DMI - ESTUDO TÉCNICO PRELIMINAR - AMD 71/2023

Brasília, 13 de março de 2026.

1. DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS (ART. 12, INC. I)

1.1. Descrição geral da necessidade

Este Estudo Técnico Preliminar tem como objetivo avaliar os cenários e a viabilidade para assegurar a continuidade, atualização e evolução do sistema institucional de backup da Câmara Legislativa do Distrito Federal.

1.2. Motivação e Justificativa

1.2.1. A eventual indisponibilidade de sistemas corporativos produz impacto direto sobre a produtividade dos servidores e, consequentemente, sobre o desempenho institucional. Além disso, impactam também sobre os clientes externos, parceiros, e usuários do portal da CLDF na Internet, interessados nas informações e nos serviços direcionados aos órgãos públicos e à sociedade.

1.2.2. A disponibilidade das soluções, para ser garantida, necessita de suporte proativo e reativo a eventuais falhas. A DMI (Diretoria de Modernização e Informática) tem atuado continuamente e fortemente no cumprimento dessas determinações, por meio da renovação do parque computacional da Casa, investimentos em gerenciamento e segurança, aquisição de novos produtos, incorporação de novas tecnologias, entre outros. Em outras palavras, os serviços de infraestrutura são constantemente revistos e atualizados de forma a melhor espelhar os anseios e necessidades da Casa, em conformidade com as suas metas e objetivos propostos.

1.2.3. A DMI projeta soluções de alta disponibilidade por meio de técnicas e equipamentos com características para isso. Porém, sempre há a possibilidade de falhas com perda de dados.

1.2.4. A solução de backup realiza cópias de dados institucionais diariamente para, na ocorrência de uma falha com perda de dados, esses dados possam ser restaurados com o menor impacto possível para a Casa.

1.2.5. Assim, é necessário que a CLDF possua um sistema atualizado de cópias de segurança com os equipamentos devidamente dimensionados e com serviço de suporte de empresa especializada na solução.

1.2.6. Em 2020 a Câmara Legislativa celebrou contrato (0148628) de atualização e evolução do antigo sistema de backup de dados da CLDF, contando com equipamento, software e serviço de suporte pelo prazo de 60 meses. Esse contrato se encerra em 29/10/2025, deixando a Casa sem suporte e impossibilitada de atualizar os programas a partir dessa data.

1.2.7. Além de dispor de sistema atualizado e equipamentos dimensionados, a CLDF necessita do suporte de empresa especializada para assegurar a confiabilidade e a continuidade da solução.

1.2.8. Vale ressaltar que a melhor prática de mercado, em acordo com a NBR ISO/IEC 27002/2022, no seu item 8.13 (c) diz que o "*armazenamento de backup em um local remoto e seguro, a uma distância suficiente para escapar de qualquer dano causado por um desastre no local principal*". Essa melhor prática foi parcialmente incorporada na POSID, que menciona no art. 95, VIII, do Ato da Mesa Diretora Nº 125, de 2020, que é atribuição do administrador de backup "*armazenar as mídias de backup em cofre próprio, localizado em prédio diferente do local onde o backup é realizado.*". Esta incorporação parcial decorreu da dificuldade técnica em implantar completamente a boa prática da ISO ao tempo da escrita da POSID, quando serviços de nuvem pública não eram disseminados como atualmente. Hoje, percebe-se como viável a implantação completa da boa prática da referida norma técnica, e como um direcionador para as decisões desta contratação.

1.3. Previsão da contratação no Plano de Contratações Anual e alinhamento ao PDTI

1.3.1. O objeto desta contratação está alinhado com o Plano de Contratações Anual de Soluções de TI — PCA/STI — 2026 (2568729), Tabela I, item 6:

#	Solução de TI Unidade técnica Alinhamento Estratégico com o PEI Alinhamento Estratégico com o PDTI Prazo estimado (dias) para publicação do edital	Unidade técnica	Alinhamento Estratégico com o PEI	Alinhamento Estratégico com o PDTI	Prazo estimado (dias) para publicação do edital
6	Aquisição de itens relacionados a renovação e evolução do ecossistema de backup institucional e armazenamento em nuvem	SEINF	OE12 — Assegurar a estrutura física e de segurança pessoal e predial OE-TI-04 — Modernizar a Infraestrutura Digital para Garantir Resiliência 32	OE-TI-04 — Modernizar a Infraestrutura Digital para Garantir Resiliência	32

1.3.2. O objeto desta contratação está alinhado com o Detalhamento de Despesa Setorial - DSD:

ID	PROGRAMA DE TRABALHO	DESCRIÇÃO	ELEMENTO DE DESPESA	SEC/ UNIDADE	META	AÇÃO	DESCRIÇÃO DA DESPESA
318	01.126.8204.2557.2627	GESTÃO DA INFORMAÇÃO E DOS SISTEMA DE T.I. - CLDF	33.90.40 - Serviços de Tecnologia da Informação e Comunicação - Pessoa Jurídica	05 - GQS: DMI	14 - Contratos de Soluções de TI gerenciados e fiscalizados para garantia da conformidade.	14.03 - Executar contrato de solução de backup de dados da CLDF.	14.03.01 - Solução de backup de dados da CLDF.

1.3.3. O objeto desta contratação está alinhado com o Plano Diretor de Tecnologia da Informação – PDTI 2026-2027 da CLDF, conforme descrito abaixo:

1.3.3.1. Anexo A - Inventário de Necessidades de TI priorizado: A021 - Renovar e Evoluir o Ecossistema de Backup Institucional e Armazenamento em Nuvem.

1.3.3.2. Anexo B - Contratações de TI: B017 - Adquirir e/ou evoluir solução de backup e proteção de dados (appliance, mídias e serviços), com garantia e suporte.

OE12 — Assegurar a estrutura física e de segurança pessoal e predial (incl. estrutura de comunicação e tecnológica)			
OE-TI-04 — Modernizar a Infraestrutura Digital para Garantir Resiliência			
ID	Unidade Técnica	Necessidade	Classificação
B017	Setor de Infraestrutura da Informação - SEINF	A021 - Renovar e Evoluir o Ecossistema de Backup Institucional e Armazenamento em Nuvem.	Iniciativa Estruturante ou de Sustentação

1.4. Contratações correlatas e/ou interdependentes

1.4.1. O processo 00001-00028965/2023-33, que gerou o Contrato 20/2025 (2176139), trata da contratação de *SERVIÇOS ESPECIALIZADOS DE OPERAÇÃO, SUPORTE E SUSTENTAÇÃO À INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO DA CÂMARA LEGISLATIVA DO DISTRITO FEDERAL (CLDF), EM REGIME 24×7, E DE CENTRAL DE SERVIÇOS ORGANIZADA NO MODELO DE SERVICE DESK (N1, N2 E N3)* previu uma categoria chamada "Backup e Armazenamento de Dados".

1.4.1.1. O Anexo II do Termo de Referência da Contratação (2058879) descreve as qualificações dos profissionais de cada um dos perfis. O item 2.4 do Anexo apresenta as qualificações do perfil "Backup e Armazenamento de Dados", descrita abaixo:

> *2.4. Backup e de Armazenamento de Dados*
> *2.4.1. Suporte em Backups Sênior*
> *A equipe que comporá esta categoria ter ao menos um profissional com as seguintes certificações e qualificações:*
> *2.4.1.1. Certificações:*
> *a) AdministrationofVeritasNetBackup 8.0 ou superior;*
> *2.4.1.2. Capacitação:*
> *a) Windows Server 2019 ou superior - Carga-horária mínima de 20h; e*
> *b) Linux - Administração do Sistema - Carga-horária mínima de 20h.*
> *c) Armazenamento de objetos em padrão S3 – Carga-horária mínima de 30h*
> *d) ISO 22301 – Planos de continuidade de negócio – Carga horária mínima de 30h*
> *2.4.1.3. Conhecimentos:*
> *a) Possuir conhecimentos comprovados em planos de continuidade de negócio, backup e restauração;*
> *b) Possuir conhecimentos comprovados em uso de armazenamentos em formato S3;*
> *c) Possuir conhecimentos comprovados em administração de ambiente de backup baseado em Veritas NetBackup*

1.4.2. O Processo 00001-00038757/2024-23 trata da *AQUISIÇÃO DE INFRAESTRUTURA DE ARMAZENAMENTO DE DADOS,* o que poderá ampliar a demanda por backups na CLDF, em razão do aumento da capacidade de armazenamento e do consequente crescimento no uso desses recursos.

1.4.3. O Processo 00001-00021228/2022-29 trata do registro de preços destinado à futura contratação de serviços de implantação, adequação, certificação, expansão e manutenção de redes de cabeamento estruturado e fibras ópticas na CLDF. Essa iniciativa é fundamental para garantir que a infraestrutura de conectividade da Casa esteja preparada para suportar novos projetos estratégicos de TI, como a contratação do appliance de backup.

1.4.3.1. A solução de backup em análise depende diretamente da interligação por meio de cabeamento óptico de alta capacidade entre o appliance e os demais componentes críticos da infraestrutura tecnológica, como switches ToR, storages e o datacenter (CPD).

1.5. Necessidades de negócio

1.5.1. Continuidade dos serviços de TIC: Garantir que a execução de cópias de segurança ocorra de forma regular e confiável, assegurando a

disponibilidade de dados para restauração em caso de falhas, incidentes ou desastres.

1.5.2. Conformidade: Atender às normas e diretrizes institucionais, incluindo o planejamento estratégico da organização (PEI 2030 - Ato da Mesa Diretora nº 146 de 2022), o planejamento de TIC (PDTI-2024/2025 - Ato da Mesa Diretora nº 43 de 2024), a Política de Segurança da Informação Digital (POSID-CLDF - Ato da Mesa Diretora nº 125 de 2020), e as boas práticas da NBR ISO/IEC 27002/2022, de modo a assegurar práticas adequadas de armazenamento e recuperação de dados, inclusive:

1.5.2.1. Armazenamento de backup em um local remoto e seguro, a uma distância suficiente para escapar de qualquer dano causado por um desastre no local principal.

1.5.2.2. Capacidade de realização de backups full e diferencial-incremental.

1.5.3. Manutenção e sustentabilidade: Disponibilizar e manter atualizados os recursos de software e hardware de backup, assegurando suporte contínuo e capacidade de acompanhar a evolução da demanda de dados.

1.5.4. Garantia e suporte: Viabilizar contrato que contemple suporte integral ao sistema de backup e aos equipamentos associados, garantindo atendimento ágil e especializado durante todo o período de vigência.

1.5.5. Segurança e privacidade: Implementar mecanismos que assegurem a integridade e a confidencialidade das cópias de segurança, protegendo os dados institucionais contra acessos indevidos, vazamentos ou corrupção.

1.5.6. Eficiência operacional: Adotar solução de gerenciamento menos custoso e de operação simplificada, considerando que a equipe técnica disponível para administração é reduzida.

1.6. Necessidades tecnológicas

1.6.1. Alta disponibilidade: Assegurar que o sistema de backup opere com redundância e tolerância a falhas, garantindo a disponibilidade dos dados institucionais em caso de incidentes.

1.6.2. Mitigação de riscos relativos a mudança e migração: Reduzir riscos na transição contratual, seja na renovação do sistema atual, seja em eventual substituição, de modo a preservar cópias de segurança já existentes e evitar perda de dados históricos.

1.6.3. Gerenciamento e monitoração: Dispor de ferramentas que permitam acompanhar em tempo real o status das rotinas de backup, geração de alertas e relatórios de falhas, garantindo maior confiabilidade ao processo.

1.6.4. Escalabilidade e flexibilidade: Permitir a expansão da capacidade de armazenamento, acompanhando o crescimento do volume de dados da Casa.

1.6.5. Auditoria e controle: Disponibilizar mecanismos de rastreabilidade e registro de atividades de backup e restauração.

1.6.6. Atualização tecnológica: Garantir que a solução acompanhe a evolução do mercado, possibilitando a substituição modular de componentes e integração com soluções em nuvem.

1.7. Demais requisitos

1.7.1. Compatibilidade e integração: Assegurar que a solução de backup seja compatível com os sistemas, protocolos e plataformas já utilizados pela CLDF.

1.7.2. Níveis de serviço: Estabelecer SLAs que contemplem tempos de resposta adequados para falhas de backup, restauração de dados e atualizações do sistema.

1.7.3. Continuidade do negócio: Garantir que, em situações de falha ou indisponibilidade, as cópias de segurança possam ser restauradas no menor tempo possível, assegurando a operação dos serviços críticos.

1.7.4. Economicidade: Selecionar uma solução que preserve os investimentos já realizados, assegure a melhor relação custo-benefício e minimize custos operacionais com treinamento, migração, manutenção e operação.

2. ANÁLISE COMPARATIVA DAS SOLUÇÕES (ART. 12, INC. II)

2.1. **Cenário atual:** Para que possamos avaliar os cenários possíveis, é essencial compreender o cenário atual do sistema de backup institucional da CLDF.

2.1.1. **Sistema de backup:** O sistema de backup atual da CLDF é composto por um conjunto de software e hardware, conforme informações demonstradas abaixo:

Software	Veritas NetBackup
Hardware	Appliance Veritas 5250
	Biblioteca de fitas Oracle SL-150

Tabela 2.1 - Componentes do sistema de backup atual da CLDF

2.1.1.1. Situação do Software de backup

2.1.1.1.1. A solução de backup institucional da CLDF é implementada com a suíte Veritas NetBackup, atualmente na versão 10.5.0.1, adquirida em 2019. Essa versão está em conformidade com os requisitos operacionais da instituição e possui suporte técnico ativo, com ciclo de vida estendido até 2030, conforme informações do fabricante.

2.1.1.1.2. Na contratação anterior, o licenciamento foi obtido na modalidade baseada em sockets, modelo posteriormente descontinuado pelo fabricante. Esse formato implicava custos adicionais para cada componente, o que restringia a escalabilidade e dificultava a adoção de novas tecnologias.

2.1.1.1.3. Atualmente, o modelo de licenciamento do NetBackup é baseado na capacidade em terabytes de front-end, conforme documentação oficial da Veritas. Em eventual cenário de renovação, a CLDF poderá migrar para esse novo formato, aproveitando os investimentos já realizados e com possibilidade de desconto no valor final.

2.1.1.1.4. A suíte oferece recursos como políticas de backup, recuperação granular, suporte a múltiplas plataformas e integração com mídias de armazenamento em disco e fita. O suporte técnico disponibilizado pelo fabricante tem sido utilizado pela instituição e, até o momento, tem atendido

de forma satisfatória.

2.1.1.2. **Situação do Appliance de backup**

2.1.1.2.1. O arranjo atualmente adotado pela CLDF para a realização das rotinas de backup é estruturado em torno do Appliance Veritas 5250, solução de armazenamento dedicada a esse tipo de operação. A instalação física e a configuração inicial desse equipamento ocorreram em setembro de 2020, estando devidamente registradas e documentadas no Relatório 0241189, que descreve as especificações técnicas e as condições em que o ambiente foi implementado.

2.1.1.2.2. O appliance em questão dispõe de 9 TB de capacidade de armazenamento embarcada diretamente na controladora, recurso fundamental para garantir a disponibilidade imediata de espaço para gravações, restaurações rápidas e execução de políticas críticas de backup. Essa capacidade nativa é complementada por uma expansão externa representada por um Storage Shelf, unidade dedicada a ampliar a volumetria útil e assegurar maior flexibilidade na alocação de dados.

2.1.1.2.3. Esse Storage Shelf adicional oferece pouco mais de 65 TB de capacidade bruta, distribuídos em um conjunto de 12 discos rígidos de 8 TB cada. Entre esses discos, um foi designado como Hot Spare, ou seja, permanece em estado de espera para assumir automaticamente o lugar de qualquer disco que venha a falhar, elevando de forma significativa a resiliência da solução e reduzindo o risco de indisponibilidade em caso de problemas físicos com a mídia.

2.1.1.2.4. Todos os discos estão organizados em uma matriz de RAID 6, configuração que utiliza dois discos para armazenamento das informações de paridade, permitindo que até duas falhas simultâneas de disco ocorram sem perda de dados. Essa escolha arquitetural equilibra desempenho, capacidade e segurança, tornando o ambiente mais confiável para o armazenamento de informações institucionais críticas.

2.1.1.2.5. Em síntese, o ambiente de backup da CLDF encontra-se estruturado em um arranjo robusto, que combina a capacidade imediata do appliance Veritas 5250 com a escalabilidade e a redundância proporcionadas pelo Storage Shelf, garantindo tanto volume adequado para as demandas atuais quanto segurança frente a falhas de hardware.

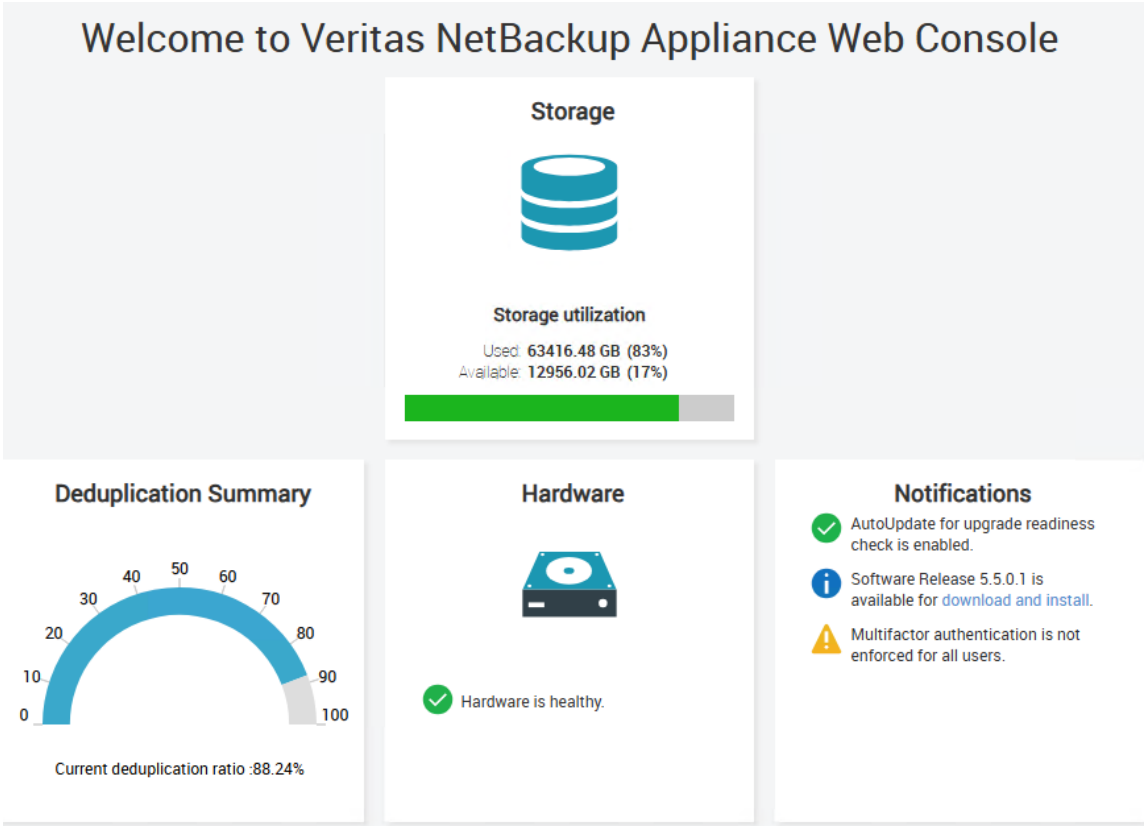


Imagem 2.1 - Tela inicial do Appliace Veritas

Figure: Veritas 5250 Appliance front panel disk slot assignments

Table: Veritas 5250 Appliance front panel disk drive configurations

Slot	RAID Configuration	Disk drive size	Disk drive role
0, 1	RAID 1	1TB	Boot / swap
2, 3	RAID 1	1TB	Log files
4 - 10	RAID 6	2TB (Available internal storage is 9.1TiB) 8TB (Available internal storage is 36.4TiB)	User data
11	RAID 6		Hot-spare

Imagem 2.2 - Configuração dos Drives

```
Hardware monitor information
+----------------+--------------+-------------+
| Name           | Manufacturer | Serial      |
+----------------+--------------+-------------+
| NetBackup 5250 | Veritas      | VTAS0017157 |
+----------------+--------------+-------------+

Hardware monitor information
+--------------------------+--------------+------------------+
| Name                     | Manufacturer | Serial No.       |
+--------------------------+--------------+------------------+
| NetBackup StorageShelf 1 | Veritas      | SHT1012651GEK2L  |
+--------------------------+--------------+------------------+
```

Imagem 2.3 - Informações do hardware

Imagem 2.4 - Equipamento instalado no rack

Imagem 2.5 - Equipamento instalado no rack

2.1.1.2.6. O Appliance Veritas 5250 foi devidamente integrado à infraestrutura de rede da CLDF por meio de sua conexão com a rede de armazenamento (SAN), estabelecendo comunicação direta com as datastores do ambiente VMware. Essa configuração permite que os backups das máquinas virtuais (VMs) hospedadas nesse ambiente sejam realizados utilizando a própria rede SAN, dispensando a necessidade de tráfego intensivo de dados pela rede LAN convencional. Como resultado, o tempo de execução das rotinas de backup é significativamente otimizado, garantindo maior

desempenho, menor impacto sobre a rede de produção e maior confiabilidade no processo de cópia.

2.1.1.2.7. Para viabilizar essa integração de alto desempenho, foram disponibilizados e instalados quatro GBICs, destinados a permitir a conexão do appliance aos switches ToR (topo de rack) por meio de links de fibra óptica de 10 Gbps. A escolha da fibra óptica, em detrimento de conexões elétricas convencionais, se justifica pela elevada largura de banda, baixa latência e imunidade a interferências eletromagnéticas, características essenciais em ambientes críticos de datacenter.

2.1.1.2.8. Dentre os quatro módulos GBIC fornecidos, dois foram instalados diretamente nas interfaces físicas eth7 e eth9 do Appliance, de modo a habilitar canais de comunicação dedicados. Os outros dois módulos foram instalados nas portas correspondentes dos switches ToR anteriores, estabelecendo, assim, o caminho físico da interconexão. Essa topologia permitiu que as interfaces eth7 e eth9 fossem agrupadas (bonded) em uma configuração lógica única, sob um mesmo endereço IP, por meio da utilização do protocolo LACP (Link Aggregation Control Protocol – IEEE 802.3ad).

2.1.1.2.9. Esse arranjo de agregação traz benefícios expressivos: além de balancear o tráfego de rede de forma inteligente entre as duas interfaces, distribuindo as cargas de comunicação, também agrega tolerância a falhas. Caso uma das interfaces ou caminhos físicos venha a apresentar problemas, a outra permanece operacional, assegurando a continuidade da conectividade e evitando pontos únicos de falha. Dessa forma, a rede LAN pode ser utilizada de forma mais eficiente, permitindo que tanto os backups quanto outras rotinas administrativas dependentes de comunicação em rede mantenham-se estáveis.

2.1.1.2.10. Todo o processo de identificação dos cabos ópticos, interfaces físicas do appliance e respectivas portas de switch, bem como o mapeamento detalhado das conexões, foi registrado e encontra-se documentado em diagrama específico, apresentado a seguir. Esse mapeamento cumpre não apenas uma função técnica, mas também de governança e rastreabilidade, facilitando futuras manutenções, expansões ou substituições de componentes de rede.

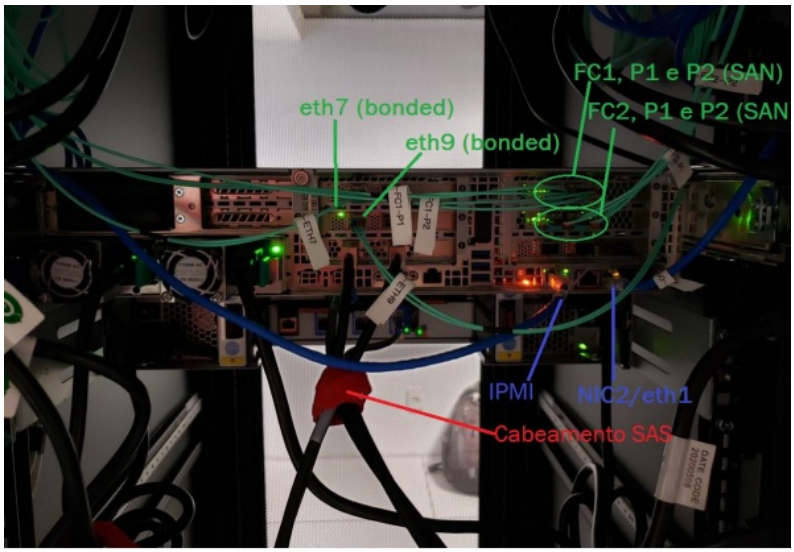


Imagem 2.6 - Interfaces utilizadas no switch SAN

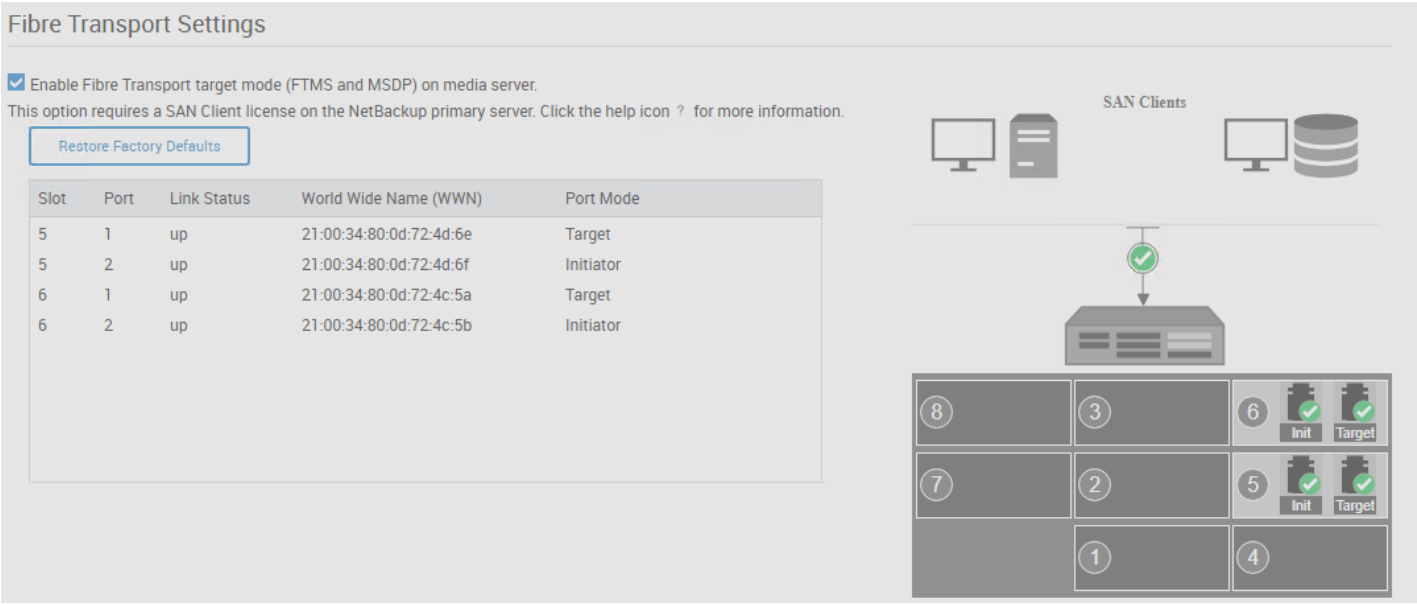
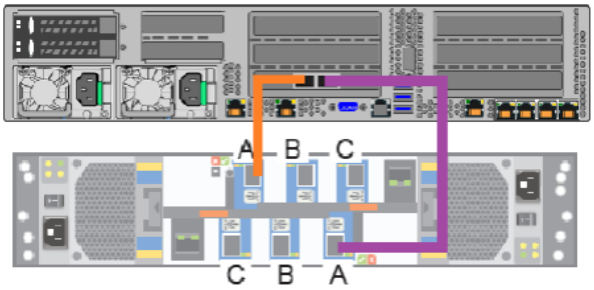


Imagem 2.7 - Portas utilizadas

2.1.1.2.11. A conexão do cabeamento SAS referente à Storage Shelf está representada na imagem 2.8:



2.8 - Esquema de cabeamento do Storage Shelf

2.1.1.3. **Situação da biblioteca de fitas**

2.1.1.3.1. A biblioteca de fitas atualmente em operação na CLDF é a Oracle StorageTek SL150 Modular Tape Library, equipada com tecnologia LTO-5, a qual já é considerada obsoleta no mercado de armazenamento de dados. O sistema possui ainda 2 portas RJ-45 IPv4 dedicadas ao monitoramento, possibilitando a administração e o acompanhamento remoto de seu funcionamento.

2.1.1.3.2. Embora a solução ainda esteja amparada por contrato de manutenção vigente (Contrato 8/2023, Processo 00001-00044045/2022-81), o referido contrato tem término previsto para 29 de setembro de 2026, coincidindo com o fim do suporte do fabricante.

2.1.1.3.3. **Informações técnicas da biblioteca de fitas:**

2.1.1.3.3.1. Support Identifier (Oracle): 19434771 – Câmara Legislativa do Distrito Federal

2.1.1.3.3.2. Suporte do fabricante até: 29/09/2026

2.1.1.3.3.3. Marca: Oracle

2.1.1.3.3.4. Modelo: StorageTek SL150 Modular Tape Library (model family)

2.1.1.3.3.5. Número de série: 464970G+1409SY2214

2.1.1.3.3.6. Capacidade de mídias: 10 gavetas com 15 fitas LTO-5 cada, totalizando 150 fitas

2.1.1.3.3.7. Drives instalados: 6 unidades LTO-5

Drive	Type	Serial Number	Firmware Version	Interface	Port speed	WWNN
Module 1 Top Drive	HP LTO 5	HU14030V1G	Y5BS	Fibre	8 Gb/s	500104f000d2238b
Module 1 Bottom Drive	HP LTO 5	MXP50904E7	Y68S	Fibre	8 Gb/s	500104f000d2238e
Module 3 Top Drive	HP LTO 5	HUL7419CA8	Y6IS	Fibre	8 Gb/s	500104f000d22397
Module 3 Bottom Drive	HP LTO 5	HU13510GW9	Y5BS	Fibre	8 Gb/s	500104f000d2239a
Module 5 Top Drive	HP LTO 5	HU14030V4K	Y5BS	Fibre	8 Gb/s	500104f000d223a3
Module 5 Bottom Drive	HP LTO 5	HUL71183M5	Y6KS	Fibre	8 Gb/s	500104f000d223a6

Tabela 2.2 - Dados da biblioteca de fitas

2.1.1.3.4. Dada a descontinuação do equipamento, substituído em 2012 pelo modelo SL500, recomenda-se o planejamento para retirada do equipamento de produção ao final da vigência contratual em 2026. Essa medida visa mitigar riscos operacionais e garantir a continuidade dos serviços de backup com soluções mais modernas e sustentáveis.

2.1.2. **Volume de dados**

2.1.2.1. Atualmente, são gerados aproximadamente 11,15 TB de dados por dia nas rotinas de backup da CLDF. Desse total, cerca de 46% são armazenados em fitas magnéticas, enquanto o restante é direcionado ao Appliance de backup. Isso representa um consumo médio diário de 5,14 TB em fitas e 6,01 TB no Appliance.

2.1.2.2. Como essas cópias possuem prazos de retenção definidos, à medida que novas cópias são geradas diariamente, as mais antigas expiram, liberando espaço de armazenamento.

2.1.2.3. **Volumes por faixa de retenção**

Categoria	Tempo de retenção	Volume	Tipo de armazenamento	Total
Dados históricos	1 a 5 anos	366 TB	Fitas magnéticas	366 TB
Dados recentes	< 1 ano	464 TB	Fitas magnéticas	1114 TB
		650 TB[1]	Appliance backup	

Tabela 2.3 - Volumes por faixa de retenção

[1] 650TB brutos. Considerando uma taxa de deduplicação de 10:1, volume corresponde a aproximadamente 65TB líquidos

2.2. **Necessidades similares em outros órgãos ou entidades da administração pública**

2.2.1. A criação e a manutenção de cópias de segurança de dados constituem uma das principais boas práticas no campo da Segurança da Informação. Nesse sentido, é possível afirmar que a maior parte dos órgãos e entidades, tanto públicos quanto privados, adota medidas voltadas à preservação de seus dados por meio da geração e do armazenamento de backups.

2.2.2. Em decorrência disso, o mercado oferece uma ampla variedade de soluções especializadas, permitindo que cada instituição selecione a alternativa mais adequada às suas necessidades específicas.

2.2.3. Apresenta-se, na tabela 2.4 a seguir, a relação de órgãos e entidades da Administração Pública que já contrataram soluções semelhantes à pretendida por este órgão:

UASG	Órgão	Pregão Eletrônico nº
200009	MPDFT	100/2011
987427	MUNICÍPIO DE ARAPONGAS	153/2023
383500	CONSELHO FEDERAL DE CONTABILIDADE	1/2021
160163	COMANDO DA 8ª REGIÃO MILITAR	7/2016
370001	CGU	1/2020
80010	TRT 2ª REGIÃO	90026/2024
943001	GOVERNO DO ESTADO DO CEARÁ	90893/2024
200247	ARQUIVO NACIONAL	90011/2024
80025	TRT 23ª REGIÃO	16/2025
927045	TCE/AP	90007/2025
925624	FUNPEC	90001/2025
989221	PREFEITURA DE ANÁPOLIS	28/2019
389325	COREN-DF	4/2021
925989	DPE/PA	1/2023
390004	MINISTÉRIO DA INFRAESTRUTURA	90007/2025
344002	PRESIDÊNCIA/FUNDAJ	96401/2025
70011	TRE/AL	25/2022
113205	CNEN - NUCLEAR	10231/2022
154034	UNIRIO	31/2022
927312	SEBRAE	5/2024
985847	PREFEITURA DE MACAÉ	90047/2025
113205	CNEN - NUCLEAR	9/2022
167163	COMANDO 8ª REGIÃO MILITAR	25/2023
201057	ME (Ministério da Economia)	2/2022
927045	TCE/AP	90019/2024

Tabela 2.4 - Contratações similares

2.3. Cenários possíveis para contratação

2.3.1. Visando melhor detalhar a viabilidade dos cenários, dividiu-se o escopo da necessidade em 3 componentes, para se avaliar cenários viáveis para cada componente separadamente, entendendo-se que a contratação deva abranger os cenários viáveis de cada um dos componentes, cumulativamente.

2.3.2. Conhecendo o cenário atual, apresentado na seção 2.1, é possível determinar cenários possíveis para a renovação do sistema de backup institucional da CLDF. Uma vez que o sistema contém vários componentes, os cenários de cada um devem ser considerados individualmente.

Componente	Cenários
(1) Software de catálogo de backup	(a) Manutenção do software atual
	(b) Mudança para outro software com manutenção do sistema anterior apenas para leitura das cópias antigas
	(c) Mudança para outro software com migração das cópias antigas
(2) Equipamento para processamento do backup e armazenamento de backups de recuperação com alta probabilidade	(a) Aquisição de Appliance do mesmo fabricante do atual
	(b) Aquisição de Appliance de outro fabricante
(3) Armazenamento de backups de longa duração e de recuperação com baixa probabilidade	(a) Outra biblioteca de fitas
	(b) Espaço em nuvem
	(c) Equipamento de armazenamento S3 *on premises*
(4) Todos	(a) Não renovação do sistema atual de backup

Tabela 2.5 - Cenários possíveis por componente do sistema de backup

2.3.3. Descrição sucinta de cada componente da tabela 2.5:

2.3.3.1. (1) Software de Catálogo de Backup

2.3.3.1.1. 1.a – Manutenção do software atual: refere-se à continuidade do uso do sistema de catálogo de backup atualmente em operação, o que seria equivalente à renovação do contrato vigente.

2.3.3.1.2. 1.b – Migração para novo software, mantendo o sistema atual apenas para leitura: consiste na aquisição de um novo sistema de backup, que será utilizado para a realização de novas cópias. O sistema atual seria mantido exclusivamente para a restauração de backups antigos.

2.3.3.1.3. 1.c – Migração para novo software com conversão das cópias antigas: envolve a adoção de um novo sistema de backup, que será responsável pelas novas cópias. Como o novo sistema não é compatível com os backups gerados pelo software anterior, seria necessária a migração de todas as cópias antigas para o novo ambiente.

2.3.3.2. (2) Equipamento para Processamento e Armazenamento de Backups de Recuperação com Alta Probabilidade

2.3.3.2.1. 2.a – Aquisição de appliance do mesmo fabricante: considerando que a expansão do appliance Veritas 5250 atualmente em uso na CLDF é inviável, a necessidade de ampliação da capacidade pode ser atendida com a aquisição de um novo appliance do mesmo fabricante.

2.3.3.2.1.1. É importante destacar que junto da aquisição de appliance do mesmo fabricante, visando fazer um uso eficiente do recurso, vem acompanhado o serviço de migração de catálogo de backup, que consiste em migrar a infraestrutura de orquestração (componente master) do

ambiente virtualizado onde atualmente se encontra implantado para estar integrado ao equipamento appliance do fabricante.

2.3.3.2.1.2. Vale ressaltar que a aquisição deste appliance deve vir acompanhada de cabeamento necessário à sua instalação.

2.3.3.2.2. 2.b – Aquisição de appliance de outro fabricante: alternativamente, a expansão da capacidade de armazenamento on-premises pode ser realizada por meio da aquisição de um equipamento de outro fornecedor.

2.3.3.2.2.1. Vale ressaltar que a aquisição deste appliance deve vir acompanhada de cabeamento necessário à sua instalação.

2.3.3.3. (3) Armazenamento de Backups de Longa Duração e de Recuperação com Baixa Probabilidade

2.3.3.3.1. 3.a – Nova biblioteca de fitas: manutenção da estratégia atual de armazenamento em fitas, com a substituição da biblioteca existente por um novo equipamento similar.

2.3.3.3.1.1. Vale ressaltar que a aquisição deste equipamento deve vir acompanhada de cabeamento necessário à sua instalação.

2.3.3.3.2. 3.b – Armazenamento em nuvem: utilização de serviços de nuvem para prover o armazenamento de longo prazo e de baixa frequência de recuperação, com movimentação das imagens constantes das fitas atuais para o novo ambiente.

2.3.3.3.3. 3.c – Equipamento de armazenamento S3 on-premises: aquisição de um equipamento de armazenamento de grande capacidade, com tecnologia compatível com o protocolo S3, normalmente utilizado em ambientes de nuvem, mas instalado localmente.

2.3.3.3.3.1. Vale ressaltar que a aquisição deste equipamento deve vir acompanhada de cabeamento necessário à sua instalação.

3. ANÁLISE COMPARATIVA DE VIABILIDADE

3.1. Software de catálogo de backup

3.1.1. A seguir, apresenta-se a tabela 3.1 com os cenários avaliados para o componente de software de backup, indicando a viabilidade ou não de cada opção em relação aos requisitos de negócio, tecnológicos e demais requisitos estabelecidos.

Requisitos		Cenários		
		(1.a) Manutenção do software atual	(1.b) Mudança para outro sistema com manutenção do sistema anterior apenas para leitura das cópias antigas	(1.c) Mudança para outro sistema com migração das cópias antigas
Negócio	Continuidade dos serviços de TIC	Atende	Atende	Atende
	Conformidade	Atende	Atende	Atende
	Manutenção e sustentabilidade	Atende	Atende	Atende
	Garantia e suporte	Atende	Atende	Atende
	Segurança e privacidade	Atende	Atende	Atende
	Eficiência operacional	Atende	Não atende	Não atende
Tecnológico	Alta disponibilidade	Atende	Atende	Atende
	Mitigação de riscos relativos a mudança e migração	Atende	Não atende	Não atende
	Gerenciamento e monitoração	Atende	Atende	Atende
	Escalabilidade e flexibilidade	Atende	Atende	Atende
	Auditoria e controle	Atende	Atende	Atende
	Atualização tecnológica	Atende	Atende	Atende
Demais requisitos	Compatibilidade e integração	Atende	Atende	Atende
	Níveis de serviço	Atende	Atende	Atende
	Manutenção e sustentabilidade	Atende	Atende	Atende
	Continuidade do negócio	Atende	Atende	Atende
	Economicidade	Atende	Não atende	Não atende
Resultado da análise		Viável	Inviável	Inviável

Tabela 3.1 - Cenários possíveis do componente de software de catálogo de backup

3.2. Equipamento para processamento do backup e armazenamento de backups de recuperação com alta probabilidade

3.2.1. A seguir, apresenta-se a tabela 3.2 com os cenários avaliados para o Appliance de backup, indicando a viabilidade ou não de cada opção em relação aos requisitos de negócio, tecnológicos e demais requisitos estabelecidos.

Requisitos		Cenários	
		(2.a) Aquisição de Appliance do mesmo fabricante do atual	(2.b) Aquisição de Appliance de outro fabricante
Negócio	Continuidade dos serviços de TIC	Atende	Atende
	Conformidade	Atende	Atende
	Manutenção e sustentabilidade	Atende	Atende
	Garantia e suporte	Atende	Atende
	Segurança e privacidade	Atende	Atende
	Eficiência operacional	Atende	Não atende
Tecnológico	Alta disponibilidade	Atende	Atende
	Mitigação de riscos relativos a mudança e migração	Atende	Não atende

	Gerenciamento e monitoração	Atende	Atende
	Escalabilidade e flexibilidade	Atende	Atende
	Auditoria e controle	Atende	Atende
	Atualização tecnológica	Atende	Atende
Demais requisitos	Compatibilidade e integração	Atende	Atende
	Níveis de serviço	Atende	Atende
	Manutenção e sustentabilidade	Atende	Atende
	Continuidade do negócio	Atende	Atende
	Economicidade	Atende	Atende
Resultado da análise		Viável	Inviável

Tabela 3.2 - Cenários possíveis do componente appliance de backup

3.3. **Armazenamento de backups de longa duração e de recuperação com baixa probabilidade**

3.3.1. A seguir, apresenta-se a tabela 3.3 com os cenários avaliados para o armazenmaneto de longa duração, indicando a viabilidade ou não de cada opção em relação aos requisitos de negócio, tecnológicos e demais requisitos estabelecidos.

Requisitos		Cenários		
		(3.a) Outra biblioteca de fitas	(3.b) Espaço em nuvem	(3.c) Equipamento de armazenamento S3
Negócio	Continuidade dos serviços de TIC	Atende	Atende	Atende
	Armazenamento de backup em um local remoto e seguro, a uma distância suficiente para escapar de qualquer dano causado por um desastre no local principal.	Não atende	Atende	Não atende
	Capacidade de realização de backups full e diferencial-incremental.	Atende	Atende	Atende
	Manutenção e sustentabilidade	Atende	Atende	Atende
	Garantia e suporte	Atende	Atende	Atende
	Segurança e privacidade	Atende	Atende	Atende
	Eficiência operacional	Não atende	Atende	Atende
Tecnológico	Alta disponibilidade	Atende	Atende	Atende
	Mitigação de riscos relativos a mudança e migração	Atende	Atende	Não atende
	Gerenciamento e monitoração	Atende	Atende	Atende
	Escalabilidade e flexibilidade	Atende	Atende	Atende
	Auditoria e controle	Atende	Atende	Atende
	Atualização tecnológica	Não atende	Atende	Atende
Demais requisitos	Compatibilidade e integração	Atende	Atende	Atende
	Níveis de serviço	Atende	Atende	Atende
	Manutenção e sustentabilidade	Atende	Atende	Atende
	Continuidade do negócio	Atende	Atende	Atende
	Economicidade	Atende	Atende	Atende
Resultado da análise		Inviável	Viável	Inviável

Tabela 3.3 - Cenários possíveis do componente biblioteca de fitas

3.4. **Não renovação do sistema atual de backup**

3.4.1. A hipótese de não renovar nenhuma solução de backup, seja software ou hardware, mostra-se inviável para a CLDF. Tal opção significaria abrir mão da proteção de dados institucionais, expondo a Casa a riscos críticos de indisponibilidade, perda de informações e descumprimento de normativos internos e legais. Além de colocar em risco a continuidade das atividades administrativas e legislativas, essa alternativa acarretaria sérias consequências à imagem institucional perante a sociedade.

3.4.1.1. Interrupção de backups: a CLDF ficaria sem execução regular de cópias de segurança, expondo sistemas e dados a falhas, incidentes ou ataques.

3.4.1.2. Perda de suporte técnico: o NetBackup ficaria sem manutenção oficial a partir de 29/10/2025, sem correções de falhas ou atualizações de segurança.

3.4.1.3. Infraestrutura obsoleta: Appliance em uso próximo do limite e sem possibilidade de expansão e biblioteca de fitas baseada em tecnologia LTO-5, ultrapassada e sem garantia de continuidade.

3.4.1.4. Impacto institucional: indisponibilidade de sistemas afetaria diretamente a produtividade dos servidores, os serviços prestados à

sociedade e a imagem da Casa.

3.4.1.5. Descumprimento de normativos: ausência de backup fere a Política de Segurança da Informação Digital (POSID-CLDF), o PDTI e as boas práticas de mercado.

4. CENÁRIOS VIÁVEIS

Como pode ser observado nas seções 2.2.1, 2.2.2, 2.2.3 e 2.2.4, os cenários viáveis que atendem aos requisitos de negócio, tecnológicos e demais são os seguintes:

Componente	Cenário viável
Software de catálogo de backup	Manutenção do sistema atual (Netbackup)
Equipamento para processamento do backup e armazenamento de backups de recuperação com alta probabilidade	Aquisição de Appliance do mesmo fabricante do atual
Armazenamento de backups de longa duração e de recuperação com baixa probabilidade	Aquisição de espaço em nuvem

Tabela 4.1 - Cenários viáveis por componente

4.1. Nota-se que somente foi encontrado um cenário viável para cada componente, e a combinação cumulativa desses forma o único cenário viável para a contratação como um todo.

4.2. Para o software Veritas NetBackup, as alternativas avaliadas em substituição ao sistema atual apresentaram elevado grau de inviabilidade técnica, operacional e financeira, o que compromete sua adoção. Diante desse cenário, recomenda-se fortemente a continuidade da solução NetBackup, com a devida renovação contratual, como medida estratégica para assegurar a proteção, integridade e disponibilidade dos dados institucionais, preservando a estabilidade e a eficiência dos processos críticos da organização.

4.3. Sobre o Appliance, reforça-se a orientação da necessidade de padronização dos equipamentos de backup. Recomenda-se, após análise, a aquisição de um novo Appliance da mesma fabricante, como medida alinhada às melhores práticas de segurança, desempenho e continuidade operacional.

4.4. Por fim, sobre o armazenamento de longa duração, as alternativas analisadas demonstram capacidade para substituir a biblioteca de fitas em sua função principal de armazenamento de cópias de segurança históricas. A opção de armazenamento em nuvem se sobressai como a solução mais adequada, especialmente pelos ganhos em conformidade e segurança. Essa alternativa está mais alinhada às diretrizes estabelecidas pela Política de Segurança da Informação Digital (POSID-CLDF) da CLDF, ao permitir o armazenamento fora das dependências físicas da Casa, agregando maior resiliência à infraestrutura de backup. Ressalta-se que a efetividade dessa solução dependerá da escolha de um serviço que atenda às limitações técnicas e operacionais da estrutura atual da CLDF, garantindo compatibilidade, escalabilidade e segurança no longo prazo.

4.5. Vale ressaltar que eficácia das imagens de backup depende da capacidade de que elas sejam restauradas. A sua restauração depende necessariamente de um componente leitor da fita, no caso, a fitoteca. A fitoteca presente na CLDF encontra-se com iminente fim de vida. Além disso, vale ressaltar que são cada vez mais raras no mercado fitotecas compatíveis com fitas LTO-5, dada a obsolescência desta geração de fitas, combinado com a decrescente demanda de mercado por fitotecas de pequeno porte, frente às novas soluções existentes (especialmente em nuvem). Neste sentido, a manutenção das fitas além do prazo de vigência do contrato de suporte da fitoteca representa um cenário de risco indesejado, motivo pelo qual entende-se tecnicamente recomendável que seja realizada movimentação desses dados para o armazenamento em nuvem contratado, e que esta atividade seja realizada ainda durante a vigência da garantia da fitoteca.

4.6. **Compatibilidade dos sistemas com o armazenamento em nuvem**

4.7. O armazenamento de backups em nuvem enfrenta algumas restrições relevantes no contexto da CLDF. A primeira está relacionada à exigência legal de que os dados sejam armazenados em território nacional, conforme estabelecido no Parecer-PG nº 108/2023 (1094802). A segunda limitação decorre das especificidades técnicas do sistema de armazenamento utilizado pela DICOM, conforme informado no documento 2165820. A terceira diz respeito à compatibilidade de armazenamento de objetos dos sistemas institucionais da CLDF.

4.8. Para facilitar a identificação e visualização das restrições, os dados foram consolidados na tabela 4.2, que considera os principais provedores de nuvem pública.

Serviço de nuvem	Possui região Brasil	NetBackup	TV Legislativa (2165820)	Armazenamento de objetos
AWS	Sim	Compatível	Compatível	Compatível
Blackblaze	Não	Compatível	Compatível	Compatível
Dropbox	Não	Não compatível	Compatível	Não compatível
Google Cloud Storage	Sim	Compatível	Compatível	Compatível
IBM	Sim	Compatível	Não compatível	Compatível
IDrive	Não	Compatível	Não compatível	Compatível
Impossible Cloud	Não	Compatível	Não compatível	Compatível
Microsoft Azure Blob Storage	Sim	Compatível	Não compatível	Não compatível
OCI	Sim	Compatível	Não compatível	Compatível
Scality	Não	Compatível	Não compatível	Compatível
Veritas	Sim	Compatível	Não compatível	Não compatível

Tabela 4.2 - Matriz de compatibilidade dos serviços de nuvem

4.9. Com base na matriz acima, podemos identificar que apenas as soluções AWS e Google Cloud Storage atendem simultaneamente a todos os requisitos de compatibilidade exigidos pela CLDF, incluindo:

4.9.1. Presença de região de armazenamento no Brasil

4.9.2. Compatibilidade com a solução de backup utilizada (NetBackup)

4.9.3. Atendimento às demandas da TV Legislativa

4.9.4. Suporte a aplicações que utilizam armazenamento de objetos (API baseada em S3)

4.10. O Relatório Conformidade LGPD e normativos (2568648) detalha minunciosamente como a solução de armazenamento em nuvem encontra-se conforme os normativos aplicáveis da POSID e LGPD.

5. SOLUÇÕES CONSIDERADAS INVIÁVEIS

5.1. Justificativa do não atendimento dos cenários inviáveis:

5.2. **Software de catálogo de backup**

5.2.1. Cenário 1.b: **Mudança para outro sistema com manutenção do sistema anterior apenas para leitura das cópias antigas** não é viável, pois:

5.2.1.1. A não manutenção do serviço de suporte do sistema anterior cria um risco de não capacidade de restauração de um backup que esteja no sistema anterior, pois caso haja uma falha no sistema anterior, a equipe técnica da CLDF não teria as condições de resolver a falha, por não ter o alto grau de especialidade do fabricante, bem como não ter acesso a alterar os sistemas envolvidos, no caso de algum bug de software, bem como de restaurar um componente de hardware defeituoso;

5.2.1.2. Pelo motivo acima, seria de alto risco manter backups armazenados unicamente em um ambiente não suportado, que iria em sentido contrário à diretriz do Ato da Mesa Diretora Nº 143, de 2022, que menciona que "*O perfil de risco da CLDF é conservador, possuindo baixo apetite para todos os tipos de risco. Ter baixo apetite ao risco significa que, de maneira geral, a CLDF não está disposta a assumir riscos médios, altos ou extremos.*";

5.2.1.3. No caso do cenário de se manter licenciados paralelamente dois sistemas de backup com serviço de suporte simultâneo, trata-se de alternativa antieconômica, pois incorreria no custo combinado dos cenários 1.a e do novo licenciamento e suporte;

5.2.1.4. Por outro lado, a possibilidade de manutenção de um sistema legado apenas para leitura sem suporte ativo representa um risco adicional em termos de segurança da informação, uma vez que sistemas sem atualizações de segurança tornam-se progressivamente mais vulneráveis a falhas e incidentes de cibersegurança. A impossibilidade de aplicação de patches de segurança e a indisponibilidade de correções por parte do fabricante deixam o ambiente suscetível a ataques explorando vulnerabilidades conhecidas. Tal cenário seria incompatível com os princípios estabelecidos nas normas ISO/IEC 27001 e 27002, que exigem o tratamento contínuo de riscos e a manutenção de controles atualizado.

5.2.1.5. Tendo-se em vista que a equipe do setor responsável por administrar os backups é reduzida, o nível de complexidade de manter dois ambientes distintos é por si só um fator de risco elevado, pois a complexidade seria multiplicada, diminuindo o nível de especialidade da equipe técnica responsável, que não poderia se focar em uma única solução em um ambiente tão crítico.

5.2.2. Cenário 1.c: **Mudança para outro sistema com migração das cópias antigas** não é viável, pois:

5.2.2.1. Não há um método de migração direta do catálogo de imagens do sistema atual para um novo sistema;

5.2.2.2. Assim a migração dependeria da restauração manual de cada imagem de backup - armazenada em fitas ou no appliance - para um meio de armazenamento intermediário. Em seguida, seria necessário realizar um novo processo de backup dessas imagens no sistema de destino;

5.2.2.3. Uma "imagem" refere-se a um conjunto de dados que pode representar um servidor completo, uma pasta específica, um banco de dados ou qualquer outro agrupamento de informações previamente armazenadas em backup;

5.2.2.4. Atualmente, o sistema de backup da CLDF possui 4.124 imagens armazenadas, abrangendo o período de 2014 até os dias atuais, assim a migração de todas essa imagens para um novo sistema acarretaria um alto custo operacional;

5.2.2.5. Durante o processo de migração das imagens, haveria a convivência simultânea de dois sistemas. A operacionalização dessa situação - incluindo os procedimentos de migração, a realização de novas cópias de segurança no novo sistema e a restauração de imagens em ambos os ambientes - seria complexa e suscetível a falhas. Qualquer erro nesse processo poderia resultar na perda de dados;

5.2.2.6. Durante o processo de migração das imagens, dois sistemas de backup precisariam operar simultaneamente. Manter ambos licenciados com suporte técnico ativo representa uma alternativa antieconômica, pois implicaria na soma dos custos do cenário 1.a (manutenção do sistema atual) com os custos de licenciamento e suporte do novo sistema. Além disso, a migração das imagens é um processo extenso e complexo, que exigiria a contratação de uma empresa especializada, considerando as limitações de pessoal da DMI. Essa necessidade tornaria o processo de atualização da tecnologia de backup significativamente mais oneroso para a Casa.

5.3. **Equipamento para processamento do backup e armazenamento de backups de recuperação com alta probabilidade**

5.3.1. Cenário 2.b: **Aquisição de Appliance de outro fabricante** não é viável, pois:

5.3.1.1. A adição de um novo equipamento de outro fabricante, com comandos igualmente complexos, implicaria um aumento significativo na complexidade do ambiente. Diante das limitações de pessoal técnico disponíveis, essa mudança representaria um acréscimo de carga operacional difícil de sustentar;

5.3.1.2. A CLDF utiliza soluções da Veritas há quase uma década, com o Appliance Veritas 5250 em operação há aproximadamente cinco anos. Esse histórico consolidou o domínio da equipe técnica sobre a plataforma, especialmente quanto à sua interface de linha de comando e às rotinas de manutenção. Tal nível de proficiência foi alcançado gradualmente e não pode ser reproduzido apenas com treinamentos pontuais em um novo fabricante, o que implicaria perda de eficiência e aumento do risco operacional durante a transição;

5.3.1.3. A introdução de um appliance de fabricante distinto implicaria um aumento significativo na complexidade do ambiente. Cada nova tecnologia adicionada amplia a necessidade de atualização contínua de conhecimentos, eleva o esforço de integração e multiplica os pontos potenciais de falha. Diante das limitações de pessoal técnico disponíveis, essa mudança representaria uma sobrecarga operacional difícil de sustentar, especialmente em um ambiente crítico como o de backup e recuperação de dados;

5.3.1.4. Outro aspecto relevante diz respeito à compatibilidade entre os equipamentos e a suíte NetBackup. Embora todos os fabricantes afirmem que suas soluções são compatíveis, ambientes heterogêneos estão mais sujeitos a falhas de conectividade do que aqueles compostos por plataformas homogêneas. Nesse sentido, manter todos os recursos sob o mesmo fabricante - no caso, Veritas - contribui para a estabilidade operacional e reduz o risco de incompatibilidades futuras;

5.3.1.5. Além disso, a padronização facilita o suporte técnico. Contar com um único fornecedor para toda a solução integrada evita conflitos na definição de responsabilidades e tende a simplificar o processo de resolução de problemas, tornando o atendimento mais ágil e eficiente;

5.3.1.6. Por fim, destaca-se uma característica nativa do equipamento Veritas: a capacidade de executar toda a plataforma de software diretamente no próprio Appliance. Essa característica representa uma vantagem significativa em termos de simplificação da infraestrutura;

5.3.1.7. Vale ressaltar ainda que no caso de implantação de equipamento de fabricante diverso daquele do software de catálogo, a função de desduplicação dos dados executada dentro do appliance não se aproveita para os dados armazenados em nuvem, devendo-se executar mais uma camada de desduplicação pelo software de catálogo dentro do ambiente virtualizado transacional. Esse fator gera uma duplicidade de processamento que vai contra o princípio da eficiência de reuso de componentes computacionais. Ainda, vale lembrar que como um ecossistema fechado, o appliance de backup estabelece um perímetro de segurança mais recomendável para a manipulação dos dados protegidos, reduzindo os riscos de vazamentos ou de quebras de integridade, que poderiam ocorrer em ambiente diverso. Assim sendo, mostra-se um ganho de eficiência computacional combinado com mitigação de riscos de segurança o uso de um appliance do mesmo fabricante do software de catálogo de backup;

5.3.1.8. Em complementação aos itens acima, destaca-se que o equipamento veritas é a única solução capaz de processar todo o ecossistema de componentes da solução de backup dentro do ambiente *on premises*, criando independência funcional em relação ao ambiente transacional. Em razão disso, decorrem dois ganhos importantes, a saber: (1) a segregação arquitetural do ambiente de processamento de backup do processamento transacional negocial, reduzindo as chances de impactos cruzados de degradações de desempenho e (2) a capacidade de operação do ambiente de backup para restaurações mesmo quando toda a infraestrutura transacional seja impactada num cenário de desastre, melhorando a capacidade de continuidade de negócio institucional.

5.3.1.9. A adoção de um Appliance capaz de assumir ambas as funções (Master e Media Server) permitiria consolidar a estrutura computacional, reduzindo a necessidade de servidores adicionais e os custos associados com equipamento e licenciamento de sistemas operacionais. Essa simplificação é especialmente vantajosa em um ambiente com restrições de pessoal técnico, como é o caso da CLDF.

5.4. **Armazenamento de backups de longa duração e de recuperação com baixa probabilidade**

5.4.1. Cenário 3.a: **Outra biblioteca de fitas** não é viável, pois:

5.4.1.1. A Política de Segurança da Informação Digital da CLDF (POSID), instituída pelo Ato da Mesa Diretora nº 125/2020, determina em seu Artigo 96, inciso VIII, que é responsabilidade do Administrador de Backup: *"Armazenar as mídias de backup em cofre próprio, localizado em prédio diferente do local onde o backup é realizado."*;

5.4.1.2. A necessidade de negócio "1.5.2.1 – Armazenamento do backup em prédio distinto daquele onde o backup é realizado" está alinhada com as boas práticas estabelecidas pela norma ABNT ISO/IEC 27002, seção 8.13, item C, que recomenda: *"O armazenamento de backup deve ser feito em local remoto e seguro, a uma distância suficiente para evitar danos causados por desastres no local principal."*

5.4.1.3. Dessa forma, é imprescindível priorizar o armazenamento das cópias de segurança em local remoto, garantindo a preservação dos dados mesmo em caso de falhas ou desastres no ambiente principal;

5.4.1.4. O uso de fitas magnéticas para armazenamento de backup, embora tenha sido uma solução amplamente adotada por décadas, está cada vez sendo menos adotada por organizações de porte pequeno e médio, tendo-se em vista a facilidade entregue por soluções como nuvem computacional, onde efetivamente são implantadas mídias de alta densidade com melhor ganho de escala por instituições que entregam serviços comuns a diversas outras de maneira simplificada e com maior valor agregado. Assim sendo, as instituições de pequeno e médio porte ganham mais agilidade, escalabilidade e segurança, providas por instituições que conseguem manter equipes altamente especializadas e ambiente com alta resiliência a riscos ambientais. As fitas apresentam limitações significativas, como o tempo elevado para recuperação de dados e sensibilidade física, devendo idealmente ser armazenadas em localidade com requisitos de difícil cumprimento por organizações com limitações orçamentárias. Com o avanço das tecnologias de armazenamento digital, que contam com inteligência de movimentação simplificada de dados entre diferentes *tiers*, aliada com técnicas de alta densidade de armazenamento situadas em provedores de serviço em nuvem, muitas organizações estão migrando para alternativas mais eficientes e confiáveis, deixando as fitas como uma opção cada vez menos viável no cenário corporativo atual, rumando a um modelo de responsabilidade compartilhada e custeio *on demand*, entregando a complexidade e custos fixos a uma instituição capaz de absorvê-los com mais eficiência e eficácia.

5.4.2. Cenário 3.c: **Equipamento de armazenamento S3** não é viável, pois:

5.4.2.1. Conforme mencionado no item 5.4, as cópias de segurança não devem ser armazenadas no mesmo ambiente físico onde os dados originais estão localizados. Essa prática contraria os princípios de segurança da informação adotados pela CLDF, que visam garantir a resiliência e a preservação dos dados em caso de falhas ou desastres;

5.4.2.2. Esta solução é capaz de estender o ambiente de armazenamento de backup além daquele comportado dentro dos apliances de backup, mas não é capaz, por si só, de atender a todos os requisitos para este item, em razão de não estar em localidade remota. Neste sentido, esta solução pode ser eventualmente adquirida para complementar as demais, desde que também implantada solução que garanta o armazenamento *off-site*. Por se tratar de solução que atenderia não somente o ambiente de backup, a referida solução deve compor processo de contratação distinto deste.

6. ANÁLISE COMPARATIVA DE CUSTOS (ART. 12, INC. III)

6.1. A análise comparativa de custos considerou apenas as soluções técnica e funcionalmente viáveis, levando em conta o Custo Total de Propriedade (Total Cost of Ownership - TCO). O TCO foi calculado com base nos custos inerentes ao ciclo de vida dos bens e serviços de cada solução, incluindo aquisição, insumos, garantia técnica estendida, manutenção, migração e treinamento. A memória de cálculo foi elaborada para garantir a transparência dos valores considerados.

6.2. A solução viável é composta pelos seguintes itens, cumulativamente:

6.2.1. **Software de catálogo de backup:** A manutenção do software atual, com a renovação do contrato do Veritas NetBackup, parece ser a alternativa mais viável tanto sob o ponto de vista técnico quanto econômico. Essa opção assegura a continuidade dos serviços de TIC, mantendo todas as funcionalidades já implementadas, com baixo risco de interrupções ou perda de dados. O modelo atual de licenciamento, agora baseado em capacidade de front-end (por TB), parece ser suficiente para atender à demanda identificada, com possibilidade de expansão por meio de aditivos contratuais. Trata-se também da solução de menor custo operacional, pois aproveita a infraestrutura existente e evita despesas adicionais com reimplantação ou migração.

6.2.2. **Equipamento para processamento do backup e armazenamento de backups de recuperação com alta probabilidade:** A aquisição de appliance do mesmo fabricante do equipamento atualmente em uso parece ser a alternativa mais adequada para a CLDF. Esse cenário garante a continuidade dos serviços de TIC sem a necessidade de reimplementações das rotinas já estabelecidas, assegurando maior eficiência operacional e reduzindo o risco de falhas ou de incompatibilidades. Além disso, o aproveitamento da base tecnológica já consolidada resulta em menor custo operacional, uma vez que não exige ferramentas adicionais de integração, auditoria ou monitoramento. Trata-se, portanto, de uma solução que combina viabilidade técnica com economicidade, permitindo expansão futura de forma consistente com a infraestrutura existente.

6.2.3. **Armazenamento de backups de longa duração e de recuperação com baixa probabilidade:** A utilização de espaço em nuvem atende integralmente às necessidades de negócio, conformidade e atualização tecnológica, além de trazer ganhos relevantes de segurança. Esse cenário demanda atenção especial durante a implementação, especialmente quanto à privacidade dos dados e à correta integração com os sistemas externos. A nuvem se apresenta como uma opção robusta, escalável e flexível, que acompanha a evolução tecnológica e oferece economicidade adequada.

6.3. Perceba-se que foi encontrada apenas uma solução viável, composta por 3 suítes, conforme visto acima, cada qual para atender a uma parte do escopo da necessidade.

6.4. **O levantamento de custos considerou a estimativa da demanda:**

6.4.1. Considerando os dados apresentados na seção 2.1.2 (volume de dados), podemos observar que o ambiente atual possui 366 TB de dados históricos, com retenção de 1 a 5 anos, armazenados em fita magnética, e 1.114 TB de dados recentes, com retenção inferior a 1 ano, armazenados em fitas magnética e no Appliance de backup.

6.4.2. São gerados aproximadamente 11,15 TB de dados por dia nas rotinas de backup da CLDF. Desse total, cerca de 46% são armazenados em fitas magnéticas, enquanto o restante é direcionado ao Appliance de backup. Isso representa um consumo médio diário de 5,14 TB em fitas e 6,01 TB no Appliance.

6.4.3. Além dos dados atualmente armazenados, é necessário considerar outros fatores para estimar corretamente os volumes demandados. No caso do componente de software, o item 2.2.1 deste documento demonstrou que o cenário viável é a renovação do NetBackup, cuja modalidade de licenciamento foi alterada: deixou de ser baseada em sockets e passou a considerar a capacidade em terabytes de front-end. Por isso, torna-se essencial definir a volumetria de dados em front-end (dados originais) a fim de dimensionar corretamente o licenciamento.

6.4.4. É igualmente necessário estimar o volume destinado ao armazenamento em nuvem.

6.4.5. Os dados que exigem recuperação rápida permanecerão armazenados localmente no Appliance, contribuindo para a otimização dos custos de nuvem. A categorização dos dados de acordo com o prazo de recuperação esperado permitirá uma gestão mais eficiente dos recursos, com alocação adequada de espaço e redução de despesas operacionais.

6.4.6. Importante salientar, também, que atualmente o ambiente encontra-se em condição de contingência, com cópias de segurança restritas apenas aos dados mais críticos, por conta do espaço disponível no Appliance de backup (~10% de espaço livre) e no storage da CLDF (<10% de espaço livre). Assim, será necessário projetar o volume adicional requerido para proteger os dados que hoje não estão contemplados nas rotinas de backup.

6.4.7. Cabe destacar que há um projeto em andamento para aquisição de novos storages de dados (00001-00038757/2024-23), já que o ambiente de armazenamento de dados ativos, não relacionados às cópias de segurança, também se encontra em contingência, em virtude da limitação de espaço nos storages disponíveis.

6.4.8. Por fim, deve-se projetar o crescimento do volume de armazenamento ao longo da vigência contratual, de modo a garantir a sustentabilidade da solução diante da evolução natural da demanda.

6.4.9. **Volume estimado de front-end para o licenciamento do software**

6.4.9.1. A modalidade de licenciamento adquirido pela CLDF, por socket, foi descontinuada. Porém, segundo informações do fornecedor, ela poderá ser convertida para nova modalidade resultando em licenciamento de 25 TB de Front-End.

6.4.9.2. Com base no Relatório 2338749, elaborado a partir dos dados extraídos da ferramenta de backup, foi possível mapear as cópias atualmente configuradas e, por meio do cruzamento dessas informações com os sistemas internos, identificar as demandas reprimidas e os workloads ainda não protegidos. A Tabela 6.1 detalha as volumetrias por item, permitindo a validação da volumetria necessária para o correto dimensionamento do licenciamento do software. O valor estimado de front-end protegido, calculado a partir de dados obtidos na ferramenta de backup, é de aproximadamente 65 TB.

Item	Volume
Objetos atualmente protegidos	65,37 TB
Demandas reprimidas de backup atualmente armazenadas	
Espaço NDMP não protegido	25,5 TB
Espaço S3 não protegido	6,5 TB
Espaço VMWare não protegido	134,8 TB
Demanda reprimida de storage	
Arquivos DICOM de edição de vídeos (estimado pelo uso)	50 TB
Logs (estimado)	50 TB
Outras demandas reprimidas de armazenamento aguardando implantação de novo storage (portal, bancos de dados, SIEM etc)	60 TB
Total	**392,17 TB**

Tabela 6.1 - Itens de front-end

6.4.9.3. Na estimativa de volumetria do ambiente de backup, é fundamental contemplar não apenas os dados atualmente protegidos, mas também os acréscimos adicionais que decorrem de uma série de fatores estruturais e operacionais.

6.4.9.4. Em primeiro lugar, deve-se destacar a existência de um volume aproximado de 160 TB de demandas reprimidas de backup, originadas pelo fato de que, até o momento, somente os dados considerados mais críticos vêm sendo efetivamente incluídos nas rotinas de cópia. Essa limitação decorre tanto de restrições de capacidade quanto da necessidade de priorizar informações essenciais para a continuidade dos serviços, o que acaba por deixar uma parcela significativa dos workloads institucionais sem cobertura adequada de proteção.

6.4.9.5. Paralelamente, observa-se ainda um montante adicional de cerca de 160 TB de demandas reprimidas relacionadas ao storage, conforme detalhado na Tabela 6.1. Esse valor evidencia que parte do parque de armazenamento institucional não está devidamente contemplada pelas rotinas de backup vigentes, ampliando o risco de indisponibilidade e perda de dados em caso de incidentes.

6.4.9.6. Esses dois componentes, demandas reprimidas de backup e de storage, devem ser projetados junto às taxas de crescimento natural da informação no ambiente corporativo, o que reforça a importância de adotar uma estimativa de volumetria mais abrangente e alinhada à realidade futura da instituição.

6.4.9.7. A tabela 6.2 apresenta, de forma consolidada, os dados estimados de volumetria por ano de utilização, permitindo visualizar de maneira progressiva a evolução da necessidade de capacidade e subsidiando o correto dimensionamento da solução a ser contratada.

Ano	Volume (TB)
2025	392,17 (volume atual + contingências)[1]
2026	431,39
2027 (previsto para fim do contrato)	474,53

Tabela 6.2 - Estimativa por ano
[1] Baseado na Tabela 6.1

6.4.9.8. Estima-se que um volume inicial de 392,17 TB de Front-End — correspondente à capacidade atualmente utilizada somada às contingências previstas para 2025 — seja suficiente para atender à demanda imediata.

6.4.9.9. As projeções indicam crescimento para 431,39 TB em 2026 e 474,53 TB em 2027, ano em que está previsto o encerramento do contrato vigente.

6.4.9.10. Considerando a possibilidade de aditivo contratual de até 25%, conforme previsto na legislação, essa expansão mostra-se adequada para cobrir todo o período contratual até 2027, incluindo as estimativas de crescimento de dados.

6.4.9.11. Dessa forma, há uma necessidade de licenciamento para 392,17 TB, visando atender à demanda já consolidada, o que garante maior economicidade e permite expansão futura, caso necessário.

6.4.9.12. Como a CLDF já possui licenciamento para 25 TB, será necessária a aquisição adicional de 365 TB de Front-End. Entretanto, visando mitigar riscos de insuficiência, considerando as taxas de erro de previsão orgânica de crescimento, recomenda-se 375TB. Vale ressaltar que, em função da conversão do 25TB após o primeiro ano contratual, considerando-se as renovações de contrato, o respectivo item passa a ter quantitativo de 400TB para comportar os já convertidos a partir da primeira renovação contratual.

6.4.9.13. Adicionalmente, recomenda-se que a contratação seja formalizada por meio de ata de registro de preços, viabilizando acréscimos subsequentes, se necessários, sem a obrigatoriedade de instaurar um novo processo licitatório. Ressalta-se que contratações desse tipo sempre carregam uma incerteza inerente, uma vez que as estimativas de crescimento podem variar significativamente ao longo do tempo, o que reforça a importância de adotar mecanismos que permitam flexibilidade e ajustes futuros.

6.4.9.14. A memória de cálculo utilizada para obter todos os valores pode ser visualizada no Documento SEI 2341893.

6.4.10. **Volume estimado de dados para Appliance**

6.4.10.1. O appliance será utilizado como armazenamento de curto prazo, destinado a dados com maior probabilidade de exigirem recuperação rápida. Também funcionará como repositório temporário para envio de informações à nuvem, contribuindo para a ampliação da janela de backup e para a otimização do uso do link de Internet.

6.4.10.2. Além disso, atuará como central de processamento de backup, hospedando os serviços relacionados e realizando a desduplicação dos dados.

6.4.10.3. Para garantir uma gestão eficiente dos dados, é necessário definir os volumes destinados à retenção de curto e longo prazo.

6.4.10.4. **Volumes por faixa de retenção baseado no cenário atual**

Categoria	Tempo de retenção	Volume	Tipo de armazenamento	Total
Dados históricos	1 a 5 anos	366 TB	Fitas magnéticas	366 TB
Dados recentes	< 1 ano	464 TB	Fitas magnéticas	1114 TB
		650 TB[1]	Appliance backup	

Tabela 6.3 - Volumes por faixa de retenção

[1] 650TB brutos. Considerando uma taxa de deduplicação de 10:1, volume corresponde a aproximadamente 65TB líquidos

6.4.10.5. Acrescentando a isso as demandas reprimidas apontadas na tabela 6.1 temos:

Item	Volume	Críticos (%)	Total (TB)
Espaço NDMP não protegido	25,5 TB	50	12,75
Espaço S3 não protegido	6,5 TB	100	6,5
Espaço VMWare não protegido	134,8 TB	50	67,4
Demanda reprimida de storage			
Arquivos DICOM de edição de vídeos (estimado pelo uso)	50 TB	50	25
Logs (estimado)	50 TB	100	50
Outras demandas reprimidas de armazenamento aguardando implantação de novo storage (portal, bancos de dados, SIEM etc)	60 TB	50	30
Total	**392,17 TB**		**191,65**

Tabela 6.4 - Avaliação de dados críticos

6.4.10.6. Os dados do cenário atual recentes (cerca de 1,1 PB) somados ao total esperando em virtude da demanda reprimida (191,65 TB) resultam em aproximadamente 1,3 PB e deverão ser acomodados nos appliances, tanto no atual quanto no novo.

Ano	Volume (PB)
2025	1,3
2026	1,43
2027	1,573

Tabela 6.5 - Projeção de crescimento de 10% ao ano

6.4.10.7. Com base na projeção de crescimento até o fim do contrato mostrada acima, será necessário um acréscimo de 923 TB em capacidade lógica. Assim, para atender à demanda, o novo appliance de backup deverá oferecer, no mínimo, 100 TB de capacidade física não desduplicada.

6.4.10.8. A capacidade inicial de armazenamento foi definida, portanto, em 140 TB em razão das características dos modelos avaliados.

6.4.10.9. Com o encerramento da operação do appliance atual em 2028, a capacidade total disponível será reduzida de 65TB, o que será insuficiente para atender à demanda projetada até o final do contrato, em 2028.

6.4.10.10. Para viabilizar futuras expansões sem a necessidade de novo processo licitatório, recomenda-se que a aquisição seja formalizada por meio de ata de registro de preços, incluindo a gaveta de armazenamento para ampliação da capacidade do appliance.

6.4.11. **Volume estimado de dados em fita para movimentação para armazenamento em nuvem**

6.4.11.1. Com o objetivo de manter a eficácia das imagens de backup atualmente armazenadas em fita, essas deverão ser movimentadas para armazenamento em nuvem, em quantidade equivalente ao armazenamento total atualmente hospedado em fita, correspondente a 950TB.

6.4.12. **Volume estimado de dados para armazenamento em nuvem**

6.4.12.1. O volume estimado de dados para armazenamento em nuvem possui memória de cálculo minuciosa constante do Relatório Memória de Cálculo Grupo 2 (2568644).

6.4.12.2. Com o objetivo de garantir a sustentabilidade da solução de backup e otimizar custos operacionais, é necessário definir não apenas a volumetria total a ser contratada, mas também a estratégia de alocação dos dados em diferentes níveis de armazenamento em nuvem (tiers). Essa abordagem permite categorizar os dados institucionais de acordo com sua criticidade, frequência de acesso e tempo de retenção, direcionando-os para camadas de armazenamento que ofereçam o equilíbrio mais adequado entre custo e desempenho.

6.4.12.3. Dessa forma, dados críticos e de recuperação rápida permanecem em camadas de alta disponibilidade, enquanto informações de menor prioridade ou com prazos de retenção mais longos podem ser direcionadas a camadas de menor custo, ainda assim garantindo conformidade com os requisitos institucionais de segurança e acessibilidade.

6.4.12.4. A tabela 6.6 a seguir apresenta os principais tiers de armazenamento em nuvem considerados na análise, suas características de retenção, frequência de acesso e níveis de disponibilidade:

Nome	Produto	Adequação

Tier 1	AWS S3 Standard ou Google Cloud Storage Standard	Retenção de até 30 dias ou leituras com frequência maior ou igual a 30 dias ou que requeira disponibilidade de acesso de 99,99%
Tier 2	AWS S3 Infrequent Access ou Google Cloud Nearline storage	Retenção de 30 dias a 90 dias ou leituras com frequência maior ou igual a 90 dias e menor que 30 dias ou que requeira disponibilidade de acesso de 99,9%
Tier 3	AWS S3 Glacier Instant Retrieval ou Google Cloud Coldline storage	Retenção de 90 dias a 180 dias ou leituras com frequência maior ou igual a 180 dias e menor que 90 dias ou que requeira disponibilidade de acesso de 99,9%
Tier 4	AWS S3 Glacier Instant Retrieval ou Google Cloud Coldline storage	Retenção de 180 dias a 365 dias ou leituras com frequência maior ou igual a 365 dias e menor que 180 dias ou que requeira disponibilidade de acesso de 99,9%
Tier 5	AWS S3 Glacier Deep Archive ou Google Cloud Archive storage	Retenção maior que 365 dias ou leituras com frequência menor que 365 dias ou que requeira disponibilidade de acesso de 99,9%

Tabela 6.6 - Tiers de armazenamento

6.4.12.5. Considerando as informações organizadas na tabela 6.6, a tabela 6.7 demonstra as estimativas de armazenamento em nuvem.

		Tier 1	Tier 2	Tier 3	Tier 4	Tier 5
Backup (2341893)	Espaço (TB)	360	0,3	0	0,45	366
	Espaço (GB)	360000	300	0	450	366000
	Espaço (KB)	3,6E+11	300000000	0	450000000	3,66E+11
	Tamanho médio por arquivo (KB)	4.049,84	1.042,79	0	17.397,33	1.694,18
	Quantidade de arquivos	88.892.400,69	287.688,65	0,00	25.866,04	216.033.715,43
	Transações de escrita por mês	6720	3052	0	77	67
	Transações de leitura por mês	93210,43794	301,6634158	0	27,12250673	226527,7692
	Volume lido por mês (GB)	360	0,3	0	0,45	366
TV Legislativa (1304807)	Espaço (TB)	28	28	14	0	70
	Espaço (GB)	28000	28000	14000	0	70000
	Espaço (KB)	28000000000	28000000000	14000000000	0	70000000000
	Tamanho médio por arquivo (KB)	3.033.000	3.033.000	3.033.000	0	3.033.000
	Quantidade de arquivos	9.231,78	9.231,78	4.615,89	0,00	23.079,46
	Transações de escrita por mês	2.160	2.160	1.080	0	1.800
	Transações de leitura por mês	1.200	1.200	600	0	10
	Volume lido por mês (GB)	3553,28	3553,28	1781,76	0	30
SEDA (2135663)	Espaço (TB)	0	0	0	0	11,7
	Espaço (GB)	0	0	0	0	11700
	Espaço (KB)	0	0	0	0	11700000000
	Tamanho médio por arquivo (KB)	0	0	0	0	1.279.566
	Quantidade de arquivos	0,00	0,00	0,00	0,00	9.143,73
	Transações de escrita por mês	0	0	0	0	0
	Transações de leitura por mês	0	0	0	0	0
	Volume lido por mês (GB)	0	0	0	0	117
Aplicações de uso interno (baseado no atual ambiente S3), considerando replicação de dados, e leitura correspondente a 0,1% da do ambiente atual	Espaço (TB)	12	0	0	0	0
	Espaço (GB)	12000	0	0	0	0
	Espaço (KB)	12000000000	0	0	0	0
	Tamanho médio por arquivo (KB)	6.135	0	0	0	0
	Quantidade de arquivos	1.955.990,22	0,00	0,00	0,00	0,00
	Transações de escrita por mês	55.000.000	0	0	0	0
	Transações de leitura por mês	300.000	0	0	0	0
	Volume lido por mês (GB)	160	0	0	0	0

Tabela 6.7 - Estimativas de armazenamento em nuvem

6.5. Itens a serem contratados

6.5.1. A estimativa dos itens a serem contratados foi elaborada a partir da análise dos cenários viáveis identificados neste Estudo Técnico Preliminar: a renovação do software Veritas NetBackup, a aquisição de appliance do mesmo fabricante atualmente em uso e a utilização de armazenamento em nuvem para dados de longa retenção. Além desses componentes principais, foram incorporados serviços e recursos complementares, indispensáveis para assegurar a continuidade, a eficiência operacional e a atualização tecnológica da solução como um todo.

6.5.2. A subscrição do Veritas NetBackup com suporte e garantia por 12 meses, aliada à conversão do modelo de licenciamento de socket/cliente para capacidade em terabytes de front-end, garante que o software permaneça atualizado e aderente ao formato comercial atualmente oferecido pelo fabricante. Esse passo é fundamental para manter a cobertura de suporte oficial e preservar os investimentos já realizados.

6.5.3. Com relação ao Appliance, a aquisição da controladora e da gaveta (Expansion Shelf) em unidades distintas parece ser a alternativa mais viável, pois possibilita dimensionar a infraestrutura de forma modular e escalável. Essa estratégia permite alinhar a capacidade contratada à demanda real da instituição, evitando custos desnecessários com equipamentos superdimensionados e garantindo maior flexibilidade para acompanhar o crescimento da volumetria de dados ao longo da vigência contratual. Além disso, a compra separada contribui para a otimização dos recursos financeiros, assegurando que cada componente seja adquirido na medida exata da necessidade. Nesse contexto, foram avaliadas as opções disponibilizadas pelo fabricante, que correspondem aos diferentes modelos de appliance da linha NetBackup, cada um com características específicas de desempenho e capacidade.

6.5.4. Atualmente, o fabricante disponibiliza dois modelos principais de Appliance para essa categoria de solução: o NetBackup Flex 5260 Appliance (2342370) e o NetBackup Flex 5360 Appliance Series (2342374). Ambos foram considerados no presente estudo, de forma a identificar aquele que melhor se adequa às demandas de volumetria, desempenho e escalabilidade da instituição.

6.5.5. As principais diferenças entre os dois modelos disponíveis são resumidos a seguir:

Características/Modelo	NetBackup Flex 5260 Appliance (2342370)	NetBackup Flex 5360 Appliance Series (2342374)
Alta disponibilidade por meio de redundância da controladora	Não	Sim
Capacidade máxima	442 TB	2 PB
Tamanhos dos módulos adicionais (gaveta/expansion shelf)	72 TB	132, 264 ou 528 TB (a depender da configuração do driver instalado na gaveta)
Thoughput Máximo	30.74 TB/hour	72.76 TB/hour
Número máximo de portas 25–10 GB Ethernet	6*	8 (podendo chegar a 16 com controladora adicional)
Número máximo de portas 32 GB Fibre Channel	8*	6 (podendo chegar a 12 com controladora adicional)
Fonte de alimentação redundante	Sim	Sim

Tabela 6.8 - Características dos modelos de equipamentos atuais
* Há um número limitado de cobinações de portas 25-10 GB Ethernet e 32 GB FC, conforme 2355057 (https://www.veritas.com/support/en_US/doc/160061037-160061040-0/v160510921-160061040)

6.5.5.1. Ambos os equipamentos possuem características semelhantes em termos de segurança:

6.5.5.1.1. Autenticação por certificado

6.5.5.1.2. Autorização baseada em função (role-based)

6.5.5.1.3. Autenticação multifator

6.5.5.1.4. Aprovação por quórum

6.5.5.1.5. Controle de acesso à rede

6.5.5.1.6. Isolamento de rede (airgap)

6.5.5.1.7. Segmentação de rede

6.5.5.1.8. Isolamento de aplicações

6.5.5.1.9. Controle de acesso a recursos

6.5.5.1.10. Varredura contra malware

6.5.5.1.11. Detecção de anomalias

6.5.5.1.12. Imutabilidade de dados

6.5.5.1.13. Bloqueio de retenção imutável/compliance clock

6.5.5.1.14. Gerenciamento de privilégios com acesso zero trust

6.5.5.1.15. Controle de acesso obrigatório

6.5.5.1.16. Computação segura e indelével

6.5.5.1.17. Ofuscação de dados sensíveis

6.5.6. Uma vez que ambos equipamentos atendem à demanda, o NetBackup Flex 5260 Appliance é o recomendado por ser o de menor preço.

6.5.7. A controladora Veritas Flex Appliance 5260 de 9 TB concentra o processamento, o gerenciamento e a lógica de controle do ambiente de backup. É o elemento central que integra o hardware ao software Veritas NetBackup, coordenando as rotinas de gravação e recuperação de dados e garantindo o funcionamento de toda a solução. A gaveta de expansão de 72 TB, por sua vez, agrega capacidade adicional de armazenamento e pode ser incorporada conforme a evolução da demanda. Por se tratar de um componente modular, possibilita que a CLDF aumente sua capacidade de forma gradativa e planejada, sem a necessidade de investimentos imediatos em infraestrutura além do necessário.

6.5.8. Essa composição, portanto, parece ser a mais adequada para garantir a sustentabilidade do ambiente, oferecendo equilíbrio entre desempenho, flexibilidade e economicidade.

6.5.9. Embora o Processo 00001-00021228/2022-29 trate da contratação de serviços de cabeamento estruturado em âmbito mais amplo, faz-se necessário que o appliance de backup seja entregue acompanhado do fornecimento e instalação do cabeamento óptico específico para sua interligação com o CPD. Esse cabeamento deve garantir conectividade de alta velocidade e baixa latência, assegurando o desempenho adequado das rotinas de backup e recuperação, além de oferecer maior confiabilidade e escalabilidade à solução como um todo.

6.5.10. Além disso, a manutenção do suporte ao appliance 5250 até 31 de dezembro de 2028 garante o melhor aproveitamento dos ativos já existentes, assegurando que continuem operando de forma integrada ao novo ambiente até o final de seu ciclo de vida. Isso possibilita uma transição gradual e otimiza o uso dos recursos da Casa, sem gerar descontinuidade operacional.

6.5.11. Além da aquisição de software e hardware, é importante contemplar itens de transferência de conhecimento e treinamento, com conteúdo referente aos componentes da solução, de modo a capacitar a equipe técnica da Casa para operar a solução de forma eficiente, e de serviços especializados de migração do servidor de catálogo, assegurando a correta transição entre o ambiente atual e o novo modelo de licenciamento.

6.5.12. O ambiente de backup atualmente encontra-se com servidor de gerenciamento de catálogo (*master*) implantado em máquina virtual Windows, que é fruto de uma evolução realizada já há várias gerações da solução de backup institucional. Nos últimos anos, com a consolidação da plataforma computacional prioritariamente sobre sistema operacional Linux, tentou-se migrar o servidor *master* para sistema operacional Linux. Em razão das proteções nativas da solução de backup contra exploits, mitigando a superfície de ataque, manipulações profundas sobre esse serviço somente podem ser feitos pelo fabricante do software e, por esse motivo, a referida migração para sistema operacional Linux nunca foi feita até então, pois dependia de um serviço que a CLDF não contratara anteriormente. Assim sendo, mostra-se importante que a contratação compreenda o serviço de migração de catálogo.

6.5.13. Um dos indicadores mais relevantes para a solução de backup adotada é a capacidade de restaurar uma operação indisponível de sistema de informação com o menor tempo possível. Esse indicador é quantificado na forma do RTO (objetivo de tempo de recuperação). Visando mitigar o RTO, mostra-se necessário que o ambiente de backup não possua dependência funcional com o ambiente transacional, pois uma

indisponibilidade no ambiente transacional poderia afetar a orquestração das operações de restauração de backup caso esse dependência seja presente. Neste sentido. nas versões mais modernas, o sistema NetBackup permite a execução do servidor de catálogo dentro do appliance de backup, caso seja utilizado o appliance do mesmo fabricante. Essa característica mostra-se como alternativa excelente para resolver a necessidade da não dependência funcional. Entretanto, para que o servidor de catálogo seja migrado para ser usado dentro do appliance de backup, é essencial que seja realizada a migração do catálogo. Assim sendo, não obstante a necessidade citada no parágrafo acima, neste momento mostra-se indispensável a contratação deste item.

6.5.14. Uma vez que a presente contratação visa estabelecer uma arquitetura sem interdependência funcional entre o ambiente de backup e o ambiente transacional, para que a função de gerenciamento seja transferida para dentro do *appliance* de backup, mostra-se necessária a migração do catálogo de backup, que é um serviço que só pode ser realizado pelo fabricante da solução, em razão das limitações existentes feitas para garantir a segurança do software.

6.5.15. Considerando-se a criticidade do ambiente de backup para a continuidade de negócios, dado que trata-se de relevante vetor para a recuperação de desastres, mostra-se recomendável a contratação de pacote de serviços pelo fabricante, buscando a mitigação de riscos operacionais. Ademais da maior especialidade, o referido item reforça a visão da continuidade da Administração Pública além do tempo de vida da contratada e reduz os riscos relacionados a não prestação, trazendo o fabricante para a responsabilidade sobre a recuperação de desastres.

6.5.16. Considera-se, ainda, a contratação de serviços de movimentação do acervo atualmente armazenado em fitas para ambiente em nuvem, tendo em vista a proximidade do término do contrato de manutenção da fitoteca em uso. O acervo é composto por aproximadamente 450 fitas, cada uma com capacidade média de 2,2 TB, totalizando 950 TB de dados a serem contemplados na estratégia de movimentação. Essa medida visa assegurar a continuidade do acesso às informações históricas, reduzir a dependência de tecnologia já obsoleta e alinhar a política de backup da instituição a soluções mais modernas, seguras e escaláveis.

6.5.17. Deverão ser contratadas unidades de serviço em nuvem para armazenamento de objetos, podendo ser Amazon Web Services (AWS) ou Google Cloud Platform (GCP). Esse item será destinado a compor a estratégia de backup institucional, possibilitando a guarda de cópias em ambiente externo, com alta disponibilidade, escalabilidade sob demanda e mecanismos avançados de segurança. A adoção de armazenamento em nuvem junto a esses provedores reduz a dependência de infraestrutura física local e assegura maior resiliência contra falhas ou incidentes no datacenter da CLDF.

6.5.18. Assim, os itens abaixo parecem ser os mais adequados, pois consolidam em um único contrato os componentes de software, hardware, nuvem e serviços necessários para garantir a integridade, a disponibilidade e a continuidade da política institucional de backup da CLDF:

6.5.18.1. Subscrição Veritas Netbackup, modalidade de licenciamento por front-end, com suporte e garantia para 12 meses

6.5.18.2. Conversão do licenciamento do Veritas Netbackup por socket para subscrição com suporte e garantia para 12 meses

6.5.18.3. Aquisição Controladora Veritas Flex Appliance 5260 com suporte e garantia para 60 meses

6.5.18.4. Aquisição Gaveta Veritas Flex Appliance 5260 com suporte e garantia para 60 meses

6.5.18.5. Suporte e Garantia do Appliance 5250 até o fim de vida (previsto para 31 de dezembro de 2028, conforme documento 2342346 e link oficial)

6.5.18.6. Migração dos dados em fita para a nuvem

6.5.18.7. Unidades de serviço em nuvem para armazenamento de objetos em AWS ou GCP

6.5.18.8. Transferência de Conhecimento/Treinamento

6.5.19. Em relação às unidades de serviço em nuvem, considerando-se a sensibilidade dos preços a fatores cambiais, e buscando um equilíbrio entre estabilidade contratual e mitigação de custos, estabelece-se o prazo contratual de 24 meses, renováveis por períodos sucessivos, até o limite de 120 meses.

6.6. **Quantitativo dos itens a serem contratados**

6.6.1. Considerando os itens a serem contratados, a tabela 6.9 abaixo apresenta as descrições, unidades e quantitativos por elemento.

Grupo	Item	Descrição	Unidade	Quantitativo
1	1	Subscrição Veritas Netbackup com suporte e garantia para 12 meses	FETB	400
1	2	Conversão do licenciamento do cliente por socket/cliente para subscrição do Veritas Netbackup por capacidade com suporte e garantia para 12 meses	FETB	25
1	3	Aquisição Controladora Veritas Flex Appliance 5260 - 9TB com suporte e garantia para 60 meses	Unidade	2
1	4	Aquisição Gaveta Veritas Flex Appliance 5260 - 72 TB com suporte e garantia para 60 meses	Unidade	12
1	5	Suporte e Garantia do Appliance 5250 até o end of life (dez/28)	Unidade	1
1	6	Serviço de instalação e configuração	Unidade	1
1	7	Transferência de Conhecimento/Treinamento	Turma	2
1	8	Serviço de Migração do Servidor de catálogo	Serviço	1
1	9	Serviço de Migração dos dados em fita para a nuvem	TB	950
1	10	Suporte técnico especializado de toda a solução	Serviço	1
2	11	Unidades de serviço em nuvem para armazenamento de objetos em AWS ou GCP	USN/mês	21.553 517.272 para 24 meses

Tabela 6.9 - Itens e quantiativos a serem contratados

6.7. O cálculo dos custos totais de propriedade (TCO) e mapa comparativo dos custos totais é o que segue:

		Estimativa de custos ao longo dos anos	

Solução viável	Descrição da solução	Ano 1	Ano 2	Total
1	Grupo 1 - subscrição de licenças netbackup, mais aquisição de appliance, serviços de suporte, garantia, transferência de conhecimento e migrações	**R$ 14.665.844,93**	- *tendo-se em vista o contrato ser anual, não se considera o ano 2	**R$ 14.665.844,93**
1	Grupo 2 - Unidades de serviço em nuvem para armazenamento de objetos em AWS ou GCP	**R$ 1.836.315,60**	**R$ 1.836.315,60**	**R$ 3.672.631,20**

Tabela 6.10 - Custos totais de propriedade

7. ESTIMATIVA DO CUSTO TOTAL DA CONTRATAÇÃO (ART. 12, INC. IV)

Grupo	Item	Descrição	Unidade	Quantitativo	Preço unitário	Preço total
1	1	Subscrição Veritas Netbackup com suporte e garantia para 12 meses	FETB	400	R$ 6.384,74	R$ 2.553.896,00
1	2	Conversão do licenciamento do cliente por socket/cliente para subscrição do Veritas Netbackup por capacidade com suporte e garantia para 12 meses	FETB	25	R$ 7.222,50	R$ 180.562,50
1	3	Aquisição Controladora Veritas Flex Appliance 5260 - 9TB com suporte e garantia para 60 meses	Unidade	2	R$ 797.621,21	R$ 1.595.242,42
1	4	Aquisição Gaveta Veritas Flex Appliance 5260 - 72 TB com suporte e garantia para 60 meses	Unidade	12	R$ 696.865,83	R$ 8.362.389,96
1	5	Suporte e Garantia do Appliance 5250 até o end of life (dez/28)	Unidade	1	R$ 429.797,66	R$ 429.797,66
1	6	Serviço de instalação e configuração	Unidade	1	R$ 69.530,00	R$ 69.530,00
1	7	Transferência de Conhecimento/Treinamento	Turma	2	R$ 15.600,00	R$ 31.200,00
1	8	Serviço de Migração do Servidor de catálogo	Serviço	1	R$ 473.976,39	R$ 473.976,39
1	9	Serviço de Migração dos dados em fita para a nuvem	TB	950	R$ 815,00	R$ 774.250,00
1	10	Suporte técnico especializado de toda a solução	Serviço	1	R$ 195.000,00	R$ 195.000,00
2	11	Unidades de serviço em nuvem para armazenamento de objetos em AWS ou GCP por 24 meses	USN	21.553/mês 517.272 para 24 meses	R$ 7,10	R$ 3.672.631,20
	TOTAL					**R$ 18.338.476,13**

Tabela 7.1 - Estimativa do custo total da contratação

8. DECLARAÇÃO DA VIABILIDADE DA CONTRATAÇÃO (ART. 12, INC. V)

8.1. Após a análise realizada pela Equipe de Planejamento da Contratação, conclui-se pela **viabilidade** da contratação de solução de backup corporativo destinada a assegurar a continuidade, a integridade e a disponibilidade das informações institucionais da Câmara Legislativa do Distrito Federal.

8.2. A avaliação considerou:

8.2.1. Necessidade institucional: a atual solução encontra-se limitada em capacidade e baseada em tecnologia considerada obsoleta (LTO-5), não atendendo integralmente às demandas reprimidas de backup e de storage, o que coloca em risco a preservação dos dados críticos da Casa.

8.2.2. Aspectos técnicos: a contratação contempla solução moderna, modular e escalável, capaz de suportar o crescimento projetado da volumetria de dados, integrando-se ao ambiente VMware e às rotinas operacionais vigentes. A arquitetura proposta, baseada em appliances Veritas NetBackup, atende aos requisitos de desempenho, resiliência, segurança e governança tecnológica.

8.2.3. Aspectos econômicos: a aquisição em modelo modular (licenciamento e gavetas de expansão) e a escolha entre os modelos disponibilizados pelo fabricante permitem otimizar recursos financeiros, evitando custos de superdimensionamento e garantindo o melhor aproveitamento do investimento ao longo do ciclo contratual.

8.2.4. Aspectos legais: o processo de contratação observa os preceitos estabelecidos pela Lei nº 14.133/2021, bem como as normas internas da CLDF (AMD 71/2023 e correlatos).

8.3. Diante do exposto, a Equipe de Planejamento da Contratação declara **viável** a contratação da solução de backup, uma vez que esta atende de forma adequada aos requisitos técnicos, operacionais, legais e orçamentários da instituição, garantindo a proteção e a continuidade dos serviços de Tecnologia da Informação essenciais ao funcionamento da CLDF.

8.4. **Parcelamento ou não da contratação:**

8.4.1. Conforme estabelecido no art. 40 da Lei Federal nº 14.133, de 2021, e no art. 13, § 3º do Ato da Mesa Diretora nº 71, de 2023, o parcelamento do objeto é a regra nas contratações públicas, visando ampliar a competitividade e o melhor aproveitamento dos recursos de mercado. Neste sentido, verifica-se que o item do armazenamento em nuvem, pela sua natureza, pode e deve ser parcelado em um grupo separado dos demais. Por outro lado, os demais itens, após análise técnica e de negócio aprofundada, não são tecnicamente viáveis de serem parcelados entre si, dada a alta correlação de atividades de implantação e necessidade de abordagem unificada para mitigar riscos da contratação.

9. PROVIDÊNCIAS A SEREM ADOTADAS PELA ADMINISTRAÇÃO PREVIAMENTE À CELEBRAÇÃO DO CONTRATO

9.1. Para assegurar a boa gestão e a execução bem-sucedida do contrato, a Câmara Legislativa do Distrito Federal (CLDF) adotará as seguintes providências prévias, em conformidade com o Art. 18, § 1º, X, da Lei nº 14.133/2021:

9.1.1. **Designação Formal da Equipe de Fiscalização:** Será formalmente designada, por meio de Portaria, a equipe responsável pela fiscalização e gestão do contrato. A equipe será composta pelo Gestor do Contrato e pelos Fiscais Técnico, Requisitante e Administrativo, bem como seus

respectivos substitutos, em estrita observância ao que dispõe o Ato da Mesa Diretora nº 71, de 2023.

9.1.2. **Capacitação da Equipe de Fiscalização:** Garantir que os servidores designados para a fiscalização, em especial o Fiscal Técnico e o Gestor, possuam a capacitação necessária para compreender o escopo da solução, os níveis de serviço acordados e os procedimentos de gestão contratual, a fim de realizar um acompanhamento eficaz.

9.1.3. **Adequação do Ambiente Técnico para Integração:** A Área Técnica de TI (SEINF/DMI) realizará as configurações necessárias para permitir a coleta de telemetria e a integração da nova plataforma, incluindo, mas não se limitando a:

9.1.3.1. **Liberação de Acessos:** Ajuste de regras em firewalls e outros dispositivos de segurança para permitir a comunicação dos agentes da solução com a plataforma em nuvem do contratado.

9.1.3.2. **Reserva Orçamentária:** A área administrativa competente providenciará a devida reserva dos créditos orçamentários necessários para cobrir as despesas do contrato no exercício financeiro vigente, garantindo a disponibilidade de recursos para o pagamento conforme o cronograma físico-financeiro a ser estabelecido.

10. DESCRIÇÃO DE POSSÍVEIS IMPACTOS AMBIENTAIS E RESPECTIVAS MEDIDAS MITIGADORAS

10.1. Em conformidade com o Art. 18, § 1º, XII, da Lei nº 14.133/2021, foi realizada a análise dos possíveis impactos ambientais decorrentes da presente contratação:

10.1.1. **Impacto Ambiental Direto:** A contratação tem como objeto principal a subscrição de licenças de software, prestação de serviços técnicos especializados, aquisição de hardware e contratação de serviços em nuvem. Desta forma, não há impacto ambiental direto significativo, como a geração de resíduos sólidos (lixo eletrônico) ou o consumo de recursos naturais para a fabricação de bens pela CLDF.

10.1.2. **Impactos Ambientais Indiretos e Medidas Mitigadoras:**

10.1.2.1. **Consumo de Energia Elétrica:** O principal impacto indireto está associado ao consumo de energia elétrica pelos data centers que hospedam a solução, tanto o local para os hardwares adquiridos, bem como os de nuvem pública para os créditos em nuvem pública.

10.1.2.1.1. **Medida Mitigadora:** A escolha por solução prioritariamente em nuvem para armazenamento dos backups, além de atender aos requisitos de conformidade, também mitigam o impacto ambiental, tendo-se em vista que os provedores de nuvem pública já dispõem de mecanismos de redução e compensação de pegada de carbono em patamar de maturidade elevado.

10.1.2.2. **Descarte de Equipamentos:**

10.1.2.2.1. **Medida Mitigadora:** Não se aplica diretamente, pois serão acrescidos equipamentos, e não substituídos, mantendo-se o suporte do equipamento atualmente implantado.

10.1.2.3. **Deslocamento de Pessoal:**

10.1.2.3.1. **Medida Mitigadora:** A natureza da solução, gerenciada pelas interfaces digitais, e a prestação de suporte técnico majoritariamente por canais digitais reduzem a necessidade de deslocamento de técnicos, diminuindo a emissão de gases de efeito estufa associada ao transporte.

11. RESPONSÁVEIS

EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO			
Integrante	**Nome**	**Matrícula**	**Lotação**
Requisitante	WALÉRIO OLIVEIRA CAMPORÊS	24.872	DMI
Técnico	CLEBER MARCOS DE TOLEDO	12.551	SEINF

ÁREA TÉCNICA DE TI		
NOME DA ÁREA TÉCNICA DE TI	**NOME DO CHEFE OU SUBSTITUTO**	**Matrícula**
SEINF	AIRTON BORDIN JUNIOR	23.994

11.1. Para contato dos responsáveis, deverá sempre ser usado o e-mail seinf@cl.df.gov.br e dmi@cl.df.gov.br.

12. APROVAÇÃO E DECLARAÇÃO DE CONFORMIDADE

Aprovo este Estudo Técnico Preliminar e atesto sua conformidade às disposições do AMD nº 71 de 2023 da CLDF, bem como à Lei 14.133/2021.

GUILHERME CALHAU MOTTA

Secretário Executivo da Quarta Secretaria

Câmara Legislativa do DF

* O AMD 71/2023, Art. 12, § 3º determina que, caso o Chefe da Área de TI (Diretor da DMI) componha a Equipe de Planejamento, a aprovação do ETP deve ser realizada pela autoridade diretamente superior.

Conforme AMD nº 71, de 2023, art. 12, § 2º, o Estudo Técnico Preliminar da Contratação será assinado pelos Integrantes Técnico e Requisitante da contratação e pelo Chefe da respectiva Área Técnica de TI e aprovado pelo Chefe da Área de TI. Caso o Chefe da Área Técnica de TI ou o Chefe da Área de TI venha a compor a Equipe de Planejamento da Contratação, a autoridade que assinará o Estudo Técnico Preliminar da Contratação juntamente com os Integrantes Técnico e Requisitante será aquela diretamente superior ao respectivo Chefe, conforme § 3º.

Documento assinado eletronicamente por **WALERIO OLIVEIRA CAMPORES - Matr. 24872**, **Diretor(a) de Modernização e Inovação Digital**, em 13/03/2026, às 12:25, conforme Art. 30, do Ato da Mesa Diretora n° 51, de 2025, publicado no Diário da Câmara Legislativa do Distrito Federal nº 62, de 27 de março de 2025.

Documento assinado eletronicamente por **CLEBER MARCOS DE TOLEDO - Matr. 12551**, **Analista Legislativo**, em 13/03/2026, às 12:28, conforme Art. 30, do Ato da Mesa Diretora n° 51, de 2025, publicado no Diário da Câmara Legislativa do Distrito Federal nº 62, de 27 de março de 2025.

Documento assinado eletronicamente por **PEDRO CUNHA REGO CELESTIN - Matr. 22858**, **Chefe do Setor de Infraestrutura de Tecnologia da Informação**, em 13/03/2026, às 13:07, conforme Art. 30, do Ato da Mesa Diretora n° 51, de 2025, publicado no Diário da Câmara Legislativa do Distrito Federal nº 62, de 27 de março de 2025.

A autenticidade do documento pode ser conferida no site:
http://sei.cl.df.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0
Código Verificador: **2574124** Código CRC: **6EBF4ADF**.