidade, com realização de "failover" automático."

49. Conforme o documento de ponto a ponto "PAP - Presidência da Republica NetApp.xlsx", a recorrida utiliza a documentação "Learn_about_ONTAP" para comprovação do item, no entanto não se identifica o texto mencionado, e o mesmo não comprova que o equipamento opera sem ponto único de falha. A licitante deve comprovar com o documento correto.

50. Na página 1 do documento "HA_pair_management.pdf", o termo "Takeover" é descrito como um PROCESSO — e não como um evento instantâneo:

"Takeover is the process in which a node assumes control of its partner's storage."

[Em tradução livre]:

"Takeover é o processo no qual um nó assume o controle do armazenamento do seu parceiro."

51. A palavra-chave aqui é processo. Se fosse instantâneo, a documentação usaria um dos termos abaixo, mas não utiliza:

(i) instant failover

(ii) immediate failover

(iii) zero-time switchover

52. O "takeover" depende da detecção de falha, que por si só leva tempo. Exemplo do texto:

"When one node in an HA pair encounters an error and stops processing data, its partner detects the failed status of the partner and takes over all data processing from that controller."

[Em tradução livre]:

"Quando um nó em um par HA encontra um erro e para de processar dados, seu parceiro detecta o status de falha do outro e assume todo o processamento de dados desse controlador."

53. A sequência é: Falha ocorre > O nó parceiro detecta > O nó parceiro assume.

54. Ou seja, detectar a falha nunca é instantâneo e esse tempo é variável e sempre maior de 0, podendo levar segundos ou minutos.

55. A documentação deixa claro que o processo de takeover é um processo, não um evento instantâneo, que depende da detecção de heartbeats, análise de estado, decisões de failover, boot, retomada de aggregates e outros. Todos os itens, provam que tecnicamente o takeover não é imediato, contínuo ou sem impacto, diferente de arquiteturas de ponta como controladoras ativo-ativo simétrico.

56. Sendo assim, o failover não é instantâneo e automático, depende de um processo prolongado para validação da perda da controladora principal."

17. CONTRARRAZÕES SERVIX

17.1 A seguir as contrarrazões apresentadas pela Recorrida em relação aos itens "2.1.1" e "2.2.1" do Termo de Referência.

a) Da alegação de não atendimento aos itens 2.1.1 e 2.2.1.

Sobre o item 2.1.1:

"2.1.1. O equipamento de armazenamento de dados deve ser constituído de, no mínimo, 02 (duas) controladoras de discos, operando na modalidade de cluster sem ponto único de falha, de modo a implementar total e plena disponibilidade, com realização de "failover" automático."

"A Compwire afirma que não atendemos os requisitos, pois o failover não é instantâneo nem automático, entretanto, no mesmo documento apresentado, caso a licitante tivesse continuado a leitura teria lido a seguinte afirmação: "

(...)

"Cluster nodes are configured in high-availability (HA) pairs for fault tolerance and nondisruptive operations."

Tradução livre:

"Os nós do cluster são configurados em pares de alta disponibilidade (HA) para tolerância a falhas e operações sem interrupção."

"By default, takeovers occur automatically in any of the following situations:

- A software or system failure occurs on a node that leads to a panic. The HA pair controllers automatically fail over to their partner node. After the partner has recovered from the panic and booted up, the node automatically performs a giveback, returning the partner to normal operation.

- A system failure occurs on a node, and the node cannot reboot. For example, when a node fails because of a power loss, HA pair controllers automatically fail over to their partner node and serve data from the surviving storage controller."

"Tradução livre:

"Por padrão, os takeovers ocorrem automaticamente em qualquer uma das seguintes situações:

- Ocorre uma falha de software ou de sistema em um nó que resulta em panic. Os controladores do par HA executam automaticamente o failover para o nó parceiro. Após o parceiro se recuperar do panic e reinicializar, o nó executa automaticamente o giveback, retornando o parceiro à operação normal.

- Ocorre uma falha de sistema em um nó, e o nó não consegue reinicializar. Por exemplo, quando um nó falha devido à perda de energia, os controladores do par HA executam automaticamente o failover para o nó parceiro e passam a fornecer os dados a partir do controlador de armazenamento sobrevivente."

Como a própria licitante afirma, as palavras-chave são fundamentais. Logo a palavra a ser procurada deve ser "automática" conforme o item mencionado. Como comprovado em documentação na própria página citada, é possível comprovar o atendimento ao requisito estabelecido, evidenciando mais uma tentativa da licitante de induzir a Presidência ao erro.

Além disso, apesar de estar claro na documentação apresentada que a arquitetura da Netapp não possui pontos de falha, destaca-se a seguinte documentação: <https://docs.netapp.com/us-en/ontap-apps-dbs/epic/epic-ontap-availability.html>

(...)

Onde pode ser validado, nas mesmas palavras utilizadas, o atendimento integral do item solicitado. Por fim, a tecnologia NetApp ONTAP é validada por auditores externos renomados, como o IDC, que comprovaram a disponibilidade de 99,9999% (seis noves) da solução, com base em dados empíricos. Fonte: <https://www.netapp.com/media/97794us51241123.pdf>

18. PARECER TÉCNICO

18.1 Nos itens 2.1.1 e 2.2.1, transcritos abaixo, não constam o termo instantâneo, mas sim automático. Portanto, a alegação da Recorrente não se sustenta.

"O equipamento de armazenamento de dados deve ser constituído de, no mínimo, 02 (duas) controladoras de discos, operando na modalidade de cluster sem ponto único de falha, de modo a implementar total e plena disponibilidade, com realização de "failover" automático."

18.2 Conforme as contrarrazões da Recorrida, a documentação apresentada deixa claro que a arquitetura da Netapp não possui ponto único de falha.

19. RAZÕES COMPWIRE

19.1 A seguir as razões apresentadas pela Recorrente em relação aos itens "2.1.10" e "2.2.10" do Termo de Referência.

"III.II. NÃO ATENDIMENTO DA SOLUÇÃO DA RECORRIDA "2.1.10" E "2.2.10":

57. O Edital estabelece no Item 2.1.10 (ao que tange o Storage Tipo 1 – AFFC80) e 2.2.10 (ao que tange o Storage Tipo 2 – FAS50):

"2.1.10. Suportar failover automático de controladora e mecanismo de proteção de cache em caso de falha de energia ou falha de qualquer outro componente do storage."

58. A Recorrente utiliza a seguinte comprovação no documento de ponto a ponto "PAP - Presidência da Republica NetApp.xlsx":

59. Na página 1 do documento "HA_pair_management.pdf", o termo "Takeover" é descrito como um PROCESSO — e não como um evento instantâneo:

"Takeover is the process in which a node assumes control of its partner's storage."

[Em tradução livre]:

"Takeover é o processo no qual um nó assume o controle do armazenamento do seu parceiro."

60. A palavra-chave aqui é processo. Se fosse instantâneo, a documentação usaria um dos termos abaixo, mas não utiliza:

(i) instant failover

(ii) immediate failover

(iii) zero-time switchover

61. O "takeover" depende da detecção de falha, que por si só leva tempo. Exemplo do texto:

"When one node in an HA pair encounters an error and stops processing data, its partner detects the failed status of the partner and takes over all data processing from that controller."

[Em tradução livre]:

"Quando um nó em um par HA encontra um erro e para de processar dados, seu parceiro detecta o status de falha do outro e assume todo o processamento de dados desse controlador."

62. A sequência é: Falha ocorre > O nó parceiro detecta > O nó parceiro assume.

63. Ou seja, detectar a falha nunca é instantâneo e esse tempo é variável e sempre maior de 0, podendo levar segundos ou minutos.

64. A documentação deixa claro que o processo de takeover é um processo, não um evento instantâneo, que depende da detecção de heartbeats, análise de estado, decisões de failover, boot, retomada de aggregates e outros. Todos os itens, provam que tecnicamente o takeover não é imediato, contínuo ou sem impacto, diferente de arquiteturas de ponta como controladoras ativoativo simétrico.

65. Sendo assim, o failover não é instantâneo e automático, depende de um processo prolongado para validação da perda da controladora principal.

66. Ademais, a Recorrida comprova o mecanismo de proteção de dados em caso de falha de energia apenas para o módulo NVRAM/NVME, que conforme o documento de especificação do AFF C80 é de 128 GB total e do FAS50 é de 32 GB total.

Documento "[AFFC80] ControllerSpecifications.pdf", página 2

Documento "[FAS50] ControllerSpecifications.pdf", página 2

67. Porém, não há na documentação oficial comprovando que a memória cache (RAM) é automaticamente protegido contra falha de energia, para que ocorra o "destage", isto é: forçar a transferência dos dados da RAM, memória volátil, para os discos de armazenamento do Storage. A RAM dos equipamentos NetApp é a memória mais impactante visto a sua capacidade total de 512 GB para o AFF C80 e 128 GB para o FAS50.

68. O que fica claro é que em caso de falha, todos os dados nessa memória RAM serão perdidos, estando em desacordo com os requisitos de proteção de dados e sistema seguro para o armazenamento dos dados produtivos do Contratante."

20. CONTRARRAZÕES SERVIX

20.1 A seguir as contrarrazões apresentadas pela Recorrida em relação aos ITENS "2.1.10" e "2.2.10" do Termo de Referência.

"b) Da alegação de não atendimento aos itens 2.1.10 e 2.2.10.

Ao item de alegado descumprimento.

"2.1.10. Suportar failover automático de controladora e mecanismo de proteção de cache em caso de falha de energia ou falha de qualquer outro componente do storage."

Novamente a licitante insiste no não atendimento do failover automático, que está claro na mesma página em que ela afirma que não possui a comprovação.

Em relação ao "mecanismo de proteção de cache em caso de falha de energia ou falha de qualquer outro componente do storage", nossa comprovação é clara, é realizado o destage na NVRAM (cache) da controladora nos dados em trânsito após uma perda de energia.

Caso a licitante não tenha o conhecimento, podemos explicitar. Os conceitos de memória cache e memória RAM são diferentes, dessa forma não faz sentido nenhum usar como balizamento a memória RAM para atendimento deste item.

A memória RAM é volátil e utilizada para armazenar dados temporários que suportam o processamento imediato do sistema. Já a NVRAM é não volátil e utilizada justamente para preservar as informações mesmo sem energia, funcionando frequentemente como um cache seguro para dados ainda não gravados em disco.

Dessa forma, atendemos integralmente ao que foi solicitado no item em questão. Além disso, como mecanismo adicional de proteção, as operações de escrita na solução NetApp ONTAP são protegidas na NVRAM (memória não volátil) e copiadas para a NVRAM da outra controladora, garantindo a integridade dos dados mesmo em caso de falha. Este mecanismo assegura que as operações de escrita não sejam perdidas e que a continuidade dos dados seja mantida.

https://kb.netapp.com/on-prem/ontap/Ontap_OS/OSKb/NVRAM_purpose_during_ONTAP_outage

21. PARECER TÉCNICO

21.1 Conforme documentação citada nas contrarrrazões da Recorrida, endereço https://kb.netapp.com/on-prem/ontap/Ontap_OS/OS-Kb/NVRAM_purpose_during_ONTAP_outage, destaca-se o trecho abaixo.

"In the event of a power failure or other disruption during the write process, the filesystem consistency is still maintained because the active pointers are still pointing to the pre-change data.

The write that was interrupted is still available in local NVRAM upon next boot.

This data is checked for and when found, is replayed to the local memory buffer and immediately re-processed through the WAFL and RAID layers and written to disk during the next CP."

[Tradução Livre]

"Em caso de falha de energia ou outra interrupção durante o processo de gravação, a consistência do sistema de arquivos ainda é mantida, pois os ponteiros ativos ainda apontam para os dados anteriores à alteração.

A gravação que foi interrompida ainda estará disponível na NVRAM local na próxima inicialização.

Esses dados são verificados e, quando encontrados, são reproduzidos no buffer de memória local e imediatamente reprocessados pelas camadas WAFL e RAID, sendo gravados em disco durante o próximo CP."

21.2 Em razão do trecho transcrito acima, em destaque, o argumento da Recorrente não se sustenta, conforme pode ser comprovado também na seguinte esclarecimento da Recorrida:

"A memória RAM é volátil e utilizada para armazenar dados temporários que suportam o processamento imediato do sistema. Já a NVRAM é não volátil e utilizada justamente para preservar as informações mesmo sem energia, funcionando frequentemente como um cache seguro para dados ainda não gravados em disco.

Dessa forma, atendemos integralmente ao que foi solicitado no item em questão. Além disso, como mecanismo adicional de proteção, as operações de escrita na solução NetApp ONTAP são protegidas na NVRAM (memória não volátil) e copiadas para a NVRAM da outra controladora, garantindo a integridade dos dados mesmo em caso de falha. Este mecanismo assegura que as operações de escrita não sejam perdidas e que a continuidade dos dados seja mantida."

21.3 Portanto, a Recorrida comprovou que cumpriu as exigências referentes aos itens "2.1.10" e "2.2.10" do Termo de Referência.

21.4 RAZÕES COMPWIRE

21.5 A seguir as razões apresentadas pela Recorrente em relação aos itens "2.1.68" e "2.2.69" do Termo de Referência.

"III.III. NÃO ATENDIMENTO DA SOLUÇÃO DA RECORRIDA AO ITEM "2.1.68" E "2.2.69"

69. O Edital estabelece no Item 2.1.68 (ao que tange o Storage Tipo 1 – AFFC80) e 2.2.69 (ao que tange o Storage Tipo 2 – FAS50):

"2.1.68. Suportar a replicação assíncrona e/ou síncrona de sistemas de arquivos (NAS) e LUNs (SAN), para sistemas de armazenamento do mesmo fabricante, onde a replicação assíncrona poderá ocorrer localmente (para as mesmas controladoras que compõe o cluster), e remotamente (para outras controladoras em outro cluster de armazenamento)."

70. A Recorrida utiliza a seguinte comprovação no documento de ponto a ponto "PAP - Presidência da Republica NetApp.xlsx":

71. A tecnologia SnapMirror é utilizada para replicação de volumes entre storages ou entre HA pairs distintos remotamente conforme documentado pelo próprio fabricante.

72. No ONTAP, não existe replicação ou movimentação interna de dados entre controladoras que compõem um mesmo HA pair. Isso ocorre porque o failover entre controladoras não é baseado em espelhamento de blocos ou cópia de volumes, mas sim em espelhamento de NVRAM (log de escrita), garantindo apenas continuidade em caso de falha — e não compartilhamento ativo-ativo de dados. Ou seja, não há replicação de volume entre Node A e Node B dentro do mesmo par HA.

Documento <https://docs.netapp.com/us-en/ontap/concepts/high-availability-pairs-concept.html>

73. O ponto essencial que comprova isso é a arquitetura de aggregates, onde: No ONTAP, cada aggregate é pertencente a um único node (controladora), contendo conjuntos de discos e volumes exclusivos e independentes. Conforme documentação pública https://kb.netapp.com/on-prem/ontap/Ontap_OS/OS-Kb/What_is_an_aggregate.

"What is an aggregate?

An aggregate is a collection of disks (or partitions) arranged into one or more RAID groups. It is the most basic storage object within ONTAP and is required to allow for the provisioning of space for connected hosts.

How is an aggregate created?

(...)

Note that in order to create an aggregate on a given node, all of the required disks must be owned by the respective node."

[Em tradução livre]:

"O que é um agregado?

Um agregado é uma coleção de discos (ou partições) organizados em um ou mais grupos RAID. É o objeto de armazenamento mais básico dentro do ONTAP e é necessário para permitir o provisionamento de espaço para hosts conectados.

Como é criado um agregado?

(...)

Note que, a fim de criar um agregado em um determinado nó, todos os discos necessários devem ser propriedade do respectivo nó."

74. E pela documentação de "command reference" no link público <https://docs.netapp.com/us-en/ontap-cli/storage-aggregate-create.html>.

"[-node {<nodename> | local}] - Node

This parameter specifies the home node for the aggregate. If this parameter is not specified, ONTAP selects the node where the aggregate is created."

[Em tradução livre]:

"[-node {<nodename> | local}] - Nó

Este parâmetro especifica o nó home para o agregado. Se este parâmetro não for especificado, o ONTAP seleciona o nó onde o agregado é criado."

75. O node parceiro tem acesso físico aos discos apenas para possibilitar takeover em caso de falha, porém em operação normal os dados só são acessados e servidos pelo node proprietário daquele aggregate. Assim, os volumes de um node não são acessados ou utilizados pelo outro, mesmo estando dentro do mesmo storage e do mesmo cluster.

76. Portanto, cada node (controladora) opera seu próprio aggregate (conjunto de volumes), sem compartilhamento ativo de I/O ou movimentação de dados entre elas.

77. Com isso, fica evidente que o sistema NetApp não realiza replicação de dados entre as controladoras que compõem um mesmo HA pair. Não há mecanismo de movimentação ou duplicação automática de volumes entre os dois nodes. A única forma de replicação de volumes é através do SnapMirror — tecnologia desenhada para replicação entre HA pairs distintos ou entre clusters diferentes.

78. Diante disso, entendemos que o item 2.1.68 e 2.2.69 exige capacidade de replicação local entre quaisquer controladoras do cluster, e não apenas entre pares distintos via SnapMirror. Sendo assim, a NetApp não atende ao requisito, uma vez que seu modelo é baseado em propriedade exclusiva de aggregate/volumes por node e não prevê replicação ou espelhamento de volumes entre controladoras do mesmo HA pair. Desta forma, a solução se mostra inapta ao atendimento integral do certame."

22. CONTRARRAZÕES SERVIX

22.1 A seguir as contrarrrazões apresentadas pela Recorrida em relação aos ITENS "2.1.68" e "2.2.69" do Termo de Referência.

"c) Da alegação de não atendimento aos itens 2.1.68 e 2.2.69.

Sobre os itens:

"2.1.68. Suportar a replicação assíncrona e/ou síncrona de sistemas de arquivos (NAS) e LUNs (SAN), para sistemas de armazenamento do mesmo fabricante, onde a replicação assíncrona poderá ocorrer localmente (para as mesmas controladoras que compõe o cluster), e remotamente (para outras controladoras em outro cluster de armazenamento)."

A licitante afirma no recurso:

"71. A tecnologia SnapMirror é utilizada para replicação de volumes entre storages ou entre HA pairs distintos remotamente conforme documentado pelo próprio fabricante.

72. No ONTAP, não existe replicação ou movimentação interna de dados entre controladoras que compõem um mesmo HA pair. Isso ocorre porque o failover entre controladoras não é baseado em espelhamento de blocos ou cópia de volumes, mas sim em espelhamento de NVRAM (log de escrita), garantindo apenas continuidade em caso de falha — e não compartilhamento ativo-ativo de dados. Ou seja, não há replicação de volume entre Node A e Node B dentro do mesmo par HA."

Entretanto na comprovação é claro que o Snapmirror é realizado a nível de volume e suportada em qualquer plataforma FAS e AFF, logo, a replicação entre controladoras é suportada, não sendo limitada pelas camadas subjacentes de armazenamento.

Novamente, a licitante confunde conceitos que não fazem sentido algum. O fato de cada node operar seu agregado não significa que não possa existir relação de replicação entre elas.

Para confirmação do que foi explicitado segue documentação oficial: <https://www.netapp.com/media/17174-tr4733.pdf>, Página 15:

"Starting with ONTAP 9.14.1, NetApp has qualified SM-S for replication between two volumes within the same cluster. These volumes may be in the same SVM or two different SVMs within the same cluster. These volumes can be hosted on different HA pairs or the same HA pair."

Tradução:

"A partir do ONTAP 9.14.1, a NetApp qualificou o SM-S para replicação entre dois volumes dentro do mesmo cluster. Esses volumes podem estar na mesma SVM ou em duas SVMs diferentes dentro do mesmo cluster. Eles podem estar hospedados em pares de HA distintos ou no mesmo par de HA."

Além disso, na documentação: <https://docs.netapp.com/us-en/ontap/data-protection/create-replication-relationship-task.htm>, demonstra-se o passo a passo para implementação de relacionamentos do Snapmirror, onde podemos marcar como "local" ou "remoto". A documentação da NetApp demonstra claramente exemplos de replicação utilizando recursos locais, atendendo plenamente ao requisito do edital."

23. PARECER TÉCNICO

23.1 Conforme contrarrrazão da Recorrida, "Snapmirror é realizado a nível de volume e suportada em qualquer plataforma FAS e AFF, logo, a replicação entre controladoras é suportada, não sendo limitada pelas camadas subjacentes de armazenamento."

Para confirmação do que foi explicitado segue documentação oficial: <https://www.netapp.com/media/17174-tr4733.pdf>, Página 15:

"Starting with ONTAP 9.14.1, NetApp has qualified SM-S for replication between two volumes within the same cluster. These volumes may be in the same SVM or two different SVMs within the same cluster. These volumes can be hosted on different HA pairs or the same HA pair."

Tradução:

"A partir do ONTAP 9.14.1, a NetApp qualificou o SM-S para replicação entre dois volumes dentro do mesmo cluster. Esses volumes podem estar na mesma SVM ou em duas SVMs diferentes dentro do mesmo cluster. Eles podem estar hospedados em pares de HA distintos ou no mesmo par de HA."

23.2 Portanto, a Recorrida comprovou que cumpriu as exigências referentes aos itens "2.1.68" e "2.2.69" do Termo de Referência.

24. RAZÕES COMPWIRE

24.1 A seguir as razões apresentadas pela Recorrente em relação aos itens "2.1.84.3" e "2.2.84.3" do Termo de Referência.

"III.IV. NÃO ATENDIMENTO DA SOLUÇÃO DA RECORRIDA AO ITEM "2.1.84.3" E "2.2.84.3":

79. O Edital estabelece no Item 2.1.84.3 (ao que tange o Storage Tipo 1 – AFFC80) e 2.2.84.3 (ao que tange o Storage Tipo 2 – FAS50):

"2.1.84.3. A funcionalidade poderá ser configurada para receber alertas quando uma nova extensão de arquivo for detectada ou quando um snapshot automático for tirado."

80. A Recorrida utiliza a seguinte comprovação no documento de ponto a ponto "PAP - Presidência da Republica NetApp.xlsx":

81. Utilizando do documento "Workload_Security.pdf", a Recorrida está apenas comprovando que a funcionalidade de detecção de ataque ransomware pode realizar snapshots automáticos, porém, em nenhum momento o documento técnico estabelece a criação de alertas em casos de uma nova extensão de arquivo for detectada.

82. Vale ressaltar, que a única menção sobre alertas de extensão de arquivos é devido à possíveis alertas desnecessários de extensões já conhecidas do ambiente.

"Allowed File Types Policies

If a ransomware attack is detected for a known file extension, and alerts are being generated on the Alerts screen, then that file extension can be added to an allowed file types list to prevent unnecessary alerting."

(Workload_Security.pdf, p. 62)

[Em tradução livre]:

"Políticas de tipos de arquivo permitidos

Se um ataque de ransomware for detectado para uma extensão de arquivo conhecida e alertas estiverem sendo gerados na tela de Alertas, essa extensão de arquivo poderá ser adicionada a uma lista de tipos de arquivo permitidos para evitar alertas desnecessários."

83. Sendo assim, está claro que Recorrida não atende completamente este item, bem como os demais ora aventados, motivo pelo qual deve ser desclassificada do Edital Pregão Eletrônico nº 90037/2025-AS."

25. CONTRARRAZÕES SERVIX

25.1 A seguir as contrarrrazões apresentadas pela Recorrida em relação aos itens "2.1.84.3" e "2.2.84.3." do Termo de Referência.

"d) Da alegação de não atendimento aos itens 2.1.84.3 e 2.2.84.3.

Sobre o item:

"A funcionalidade poderá ser configurada para receber alertas quando uma nova extensão de arquivo for detectada OU quando um snapshot automático for tirado."

Para esclarecimento à licitante, o "ou" significa que a funcionalidade de anti-ransomware da licitante pode ser configurada para receber alertas quando uma nova extensão de arquivos for detectada OU a funcionalidade de anti-ransomware da licitante pode ser configurada para receber alertas quando um snapshot automático for tirado. Apenas um dos pontos é suficiente para atendimento do item.

Mas para que não tenha qualquer dúvida, apresentamos a seguinte documentação: <https://docs.netapp.com/us-en/ontap/anti-ransomware/manage-parameters-task.html>

How attack detection works

When Autonomous Ransomware Protection (ARP) is in a learning or evaluation mode, it develops baseline values for volume behaviors. These include entropy, file extensions, and, beginning with ONTAP 9.11.1, IOPS. These baselines are used to evaluate ransomware threats. For more information about these criteria, see [what ARP detects](#).

Certain volumes and workloads require different detection parameters. For example, the ARP-enabled volume might host numerous types of file extensions, in which case you may want to modify the threshold count for never-before-seen file extensions to a number greater than the default of 20 or disable warnings based on never-before-seen file extensions. Beginning with ONTAP 9.11.1, you can modify the attack detection parameters so they better fit your specific workloads.

Beginning with ONTAP 9.14.1, you can configure alerts when ARP observes a new file extension and when ARP creates a snapshot. For more information, see [Configure ARP alerts](#).

Demonstrando mais uma vez uma tentativa da licitante de levar a Presidência ao entendimento errado."

26. PARECER TÉCNICO

26.1 A Recorrida comprovou o atendimento aos itens "2.1.84.3" e "2.2.84.3" do Termo de Referência pela documentação citada em conformidade com os esclarecimentos apresentados, conforme o endereço: <https://docs.netapp.com/us-en/ontap/anti-ransomware/manage-parameters-task.html#how-attack-detection-works>.

"Beginning with ONTAP 9.14.1, you can configure alerts when ARP observes a new file extension and when ARP creates a snapshot. For more information, see [Configure ARP alerts](#)."

[Tradução livre]

"A partir do ONTAP 9.14.1, você pode configurar alertas quando o ARP detectar uma nova extensão de arquivo e quando o ARP criar um snapshot. Para obter mais informações, consulte [Configurar alertas do ARP](#)."

27. CONTRARRAZÕES COMPLEMENTARES SERVIX

27.1 A seguir as contrarrrazões complementares apresentadas pela empresa SERVIX, em relação a itens não atendidos pela COMPWIRE.

Vale ressaltar os seguintes itens:

2.1.51. e 2.2.50. Deve ser fornecida com a funcionalidade de "snapshot", ou "point-in-time backup", de quaisquer áreas de dados (volume/partição) da solução, que deverá ser implementado através de administração de ponteiros aos blocos de dados, com capacidade de armazenar, no mínimo, 1023 versões por cada volume/partição, ou seja, tanto na área alocada como SAN como na área alocada como NAS, existente no equipamento.

2.1.68.2. e 2.2.69.2 Permitir a replicação assíncrona de todas as configurações do equipamento como: compartilhamentos, políticas de segurança, cotas, snapshots e todas as demais funcionalidades exigidas neste termo.

2.1.69. e 2.2.70. Possuir ferramenta nativa de análise de arquivos para volumes NAS que faça a análise em tempo real e permita realizar no mínimo as seguintes tarefas:

2.1.69.1. e 2.2.70.1. Visualizar os volumes, diretórios e arquivos mais utilizados.

2.1.69.2. e 2.2.70.2. Quantidade de dados adicionados/gravados no último mês.

2.1.69.3. e 2.2.70.3. Quem são os usuários mais ativos e menos ativos.

2.1.69.4. e 2.2.70.4. Quantidade de dados inativos no storage, permitindo uma movimentação desse dado para um outro ambiente, caso necessário.

2.1.69.5. e 2.2.70.5. Histograma dos arquivos com modificações e histórico de acesso.

2.1.69.6. e 2.2.70.6. Quantidade de diretórios e arquivos existem dentro de um file server.

2.1.69.7. e 2.2.70.7. Deverá possuir a capacidade de exportar os dados de atividade em formato CSV que exibirá todos os dados pontuais capturados para o volume selecionado.

2.1.77. e 2.2.78. Deverá suportar os protocolos iSCSI e FCP para os ambientes operacionais com VMware ESX, Red Hat Linux e Microsoft Windows via Microsoft-Logo Certified, constando na HCL da Microsoft. Deverá ser comprovado via site do fabricante.

Tais itens não foram devidamente comprovados em documentação nem durante a diligência e, de forma conveniente, sequer foram mencionados pela licitante em sua defesa em recurso. A decisão de desclassificação deve ser mantida, considerando que a apresentação incompleta de argumentos pode refletir inconsistências ou não conformidades que impactam negativamente a capacidade da Compwire de atender plenamente os requisitos do edital."

28. PARECER TÉCNICO

28.1 Conforme exposto pela Recorrida, em relação aos itens mencionados nas contrarrrazões complementares e na diligência realizada, a Recorrente não atendeu completamente às exigências do Edital, com destaque aos itens 2.1.51 , 2.2.50, 2.1.68.2, 2.2.69.2, 2.1.69. 2.2.70.

"Tais itens não foram devidamente comprovados em documentação nem durante a diligência e, de forma conveniente, sequer foram mencionados pela licitante em sua defesa em recurso."

CONCLUSÃO

29. Pelo exposto, a área técnica da Presidência da República confirma que a proposta apresentada pela empresa **COMPWIRE INFORMÁTICA LTDA** não atende completamente a especificação técnica contida no Termo de Referência, mantendo-se as justificativas que acarretaram em não aceitação. No que se refere a empresa **SERVIX INFORMÁTICA LTDA**, mantém-se o parecer de que a proposta apresentada por esta empresa atende completamente ao exigido no Termo de Referência do edital do Pregão, na forma eletrônica, nº 90037/2025.

DA CONCLUSÃO

13. Em razão dos fatos registrados no Recurso, **CONHEÇO** o Recurso interposto pela **RECORRENTE**, por ser tempestivo e estar nos moldes legais para, no mérito, julgar **IMPROCEDENTE**, com base no parecer técnico exarado pela área técnica demandante, **MANTENDO** a empresa **SERVIX INFORMÁTICA LTDA** como vencedora do certame.
14. Os autos do processo permanecerão com vista franqueada aos interessados. Esta decisão de recurso encontra-se disponível nos sites: <https://www.gov.br/casacivil/pt-br/acesso-a-informacao/licitacoes-e-contratos/secretaria-de-administracao/licitacoes> e www.gov.br/compras.

CLAUDEMBERQUE MONTEIRO FERREIRA
Pregoeiro



Documento assinado eletronicamente por **Claudemberque Monteiro Ferreira, Pregoeiro(a)**, em 11/12/2025, às 17:00, 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 **7209062** e o código CRC **4F9D61FD** no site: https://protocolo.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0