

PRESIDÊNCIA DA REPÚBLICA
Casa Civil
Secretaria-Executiva
Secretaria de Administração
Diretoria de Tecnologia
Coordenação-Geral de Infraestrutura Tecnológica
Coordenação do Centro de Dados

Brasília, 17 de novembro de 2025.

À Coordenação-Geral de Infraestrutura Tecnológica,
Assunto: **Pregão, na forma eletrônica, nº 90037/2025 – Análise e parecer de proposta e documentação de diligência.**

1. Em atenção ao Despacho 7133713 (COLIT/COLIC/DILOG/SA/SE/CC/PR) referente ao Pregão, na forma eletrônica, nº 90037/2025, que solicita que seja informado se a proposta, considerando ainda a documentação de diligência apresentada, atende ou não ao exigido no Termo de Referência, esta Coordenação de Centro de Dados encaminha análise da diligência da empresa licitante a seguir.

EMPRESA	CNPJ	GRUPO	PROPOSTA	QUALIFICAÇÃO TÉCNICA	DILIGÊNCIA
COMPWIRE INFORMATICA LTDA	01.181.242/0003-53	ÚNICO	7105063 / 7106709	7107185	7133459

2. Segue análise aos pedidos de diligência para os itens do Termo de Referência indicados no Despacho (7126124) e relacionados novamente neste Despacho com a resposta da LICITANTE transcrita a partir do documento de diligência (7133459).

2.1. **Itens 2.1.3 e 2.2.3 do Termo de Referência**

2.1.1. Exigência: *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.*

2.1.2. Análise: De acordo com o site <https://e.huawei.com/br/products/storage/all-flash-storage>, o equipamento mais recente da HUAWEI é o **OceanStor Dorado All-Flash Storage** e não o ofertado na proposta, o **OceanStor Capacity Flash 5510**. O trecho a seguir foi extraído do referido site: “Armazenamento convergente de blocos, arquivos e objetos, com recursos abrangentes de classe empresarial. O algoritmo inteligente Flashlink® alcança um desempenho 50% superior ao da geração anterior de sistemas de armazenamento. Detecção integrada de ransomware para blocos e arquivos, garantindo a resiliência dos ativos de dados.”

2.1.3. **Pedido de Diligência:** Solicita-se esclarecimentos ao LICITANTE a respeito desta questão.

2.1.4. **Resposta da LICITANTE:**

No atual portfólio de storages All-Flash da Huawei, Dorado V6 e Capacity Flash são as últimas famílias lançadas, sendo o Capacity Flash anunciado após o lançamento do Dorado V6. Os equipamentos são de linhas de produto distintas: Dorado é a linha de armazenamento voltada para performance e Capacity Flash é a linha voltada para armazenamento de alta capacidade.
<https://e.huawei.com/hk/products/storage/all-flash-storage/5x10-series>
Ademais, reforçamos que esse item está comprovado na declaração oficial da fabricante para o dito pregão.

2.1.5. **Análise da Diligência:** Conforme apresentado no site da fabricante <https://e.huawei.com/br/products/storage/all-flash-storage>, a geração mais recente do equipamento OceanStor All-Flash é a Nova Geração do OceanStor Dorado (OceanStor Dorado 3000, 5000, e 6000 - Version: V700R001), lançada em setembro de 2025, no HUAWEI CONNECT 2025. E, conforme consta no site <https://support.huawei.com/enterprise/en/bulletins-product/ENWS2000013060>, o equipamento ofertado é de uma família que encontra-se com prazo de expiração definido. Então, entendemos que o equipamento ofertado não pertence à família de equipamentos All-Flash mais recente para atendimento aos requisitos do Termo de Referência.

2.2. **Itens 2.1.5 e 2.2.5 do Termo de Referência**

2.2.1. Exigência: *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.*

2.2.2. Análise: O Termo de referência exige que o equipamento ofertado deverá ser o mais recente disponível no portfólio do fabricante. De acordo com o site <https://e.huawei.com/br/products/storage/all-flash-storage>, o equipamento mais recente é o storage “OceanStor Dorado All-Flash” e não o “OceanStor Capacity Flash 5510” ofertado na proposta.

2.2.3. **Pedido de Diligência:** Solicita-se esclarecimentos sobre esta questão.

2.2.4. **Resposta da LICITANTE:**

No atual portfólio de storages All-Flash da Huawei, **Dorado V6** e **Capacity Flash** são as últimas famílias lançadas, sendo o Capacity Flash anunciado após o lançamento do Dorado V6. Os equipamentos são de linhas de produto distintas: Dorado é a linha de armazenamento de discos TLC e Capacity Flash é a linha de armazenamento de alta capacidade, utilizando discos QLC.
Fonte: <https://e.huawei.com/hk/products/storage/all-flash-storage/5x10-series> e “Huawei OceanStor 53105510 Capacity Flash Storage Data Sheet.pdf”
Ademais, reforçamos que esse item está comprovado na declaração oficial da fabricante para o dito pregão.

2.2.5. **Análise da Diligência:** O equipamento ofertado Huawei **OceanStor 5510 Capacity Flash Storage** foi lançado e disponibilizado para o mercado em 15 de janeiro de 2024, praticamente a 60 dias de completar 24 meses, enquanto a nova geração do **storage OceanStor Dorado all-flash** foi lançada em setembro de 2024, conforme publicado em <https://www.datacenterdynamics.com/en/news/huawei-launches-dorado-v7-all-flash-storage-solution/>, e o novo modelo foi lançado em setembro de 2025. Portanto, o equipamento ofertado não é o mais recente disponível no portfólio do fabricante.

2.3. **Itens 2.1.43 e 2.2.41 do Termo de Referência:**

2.3.1. Exigência: Permitir a criação de pelo menos 10.000 LUN’s por par de controladora.

2.3.2. Análise: Falta documentação para comprovar estes itens.

2.3.3. **Pedido de Diligência:** Indicar na documentação o trecho que comprova os itens 2.1.43 e 2.2.41.

2.3.4. **Resposta da LICITANTE:** O Capacity Flash 5510 ofertado para o Item 1 e Item 2, com 512GB de Cache total, permite a criação de 16.384 LUNs em uma Storage Pool do storage, atendendo plenamente ao solicitado. Ademais, reforçamos que esse item está comprovado na declaração oficial da fabricante para o dito pregão. (...)

2.3.5. **Análise da Diligência:** De fato, a informação está disponível apenas na ferramenta *Specifications Query* da fabricante, e não havia sido apresentada na proposta. Considerando a captura de tela exibida pela LICITANTE, o equipamento atende ao número de LUN's exigido por par de controladora.

2.4. **Itens 2.1.51 e 2.2.50 do Termo de Referência:**

2.4.1. Exigência: *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.*

2.4.2. **Análise:** Esta funcionalidade deverá ser executada internamente ao equipamento, sem consumir ciclo de CPU dos sistemas clientes conectados e sem gerar movimentação de dados de nenhum tipo. Não está claro na documentação se funcionalidade pode ser executada sem gerar movimentação de dados de nenhum tipo.

2.4.3. **Pedido de Diligência:** Indicar na documentação o trecho que comprove os itens 2.1.51 e 2.2.50.

2.4.4. **Resposta da LICITANTE:** Usualmente, nenhum storage Huawei utiliza de performance dos clientes (hosts) do ambiente para realizar suas próprias funcionalidades. Para facilitar, no documento “*OceanStor 2x00, 5x10 Series 6.1.x Product Description.pdf*”, página 4, está descrito:

“● Advanced data protection
–HyperSnap supports writable snapshots. Snapshot creation and activation have no impact on performance.”

2.4.5. **Análise da Diligência:** A comprovação original, quanto à quantidade de versões por cada volume/partição, cita o componente *HyperCDP*, enquanto a resposta dada quanto à não movimentação de dados menciona o componente *HyperSnap*. Não está claro se, individualmente, algum desses componentes atende por completo aos itens 2.1.51 e 2.2.50 do TR. A LICITANTE comprovou parcialmente esta exigência.

2.5. **Itens 2.1.66 e 2.2.65. do Termo de Referência:**

2.5.1. **Exigência:** *Possuir plug-in para integração com o vCenter (VMware), de forma que seja permitido configurar políticas de acesso ao sistema diretamente do vCenter e permita visualização de informações do sistema de armazenamento.*

2.5.2. **Análise:** Não há descrição na documentação indicando se o plug-in permite configurar políticas de acesso ao sistema diretamente pelo vCenter ou visualizar informações do sistema de armazenamento.

2.5.3. **Pedido de Diligência:** Indicar na documentação o trecho que comprove os itens 2.1.66 e 2.2.65.

2.5.4. **Resposta da LICITANTE:** O Capacity Flash possui completa integração com VMware, utilizando tanto o plug-in do vSphere/vCenter quanto das funcionalidades adicionais para storage.

O plug-in “OceanStor VMware Next Generation Client Plug-in” está no site da Huawei para download:

<https://support.huawei.com/enterprise/en/software/250381796-ESW2000208323>

Para facilitar, no documento “*OceanStor 2x00, 5x10 Series 6.1.x Product Description.pdf*”, página 7, está descrito:

“– Integrated management
Supports VMware vCenter Plug-in and Hyper-V System Center for management. In addition, the storage system supports VMware vStorage APIs for Storage Awareness (VASA), vStorage APIs for Array Integration (VAAD), and Volume Shadow Copy Service (VSS) Provider to facilitate management.”

Ademais, reforçamos que esse item está comprovado na declaração oficial da fabricante para o dito pregão.

2.5.5. **Análise da Diligência:** A resposta confirma a existência do plug-in, sem menção à configuração de políticas de acesso ao sistema diretamente pelo vCenter, exceto pela declaração da fabricante.

2.6. **Itens 2.1.67 e 2.2.68 do Termo de Referência:**

2.6.1. **Exigência:** *Permitir gerenciamento de qualidade de serviço (QoS) para definir o limite de IOPs (I/O por segundo) e/ou MB/s (Megabytes por segundo) que será utilizado em nível de arquivos, volumes e LUN. Essa funcionalidade deve ser capaz de estabelecer tanto uma quantidade máxima, quanto uma quantidade mínima de banda e/ou IOPS.*

2.6.2. **Análise:** A documentação não atesta o gerenciamento de QoS em nível de arquivos individuais, apenas em nível de sistema de arquivos.

2.6.3. **Pedido de Diligência:** Indicar na documentação o trecho que comprove os itens 2.1.67 e 2.2.68.

2.6.4. **Resposta da LICITANTE:** O gerenciamento de Qualidade de Serviço (QoS) em nível de File System é a abordagem tecnicamente correta, o QoS a nível de arquivo individual não é uma função padrão em sistemas de armazenamento NAS enterprise por duas razões técnicas críticas:

Do ponto de vista administrativo, é impraticável e computacionalmente inviável gerenciar políticas de performance para arquivos individuais, pois são dados prioritariamente não-estruturados, como por exemplo imagens, documentos e pdf, sendo eles dados não editáveis em larga escala. Um único sistema de arquivos (File System) pode conter bilhões de arquivos. A aplicação, o monitoramento e a aplicação de políticas de QoS individuais (IOPS Mín/Máx, Banda Mín/Máx) para cada um desses bilhões de objetos geraria uma sobre carga extrema de metadados e processamento. As controladoras seriam consumidas pela gestão dessas micropolíticas, em vez de processar I/O, tornando o sistema inutilizável.

Vale ressaltar que as principais fabricantes do mercado como Huawei, Dell, IBM, NetApp e outros atendem principalmente a nível de File System ou Dtree.

No documento “*OceanStor Capacity Flash Storage 6.1.8 Technical White Paper.pdf*”, página 55, está descrito:

“5.2 SmartQoS (Intelligent Quality of Service Control)
SmartQoS dynamically allocates storage system resources to meet the performance objectives of applications. You can set upper and lower limits on IOPS, bandwidth, or response latency for specific applications. Based on the limits, SmartQoS can accurately limit performance of these applications, preventing them from contending for storage resources with critical applications.
SmartQoS uses object-specific I/O priority scheduling and I/O traffic control (including upper limit control and minimum performance guarantee) to guarantee the service quality.”

A solução atende à implementação técnica padrão de mercado, onde o controle é aplicado ao file system para gerenciar a performance e o QoS como um todo.

2.6.5. **Análise da Diligência:** **Análise da Diligência:** A resposta da Licitante foi considerada aceita para os itens em questão.

2.7. **Itens 2.1.68.1 e 2.2.69.1 do Termo de Referência:**

2.7.1. **Exigência:** *Permitir o uso das tecnologias de replicação de modo concomitante com as tecnologias de redução de dados, tanto a deduplicação como a compressão, sem a necessidade de reidratar os dados para replicar.*

2.7.2. **Análise:** O texto da documentação apresentada comprova apenas a compressão. Não houve referência à deduplicação concomitante com tecnologia de replicação.

2.7.3. **Pedido de Diligência:** Indicar na documentação o trecho que comprove os itens 2.1.68.1 e 2.2.69.1.

2.7.4. **Resposta da LICITANTE:**

Primeiro, é importante entender como funciona a redução de dados nos equipamentos Huawei. No documento “*OceanStor Capacity Flash Storage 6.1.8 Technical White Paper.pdf*”, página 51, é representado pela figura 5-1 o processo completo de Adaptive deduplication and compression da solução, como vemos a seguir: (...) Esse processo é realizado com uso de deduplicação e compressão inline, isto é, antes de armazenar o dado nos discos (storage pool). Para tal, é criado o Fingerprint table onde está mapeado todos os blocos e a localização dos dados deduplicados, metadados e seus ponteiros. Como o Capacity Flash utiliza desse processo para todo dado escrito no storage, ao realizar uma replicação, todos os dados replicados já estarão hidratados e serão replicados junto com a Fingerprint table, para que assim possa ser reidratado no storage target, após a replicação, quando necessário. A compressão descrita na comprovação é a *post-process compression* também utilizada na replicação. Sendo assim, a solução atende ao item.

2.7.5. **Análise da Diligência:** A resposta da Licitante foi considerada aceita para os itens em questão.

2.8. **Itens 2.1.68.2 e 2.2.69.2 do Termo de Referência:**

2.8.1. **Exigência:** *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.*

2.8.2. **Análise:** Nas páginas 93 e 96 do documento “*OceanStor Capacity Flash Storage 6.1.8 Technical White Paper.pdf*”, não há detalhamento sobre o modo como a replicação é realizada em todas as configurações citadas neste item. O texto a seguir, pág. 96, indica que o processo de replicação é realizado por meio de snapshots: “Similar to asynchronous remote replication for SAN, asynchronous remote replication for NAS periodically replicates data based on ROW snapshots.” A documentação não se refere a configurações do equipamento como: compartilhamentos, políticas de segurança e cotas, por exemplo.

2.8.3. **Pedido de Diligência:** Indicar na documentação o trecho que comprove os itens 2.1.68.2 e 2.2.69.2 em conformidade com o exigido.

2.8.4. **Resposta da LICITANTE:**

Neste item, é importante notar a característica de consistência e sincronização do dado ao ser replicado. Na página 96 do documento “OceanStor Capacity Flash Storage 6.1.8 Technical White Paper.pdf”, está descrito resumidamente destaques da funcionalidade:

“• Consistency group
Consistency groups apply to databases. Multiple LUNs, such as log LUNs and data LUNs, can be added to a consistency group so that data on these LUNs is from a consistent time in the case of periodic synchronization or fault. This facilitates data recovery at the application layer.
• Cross-array snapshot data synchronization
User snapshots of the primary LUN can be synchronized to the secondary LUN in sequence. This function is recommended when host data consistency is required.”
No documento anexoado “OceanStor 6.1.x & V700R001 HyperReplication Feature Guide for Block.pdf” está explicado que é possível realizar a sincronização da política de snapshot do storage primário (storage source) para o storage secundário (storage target), como visto na página 60:

“User Snapshot Sync
Synchronization policy of snapshots of the primary resources. Possible values are as follows:
• **Same as primary:** Snapshots of the primary resources will be synchronized to the secondary resources during pair synchronization. If a snapshot that has been synchronized to the secondary resource is deleted from the primary resource, the secondary resource will perform the same deletion operation during the next synchronization to ensure that the snapshots of primary and secondary resources are consistent.”
O parâmetro de snapshot é ajustável por questões de políticas diferentes para um ambiente de DR (Disaster Recovery). Já as configurações próprias das LUNs e File System como tamanho, IP, quotas e outras usuais na criação das mesmas sempre serão replicadas na criação do replication pair,
Para exemplificar um dos casos possíveis, caso o administrador queira expandir a capacidade de uma LUN do storage primário, também poderá ser expandida a capacidade da LUN replicada. Como descrito nas páginas 133 e 134 do “OceanStor 6.1.x & V700R001 HyperReplication Feature Guide for Block.pdf”.

“Step 1 Expand the capacity of the primary LUN and the secondary LUN respectively.
5. (Optional) Select or deselect **Only expand the local LUN**.
NOTE
– If you do not select **Only expand the local LUN**, the system will expand both the local and remote LUNs in the HyperMetro pair, remote replication pair, or DR Star trio. If you select **Only expand the local LUN**, the system will only expand the local LUN. In this case, manually expand the remote LUN to ensure the availability of HyperMetro, remote replication, or DR Star.”

Diante disso, é perceptível que o padrão das replicações é sempre replicar todas as características da LUN ou do File System, permitindo por vezes configurações opcionais em cenários específicos, como é o caso na expansão, logo abaixo:

“– You are advised to select **Only expand the local LUN** in the following scenarios:
• The link to the remote device is disconnected.
• The capacities of the local and remote LUNs are different.
• The local device is a remote device in HyperMetro or asynchronous remote replication in a DR Star trio.
• The remote LUN is in another protection relationship.”

Além de explicar como realizar a expansão, o documento demonstra em quais cenários se faz válido apenas expandir a LUN do storage primário, apesar de não ser o usual.

2.8.5. **Análise da Diligência:** A documentação apresentada menciona apenas a replicação assíncrona da funcionalidade de snapshots, sem menção à replicação de compartilhamentos, políticas de segurança ou cotas. Portanto, a resposta da Licitante foi considerada aceita parcialmente para os itens em questão.

2.9. **Itens 2.1.69 e 2.2.70 do Termo de Referência:**

2.9.1. Exigência:

2.1.69. 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. Visualizar os volumes, diretórios e arquivos mais utilizados.
- 2.1.69.2. Quantidade de dados adicionados/gravados no último mês.
- 2.1.69.3. Quem são os usuários mais ativos e menos ativos.
- 2.1.69.4. Quantidade de dados inativos no storage, permitindo uma movimentação desse dado para um outro ambiente, caso necessário.
- 2.1.69.5. Histograma dos arquivos com modificações e histórico de acesso.
- 2.1.69.6. Quantidade de diretórios e arquivos existem dentro de um file server.
- 2.1.69.7. Deverá possuir a capacidade de exportar os dados de atividade em formato CSV que exibirá todos os dados pontuais capturados para o volume selecionado.

2.2.70. Deverá 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:

- 2.2.70.1. Visualizar os volumes, diretórios e arquivos mais utilizados.
- 2.2.70.2. Quantidade de dados adicionados/gravados no último mês.
- 2.2.70.3. Quem são os usuários mais ativos e menos ativos.
- 2.2.70.4. Quantidade de dados inativos no storage, permitindo uma movimentação desse dado para um outro ambiente, caso necessário.
- 2.2.70.5. Histograma dos arquivos com modificações e histórico de acesso.
- 2.2.70.6. Quantidade de diretórios e arquivos existem dentro de um file server.
- 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.

2.9.2. **Análise:** Somente os itens 2.1.69.1, 2.1.69.6 e 2.1.69.7 foram atendidos parcialmente. Esses itens apenas descrevem a possibilidade de visualizar a utilização e a quantidade de arquivos, sem indicar que é possível identificar os mais utilizados, e mencionam a exportação de relatórios com métricas de desempenho, não necessariamente voltados a dados de atividade de arquivos. Então, as informações apresentadas não comprovam o atendimento de todas as métricas relacionadas.

2.9.3. **Pedido de Diligência:** Indicar na documentação o trecho que comprove por completo os itens 2.1.69 e 2.2.70.

2.9.4. **Resposta da LICITANTE:**

2.1.69.2 – No documento “OceanStor 6.1.x Performance Monitoring Guide.pdf”, página 425 e 452 está comprovado que é possível verificar a escrita de arquivos em diversas métrica, e medir a periodicidade dessas métricas para até 12 meses antes:

“File Write Bandwidth (KB/s): Volume of file data being written per second on a module
Write OPS: Write OPS of a specific file system (including forwarding ends)”

2.1.69.3 - Página 55 do “OceanStor 6.1.x Performance Monitoring Guide.pdf”

“About This Chapter

Service performance is limited by the performance bottlenecks in a system. Before performance optimization and problem locating, you should understand the current service status and user requirements on performance. Then use the system I/O path to locate the module where the performance problem occurs. Finally, you can locate the problem and optimize performance.

4.1 Overview

4.2 Locating Problems

4.3 Diagnosing Host Problems

4.4 Diagnosing Network and Link Problems

4.5 Diagnosing Storage Problems

4.1 Overview

For users, performance issues are reflected in slow or delayed delivery of service processes or application response.

Common performance problems are as follows:

- The I/O latency is long. Users experience a longer service response time.
- IOPS and bandwidth cannot meet service requirements.
- Performance data fluctuates greatly.”

2.1.69.4 – A funcionalidade de SmartMove é utilizada para a movimentação dos dados internos (intra-array), o que utiliza da tarefa de “quantidade de dados inativos no storage”. Conforme documento “OceanStor Capacity Flash Storage 6.1.8 Technical White Paper.pdf”, página 76:

“5.11.3 Applicable Scenarios of SmartMove

SmartMove applies in scenarios where space utilization optimization, controller load balancing, or service performance optimization is required. It also applies in the FlashEver scenario.

5.11.3.1 Space Utilization Optimization

If the usage of storage pools in a service cluster is inconsistent, you can migrate file systems between storage pools to optimize space utilization. If the space of the storage pool where a file system resides is insufficient, you can migrate the file system to another storage pool with sufficient space to meet future space growth requirements.”

2.1.69.5 – Conforme comprovado: “Capacity of the file system, which indicates the maximum capacity allocated to the thin file system. That is, the total capacity dynamically allocated to the thin file system cannot exceed this value.

All drees: controls the space usage or file quantity of each dree in the file system.

2.9.5. **Análise da Diligência:** No subitem 2.1.69.2, a métrica citada de banda instantânea (KB/s) é ordens de magnitude diferente da métrica exigida de quantidade de dados gravados no último mês (GB/mês, por exemplo).

2.1.69.3 - Documentação citada menciona apenas os impactos do desempenho do sistema aos seus usuários, sem indicar se é possível identificar os usuários mais ativos e menos ativos.
2.1.69.4 - Apesar do trecho citado pela LICITANTE (5.11.3.1) não se aplicar à exigência, um parágrafo posterior da mesma seção (5.11.3.4) comprova o atendimento da exigência.
2.1.69.5 - A documentação citada não menciona a visualização de modificações e do histórico de acesso, apenas a quantidade de arquivos e o espaço utilizado por ela. Portanto, a LICITANTE comprovou este item parcialmente.

2.10. **Itens 2.1.71 e 2.2.72 do Termo de Referência:**

2.10.1. Exigência:

2.1.71. Deverá ser fornecido com os softwares / licenças para integração com as seguintes aplicações:
2.1.71.1. Gerenciadores de bancos de dados: Microsoft SQL Server.
2.1.71.2. Sistemas e serviços: Microsoft Exchange e Microsoft Cluster Service.
2.1.71.3. Sistemas operacionais: VMware ESX, Microsoft Windows Server, Linux Red Hat.
2.1.71.4. Virtualizador: VMware

2.2.72. Deverá ser fornecido com os softwares / licenças para integração com as seguintes aplicações:
2.2.72.1. Gerenciadores de bancos de dados: Microsoft SQL Server. e Oracle
2.2.72.2. Sistemas e serviços: Microsoft Exchange e Microsoft Cluster Service.
2.2.72.3. Sistemas operacionais: VMware ESX, Microsoft Windows Server, Linux Red Hat.
2.2.72.4. Virtualizador: VMware

2.10.2. **Análise:** Não há qualquer menção ao suporte ou compatibilidade com o Microsoft Exchange ou o Microsoft Cluster Service. Consta apenas a referência genérica a “Microsoft”.

2.10.3. **Pedido de Diligência:** Indicar na documentação o trecho que comprove os itens 2.1.71 e 2.2.72 em conformidade com o exigido.

2.10.4. **Resposta da LICITANTE:** É importante notar que o Microsoft Cluster Service é uma solução integrado ao Microsoft Windows, hoje parte do Windows Server Failover Clustering (WSFC), que exige que o armazenamento compartilhado (storage) suporte um protocolo de arbitragem de LUNs. O storage Huawei atende a este requisito através do suporte nativo ao protocolo SCSI-3 Persistent Reservations (SCSI-3 PR), que é o mecanismo de locking (bloqueio) que o cluster do Windows utiliza para controlar o acesso à LUN. Quando um nó do cluster se torna "dono" de um recurso, ele coloca uma "reserva persistente" na LUN. Isso impede que o outro nó (passivo) escreva na LUN, evitando a corrupção de dados. Dito isso, o protocolo é uma funcionalidade intrínseca e padrão do sistema operacional OceanStor OS em qualquer LUN de bloco (FC ou iSCSI). E sabendo que o storage tem integração completa com o protocolo e com Microsoft Windows Server, ele se integra intrinsecamente com o WSFC. Ademais, o WSFC está na matriz de compatibilidade do Huawei OceanStor na versão 6.1.8, a solução ofertada. Já o Microsoft Exchange, é uma aplicação que opera sobre o sistema operacional Windows Server. O storage que será utilizado para armazenar os dados do Exchange (seus bancos de dados e logs) é apresentado ao sistema operacional como volumes de bloco (LUNs). Portanto, a integração do storage Huawei é comprovada pela compatibilidade com o Windows Server, já no documento de comprovação. “OceanStor Capacity Flash Storage 6.1.8 Technical White Paper.pdf”, página 172:

“13.1.1 Host Operating System
OceanStor 5310/5510 Capacity Flash Storage is compatible with mainstream host operating systems in the industry (including IBM AIX, HP-UX, Solaris, Red Hat Enterprise Linux, SuSE Linux Enterprise Server, Oracle Enterprise Linux, Windows Server, NeoKylin, Kylin (Tianjin), Hunan Kylin, Deepin, Linx-TECH Rocky, and Redflag Linux)”

2.10.5. **Análise da Diligência:** A resposta da Licitante foi considerada aceita para os itens em questão.

2.11. **Itens 2.1.72. e 2.2.73 do Termo de Referência:**

2.11.1. Exigência: *A integração, de acordo com a aplicação, deverá controlar pelo menos a criação de snapshots e recuperação de backups via snapshot.*

2.11.2. **Análise:** A resposta da Licitante, informando apenas “Ciente e de acordo” não comprova a existência da funcionalidade especificada.

2.11.3. **Pedido de Diligência:** Indicar na documentação o trecho que comprove os itens 2.1.72 e 2.2.73 em conformidade com o exigido.

2.11.4. **Resposta da LICITANTE:** Considerando que o objeto desta licitação são Sistemas de armazenamento de dados (storages), entende-se que estes serão utilizados como volumes para as aplicações lerem e escreverem os dados. Sendo assim, os storages serão apresentados como volumes de bloco (LUNs) ou File System (Sistemas de Arquivos) aos sistemas operacionais, bancos de dados e virtualizadores, compatibilidade esta comprovada nos itens 2.1.71 e 2.2.72. Logo, a funcionalidade de snapshot do storage Huawei (seja via HyperSnap ou HyperCDP) poderá ser configurada para qualquer LUN ou File System, independente da aplicação nos servidores. No documento “OceanStor Capacity Flash Storage Technical White Paper.pdf”, página 78 e 84 está descrito como gerenciar snapshots, via HyperSnap ou HyperCDP:

“6.1 HyperSnap (Snapshot)
HyperSnap is a snapshot feature of OceanStor 5310/5510 Capacity Flash Storage.
It provides different snapshot functions for SAN and NAS services. Snapshots for SAN services are readable and writable. They are considered as independent LUN objects by the hosts and must be mapped separately. Snapshots for NAS are readonly and are deployed in the snapshot directories of the file systems. They can be accessed after the file systems are mounted.
6.2 HyperCDP (Continuous Data Protection)
HyperCDP creates high-density snapshots on a storage system to provide continuous data protection (CDP). This section provides an overview of this feature.
Misoperations and virus attacks may cause data corruption. Continuous data protection is to create snapshots at a short interval to help customers restore data.
HyperCDP allows OceanStor 5310/5510 Capacity Flash Storage to continuously protect LUNs. HyperCDP is based on the lossless snapshot technology (TP and ROW). Each HyperCDP object matches a time point of the source LUN. Figure 6-5 illustrates how HyperCDP is implemented.”

Em casos de backups e recuperação de backups via snapshot, conforme questionamento respondido, o processo é realizado via software de backup (como o Veeam) que possui integração com as aplicações, seja VMware (via VMware Backup & Replication Application-Aware Processing). Nestes cenários, o storage onde os dados estão armazenados atua como repositório e disponibiliza o volume (LUN ou File System) para que o software de backup realize as ações pertinentes.

2.11.5. **Análise da Diligência:** A resposta da Licitante foi considerada aceita para os itens em questão.

2.12. **Itens 2.1.73 e 2.2.74 do Termo de Referência:**

2.12.1. Exigência: *Deverá permitir a geração, por interface gráfica, de snapshots íntegros, restore e espelhamento de máquinas virtuais.*

2.12.2. **Análise:** Não foi comprovado que o sistema realiza geração, por interface gráfica, de snapshots íntegros, restore e espelhamento de máquinas virtuais. A documentação indica a existência gráfica sem detalhar estas funcionalidades.

2.12.3. **Pedido de Diligência:** Indicar na documentação o trecho que comprove os itens 2.1.73 e 2.2.74 em conformidade com o exigido.

2.12.4. **Resposta da LICITANTE:** Utilizando do VMware plug-in VASA é possível mapear as máquinas e realizar geração e deleção de snapshots. Com a funcionalidade de VVol, cada disco da VM vira um volume lógico no storage, permitindo que o storage faça snapshots do objeto da VM. Com essa tecnologia, o VMware realiza consistência de aplicação via VASA Provider, mantendo a VM e seus snapshots consistentes, podendo assim, restaurar a VM inteira, VMDK específico ou criar um clone instantâneo. No documento “OceanStor 6.1.x Basic Storage Service Configuration Guide for Block.pdf”, página 102 e 201, subitem 5.6 Managing VVol está descrito como criar as LUNs para a gestão dos VVols

“Pág. 102

4.13.1 Configuring Basic Storage Services for VMware VVol
Virtual volume (VVol) is a new function in VMware ESXi 6.0. This section describes how to configure basic storage services for VMware VVol. Configure the VVol function by following instructions in the eSDK Enterprise Storage Plugins VASA user guide.

Pág. 201

5.6 Managing VVol

This section describes how to manage VVol.

5.6.1 Creating a PE LUN

This section describes how to create a PE LUN.

Context

PE LUNs are only used by virtual volumes (VVols) in VMware software-defined storage. VVols provide storage space for VMs. A PE LUN is used as an I/O distributor to simplify the connection between a VM and a VVol. I/Os from a VM are sent to the VVol through a PE LUN."

No documento "OceanStor Capacity Flash Storage Technical White Paper.pdf", página 78 e 84 está descrito como gerenciar snapshots, via HyperSnap ou HyperCDP, para proteger LUNs inclusive PE LUN (VVol):

"6.1 HyperSnap (Snapshot)

HyperSnap is a snapshot feature of OceanStor 5310/5510 Capacity Flash Storage.

It provides different snapshot functions for SAN and NAS services. Snapshots for SAN services are readable and writable. They are considered as independent LUN objects by the hosts and must be mapped separately. Snapshots for NAS are readonly and are deployed in the snapshot directories of the file systems. They can be accessed after the file systems are mounted.

6.2 HyperCDP (Continuous Data Protection)

HyperCDP creates high-density snapshots on a storage system to provide continuous data protection (CDP). This section provides an overview of this feature.

Misoperations and virus attacks may cause data corruption. Continuous data protection is to create snapshots at a short interval to help customers restore data.

HyperCDP allows OceanStor 5310/5510 Capacity Flash Storage to continuously protect LUNs. HyperCDP is based on the lossless snapshot technology (TP and ROW). Each HyperCDP object matches a time point of the source LUN. Figure 6-5 illustrates how HyperCDP is implemented."

2.12.5. **Análise da Diligência:** A resposta da Licitante foi considerada aceita para os itens em questão.

2.13. **Itens 2.1.77 e 2.2.78 do Termo de Referência**

2.13.1. Exigência: *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.*

2.13.2. Análise: A documentação apresentada não contém informações referentes ao VMware ESX e ao Red Hat Linux, e não comprova a compatibilidade por meio do site HCL da Microsoft.

2.13.3. **Pedido de Diligência:** Indicar na documentação o trecho que comprove os itens 2.1.77 e 2.2.78 em conformidade com o exigido.

2.13.4. **Resposta da LICITANTE:** Comprovação HCL da Microsoft: <https://www.windowsservercatalog.com/product/dac7310-6b2c-5846-d6a0-f4714f62d30c>

Comprovação do Compatibility Matrix com VMware:

HuaweiOceanStor_VMware_SANBasicConnectivity_Interoperability Matrix.pdf

Comprovação do Compatibility Matrix com Red Hat Linux:

HuaweiOceanStor_RHEL_SANBasicConnectivity_Interoperability Matrix.pdf

2.13.5. **Análise da Diligência:** A comprovação de atendimento aos itens 2.1.77 e 2.2.78 é incompatível com o atendimento aos itens 2.1.5 e 2.2.5, dado que os certificados Microsoft apresentados correspondem à versão oferecida pela LICITANTE (6.x) e estão datados até 06/ago/2021.

Dessa forma, a versão ofertada do equipamento (6.x) já havia sido lançada à época da certificação de agosto/2021, em descumprimento aos itens 2.1.5 e 2.2.5.

2.14. **Itens 2.1.80. e 2.2.81 do Termo de Referência:**

2.14.1. Exigência:

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/projects/cryptographic-module-validation-program/validated-modules/search>.

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

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

2.2.81.2. 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.

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

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

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

2.2.81.6. O sistema deverá suportar a funcionalidade de criptografia seja implementada para as áreas NAS (CIFS e NFS) e SAN (FC e iSCSI).

2.2.81.7. 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.

2.2.81.8. A comprovação da conformidade com a FIPS 140-2, serão validadas em: <https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search>.

2.14.2. Análise: O documento não menciona procedimentos de habilitação ou desabilitação exigidos no subitem 2.1.80.5, e não faz referência ao padrão FIPS. O único produto de hardware certificado em conformidade com o FIPS 140-2 é a linha de SSDs HSSD_V6 (<https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4261>) composta por discos TLC com capacidade de até 7,68 TB. Considerando que a LICITANTE apresentou em sua proposta discos de 30,72 TB, conclui-se que esses discos não possuem criptografia compatível com o padrão FIPS 140-2.

2.14.3. **Pedido de Diligência:** Indicar na documentação o trecho que comprove os itens 2.1.80 e 2.2.81 em conformidade com o exigido.

2.14.4. **Resposta da LICITANTE:** Na documentação "OceanStor Capacity Flash Storage 6.1.8 Security Technical White Paper.pdf", página 34 está descrito:

"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."

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."

Esses 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.

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.

- 2.14.5. **Análise 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.
- 2.15. **Itens 2.1.81 e 2.2.82 do Termo de Referência:**
- 2.15.1. Exigência: *Possuir integração com o framework Open Authorization (OAuth 2.0).*
- 2.15.2. Análise: A documentação apresentada pela LICITANTE não faz referência ao framework Open Authorization (OAuth 2.0)
- 2.15.3. **Pedido de Diligência:** Indicar na documentação o trecho que comprove os itens 2.1.81 e 2.2.82 em conformidade com o exigido.
- 2.15.4. **Resposta da LICITANTE:** 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:

1. Autenticação local via SSH por usuário e senha ou chave pública;
2. Autenticação multifator para acesso Web (senha + OTP);
3. Autenticação de domínio via LDAP/LDAPS integrado ao Active Directory;
4. Autorização via RADIUS com OTP para usuários de domínio e CAS-SSO (Single sign-on).

O uso de OAuth 2.0 em storages primários ainda é recente no mercado e está fortemente ligado à tendência de automatização por API e integração com plataformas de nuvem e orquestração. Atualmente, é visto que apenas a NetApp implementou a autenticação via OAuth 2.0 diretamente nas controladoras do storage para validação de tokens de acesso. 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

- 2.15.5. **Análise da Diligência:** A LICITANTE reconhece que não atende esta exigência do Termo de Referência. Ao contrário da afirmação de que "apenas a NetApp implementou a autenticação via OAuth 2.0", seguem exemplos de documentação de outros fabricantes de Storage que comprovam integração com *framework* Open Authorization (OAuth 2.0):

1. https://support.purestorage.com/bundle/m_microsoft_platform_guide/page/Solutions/Microsoft_Platform_Guide/a_Windows_PowerShell/library/common_content/
2. <https://blog.purestorage.com/purely-technical/pure1-rest-api-part-2/>
3. https://pubs.lenovo.com/storage-manager-9161/M_DCD3B74E-87EF-4B20-BE3E-F51EB866F3E8_v9.16.1.pdf
4. <https://storage-system.fujitsu.com/manual/en/axhx/authentication/overview-oauth2.html>

3. Tendo em vista as respostas aos pedidos de diligência e análise das mesmas apresentadas neste documento, para os itens do Termo de Referência em questão, conclui-se que a LICITANTE **não atendeu** completamente às exigências do Edital, em razão do descumprimento dos itens 2.1.80.8, 2.2.81.8, 2.1.81 e 2.2.82, 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.

4. Ante o exposto, encaminho processo para prosseguimento do certame licitatório.

Atenciosamente,

NELSON GONÇALVES REZENDE
Integrante Técnico

MARCO ANTONIO ROSA
Coordenador do Centro de Dados

De acordo. Encaminhe-se à Coordenação-Geral de Licitação e Contrato, conforme proposto.

WALTER LOPES NETO
Coordenador-Geral de Infraestrutura Tecnológica



Documento assinado eletronicamente por **Nelson Gonçalves Rezende, Integrante Técnico**, em 17/11/2025, às 12:29, 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 **Marco Antonio Rosa, Coordenador(a)**, em 17/11/2025, às 12:53, 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 **Walter Lopes Neto, Coordenador(a)-Geral**, em 17/11/2025, às 13:03, 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 **7135730** e o código CRC **BAE9AA7C** no site:
https://protocolo.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0