**TRIBUNAL DE CONTAS DO DISTRITO FEDERAL – TCDF**
**Secretaria de Tecnologia da Informação - STI**
Supervisão de Planejamento da Contratação - SPC

# ESTUDO TÉCNICO PRELIMINAR PARA CONTRATAÇÃO DE SOFTWARE E APPLIANCES DE BACKUP E SERVIÇO DE BACKUP NA NUVEM PARA O AMBIENTE MICROSOFT 0365/M365.

## 1. DA DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

1.1. A presente análise tem por objetivo demonstrar a viabilidade técnica da contratação de empresas para a realização do seguinte objeto:

1.1.1. Provimento de solução de backup, envolvendo software e *appliances* de backup e serviço de backup na nuvem para o ambiente Microsoft O365/M365, com garantia e suporte técnico por 60 meses, e treinamento na solução.

1.2. **DIAGNÓSTICO**

1.2.1. O software e o ***appliance*** atualmente em uso no TCDF estão em perfeito funcionamento e atendem às necessidades da Instituição, isto é, a salvaguarda dos dados. Porém, em virtude do tempo decorrido desde a contratação, algumas questões precisam ser consideradas, quais sejam:

1.2.1.1. **Equipamento em fase final de suporte e garantia**: a garantia e o suporte da solução de backup findam em 23/02/2026 e a renovação não é possível, visto que o modelo atualmente em uso no Tribunal (DD 6300) **não é mais comercializado,** conforme comunicação presente no e-DOC 3CA0BF19.

1.2.1.2. **Tempo de retenção**: conforme apresentado na Informação n° 2/2025 – COGINF (e-DOC 7DF6B8CB), no Estudo Técnico Preliminar (ETP) da contratação do atual ***appliance*** de backup (e-DOC 2E462D1F), tomando por base o tempo de retenção que já vinha sendo praticado pela STI e visando unificar e aumentar o período de guarda dos backups, definiu-se o prazo de guarda dos backups em 6 (seis) meses (backups incrementais do mês corrente ao backup e o último backup full dos últimos cinco meses). Porém, após a chegada do equipamento de backup, verificou-se que as tecnologias de *data reduction* implementadas eram muito melhores que o previsto, o que possibilitou aumentar o tempo de retenção dos dados. Assim, atualmente o período de retenção dos backups está da seguinte forma:

| Objeto de backup | Período de retenção (meses) |
|---|---|
| Imagens de máquinas virtuais | 6 |
| Dados de servidores Linux | 24 |
| Dados de servidores Windows | 24 |
| Dados do sistema de gestão de pessoas | 72 |
| Bancos de dados SQL Server | 24 |

1.2.1.3. Por falta de uma **política de backup institucional,** elaborada por unidade ou grupo competente, conforme preconizado pela ABNT NBR ISO/IEC 27002:2022, a Gerência de Infraestrutura de TI (GEINT), entendendo a importância do tema, definiu, baseado no histórico de salvaguarda de dados de projetos anteriores, a atual periodicidade de execução dos backups e o tempo de retenção.

1.2.1.3.1. Acrescenta-se que ainda não há a política de backup mencionada e a GEINT, novamente, ficará a cargo da definição da periodicidade e tempo de retenção dos backups para esta contratação. Dada a importância do tema e para que o Tribunal não fique sem suporte e garantia dos equipamentos de backup, não será possível, para esta contratação, aguardar a criação do grupo de trabalho sugerido na Informação n° 2/2025 – COGINF.

1.2.1.4. **Proteções contra ransomware e outros ataques ao sistema de backup**: o software e appliances atuais do TCDF não contam com proteções modernas contra ransomware e outros ataques.

1.2.1.4.1. A crescente sofisticação dos ataques cibernéticos, especialmente o ransomware, tornou essencial a adoção de soluções de backup que ofereçam mecanismos modernos de proteção. O ransomware tem como alvo não apenas os dados de produção, mas também os repositórios de backup, visando inutilizar a última linha de defesa das organizações. Por isso, investir em softwares e appliances de backup que contemplem funcionalidades avançadas de segurança é uma estratégia fundamental para garantir a continuidade dos negócios e a integridade das informações corporativas.

1.2.1.4.2.

1.2.1.4.3. Uma solução de backup robusta deve incorporar camadas de proteção contra ransomware, como a imutabilidade dos backups e o isolamento das cópias de segurança. Backups imutáveis garantem que, mesmo que o ambiente de produção seja comprometido, os dados armazenados não poderão ser alterados ou deletados durante o período de retenção. Além disso, a separação física ou lógica dos repositórios de backup dificulta o acesso indevido por agentes maliciosos, agregando um importante nível de segurança adicional.

1.2.1.4.4. Outro aspecto crucial é a capacidade do software de backup em realizar a verificação contínua de vírus e malwares nos dados protegidos. A varredura automática dos arquivos garante que cópias contaminadas não sejam restauradas inadvertidamente em momentos de recuperação, evitando uma reinfecção do ambiente. Esse tipo de funcionalidade é especialmente relevante em um cenário onde ameaças avançadas podem permanecer dormentes por longos períodos antes de serem ativadas.

1.2.1.4.5. Por fim, a escolha de appliances e softwares de backup com recursos modernos de proteção permite ao TCDF cumprir requisitos regulatórios e melhores práticas de governança.

1.2.1.5. **Backup dos dados do Tribunal que estão na nuvem Microsoft**: atualmente, o Tribunal não possui backup dos dados que estão na nuvem.

1.2.1.5.1. Mesmo ambientes Microsoft hospedados na nuvem, como Microsoft 365 e Azure, estão sujeitos a riscos como exclusão acidental, ataques de ransomware, falhas humanas e limitações nos mecanismos nativos de recuperação.

1.2.1.5.2. Por isso, manter backups independentes do ambiente Microsoft na nuvem é fundamental para assegurar a continuidade do negócio do TCDF e proteger o patrimônio digital da Corte. Soluções especializadas permitem recuperar dados críticos de forma granular e com retenção personalizada, proporcionando maior segurança e controle diante das ameaças e desafios do cenário digital atual.

1.2.1.5.3. Demandas dos potenciais gestores e usuários das soluções propostas neste Estudo Técnico Preliminar envolvem:

1.2.1.5.4. Continuidade dos serviços da Corte;

1.2.1.5.5. Recuperação de desastres.

1.2.1.5.6. Projetos similares a este em outros órgãos da administração pública são comuns

## 2. DA IDENTIFICAÇÃO DA MELHOR SOLUÇÃO

### 2.1. SITUAÇÃO ATUAL

2.1.1. Atualmente, a estrutura de backup do TCDF é composta pelo software **Dell Networker** e por 2(dois) appliances Dell Data Domain. A solução foi contratada por intermédio do Processo Administrativo Eletrônico n.º 24668/2019-e.

2.1.2. A estrutura de backup utilizada pelo Tribunal foi explicada, em detalhes, por meio da Informação n° 2/2025 – COGINF (e-DOC 7DF6B8CB), encaminhado à Presidência do TCDF, e, inclusive, debatido no Comitê Gestor de Tecnologia da Informação (CGTI).

### 2.2. CONSIDERAÇÕES INICIAIS

2.2.1. Só é possível prover a demanda adquirindo ou subscrevendo nova solução de backup, visto que vários problemas elencados no item de Diagnóstico deste Estudo Técnico Preliminar não poderão ser resolvidos sem novo equipamento, em especial a falta de suporte técnico e a proteção contra ameaças avançadas.

### 2.3. INFORMAÇÕES DO MERCADO

2.3.1. Para justificar a escolha de uma solução ou outra, dentre várias presentes no mercado, faz-se necessário o estudo das principais arquiteturas possíveis para soluções de backup. Dessa forma, nos tópicos abaixo serão apresentadas as diferentes formas de se organizar a soluções de backup presentes no mercado.

2.3.2. **Software de backup com appliance de backup**

2.3.2.1. Nesta arquitetura, o software de backup é integrado a um appliance dedicado, que reúne hardware e software otimizados especificamente para backup, armazenamento e recuperação de dados. Os appliances geralmente incluem recursos avançados, como deduplicação, compressão, criptografia e, frequentemente, proteção contra ransomware.

**2.3.2.2. Pontos fortes:**

2.3.2.2.1. Simplicidade de gerenciamento: o appliance é entregue pronto para uso, com integração nativa ao software de backup, reduzindo a complexidade operacional e facilitando o suporte.

2.3.2.2.2. Desempenho otimizado: os recursos de hardware e software são projetados para operar de forma conjunta, proporcionando alta velocidade de backup, recuperação e replicação.

2.3.2.2.3. Taxas elevadas de redução de dados: a deduplicação e compressão embarcadas nos appliances proporcionam reduções significativas no volume armazenado, economizando espaço, largura de banda e custos de retenção.

2.3.2.2.4. Segurança aprimorada: soluções modernas oferecem imutabilidade, detecção de anomalias, isolamento lógico e integração com verificadores de malware, reforçando a proteção contra-ataques.

2.3.2.2.5. Suporte unificado (quando hardware e software são do mesmo fabricante): facilita o diagnóstico e resolução de problemas, pois o fabricante é responsável tanto pelo software quanto pelo hardware.

2.3.2.2.6. Escalabilidade: muitos appliances permitem expansão modular, acompanhando o crescimento do ambiente sem reestruturações complexas.

**2.3.2.3. Ponto fraco:**

2.3.2.3.1. Custo inicial elevado: o investimento na aquisição do appliance pode ser superior ao de arquiteturas baseadas apenas em software ou storage tradicional.

2.3.3. **Software de backup com storage**

2.3.3.1. Nesta arquitetura, o software de backup armazena os dados em storages tradicionais, como SAN (Storage Area Network) ou NAS (Network Attached Storage). Essa arquitetura permite maior flexibilidade na escolha dos componentes.

**2.3.3.2. Pontos fortes:**

2.3.3.2.1. Flexibilidade de escolha: permite combinar diferentes softwares de backup com variados storages, escolhendo equipamentos conforme orçamento e necessidade.

2.3.3.2.2. Facilidade de expansão: é relativamente simples aumentar a capacidade do storage conforme o crescimento do volume de dados.

2.3.3.2.3. Aproveitamento de infraestrutura existente: pode reutilizar storages já presentes no ambiente, reduzindo custos iniciais.

2.3.3.2.4. Integração: muitos storages suportam recursos como snapshots e replicação, potencializando as estratégias de proteção de dados.

2.3.3.2.5. Possibilidade de deduplicação: dependendo do storage e do software, é possível implementar deduplicação e compressão, embora muitas vezes com taxas inferiores às dos appliances dedicados.

#### 2.3.3.3. Pontos fracos:

2.3.3.3.1. Possíveis problemas de compatibilidade: nem todos os storages oferecem integração total com todos os softwares de backup.

2.3.3.3.2. Segurança variável: recursos avançados de proteção, como imutabilidade e detecção de ransomware, nem sempre estão presentes ou dependem de integrações adicionais.

2.3.3.3.3. Desempenho variável: o desempenho pode ser impactado se o storage não for dimensionado corretamente para as cargas de backup e restauração.

2.3.3.3.4. Redução de dados geralmente inferior: as taxas de deduplicação e compressão podem ser menores do que as oferecidas por appliances otimizados.

### 2.3.4. Software de backup com backup em fitas

2.3.4.1. Esta arquitetura utiliza o software de backup para gerenciar a gravação dos dados em fitas magnéticas, tradicionalmente conhecidas como LTO (Linear Tape-Open). É uma solução consolidada para arquivamento e retenção de longo prazo.

**2.3.4.2. Pontos fortes:**

2.3.4.2.1. Custo por TB muito baixo: fitas são economicamente vantajosas para grandes volumes de dados e retenção prolongada.

2.3.4.2.2. Longevidade e durabilidade: fitas armazenadas corretamente têm vida útil superior a mídias de disco convencionais.

2.3.4.2.3. Desconexão física: o armazenamento offline dificulta ataques diretos, especialmente ransomware.

2.3.4.2.4. Capacidade de arquivamento: bom para cumprir exigências legais e regulatórias de retenção de dados por vários anos.

2.3.4.2.5. Deduplicação via software: alguns softwares de backup oferecem deduplicação antes da gravação em fita, reduzindo o volume, mas normalmente com eficiência inferior às soluções baseadas em disco.

**2.3.4.3. Pontos fracos:**

2.3.4.3.1. Desempenho de recuperação: a restauração é consideravelmente mais lenta em relação a discos ou appliances modernos.

2.3.4.3.2. Gestão operacional: o manuseio físico das fitas exige procedimentos rigorosos e recursos humanos dedicados.

2.3.4.3.3. Risco de perda ou dano físico: fitas podem ser extraviadas ou danificadas se não forem armazenadas corretamente.

2.3.4.3.4. Limitações tecnológicas: falta de recursos avançados como imutabilidade nativa e integração com verificadores de ameaças.

2.3.5. **Backup as a Service (BaaS)**

2.3.5.1. Nesta modalidade, a organização contrata um serviço externo (em nuvem) para proteger seus dados, sem a necessidade de infraestrutura local. O provedor é responsável por toda a operação, armazenamento, atualização e segurança dos backups.

**2.3.5.2. Pontos fortes:**

2.3.5.2.1. Simplicidade operacional: elimina a necessidade de aquisição,

manutenção e atualização de infraestrutura local, facilitando a gestão de backup.

2.3.5.2.2. Escalabilidade: permite rápida expansão ou redução do ambiente de backup, conforme a demanda da organização.

2.3.5.2.3. Acesso a tecnologias modernas: provedores BaaS geralmente oferecem deduplicação, compressão, criptografia e proteção contra ransomware de última geração.

2.3.5.2.4. Alta disponibilidade: o backup na nuvem oferece redundância e resiliência geográfica, reduzindo riscos de perda total de dados locais.

2.3.5.2.5. Atualizações automáticas: a infraestrutura e o software são constantemente atualizados pelo provedor, garantindo acesso a novos recursos e correções de segurança.

**2.3.5.3. Pontos fracos:**

2.3.5.3.1. Custos de nuvem imprevisíveis: o modelo de cobrança por capacidade, transferência e retenção pode gerar custos recorrentes elevados e difíceis de prever, especialmente em ambientes com grandes volumes de dados ou necessidades de recuperação frequentes.

2.3.5.3.2. Dependência da conectividade: a velocidade e a disponibilidade para backup e restauração dependem da qualidade da conexão com a internet.

2.3.5.3.3. Controle limitado: personalizações avançadas, integrações específicas e políticas detalhadas podem ser limitadas conforme o serviço contratado.

2.3.5.3.4. Privacidade e conformidade: deve-se avaliar se o provedor atende a todos os requisitos regulatórios e de segurança do setor.

2.3.5.3.5. Risco de lock-in: trocar de provedor pode ser oneroso e complexo devido à grande quantidade de dados armazenados e integrações proprietárias.

## 2.4. JUSTIFICATIVA TÉCNICA

2.4.1. A opção pela arquitetura software de backup com storage tradicional foi descartada devido à sua menor eficiência na redução de dados, à ausência de recursos nativos, na grande maioria, de proteção avançada contra ameaças cibernéticas e à necessidade de maior esforço de integração e gestão. Embora permita o reaproveitamento de infraestrutura já existente e ofereça flexibilidade na escolha de componentes, a maioria dos storages tradicionais não dispõe de mecanismos tão otimizados de deduplicação, compressão e imutabilidade quanto os appliances especializados. Isso pode resultar em maior consumo de espaço, custos operacionais mais altos e um nível de proteção inferior diante de ameaças como ransomware.

2.4.2. A arquitetura de software de backup com fitas também apresenta limitações que a tornam inadequada para a realidade de ambientes modernos. Apesar de seu baixo custo por terabyte e da proteção física oferecida pelo air gap, o uso de fitas acarreta desafios operacionais importantes, como lentidão na restauração, dependência de processos manuais e falta de automação. Além disso, fitas não oferecem recursos nativos de proteção contra ataques digitais sofisticados.

2.4.3. No caso do Backup as a Service (BaaS), a principal preocupação reside nos custos recorrentes e potencialmente imprevisíveis da nuvem, que podem crescer além do planejado conforme o volume de dados e as demandas de restauração aumentam. Porém, esse modelo vem se consolidando como alternativa prática e eficiente para proteger serviços já hospedados em nuvem, como é o caso do Microsoft 365 (O365/M365). Nesse cenário, os dados residem fora do datacenter local e podem ser copiados para outro provedor de nuvem de forma ágil, com menor dependência da infraestrutura interna de TI.

2.4.4. Por outro lado, a utilização do BaaS para realizar o backup de dados armazenados em servidores locais de um datacenter não é adequada. Isso ocorre porque, em cenários de grande volume de dados, o envio e a recuperação integral pela internet esbarram em gargalos de largura de banda, elevando os tempos de backup e, principalmente, de restauração em caso de desastre. Fabricantes como Dell, HPE, Huawei, Veritas e ExaGrid oferecem appliances otimizados para alta taxa de transferência local — variando de dezenas a centenas de terabytes por hora— desempenho impraticável em links convencionais de internet. Portanto, para ambientes on-premise, soluções dedicadas de backup em appliances permanecem a escolha mais segura e eficiente

2.4.5. Frente às limitações apresentadas pelas outras arquiteturas, para os dados armazenados localmente, a escolha pela arquitetura de software de backup com appliance de backup (que é a atual estrutura do TCDF), mostra-se a mais equilibrada e robusta. Esta solução permite que o Tribunal escolha o melhor software para suas necessidades (em termos de usabilidade, integração e suporte a diferentes cargas de trabalho) e, ao mesmo tempo, utilize appliances de backup com tecnologias avançadas de deduplicação, compressão, imutabilidade e proteção contra ameaças modernas. Isso garante eficiência na redução de dados, menor uso de espaço, maior velocidade nas operações de backup e restauração e proteção contra ataques como ransomware.

2.4.6. Além disso, a combinação de software e appliance traz flexibilidade e liberdade para o Tribunal, evitando o lock-in tecnológico e permitindo negociações mais vantajosas em futuras expansões ou atualizações. O mercado já oferece alta interoperabilidade entre soluções líderes, com certificações e integrações testadas, o que proporciona confiabilidade operacional e facilidade de suporte, seja por meio dos próprios fabricantes ou de integradores especializados.

2.4.7. Destaca-se que tanto os appliances quanto os softwares líderes oferecem recursos avançados de auditoria, retenção personalizada e controle granular dos acessos. A possibilidade de crescimento modular, a performance superior nos processos de backup/restauração e a resiliência contra ameaças cibernéticas tornam essa arquitetura a escolha mais alinhada com as demandas do Tribunal.

2.4.8. Assim, a decisão por essa arquitetura reflete a busca pelo melhor equilíbrio entre flexibilidade, segurança, desempenho e previsibilidade operacional, garantindo proteção eficaz dos dados, facilidade de gestão e preparo para os desafios tecnológicos dos próximos anos.

2.4.9. Por fim, para o ambiente Microsoft 365, que está na nuvem, tanto a arquitetura de software e appliance, quanto a BaaS atenderiam a demanda de salvaguarda dos dados. Dessa forma, optar-se-á pela estrutura mais econômica, que será apresentada no próximo tópico deste ETP.

## 2.5. JUSTIFICATIVA ECONÔMICA

2.5.1. Ao considerar investimentos em soluções de backup, a análise econômica vai além do custo inicial de aquisição dos equipamentos e licenças. É fundamental avaliar todo o ciclo de vida da solução, os custos operacionais, os ganhos de eficiência e as economias indiretas

resultantes da arquitetura escolhida. A combinação de software de backup com appliance de backup se destaca justamente por proporcionar vantagens econômicas robustas ao longo do tempo.

2.5.2. O primeiro grande diferencial econômico dessa arquitetura é a elevada taxa de redução de dados proporcionada por recursos avançados de deduplicação e compressão nos appliances. Com isso, a necessidade de espaço físico para armazenamento é drasticamente reduzida, diminuindo o investimento em discos, energia elétrica e refrigeração. Em ambientes onde o volume de dados cresce rapidamente, essa eficiência faz toda a diferença, representando uma economia contínua e sustentável no consumo de recursos de storage.

2.5.3. Outro ponto relevante é o impacto positivo sobre a infraestrutura de rede. Como os dados duplicados não são armazenados novamente, o tráfego entre servidores e appliances é menor, otimizando o uso da banda e reduzindo custos com upgrades ou contratação de links mais robustos para replicação e backup remoto.

2.5.4. O modelo appliance, aliado a um software robusto, também contribui para reduzir custos com gestão e suporte. O gerenciamento centralizado, a facilidade de monitoramento e a automação dos processos diminuem a necessidade de intervenções manuais e de profissionais altamente especializados para atividades rotineiras. Isso libera a equipe de TI para focar em iniciativas estratégicas, permitindo ganhos de produtividade.

2.5.5. A arquitetura permite ainda um crescimento modular, evitando investimentos excessivos de uma só vez. É possível expandir a capacidade dos appliances conforme a demanda, sem desperdício de recursos e sem a necessidade de grandes projetos de redesenho da solução.

2.5.6. Além disso, ao proporcionar alta performance nas rotinas de backup e restauração, essa arquitetura minimiza o tempo de indisponibilidade em caso de incidentes. O impacto financeiro da interrupção de operações costuma ser elevado, e uma solução capaz de restaurar dados com rapidez protege o Tribunal de prejuízos operacionais, perda de produtividade e danos à reputação.

2.5.7. Outro ponto importante é o aumento da segurança contra ameaças digitais, como ransomware, que podem gerar enormes prejuízos à imagem da Corte e, em última análise, à população do Distrito Federal. Com proteção nativa contra ataques e recursos como imutabilidade e isolamento dos dados, o risco de precisar recorrer a soluções emergenciais, pagar resgates ou sofrer outros prejuízos é reduzido.

2.5.8. Em síntese, a arquitetura de software de backup com appliance de backup oferece não só um excelente custo-benefício imediato, mas, sobretudo, uma economia sustentável e estratégica ao longo do tempo, equilibrando eficiência operacional, proteção robusta dos dados e flexibilidade para o crescimento do negócio.

2.5.9. No caso específico do ambiente Microsoft 365, adoção de backup em nuvem apresenta vantagens técnicas e econômicas relevantes quando comparada à aquisição de appliances físicos dedicados. Enquanto os appliances de backup oferecem alto desempenho e baixa latência para grandes volumes de dados locais, seu custo por terabyte tende a ser significativamente mais elevado, tanto pelo investimento inicial em hardware quanto pela necessidade de manutenção, energia, refrigeração e atualizações constantes.

2.5.10. Para esse backup, o requisito de desempenho de rede não é um fator crítico, pois os dados já residem nativamente na nuvem. Diferentemente dos cenários on-premises, onde grandes volumes precisam ser transferidos rapidamente para atender a janelas de backup e tempos de recuperação, os backups do M365 envolvem recuperação granular de e-mails, arquivos do OneDrive, SharePoint e Teams, com menor impacto em largura de banda. Assim, a contratação de backup em nuvem para o ambiente Microsoft mostra-se tecnicamente mais adequada e financeiramente vantajosa, assegurando proteção contínua dos dados institucionais sem a necessidade de investimentos onerosos em appliances locais, cujo diferencial de desempenho não seria plenamente aproveitado nesse contexto.

2.5.11. Para comprovar a vantajosidade da contração de backup em nuvem para o ambiente Microsoft, em comparação ao backup 100% local, solicitou-se a fornecedores cotações que contemplassem os dois cenários. Essas cotações estão nos e-DOCs: CDF63155, 11EE0EC4 e 1EA9DA27.

2.5.12. Conforme se percebe, o cenário que aborda as duas arquiteturas, isto é, backup em appliances locais para dados de sistemas locais e backup em nuvem para o ambiente Microsoft, é mais econômico para o Tribunal.

UNITECH

## PROPOSTA COMERCIAL

**AO Tribunal de Contas do Distrito Federal – TCDF**

A Unitech, inscrita no CNPJ 03.535.902/0001-10, situada na SHS Quadra 06, Bloco A, Sala 102 - Asa Sul, Brasília/DF, vem, por meio desta, apresentar sua proposta de fornecimento de Solução BACKUP.

**CENÁRIO 1: BACKUP LOCAL + CLOUD**

| ITEM | DESCRIÇÃO DO ITEM | | UND | VALOR UNITÁRIO | VALOR TOTAL |
|---|---|---|---|---|---|
| 1 | **Aquisição de solução de Backup local + cloud** | Data Domain 6410 com Cyber Recovery | 2 | R$ 3.343.401,50 | R$ 6.686.803,00 |
| | | Servidor para CommServe Server e Media Agent | 2 | R$ 191.875,00 | R$ 383.750,00 |
| | | Licenças Commvault B&R + Cloud Storage | 1 | R$ 1.731.210,00 | R$ 1.731.210,00 |
| | | Licenças Commvault Cloud Cyber Recovery | 1 | **R$ 680.705,00** | R$ 680.705,00 |
| Valor total | | | | | R$ 9.482.468,00 |

Figura 1 – Backup local + backup na nuvem

**CENÁRIO 2 - BACKUP LOCAL**

| ITEM | DESCRIÇÃO DO ITEM | | UND | VALOR UNITÁRIO | VALOR TOTAL |
|---|---|---|---|---|---|
| 1 | **Aquisição de solução de Backup local + cloud** | Data Domain 9410 com Cyber Recovery | 2 | R$ 4.817.109,50 | R$ 9.634.219,00 |
| | | Servidor para CommServe Server e Media Agent | 2 | R$ 185.275,00 | R$ 370.550,00 |
| | | Licenças Commvault B&R + Cloud Storage | 1 | R$ 1.674.100,00 | R$ 1.674.100,00 |
| | | Licenças Commvault Cloud Cyber Recovery | 1 | R$ 658.190,00 | R$ 658.190,00 |
| Valor total | | | | | R$ 12.337.059,00 |

VALOR TOTAL: R$12.337.059,00 (Doze milhões, trezentos e trinta e sete mil e cinquenta e nove reais)

Figura 2 – Backup 100% local

O2 Soluções em tecnologia digital Ltda.

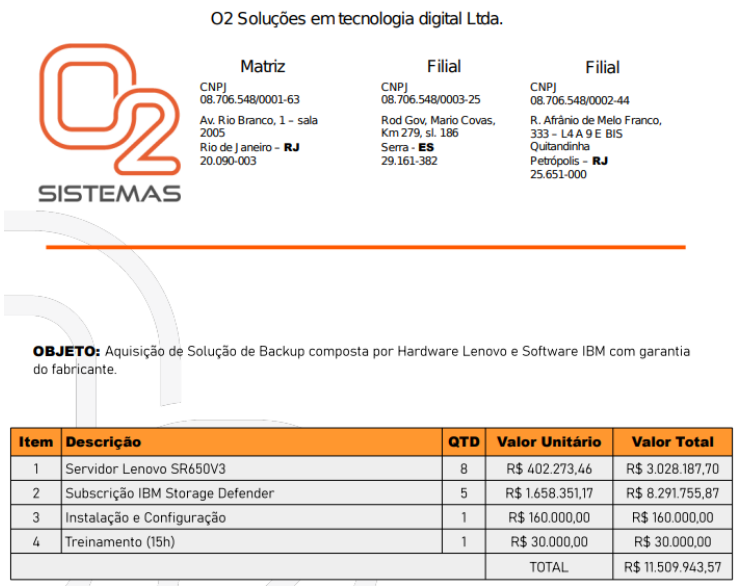
SISTEMAS

| Matriz | Filial | Filial |
|---|---|---|
| CNPJ 08.706.548/0001-63 | CNPJ 08.706.548/0003-25 | CNPJ 08.706.548/0002-44 |
| Av. Rio Branco, 1 – sala 2005 Rio de Janeiro – **RJ** 20.090-003 | Rod Gov, Mario Covas, Km 279, sl. 186 Serra - **ES** 29.161-382 | R. Afrânio de Melo Franco, 333 – L4 A 9 E BIS Quitandinha Petrópolis – **RJ** 25.651-000 |

**OBJETO:** Aquisição de Solução de Backup composta por Hardware Lenovo e Software IBM com garantia do fabricante.

| Item | Descrição | QTD | Valor Unitário | Valor Total |
|---|---|---|---|---|
| 1 | Servidor Lenovo SR650V3 | 8 | R$ 292.092,96 | R$ 2.336.743,73 |
| 2 | Subscrição IBM Storage Defender | 5 | R$ 488.003,86 | R$ 2.440.019,30 |
| 3 | Subscrição IBM Storage Protect for Cloud | 5 | R$ 239.764,48 | R$ 1.198.822,40 |
| 4 | Instalação e Configuração | 1 | R$ 160.000,00 | R$ 160.000,00 |
| 5 | Treinamento (15h) | 1 | R$ 30.000,00 | R$ 30.000,00 |
| | | | TOTAL | R$ 6.165.585,43 |

Figura 3 – Backup local + backup na nuvem



O2 Soluções em tecnologia digital Ltda.

| Matriz | Filial | Filial |
|---|---|---|
| CNPJ 08.706.548/0001-63 | CNPJ 08.706.548/0003-25 | CNPJ 08.706.548/0002-44 |
| Av. Rio Branco, 1 – sala 2005 Rio de Janeiro – **RJ** 20.090-003 | Rod Gov. Mario Covas, Km 279, sl. 186 Serra - **ES** 29.161-382 | R. Afrânio de Melo Franco, 333 – L4 A 9 E BIS Quitandinha Petrópolis – **RJ** 25.651-000 |

**OBJETO:** Aquisição de Solução de Backup composta por Hardware Lenovo e Software IBM com garantia do fabricante.

| Item | Descrição | QTD | Valor Unitário | Valor Total |
|---|---|---|---|---|
| 1 | Servidor Lenovo SR650V3 | 8 | R$ 402.273,46 | R$ 3.028.187,70 |
| 2 | Subscrição IBM Storage Defender | 5 | R$ 1.658.351,17 | R$ 8.291.755,87 |
| 3 | Instalação e Configuração | 1 | R$ 160.000,00 | R$ 160.000,00 |
| 4 | Treinamento (15h) | 1 | R$ 30.000,00 | R$ 30.000,00 |
| | | | TOTAL | R$ 11.509.943,57 |

Figura 4 – Backup 100% local

## 2.6. ESCOLHA DAS SOLUÇÕES

2.6.1. São várias as soluções que podem atender às necessidades do projeto, em especial as presentes nos artigos abaixo, desde que atendam ao especificado no Termo de Referência:

2.6.1.1. Market Guide for Enterprise Backup Storage Appliances[1];

2.6.1.2. Magic Quadrant for Backup and Data Protection Platforms[2];

2.6.1.3. Magic Quadrant for Enterprise Backup and Recovery Software Solutions[3].

2.6.2. Das soluções existentes, destacam-se as consideradas líderes pelo Gartner ou aquelas com bastante representatividade no mercado: Veeam, Commvault, Rubrik, Cohesity, Dell Technologies, Druva, Veritas, ExaGrid, Hewlett Packard Enterprise.

# 3. DESCRIÇÃO DA SOLUÇÃO

## 3.1. ESPECIFICAÇÕES TÉCNICAS

### 3.1.1. **Arquitetura da solução de proteção de dados local**

[1] https://www.gartner.com/document-reader/document/4940731?ref=solrAll&refval=478132261#4b755704-a537-4b2b-949e-cdaf7fa8c633. Acessado em 01/07/2025.
[2] https://www.gartner.com/interactive/mq/6640734?ref=solrAll&refval=478132261. Acessado em 01/07/2025.
[3] https://www.gartner.com/document-reader/document/5649023?ref=solrAll&refval=478132261. Acessado em 01/07/2025.

3.1.1.1. A CONTRATADA deverá entregar a solução totalmente operacional (montada, instalada e configurada), com todas as licenças, hardware e software necessários para o pleno funcionamento da solução, devidamente pronta para utilização, em dois locais distintos, a saber:

3.1.1.1.1. Datacenter do Tribunal de Contas do Distrito Federal – TCDF (software de backup e um appliance de discos – produção);

3.1.1.1.2. Na Sala de collocation do datacenter IPEDF (Centro de Dados), da Secretaria Executiva de Tecnologia da Informação e Comunicação (SETIC), da Secretaria de Estado de Economia do Distrito Federal, no Setor de Administração Municipal, bloco H, 70.620-080.

3.1.1.2. A estrutura da solução será montada da seguinte forma:

3.1.1.2.1. Para o site principal (produção), serão instalados e configurados o software de backup e appliance de backup de produção;

3.1.1.2.2. Para o site de secundário (recuperação de desastres), será instalado apenas um appliance de backup, que receberá cópias diárias dos backups executados no ambiente principal.

3.1.1.3. A replicação de dados deverá estar licenciada entre os dispositivos que compõem a solução.

3.1.1.4. A solução ofertada (Hardware e Software de Backup) não poderá utilizar recursos da infraestrutura do TCDF, como, por exemplo, área do storage, criação de máquinas virtuais no ambiente de virtualização e criação de estruturas em bancos de dados do TCDF.

3.1.1.5. A solução de proteção de dados deverá implementar, com todo o licenciamento necessário, o conceito de Air Gap entre o site principal e o site backup.

3.1.1.6. A solução será composta de 3 (três) itens, agrupados em lote único.

### 3.1.2. ITEM 1 - SOFTWARE DE BACKUP LOCAL E APPLIANCES

#### 3.1.1.7. Especificações gerais

3.1.1.7.1. A fabricante do software de backup deverá estar no quadrante

do Gartner sobre o tema – Magic Quadrant for Enterprise Backup and Recovery Software Solutions, nas categorias Challengers, Leaders ou Visionaries.

3.1.1.7.2. Caso o licenciamento da solução seja perpétuo, deverá ser fornecido suporte técnico e garantia por 60 meses. Após o fim do suporte e garantia, a solução deverá continuar operacional, mesmo não recebendo mais atualizações.

3.1.1.7.3. Caso o licenciamento seja por subscrição, deverá ser fornecido por 60 meses, porém a solução deverá continuar operacional após a validade das licenças para, pelo menos, restore de backups.

3.1.1.7.4. O licenciamento da solução deve abranger:

3.1.1.7.4.1. Para o ambiente on-premise, backup e restore, irrestrito, dos dados de, no mínimo, 167 máquinas virtuais.

3.1.1.7.4.2. Caso o modelo de licenciamento da solução não seja por máquina virtual, e sim por front-end, deve-se considerar o seguinte volume de dados que será armazenado: **Front-end armazenado: 249,46 TB**

3.1.1.7.5. Caso a taxa de redução de dados de 16,7:1 não seja alcançada pela solução (software de backup + appliance de backup), a contratada deverá, a qualquer tempo, quando solicitado pela contratante, adicionar mais discos ao appliance ofertado para suportar a volumetria do projeto.

3.1.1.7.6. A verificação será feita, anualmente, em conjunto com a CONTRATADA.

3.1.1.7.7. A solução de backup e o appliance de backup deverão conter dashboards que demonstrem a taxa de redução de dados obtida pela solução de backup.

3.1.1.7.8. Possuir banco de dados ou catálogo interno, contendo informações sobre todos os arquivos e mídias onde os backups foram armazenados.

3.1.1.7.9. Possibilitar a reconstrução do catálogo ou banco de

dados no caso de perda de algum deles.

3.1.1.7.10. Permitir proteger, exportar ou replicar o catálogo interno ou banco de dados para fins de recuperação em caso de desastre.

3.1.1.7.11. O software de backup deverá suportar criptografia de dados na origem (cliente de backup), de forma que seja garantido que o dado trafegará na rede local ou na rede WAN criptografado.

3.1.1.7.12. Possuir a capacidade de atualizar os agentes clientes de backup, de forma automática e centralizada.

**3.1.1.8. Gerenciamento**

3.1.1.8.1. Possuir ambiente de gerenciamento de backup e restore via interface gráfica e linha de comando.

3.1.1.8.2. A solução de backup deverá, a partir de uma única interface, ser capaz de gerenciar e executar operações de backup/restore dos sistemas operacionais Windows, Linux e Unix Like; ambientes de virtualização baseados em KVM e FusionCompute; Microsoft Active Directory e banco de dados Microsoft SQL Server, PostgreSQL e MariaDB/MySQL.

3.1.1.8.3. No caso dos bancos de dados MariaDB e MySQL, caso a integração não seja nativa, será aceito o backup via script, a ser fornecido pela CONTRATADA.

3.1.1.8.4. Se houver múltiplos ambientes de backup, uma única interface web deverá ser capaz de monitorar e agregar as informações.

3.1.1.8.5. A arquitetura da solução deve ser flexível e escalável, permitindo sua instalação, configuração e uso em sites remotos interligados ao site principal através de WAN.

3.1.1.8.6. A solução de backup deve permitir o controle da banda utilizada ou possuir otimização durante a operação de backup, através do software de proteção de dados;

3.1.1.8.7. A console de gerência deverá suportar alta disponibilidade entre sites, para, caso o servidor de produção ativo tenha algum problema, o servidor

passivo (outro site) assuma as rotinas de backup até o servidor principal voltar a ficar operacional.

3.1.1.8.8. Possuir função de agendamento do backup através de calendário.

3.1.1.8.9. Possuir capacidade de estabelecer níveis de acesso diferenciados e configuráveis para atividades de administração e operação do software de backup.

3.1.1.8.10. Permitir a programação de tarefas de backup automatizadas em que sejam definidos prazos ou pontos de retenção dos arquivos nos discos.

3.1.1.8.11. Deve possuir políticas de ciclo de vida de forma nativa (ILM – Information Lifecycle Management), para gerenciar camadas de armazenamento.

3.1.1.8.12. Deve possibilitar múltiplas cópias com políticas de ciclo de vida (ILM – Information Lifecycle Management).

3.1.1.8.13. A solução de backup deverá enviar traps SNMP (Simple Network Management Protocol) com o objetivo de reportar eventos ocorridos na operação da solução.

**3.1.1.9. Funcionalidades de proteção de dados – backup e restore**

3.1.1.9.1. Possuir capacidade de realizar backups completos (full), incrementais e sintéticos.

3.1.1.9.2. A solução de backup deverá implementar a execução de backups completos sintéticos. Um backup completo sintético é gerado através de um backup completo tradicional (não sintetizado) anterior e de backups diferenciais subsequentes ou de um backup incremental cumulativo. O backup sintetizado deverá ser capaz de restaurar arquivos e diretórios da mesma maneira que um cliente faz a restauração de um backup tradicional;

3.1.1.9.3. A solução de backup deverá possuir a funcionalidade de agendamento automático de jobs de backup;

3.1.1.9.4. A solução de backup deverá realizar backup e restore nos seguintes sistemas operacionais e aplicações:

3.1.1.9.4.1. Microsoft Windows Server 2012 e superiores;

3.1.1.9.4.2. Ubuntu Server 14.04 e superiores;

3.1.1.9.4.3. CentOS 6 e superiores;

3.1.1.9.4.4. PostgreSQL 17 e superiores;

3.1.1.9.4.5. MariaDB 10 e superiores;

3.1.1.9.4.6. Active Directory 2016 e superiores;

3.1.1.9.4.7. Microsoft SQL Server 2019 e superiores.

3.1.1.9.5. Permitir que o backup seja feito pela rede ethernet (corporativa ou dedicada ao backup), podendo ser LAN ou WAN.

3.1.1.9.6. Permitir a execução de backup em nível de volume, diretório e arquivo.

3.1.1.9.7. Possuir a capacidade de reiniciar backups ou restores a partir do ponto de falha, após a ocorrência da mesma.

3.1.1.9.8. Todas as licenças relativas ao catálogo ou base de dados, que devem ser capazes de indexar todos os arquivos protegidos, deverão ser fornecidas em conjunto com a solução proposta.

3.1.1.9.9. O software de backup deverá ser capaz de realizar cópia de arquivos abertos sem que a consistência deles seja comprometida.

3.1.1.9.10. O software de backup deverá ser capaz de enviar alertas através de correio eletrônico com o objetivo de reportar eventos ocorridos na operação.

3.1.1.9.11. O software de backup deverá possuir a funcionalidade de agendamento automático de jobs de backup, com opção de

configuração de prioridades, para que um job de maior prioridade seja inicializado primeiro ou possuir a funcionalidade de encadeamento de jobs, para que um só inicie após o outro ter terminado.

3.1.1.9.12. Deverá possibilitar a geração de mais de uma cópia do backup sem que haja necessidade de nova conexão com o cliente.

3.1.1.9.13. O software de backup deverá possuir a funcionalidade de criar múltiplas cópias de backups armazenados, com a opção de recuperação dos dados através do site secundário se o site primário não estiver disponível.

### 3.1.1.10. Microsoft SQL Server

3.1.1.10.1. Deverá executar backup e restore do Microsoft SQL Server com as seguintes características nativas sem a necessidade de criação de scripts:

3.1.1.10.1.1. Executar backup e restore das bases de dados do Microsoft SQL Server sem parada do banco;

3.1.1.10.1.2. Executar backup de Transaction log possibilitando a criação de rotina de backup para que ocorra com intervalos de 1 (uma) hora;

3.1.1.10.1.3. Recuperação completa da Base de dados no mesmo servidor;

3.1.1.10.1.4. Recuperação completa da Base de dados em outro servidor;

3.1.1.10.1.5. Recuperação de uma base específica;

3.1.1.10.1.6. Recuperação em um momento do tempo específico;

### 3.1.1.11. Active Directory

3.1.1.11.1. Deverá executar backup do Microsoft Active Directory.

3.1.1.11.2. Possibilitar as seguintes opções de recuperação:

3.1.1.11.2.1. Recuperação de um objeto;

3.1.1.11.2.2. Recuperação de um atributo;

3.1.1.11.2.3. Recuperação de um atributo de um objeto deletado;

3.1.1.11.2.4. Permitir comparar os objetos com a produção, permitindo restaurar apenas os itens ausentes ou alterados.

**3.1.1.12. Funcionalidades de replicação de backup**

3.1.1.12.1. A solução de proteção de dados deverá ser capaz de realizar a replicação de dados entre appliances de backup do mesmo modelo localizados em sites remotos.

3.1.1.12.2. A solução de proteção de dados deverá permitir restore dos dados a partir das cópias armazenadas nos appliances de backup em disco remotos.

**3.1.1.13. Funcionalidades de controle de backup em disco**

3.1.1.13.1. A solução de backup deve permitir uso da tecnologia de deduplicação de dados para toda a capacidade licenciada, eliminando blocos repetidos, para backup/arquivamento em disco e movimentação/replicação de dados deduplicados, independente de quantitativo de dispositivos de armazenamento que compõem a infraestrutura da CONTRATANTE;

3.1.1.13.2. A solução deverá implementar deduplicação a nível de blocos, não sendo aceita a técnica de Single-Instance Storage;

3.1.1.13.3. Deverá implementar deduplicação de blocos na origem (client-side deduplication), de forma que o cliente envie apenas novos blocos de dados criados e/ou modificados a partir do último backup full;

3.1.1.13.4. Possuir a função de disk staging, ou seja, que permite o envio dos dados para disco e posteriormente do disco para outro tipo de mídia (disco ou tape).

3.1.1.13.5. Possuir a capacidade de verificar o conteúdo do

backup, de forma a garantir que esteja íntegro.

3.1.1.13.6. Deve conter, dentro do catálogo interno ou banco de dados, informações dos backups que foram realizados, possibilitando mostrar o conteúdo interno de cada backup, para facilitar a administração e o controle.

3.1.1.13.7. O software de backup e/ou a solução de proteção de dados deve ser capaz de utilizar o appliance de backup em disco como destino de backup.

3.1.1.13.8. O software de backup deverá permitir a gravação de backups Disk-to-Disk.

3.1.1.13.9. Para a configuração do repositório de dados em disco, o software de backup deverá suportar as seguintes funções:

3.1.1.13.9.1. Permitir gravação de dados de backup em compartilhamento de redes CIFS ou Network File System (NFS);

3.1.1.13.9.2. Configuração de alertas para informar falta de espaço disponível para armazenamento em disco;

3.1.1.13.9.3. Capacidade de expansão do volume de armazenamento em disco;

**3.1.1.14. Suporte de ambientes**

3.1.1.14.1. O software de backup deverá ser capaz de fazer backup e restore de ambientes virtualizados (servidores virtuais configurados em servidores físicos), com suporte à tecnologia de virtualização KVM e FusionCompute.

3.1.1.14.2. O software de backup deve possuir a capacidade de realizar backup e restore de file systems montados em dispositivos.

3.1.1.14.3. Deverá suportar backup de ambiente PROXMOX, pelo menos, via agente.

### 3.1.1.15. Funcionalidades de geração de relatórios

3.1.1.15.1. Permitir gerar relatórios customizáveis com os seguintes dados para, pelo menos 1 ano:

3.1.1.15.1.1. Backups com sucesso;

3.1.1.15.1.2. Backups com falha;

3.1.1.15.1.3. Volume de backup realizado;

3.1.1.15.1.4. Restores com sucesso;

3.1.1.15.1.5. Restores com falha;

3.1.1.15.1.6. Volume de restore realizado;

3.1.1.15.1.7. Clientes de backup configurados;

3.1.1.15.1.8. Ocupação no destino de backup;

3.1.1.15.1.9. Licenciamento e capacidade;

3.1.1.15.1.10. Taxa de deduplicação.

### 3.1.1.16. Segurança

3.1.1.16.1. A solução deverá permitir a proteção do catálogo/database de forma local. Adicionalmente a solução deverá proteger o catálogo/database do software em nuvem pública ou em algum outro meio indicado pela contratada

3.1.1.16.2. Os dados armazenados nos repositórios de backup devem estar protegidos contra alterações indesejadas, e ser imutáveis, ou seja, não podem ser modificados por agentes externos ao backup, de modo que eles só possam ser alterados ou removidos mediante expiração do backup e respeitar o período estabelecido para remoção;

3.1.1.16.3. O software de proteção de dados deverá possuir o recurso de MFA Multi-Factor Authentication para acesso a interface administrativa;

3.1.1.16.4. Deverá exigir a autenticação e autorização de um segundo

usuário (escalação) para concluir a alteração de parâmetros críticos, como, por exemplo, a deleção de uma imagem de backup;

3.1.1.16.5. O software de proteção de dados deverá entregar mecanismos de fluxo de aprovação para atividades como deleção de um backup, deleção de um cliente ou modificação de alguma tarefa de backup. O objetivo dessa funcionalidade é garantir que nenhuma informação será perdida caso alguma senha da ferramenta de backup seja comprometida;

3.1.1.16.6. A solução de backup deverá implementar criptografia de dados no destino do backup, de uma forma que seja garantido que os dados sejam criptografados, suportando chave de 256 bits.

3.1.1.16.7. A solução deve prover um dashboard para monitoramento de Ameaças, permitindo assim a visibilidade de anomalias e falhas de backup, bem como uma visualização única de alertas atuais, histórico e tendências;

3.1.1.16.8. Monitoramento Ativo: A solução deverá monitorar continuamente as métricas para atividades anômalas do sistema de arquivos, como modificações e exclusões. Quando alterações anômalas no sistema de arquivos forem detectadas, alertas deverão ser acionados para fornecer motivo para ação. A solução deverá possuir mecanismos que permitam que alertas sejam integrados a informações de segurança e gerenciamento de eventos (SIEM), outros sistemas de resposta a incidentes ou iniciar fluxos de trabalho.

3.1.1.16.9. A solução deverá ser capaz de aplicar políticas de imutabilidade tanto em discos locais quanto em storages de objeto armazenados em nuvem pública.

3.1.1.16.10. A solução deverá suportar funcionalidade de imutabilidade dos dados.

3.1.1.16.11. A solução deverá fazer a verificação de malware ao salvar os dados e antes de qualquer restauração;

**3.1.1.17. Serviço de instalação:**

3.1.1.17.1. A CONTRATADA deverá apresentar um documento de planejamento da instalação de toda a solução;

3.1.1.17.2. A CONTRATADA será responsável por toda a instalação, configuração, integração, testes e validação da solução de backup no ambiente da CONTRATANTE;

3.1.1.17.3. Durante o serviço de instalação a CONTRATADA deverá:

3.1.1.17.3.1. Realizar a instalação dos appliances, incluindo conexões física e lógicas necessárias;

3.1.1.17.3.2. Realizar a instalação do software de backup, console de gerência e integração da solução com os clientes de backup;

3.1.1.17.3.3. Configurar a integração da solução de backup com a solução de virtualização em uso no ambiente da CONTRATANTE;

3.1.1.17.3.4. Configurar o backup granular do Active Directory instalado no ambiente da CONTRATANTE;

3.1.1.17.3.5. Configurar o backup transacional das bases de dados do SQL Server instalado no ambiente da CONTRATANTE;

3.1.1.17.3.6. Configurar o backup das bases de dados PostgreSQL e MARIADB instaladas no ambiente da CONTRATANTE;

3.1.1.17.3.7. Configurar as políticas de backup incluindo período de retenção de dados, periodicidade e janelas de realização do backup;

3.1.1.17.3.8. Configurar a replicação do backup para o appliance secundário instalado no site backup da CONTRATANTE;

3.1.1.17.3.9. Integrar a solução com o Microsoft Entra ID;

3.1.1.17.3.10. Configurar o backup das soluções de nuvem Microsoft 365: Exchange Online, SharePoint Online, OneDrive

for Business e Teams;

3.1.1.17.3.11. Configurar a autenticação multifator para acesso ao ambiente, incluindo ao menos 2 (dois) perfis de usuários distintos;

3.1.1.17.3.12. Validação do backup da própria base da solução (catálogo de backup);

3.1.1.17.3.13. Configurar o envio automático de relatórios diários de sucesso, falha e estatísticas de uso e desempenho da solução de backup;

3.1.1.17.3.14. Realizar testes de backup e restauração de ao menos 2 (duas) máquinas virtuais;

3.1.1.17.3.15. Realizar testes de backup e restauração de ao menos 1 (uma) base de dados do SQL Server;

3.1.1.17.3.16. Realizar testes de backup e restauração de ao menos 1 (uma) base de dados do PostgreSQL e MARIADB;

3.1.1.17.3.17. Realizar testes de backup e restauração de ao menos 2 (duas) caixas postais do Exchange Online, incluindo restauração granular;

3.1.1.17.3.18. Realizar testes de backup e restauração de ao menos 2 (dois) drives do OneDrive, incluindo restauração individual de arquivos;

3.1.1.17.3.19. Demonstração de restauração instantânea (instant recovery) de máquinas virtuais.

3.1.1.17.3.20. Todas as atividades deverão ser executadas com base nas melhores práticas recomendadas pelo fabricante;

3.1.1.17.4. A CONTRATADA deverá entregar documento As-Built, contendo:

3.1.1.17.4.1. Diagrama técnico da arquitetura implantada;

3.1.1.17.4.2. Lista completa dos componentes instalados e suas versões;

3.1.1.17.4.3. Relação de políticas, jobs, perfis, permissões e repositórios configurados;

3.1.1.17.4.4. Procedimentos de operação e contingência para restauração em caso de acionamento do plano de Disaster Recovery;

3.1.1.17.5. A documentação deverá ser entregue em formato digital e validada pela equipe da CONTRATANTE.

**3.1.1.18. Appliance de backup em disco:**

3.1.1.18.1. Deve constar no site do fabricante (documento oficial e público) como um appliance de backup em disco, em linha de produção. Também serão aceitos servidores OEM como base de hardware, porém deverão ser certificados e homologados pelo fabricante do software de backup.

3.1.1.18.2. Fazer parte do catálogo de produtos comercializados pelo fabricante, não ter sido descontinuado e não constar em listas de final de vida (EOL), final de serviço/suporte (EOS/EOSL), final de venda (EOS).

3.1.1.18.3. Deverá ter sua compatibilidade garantida pelo fabricante do software de backup ou pelo fabricante da solução de hardware, garantindo pleno funcionamento da arquitetura ofertada.

3.1.1.18.4. Permitir a utilização de todas as funcionalidades, tecnologias e recursos especificados, sem limitação do prazo de utilização, irrestrita e sem necessidade de licenciamentos ou ônus adicionais.

3.1.1.18.5. Deve possuir interface de administração GUI e CLI.

3.1.1.18.6. O sistema de armazenamento de backup de disco deverá conter discos para tolerância a falha, que serão usados para substituir e reconstruir automaticamente o dado de backup.

3.1.1.18.7. A arquitetura da solução ofertada para o armazenamento de dados de curta e longa retenção poderá utilizar equipamentos que forneçam a

retenção de curta duração separadamente da retenção de longa duração ou ser fornecida em dispositivo único.

3.1.1.18.8. A transferência de dados de backup entre as áreas de curta e longa retenção é de responsabilidade da Solução de Backup, seja através do Software de Backup ou do Hardware de Armazenamento de Dados.

3.1.1.18.9. O appliance de backup deverá fornecer throughput mínimo de 30 TB/hr.

3.1.1.18.10. Os dados armazenados devem estar totalmente protegidos contra acesso indevido, seja através de roubo de credencias ou escalação de privilégios, impedindo inclusive ataques do tipo ransomware, utilizando proteções como “air gap”, “backup offline” ou imutabilidade segura de forma a manter as cópias de backup protegidas, seja através da desconexão da rede, do acesso direto de usuários ou da garantia da imutabilidade dos dados (WORM), assegurando a integridade e autenticidade dos dados de backup armazenados contra ataques de ransomware.

3.1.1.18.11. A solução deverá possuir formas de prevenir, evitar ou reverter ações de caráter destrutivo dos dados armazenados utilizando técnicas como atraso na deleção ou prazo de retenção.

3.1.1.18.12. O hardware para o armazenamento de dados de longa retenção dos dados de backup deverá suportar a tecnologia WORM (write once ready many) no nível de pastas e a configuração de retenções dos dados arquivados deve possuir mecanismos de preservação que garantam a imutabilidade dos dados, que impeçam ou atrasem a remoção indesejável de arquivos.

3.1.1.18.13. Não serão aceitos para a composição da solução o uso de storages de armazenamento de uso convencional (NAS, DAS, SAN), agrupamentos de servidores conhecidos como “Server Farm” ou “Fazenda de servidores” ou soluções similares.

3.1.1.18.14. Devem incluir garantia fornecida pelo FABRICANTE e suporte técnico da CONTRATADA, ambos por um período mínimo de 60 (sessenta) meses, contados da emissão do Termo de Recebimento Definitivo – TRD.

3.1.1.18.15. Os discos e fontes de alimentação deverão ser redundantes e

hot-pluggable/ swappable.

3.1.1.18.16. Devem ser novos, de primeiro uso e vir acompanhado de todos os acessórios para a devida instalação em rack padrão 19 polegadas.

3.1.1.18.17. Os equipamentos devem permitir tensão de alimentação de, no mínimo, 110V e 220V (50Hz e 60Hz), com chaveamento automático, e serem fornecidos com cabos de alimentação no padrão NBR 14136 e C13/C14 (IEC 60320).

3.1.1.18.18. Devem possuir tecnologia de deduplicação de dados, ou seja, não armazenar mais de uma vez dados idênticos, permitindo eliminar segmentos redundantes, de forma a reduzir a utilização de espaço em disco destinada ao armazenamento dos dados de backup.

3.1.1.18.19. Devem possuir a capacidade nativa de realizar a replicação local e/ou remota (via protocolo TCP/IP) dos dados entre appliances do mesmo modelo em formato deduplicado, permitindo o restore dos dados a partir das cópias armazenadas nos appliances de backup em disco remotos.

3.1.1.18.20. A replicação de dados entre appliances deverá permitir que somente os dados já deduplicados sejam transferidos localmente e/ou remotamente (via protocolo TCP/IP), de forma a diminuir o tempo necessário para a movimentação dos dados (janela de backup).

3.1.1.18.21. Deve ser fornecido com todas as licenças necessárias para a realização das operações de administração, geração de relatórios, gravação de dados, recuperação de dados, deduplicação, replicação de dados e air gap, já descontadas todas as perdas com redundâncias, paridades e de proteção do arranjo de discos.

3.1.1.18.22. Devem garantir a segurança dos dados armazenados em casos de falha de alimentação elétrica e de falha lógica de escrita/leitura.

3.1.1.18.23. Devem ser fornecidos com a seguinte conectividade:

3.1.1.18.23.1. 01 (uma) porta Gigabit Ethernet de gerência para conexão de cabos UTP CAT6 e conectores RJ-45;

3.1.1.18.23.2. 04 (quatro) portas, no mínimo, Gigabit Ethernet para conexão de cabos UTP CAT6 e conectores RJ-45;

3.1.1.18.23.3. 4 (quatro) portas de 25Gbits/s para conexão com switch SFP28, por controladora; caso o equipamento não utilize o conceito de controladora separada que consolida toda a solução, cada nó do sistema de backup deverá contar com 04 (quatro) portas de 25Gbits/s;

3.1.1.18.23.4. Devem ser fornecidos cabos de fibra óptica de 5 (cinco) metros, para cada porta de 25 Gbits/s da solução, com os respectivos transceivers (GBICs) SFP28, tanto para o appliance, quanto para o switch em que ele será conectado, com conectores do tipo LC-LC, com capacidade de se conectar a portas SFP28 dos switches;

3.1.1.18.24. Se a solução de armazenamento for baseada em gavetas de discos, a arquitetura deve ser redundante, com no mínimo 2 (dois) caminhos de acesso às gavetas.

3.1.1.18.25. Deve possuir, no mínimo, 215 TB de capacidade útil, sem considerar ganhos com deduplicação e compressão. Essa capacidade é líquida, isto é, deve ser considerada após as configurações de redundância do equipamento, em especial RAID 6 ou Erasure Code.

3.1.1.18.26. O appliance deverá ser entregue em, no máximo, 16 rack units, incluindo a controladora e as gavetas de disco.

3.1.1.18.27. Devem possuir ferramenta de gerenciamento para total administração e configuração dos appliances de backup em disco, permitindo configuração e monitoramento de equipamentos locais ou remotos, além de permitir a análise de desempenho e implementação das políticas de segurança e acesso dos usuários.

3.1.1.18.28. A solução deve ser fornecida com todos os acessórios necessários para a plena configuração, operacionalização, utilização e gerenciamento do equipamento, sem necessidade de aquisições futuras de licenças ou softwares de ativação.

3.1.1.18.29. Entende-se por deduplicação a funcionalidade que previne o armazenamento de dados duplicados, com a eliminação dos segmentos redundantes e compactação dos dados de forma a reduzir o tamanho do espaço em disco destinada ao armazenamento dos dados de backup.

3.1.1.18.30. A solução de backup deverá ser capaz de gerenciar a réplica do backup deduplicado entre os hardwares de deduplicação.

3.1.1.18.31. Deverá possuir a capacidade de deduplicação de dados no nível de segmentos ou blocos de dados repetidos, para ambientes físicos e virtuais.

3.1.1.18.32. Deverá possuir a capacidade de Replicação de Dados entre “pools” de deduplicação de maneira otimizada, enviando somente blocos únicos.

3.1.1.18.33. A tecnologia de deduplicação de dados no Hardware de curta e de longa retenção poderá ser inline, pós-processada ou em paralelo, devendo ser observados os requisitos de desempenho solicitados.

3.1.1.18.34. As soluções que executam deduplicação em paralelo e/ou pós-processada deverão possuir uma área temporária, também conhecida como área de staging ou landing zone, para manter qualquer dado sem deduplicação, para o backup ou reidratação dos dados, de forma que não seja contabilizada na área de armazenamento final dos dados.

### 3.1.3. **ITEM 2 - Software de backup para o ambiente em nuvem Microsoft (O365/M365)**

3.1.1.19. A CONTRATADA deverá entregar a solução totalmente operacional, com todas as licenças e configurações necessárias para o pleno funcionamento da solução, devidamente pronta para utilização.

3.1.1.20. A fabricante do software de backup deverá constar no quadrante do Gartner sobre o tema – Magic Quadrant for Enterprise Backup and Recovery Software Solutions nas categorias Challengers, Leaders ou Visionaries,

3.1.1.21. A solução deverá ser provida na modalidade SaaS (Software como Serviço) em Cloud pelo fabricante. Não deverá ser necessário nenhuma infraestrutura local ou IaaS (Infraestrutura como Serviço) para seu pleno funcionamento.

3.1.1.22. A solução de Proteção de Dados para Microsoft 365 a ser ofertada deve atender integralmente os requisitos especificados neste Termo, devendo ser fornecida com todas as licenças e infraestrutura que forem necessárias para entrega funcional da solução.

3.1.1.23. Deverá possuir console de gerenciamento acessível via web browser.

3.1.1.24. Deverá fornecer visualização do consumo atual de cada recurso.

3.1.1.25. Deverá ser fornecido backup e recuperação para Exchange Online, OneDrive, SharePoint Online, Azure AD/Microsoft Entra ID e Teams.

3.1.1.26. O dimensionamento e o licenciamento da solução deverão contemplar o total de licenças O365 e M365 existentes no ambiente, independentemente de já estarem atribuídas ou em estoque, garantindo cobertura integral e margem de expansão durante toda a vigência do contrato:

3.1.1.26.1. M365 E3: 1.100 licenças;

3.1.1.26.2. O365 E1: 180 licenças;

3.1.1.27. O front-end armazenado, ao longo da vigência do contrato de suporte e garantia, será de 77,31 TB, sendo:

3.1.1.27.1. One Drive: 46,28 TB;

3.1.1.27.2. Exchange: 6,46 TB;

3.1.1.27.3. SharePoint: 24,57 TB.

3.1.1.28. A política de backup a ser aplicada contemplará os últimos dois anos de backup, armazenando o último backup full de cada mês e todos os fulls (4) e incrementais (26) dos últimos 30 dias.

3.1.1.29. A solução deve ter a capacidade de contabilizar apenas os dados únicos, utilizando de técnicas de deduplicação e compressão de dados.

3.1.1.30. O backup deve incluir, obrigatoriamente:

**3.1.1.30.1. Pacote Microsoft 365:**

3.1.1.30.1.1. Exchange Online;

3.1.1.30.1.2. Calendário;

3.1.1.30.1.3. Contatos;

3.1.1.30.1.4. Tarefas;

3.1.1.30.1.5. Notas.

**3.1.1.30.2. OneDrive:**

3.1.1.30.2.1. Arquivos;

3.1.1.30.2.2. Pastas;

3.1.1.30.2.3. Permissões.

**3.1.1.30.3. SharePoint Online:**

3.1.1.30.3.1. Qualquer tipo de conteúdo dos sites, incluindo permissões e todos os metadados.

**3.1.1.30.4. Teams:**

3.1.1.30.4.1. Sites de equipes;

3.1.1.30.4.2. Membros;

3.1.1.30.4.3. Permissões de membros;

3.1.1.30.4.4. Canais;

3.1.1.30.4.5. Postagens;

3.1.1.30.4.6. Arquivos;

3.1.1.30.4.7. Wiki;

3.1.1.30.4.8. Bate-papos individuais e em grupo.

**3.1.1.30.5. Objetos do Azure AD (Entra ID).**

3.1.1.31. A solução deverá permitir:

3.1.1.31.1. Realizar backup automatizado, programável e abrangente de todos os serviços Microsoft 365 citados.

3.1.1.31.2. Adição de novos usuários nas políticas de backup, automaticamente.

3.1.1.31.3. Permitir restauração granular de itens (e-mails, arquivos, pastas, sites, chats, grupos etc.) e restauração massiva (conta/site/grupo inteiro).

3.1.1.31.4. Permitir restauração para o tenant de origem, exportação para formatos abertos (ex: PST, ZIP) e, opcionalmente, restauração cruzada entre tenants.

3.1.1.31.5. Detectar e incluir automaticamente novos usuários, grupos, caixas e sites criados após a implantação.

3.1.1.31.6. Permitir políticas múltiplas de retenção, customizáveis por serviço ou grupo.

3.1.1.31.7. Disponibilizar backup automático de todas as workloads suportadas pelo Microsoft 365.

3.1.1.31.8. Integrar-se ao Microsoft 365 exclusivamente via APIs oficiais e suportadas pela Microsoft.

3.1.1.32. Todos os backups devem estar disponíveis para restauração imediata durante todo o período de retenção.

3.1.1.33. Deverá ser possível recuperar o dado na própria nuvem ou em local alternativo, incluindo destinos externos.

3.1.1.34. Deverá ser possível pesquisar por nomes de usuário, arquivos, pastas e datas;

3.1.1.35. Deverá ser possível pesquisar e-mails em todos os backups de caixas de correio do Exchange Online.

3.1.1.36. Deverá possuir logs de auditoria, que seja possível consultar e relatar os históricos de atividades de usuários e processos do sistema.

3.1.1.37. Durante a execução dos backups, os dados deverão ser criptografados em trânsito.

3.1.1.38. A retenção dos dados de backup deve ser feita em território nacional.

3.1.1.39. O fabricante da solução de proteção de dados para Microsoft 365 deverá comprovar através de documentações oficiais a segurança física e lógica de seus data centers assim como a garantia da privacidade dos dados.

3.1.1.40. Deverá suportar duplo fator de autenticação para acesso à console na nuvem.

3.1.1.41. Deverá ser possível a configuração de backups full e incrementais.

3.1.1.42. A solução não deverá possuir taxas adicionais para ingestão (ingress) ou saída (egress) de dados do backup. Deverá possibilitar restaurações sem limites e sem custos adicionais.

3.1.1.43. Possuir relatório de consumo da volumetria utilizada versus contratada.

3.1.1.44. Deve possuir recursos de imutabilidade dos dados através de Write Once Read Many – WORM garantindo a imutabilidade para todo e qualquer dado de backup enviado para armazenamento na nuvem.

### 3.1.4. ITEM 3 - TREINAMENTO NA SOLUÇÃO

3.1.1.45. A CONTRATADA deverá ministrar treinamento para a solução ofertada (hardware e software).

3.1.1.46. O treinamento será no período vespertino e será acordado entre a equipe responsável do TCDF e a CONTRATADA;

3.1.1.47. O treinamento deverá ser ministrado na modalidade remota, por instrutor certificado na solução e todas as aulas deverão ser gravadas e fornecidas ao TCDF para download;

3.1.1.48. O treinamento deverá ser ministrado para até 8 servidores, podendo, a critério do Tribunal, ser ministrado em duas turmas;

3.1.1.49. O treinamento será ministrado em 15 (quinze) horas, sendo a carga horária diária máxima de 3 (três) horas.

3.1.1.50. O repasse de conhecimento deverá cobrir conhecimentos necessários, de toda a solução contratada, para instalação, administração, configuração, otimização, resolução de problemas e utilização da solução, sendo que o conteúdo do treinamento deverá contemplar os seguintes tópicos do conteúdo programático:

3.1.1.50.1. Visão geral dos recursos e funcionalidades da solução;

3.1.1.50.2. Tarefas de administração;

3.1.1.50.3. Tarefas de configuração;

3.1.1.50.4. Tarefas de recuperação de desastres;

3.1.1.50.5. Tarefas de backup, restore e replicação;

3.1.1.50.6. Tarefas de monitoramento.

3.1.1.51. Deverão ser utilizados laboratórios virtuais práticos para apoio ao aprendizado, em ambiente de testes, fora do ambiente de produção do Tribunal.

3.1.1.52. Após o término do curso, deverá haver entrega dos certificados de conclusão aos participantes;

3.1.1.53. Ao término do treinamento, será realizada a avaliação da ação de capacitação. Caso o treinamento não tenha sido aprovado pela maioria dos participantes, por falha da CONTRATADA, esta deverá realizar novo treinamento, sem ônus para o CONTRATANTE, com as reformulações que o TCDF julgar necessárias, inclusive com a mudança do(s) instrutor(es), caso necessário.

### 3.1.5. **Garantia e Suporte Técnico**

3.1.1.54. O prazo de garantia ON SITE do fornecimento, instalação, dos equipamentos e da solução de backup em nuvem será de 60 (sessenta) meses, no mínimo, contados da data do recebimento definitivo do objeto. Caso a CONTRATADA tenha ofertado um prazo maior, será considerado o prazo constante da sua proposta técnica.

3.1.1.55. O fornecimento, instalação, configuração das soluções, garantia e suporte on-site deverão ser prestados no:

3.1.1.55.1. Edifício Anexo do Tribunal de Contas do Distrito Federal; e

3.1.1.55.2. Na sala de collocation do datacenter IPEDF (Centro de Dados), da Secretaria Executiva de Tecnologia da Informação e Comunicação (SETIC), da Secretaria de Estado de Economia do Distrito Federal, no Setor de Administração Municipal, bloco H, 70.620-080.

3.1.1.56. A garantia será ON-SITE, ou seja, no local da instalação da solução fornecida pela CONTRATADA. Eventualmente, o TCDF poderá autorizar a retirada de equipamento ou componente com defeito, mediante Termo Circunstanciado. Neste caso, todas as despesas correrão por conta da CONTRATADA.

3.1.1.57. A CONTRATADA deverá fornecer garantia contra defeitos de fabricação e falhas no serviço de transporte e assistência técnica (instalação, configuração e manutenção corretiva), sem custos além daqueles constantes da proposta de preço e pelo prazo de garantia ofertado.

3.1.1.58. Servidores do TCDF devidamente autorizados pela STI poderão abrir o equipamento e retirar, colocar ou trocar quaisquer componentes removíveis, desde que seguindo as instruções constantes de guia ou manual do fabricante.

3.1.1.59. A garantia ON-SITE cobrirá igualmente todos os componentes dos equipamentos fornecidos pela CONTRATADA.

3.1.1.60. Durante o período de vigência do contrato o CONTRATANTE terá direito, sem ônus adicional, a todas as atualizações de versão e releases dos softwares que fazem parte da solução ofertada.

3.1.1.61. Todo equipamento ou componente defeituoso deverá ser substituído por outro novo e de igual marca e modelo, a menos que o TCDF autorize a troca por outra marca e/ou modelo.

3.1.1.62. As peças instaladas em substituição serão garantidas contra defeitos de fabricação pelo prazo restante da garantia.

3.1.1.63. Todas as despesas de frete, seguros, testes, ensaios, reinspeção e outras que recaiam sobre os equipamentos enviados para o conserto ou para substituição, que estejam cobertos pela garantia, serão suportadas pela CONTRATADA.

3.1.1.64. Durante o período de garantia a CONTRATADA executará, sem ônus adicionais, correções de falhas (bugs) de software e atualizações firmware.

3.1.1.65. A Nota Fiscal referente ao fornecimento dos equipamentos com garantia ON-SITE, será única, considerando o disposto na Lei Complementar nº 116/2003 e o Acórdão TCU nº 1.177/2014 - Plenário, haja vista que o custo dos equipamentos é superior ao dos serviços de garantia e a operação deve ser tributada pelo ICMS, em consonância com a legislação aplicável em vigor.

3.1.1.66. O pagamento dos equipamentos/serviços, incluindo a garantia ON-SITE de que trata este item, será feito de forma integral e em parcela única.

3.1.1.67. O suporte técnico da garantia ON-SITE deverá estar disponível para abertura de chamados técnicos 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana.

3.1.1.68. Os chamados técnicos serão categorizados nos seguintes níveis de severidade:

3.1.1.68.1. ALTO: Solução fora de operação, ou funcionalidades principais severamente prejudicadas, com restrições de funcionamento totais ou parciais significativas. Também se considera como ALTO os chamados técnicos em virtude de ataque de ransomware.

3.1.1.68.2. MÉDIO: Perda de funcionalidades não críticas. Operações deficientes de alguns componentes, mas o usuário continua a utilizar a solução.

3.1.1.68.3. BAIXO: Questões de caráter geral.

3.1.1.69. O nível de severidade dos chamados será definido pelo CONTRATANTE no momento de sua abertura;

3.1.1.70. São vedados a reclassificação, o encerramento e o cancelamento de chamado pela CONTRATADA sem a prévia autorização do TCDF.

3.1.1.71. Os chamados somente podem ser encerrados após a validação da solução apresentada.

**3.1.1.72. Nível Mínimo de Serviço de acordo com a severidade:**

3.1.1.72.1. ALTO: A CONTRATADA deverá iniciar o atendimento em até 01 (uma) hora e o chamado solucionado em até 24 (vinte e quatro) horas. Após o início do atendimento do chamado, a presença do técnico no local de instalação da solução deve se dar em até 02 (duas) horas.

3.1.1.72.2. MÉDIO: A CONTRATADA deverá iniciar o atendimento no prazo máximo de 01 (um) dia, solucionando o problema em até 3 (três) dias úteis. O atendimento poderá ser efetuado remotamente, nos dias úteis entre 13hs e 18hs.

3.1.1.72.3. BAIXO: A CONTRATADA deverá iniciar o atendimento no prazo máximo de 01 (um) dia, solucionando o problema em até 05 (cinco) dias úteis. O atendimento poderá ser efetuado remotamente, nos dias úteis entre 13hs e 18hs.

3.1.1.72.4. No caso de atendimentos de chamados técnicos ON-SITE, o horário de chegada do técnico no local deverá ser combinado com o CONTRATANTE;

3.1.1.72.5. Por início de atendimento entende-se a alocação de técnico devidamente qualificado para efetuar a correção do problema ou o troubleshooting preciso, com interlocução telefônica direta com a equipe do TCDF.

3.1.1.72.6. Nos casos em que for necessário a comunicação com a fabricante da solução, a CONTRATADA é quem fará a abertura dos chamados técnicos e procederá às comunicações e executará as soluções sugeridas pela fabricante.

3.1.1.72.7. Caso não seja possível cumprir o prazo estabelecido, a CONTRATADA deverá formalizar e, se solicitado pelo CONTRATANTE, substituir o equipamento ou componente defeituoso por outro, em caráter provisório (backup), mediante autorização e no prazo estabelecido pelo TCDF.

3.1.1.72.8. Para os chamados, a CONTRATADA deverá fornecer:

3.1.1.72.8.1. 1 (um) número de telefone fixo; e/ou

3.1.1.72.8.2. 1 (um) endereço eletrônico (e-mail).

3.1.1.72.9. A CONTRATADA deverá informar o nome de 1 (um) responsável pelo atendimento desses chamados técnicos, fornecendo 1 (um) número de celular e 1 (um) endereço eletrônico (e-mail) desse responsável.

3.1.1.72.10. Os chamados para agendamento de atividades planejadas, em data futura, deverão ser registrados da mesma maneira que os demais.

3.1.1.72.11. Uma vez ao mês, a contratada deverá disponibilizar técnico habilitado na solução de backup (software e hardware) para realizar suporte proativo. Na ocasião o técnico acessará o ambiente de backup do Tribunal e verificará a execução das políticas e se há algum ponto de atenção a ser corrigido. Caso haja atualizações a serem feitas no ambiente, também poderão ser realizadas nesta oportunidade. Ao final da atividade, deverá ser disponibilizado relatório das atividades. O suporte proativo poderá ser realizado de forma remota.

3.1.1.72.12. A CONTRATADA deverá emitir e entregar, para cada atendimento realizado, ordem de serviço, contendo número do atendimento, informações da solicitação, procedimentos técnicos, solução e horário início/fim, bem como manter histórico de ações e atividades realizadas.

3.1.1.72.13. É considerado dia útil aquele com expediente normal no TCDF.

3.1.1.72.14. O prazo de garantia dos serviços prestados de garantia ON-SITE executados é de, no mínimo, 90 (noventa) dias, contados da data de conclusão desses serviços, independentemente da natureza do defeito apresentado. Caso a CONTRATADA tenha oferecido prazo de garantia maior em sua proposta, este será adotado.

3.1.1.72.15. Caso o reparo referente à execução da garantia estabelecida no presente item esteja relacionado a defeitos em peças trocadas no serviço prestado anteriormente e também em peças não substituídas, mas que foram danificadas posteriormente exclusivamente em decorrência de falhas de execução desse serviço; todas essas deverão ser substituídas por peças novas, sem quaisquer ônus para o CONTRATANTE.

3.1.1.72.16. A CONTRATADA obriga-se a garantir os serviços prestados e peças fornecidas dentro de seus prazos de garantia conceituados no presente tópico e aceitos pelo CONTRATANTE, mesmo que a contagem desses prazos se estenda para além da vigência contratual, tendo em vista tratar-se de obrigação legal e contratual de reparação pelas falhas imputadas na execução do objeto e que contrariam a obrigação de correção, segurança, durabilidade

e de qualidade assumidas pela CONTRATADA na apresentação de sua proposta e quando da assinatura do contrato.

3.1.1.72.17. Além de outras penalidades previstas em Edital e em seus anexos por não cumprimento da garantia oferecida no presente tópico, a CONTRATADA será declarada inidônea pelo Tribunal de Contas do Distrito Federal, caso não cumpra a garantia assumida quando seu prazo de atendimento extrapolar o prazo de vigência contratual.

## 4. DOS REQUISITOS DA CONTRATAÇÃO

4.1. Além dos requisitos de habilitação verificados por meio do SICAF, a Contratada deverá apresentar a seguinte documentação de habilitação complementar:

4.1.1. Certidão Negativa de Débitos com a Fazenda do Distrito Federal, em conformidade com o art. 193 da Lei nº 5.172/1966 (Código Tributário Nacional), c/c o art. 68, incisos II e III, da Lei nº 14.133/2021. Esta certidão será exigida se não estiver contemplada no SICAF;

4.1.2. Declaração de que atende aos requisitos previstos no art. 2º da Lei Distrital nº 4.770, de 22 de fevereiro de 2012;

4.1.3. Registro comercial, no caso de empresário individual;

4.1.4. Ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado, em se tratando de sociedades comerciais, e, no caso de sociedades por ações, acompanhado de documentos de eleição de seus administradores e alterações ou da consolidação respectiva;

4.2. **Regulamentação legal específica**

4.2.1. Não se aplica.

4.3. **Especialização e habilitação profissional específica**

4.3.1. Não se aplica.

4.4. **Experiência pretérita**

4.4.1. Para cada um dos itens do Edital, o Licitante deverá apresentar os documentos determinados no art. 67, II da lei 14.133/21 para o fim de atestar a sua capacidade técnica.

Será exigido atestado de capacidade técnica ou certidão(ões) que comprove(m) que o licitante forneceu para órgão ou entidade da administração pública direta ou indireta, federal, estadual, municipal ou do DF, ou para empresas privadas:

4.4.1.1. Appliance de backup de, no mínimo, 100 TB e prestação de suporte técnico por, pelo menos, 36 meses; e

4.4.1.2. Solução de backup em nuvem, com capacidade de, no mínimo, 50 TB de armazenamento e prestação de suporte técnico por, pelo menos, 36 meses.

4.5. **Autorização ou licença do poder público**

4.5.1. Não se aplica.

4.6. **Vistoria Técnica**

4.6.1. A vistoria técnica não é obrigatória, porém é facultado ao licitante conhecer o datacenter e verificar onde os equipamentos serão instalados.

4.7. **Proximidade geográfica do prestador**

4.7.1. Não há obrigatoriedade de proximidade geográfica do prestador, desde que os SLAs sejam atendidos, conforme definido.

## 5. DA PREVISÃO DA CONTRATAÇÃO NO PLANO DE CONTRATAÇÃO ANUAL

5.1. **ALINHAMENTO ENTRE A NECESSIDADE DA CONTRATAÇÃO E OS PLANOS ESTRATÉGICOS DO TCDF (PDTI OU DECISÕES CGTI)**

5.1.1. Por se tratar de solução que acarreta aumento de despesa, em conformidade com o artigo 16º da Lei de Responsabilidade Fiscal (Lei Complementar nº 101, de 04 de maio de 2000) [4], ressalta-se que a presente contratação possui respaldo orçamentário no Orçamento de Informática 2025, conforme se segue:

[4] Art. 16. A criação, expansão ou aperfeiçoamento de ação governamental que acarrete aumento da despesa será acompanhado de:
I - estimativa do impacto orçamentário-financeiro no exercício em que deva entrar em vigor e nos dois subsequentes;
II - declaração do ordenador da despesa de que o aumento tem adequação orçamentária e financeira com a lei orçamentária anual e compatibilidade com o plano plurianual e com a lei de diretrizes orçamentárias.

| Orçamento de informática 2025 | |
|---|---|
| Programa de trabalho | 01.126.8231.2557.2568 |
| Descrição | GESTÃO DA INFORMAÇÃO E DOS SISTEMAS DE TECNOLOGIA DA INFORMAÇÃO - TRIBUNAL DE CONTAS DO DISTRITO FEDERAL - DISTRITO FEDERAL - REF. 018164 |
| Natureza | 3.3.90.40 - SERVIÇOS DE TEC. DA INFORMAÇÃO E COMUNICAÇÃO - PJ |
| Saldo orçamentário (13/10/2025) | 15.518.553,66 |

5.1.2. Destaca-se que a iniciativa está prevista no Plano Diretor de Tecnologia da Informação 2023-2024 do TCDF, nos seguintes objetivos estratégicos ligados à Tecnologia da Informação:

5.1.2.1. Aprimorar a gestão dos recursos de TI;

5.1.2.2. Garantir estrutura adequada à estratégia.

5.2. **DEMANDAS DOS POTENCIAIS GESTORES E USUÁRIOS DA SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO**

5.2.1. Continuidade dos serviços da Corte.

## 6. DA ESTIMATIVA DAS QUANTIDADES

6.1. Para esta contratação, várias estimativas são necessárias, desde o licenciamento do software de backup até o efetivo espaço necessário para armazenamento no appliance de backup. Antes de explorar os números relacionados à contratação, faz-se necessário explicitar o tempo de retenção dos backups que será utilizado neste projeto, visto que terá um impacto direto no tamanho dos appliances de backup.

6.2. Conforme explicitado no e-DOC 7DF6B8CB, não há política de backup institucional no TCDF. Por conta disso, a GEINT, novamente, ficará a cargo da definição da periodicidade e tempo de retenção dos backups para esta contratação. Dada a importância do tema e para que o Tribunal não fique sem suporte e garantia dos equipamentos de backup, não será possível, para esta contratação, aguardar a criação do grupo de trabalho sugerido na Informação n° 2/2025 – COGINF.

6.3. Assim, para este projeto, a GEINT julga razoável a definição do prazo de 2 anos para retenção dos backups dos arquivos que estão no ambiente Microsoft, na nuvem, e 1 ano para retenção dos arquivos locais, isto é, que estão hospedados no datacenter do Tribunal, que são, na grande

maioria, arquivos de sistemas.

6.4. O presente projeto tem como objetivo a contratação de uma solução de backup orientada para disaster recovery (DR), visando garantir a rápida recuperação dos sistemas e serviços críticos em caso de falhas, incidentes ou desastres que comprometam a infraestrutura de TI. Essa abordagem é fundamental para assegurar a continuidade das operações, minimizando o tempo de indisponibilidade e os impactos financeiros e reputacionais decorrentes de eventuais paradas. Trata-se, portanto, de uma estratégia centrada na resiliência e na retomada rápida do ambiente produtivo.

6.5. Sob essa perspectiva, é importante ressaltar que o projeto não tem por finalidade armazenar versões históricas prolongadas dos dados, tampouco substituir sistemas dedicados a arquivamento ou compliance legal de longo prazo. A proposta é adotar uma janela de retenção de backups alinhada exclusivamente com os objetivos de recuperação, conforme boas práticas internacionalmente reconhecidas. Dessa forma, evita-se o acúmulo desnecessário de dados antigos que não contribuem para a capacidade de recuperação do ambiente, ao mesmo tempo que se otimiza o uso do espaço de armazenamento e se reduzem custos operacionais.

6.6. Idealmente, as aplicações corporativas deveriam implementar mecanismos que impedissem a deleção de dados sujeitos a períodos legais de retenção, garantindo que tais informações permaneçam íntegras e acessíveis enquanto durar a obrigação legal. Nesse cenário, as próprias aplicações seriam responsáveis pelo controle da retenção, limitando a exclusão ou modificação desses dados por usuários ou processos internos, em consonância com as políticas do TCDF.

6.7. Em situações de desastre, como falhas críticas de infraestrutura ou ataques cibernéticos do tipo ransomware, o objetivo principal do backup é restaurar o ambiente no estado mais recente possível antes do incidente, garantindo mínima perda de dados e rápida retomada das operações. Por isso, os dados que efetivamente serão utilizados para recuperação são justamente os últimos backups válidos, feitos pouco antes do evento, conforme o RPO (Recovery Point Objective) definido pelo Tribunal.

6.8. Não faz sentido, do ponto de vista de continuidade de negócios, utilizar backups muito antigos para restaurar sistemas, pois isso significaria renunciar a todas as transações e alterações ocorridas desde aquele ponto, gerando um impacto ainda maior. Assim, manter longas cadeias de retenção não aumenta a capacidade de recuperação em casos de desastre — o que realmente importa é ter backups recentes, íntegros e testados, capazes de restaurar a operação o mais próximo possível do momento em que o incidente ocorreu.

6.9. As empresas líderes no mercado de backup e segurança da informação oferecem recomendações mais concretas, que apoiam a tese de retenções curtas para recuperação operacional.

6.10. A Commvault, uma empresa proeminente em soluções de backup, distingue claramente a retenção para recuperação de desastres da retenção de longo prazo. Em sua documentação, um exemplo prático é oferecido[5]:

> "Por padrão, os dados de backup de recuperação de desastres são retidos por 15 dias e 15 ciclos. Se você deseja alterar o tempo de retenção para dados de backup de recuperação de desastres, recomendamos que mantenha a configuração padrão como o mínimo e configure regras de retenção estendida definidas da seguinte forma: Semanal = 90 dias; Mensal = 180 dias."

6.11. Este trecho ilustra uma prática comum: uma retenção curta (15 dias) para recuperação rápida e operacional, com políticas de retenção estendida para outros fins, que já se aproximam do arquivamento.

6.12. A IBM, em sua documentação de serviços de recuperação de desastres, também apresenta exemplos de retenções curtas para bancos de dados em ambientes de produção6:

> "Retenção de Backup de Banco de Dados. Backups de banco de dados serão retidos pela duração padrão de 14 dias para ambientes de Produção e 7 dias para ambientes de Não Produção."

6.13. Esta prática reforça que, para a continuidade operacional, o acesso a backups de algumas semanas é geralmente considerado suficiente.

6.14. A documentação do Microsoft Azure Backup aconselha7:

> *"Use snapshots Diários e de Hora em Hora para VMs Críticas: Backups diários para cargas de trabalho não críticas (retenção de 7 a 30 dias). Snapshots de hora em hora para cargas de trabalho de missão crítica (retenção de curto prazo para recuperação rápida)."*

6.15. Dessa forma, as evidências coletadas comprovam que, para a finalidade estrita de recuperação de desastres, períodos de retenção curtos (por exemplo, de 7 a 30 dias) são não apenas suficientes,

[5] https://documentation.commvault.com/11.20/data_aging_of_disaster_recovery_data.html. Acessado em 09/07/2025.
[6] https://www.ibm.com/docs/en/mas/saas?topic=general-backups-disaster-recovery. Acessado em 09/07/2025.
[7] https://learn.microsoft.com/en-us/answers/questions/2152442/recommended-configuration-options-for-azure-backup. Acessado em 09/07/2025.

mas também a prática recomendada. Períodos mais longos estão associados ao arquivamento de dados para fins de conformidade, auditoria ou histórico8.

6.16. Passado esse assunto, com relação ao espaço necessário para o armazenamento, fez-se estimativas baseadas nas atuais taxas obtidas do appliance de backup em uso no Tribunal e em documentos públicos.

6.17. Para a estimativa do backup dos dados locais do Tribunal, isto é, do que não está na nuvem Microsoft, utilizou-se como referência principal relatórios obtidos no próprio sistema de backup do TCDF, em especial o relatório apresentado no e-DOC 9D76B465, e relatórios do storage da Corte.

6.18. Para se estimar o volume de armazenamento necessário, normalmente se utilizam alguns dados importantes, como, por exemplo, tamanho estimado do primeiro backup full, incrementos diários e política de backup. Em relatório do storage do Tribunal, verificou-se, na data de elaboração deste ETP, a utilização de 118,09 TB. Esse volume armazenado representa, para fins de estimativa, o valor do primeiro backup full da solução de backup, visto que todos os dados do Tribunal serão salvos. A variação mensal do volume de dados armazenado é de 1,5 TB, o que representa um acréscimo diário de, aproximadamente, 0,1 TB.

6.19. A política de backup que será adotada para o backup dos dados locais será a seguinte: os backups serão armazenados por 12 meses; será armazenado, para longa retenção, o último backup full de todos os meses. Para o mês corrente, haverá backups semanais e incrementais, possibilitando a recuperação de dados de forma granular no mês corrente.

6.20. A tabela abaixo apresenta a estimativa de volume de backup local, durante os 60 meses de suporte e garantia da solução (todos os valores estão expressos em terabyte – TB):

| **BACKUP LOCAL** | |
|---|---|
| | |
| Espaço utilizado em 27/06/2025 | 118,09 |
| Variação mensal | 1,5 |
| Incremento diário | 0,1 |
| | |
| **BACKUPS FULL** | |
| **Mês** | **Volume salvo em backup** |
| 1 | 118,09 |
| 2 | 119,59 |
| 3 | 121,09 |
| 4 | 122,59 |

[8] https://www.stackscale.com/blog/backup-and-data-retention/. Acessado em 09/07/2025.

| | |
|---|---|
| 5 | 124,09 |
| 6 | 125,59 |
| 7 | 127,09 |
| 8 | 128,59 |
| 9 | 130,09 |
| 10 | 131,59 |
| 11 | 133,09 |
| 12 | 134,59 |
| 13 | 136,09 |
| 14 | 137,59 |
| 15 | 139,09 |
| 16 | 140,59 |
| 17 | 142,09 |
| 18 | 143,59 |
| 19 | 145,09 |
| 20 | 146,59 |
| 21 | 148,09 |
| 22 | 149,59 |
| 23 | 151,09 |
| 24 | 152,59 |
| 25 | 154,09 |
| 26 | 155,59 |
| 27 | 157,09 |
| 28 | 158,59 |
| 29 | 160,09 |
| 30 | 161,59 |
| 31 | 163,09 |
| 32 | 164,59 |
| 33 | 166,09 |
| 34 | 167,59 |
| 35 | 169,09 |
| 36 | 170,59 |
| 37 | 172,09 |
| 38 | 173,59 |
| 39 | 175,09 |
| 40 | 176,59 |
| 41 | 178,09 |
| 42 | 179,59 |
| 43 | 181,09 |
| 44 | 182,59 |
| 45 | 184,09 |
| 46 | 185,59 |
| 47 | 187,09 |

| | |
|---|---|
| 48 | 188,59 |
| 49 | 190,09 |
| 50 | 191,59 |
| 51 | 193,09 |
| 52 | 194,59 |
| 53 | 196,09 |
| 54 | 197,59 |
| 55 | 199,09 |
| 56 | 200,59 |
| 57 | 202,09 |
| 58 | 203,59 |
| 59 | 205,09 |
| 60.1 (full do mês 60, semana 1) | 205,465 |
| 60.2 (full do mês 60, semana 2) | 205,84 |
| 60.3 (full do mês 60, semana 3) | 206,215 |
| 60.4 (full do mês 60, semana 4) | 206,59 |
| | |
| **BACKUPS INCREMENTAIS** | |
| | |
| **Quantidade** | **Volume** |
| 26 | 1,30 |

6.21. Assim, para estimar o espaço necessário de armazenamento, utiliza-se como referência os últimos períodos de backup, mais precisamente o somatório dos 12 meses finais de suporte e garantia da solução.

| **BACKUP LOCAL** | |
|---|---|
| Front-end armazenado (somatório do último backup full e incrementais do mês corrente) | 207,89 |
| Volumetria sem redução de dados (somatório dos backups realizados a partir do mês 49 e incrementais do mês corrente) | 2.998,90 |
| Volumetria com redução de dados (94,03% / 16,7:1) | 179,03 |

6.22. Nesse ponto, vale uma breve explicação sobre a técnicas de redução de dados.

6.23. A redução de dados é um conjunto de técnicas utilizadas em ambientes de armazenamento e backup para diminuir o volume de informações salvas, otimizando a utilização de espaço, largura de banda e melhorando o desempenho geral das soluções de TI. Essa prática é essencial em cenários corporativos, onde o crescimento dos dados é constante e os custos com armazenamento podem ser significativos.

6.24. Dentro desse contexto, dois dos principais métodos de redução de dados são a deduplicação e a

compressão. A deduplicação identifica e elimina blocos de dados duplicados, armazenando apenas uma cópia única e referenciando os demais apontamentos para essa cópia. Esse processo é especialmente eficiente em backups, onde grandes volumes de informações se repetem entre diferentes versões de arquivos ou sistemas.

6.25. Já a compressão atua reduzindo o tamanho dos dados ao eliminar redundâncias dentro de cada arquivo, utilizando algoritmos que reescrevem as informações de maneira mais compacta. Enquanto a deduplicação trabalha principalmente com a eliminação de cópias repetidas, a compressão lida com a estrutura interna dos dados, tornando-os menores sem perda de conteúdo. A combinação dessas técnicas potencializa a economia de espaço, tornando as soluções de backup e armazenamento mais eficientes e econômicas.

6.26. Assim, voltando à estimativa de espaço para o backup local, o valor lógico a ser armazenado será de 2998,90 TB, porém, após aplicar técnicas de redução de dados, o appliance armazenará, em 12 meses, 179,03 TB. A taxa de redução de dados utilizada como referência, isto é, 94,03% ou 16,7:1, é a média obtida atualmente na solução de proteção de dados do TCDF.

6.27. Para a estimativa do espaço necessário para o armazenamento do ambiente em nuvem do Tribunal, ou seja, do ambiente Microsoft, utilizou-se como referência inicial relatórios de uso das próprias soluções, nos últimos 180 dias.

6.28. Iniciando pelo OneDrive, abaixo estão as imagens que mostram o uso da solução:

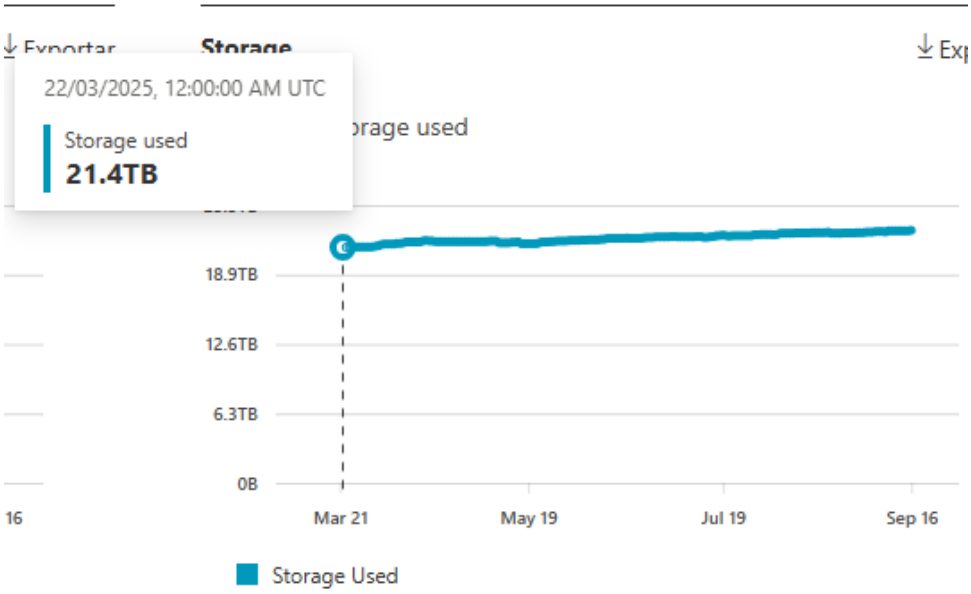



Figura 5 – Espaço em disco utilizado em 22/03/2025.

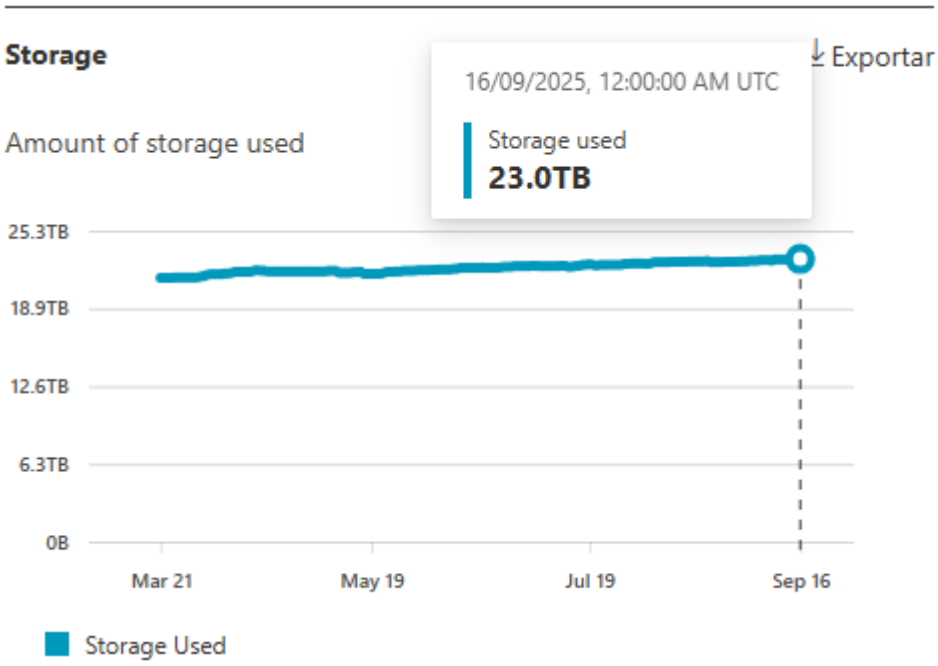



Figura 6 – Espaço em disco utilizado em 16/09/2025.

6.29. Analisando a taxa de crescimento de storage do OneDrive, percebe-se que, nos últimos 180 dias, houve um acréscimo de 0,26 TB por mês. Assim, a estimativa de armazenamento em appliance de backup ficou da seguinte forma (todos os valores estão expressos em terabyte – TB):

| One Drive | |
|---|---|
| | |
| Espaço utilizado em 16/09/2025 | 23 |
| Variação mensal | 0,26 |
| Incremento diário | 0,0087 |
| | |
| **Backups full** | |
| | |
| **Mês** | **Volume salvo em backup** |
| 1 | 23 |
| 2 | 23,26 |
| 3 | 23,52 |
| 4 | 23,78 |
| 5 | 24,04 |
| 6 | 24,3 |
| 7 | 24,56 |
| 8 | 24,82 |
| 9 | 25,08 |

| | |
|---|---|
| 10 | 25,34 |
| 11 | 25,6 |
| 12 | 25,86 |
| 13 | 26,12 |
| 14 | 26,38 |
| 15 | 26,64 |
| 16 | 26,9 |
| 17 | 27,16 |
| 18 | 27,42 |
| 19 | 27,68 |
| 20 | 27,94 |
| 21 | 28,2 |
| 22 | 28,46 |
| 23 | 28,72 |
| 24 | 28,98 |
| 25 | 29,24 |
| 26 | 29,5 |
| 27 | 29,76 |
| 28 | 30,02 |
| 29 | 30,28 |
| 30 | 30,54 |
| 31 | 30,8 |
| 32 | 31,06 |
| 33 | 31,32 |
| 34 | 31,58 |
| 35 | 31,84 |
| 36 | 32,1 |
| 37 | 32,36 |
| 38 | 32,62 |
| 39 | 32,88 |
| 40 | 33,14 |
| 41 | 33,4 |
| 42 | 33,66 |
| 43 | 33,92 |
| 44 | 34,18 |
| 45 | 34,44 |
| 46 | 34,7 |
| 47 | 34,96 |
| 48 | 35,22 |
| 49 | 35,48 |
| 50 | 35,74 |
| 51 | 36 |
| 52 | 36,26 |

| | |
|---|---|
| 53 | 36,52 |
| 54 | 36,78 |
| 55 | 37,04 |
| 56 | 37,3 |
| 57 | 37,56 |
| 58 | 37,82 |
| 59 | 38,08 |
| 60.1 (full do mês 60, semana 1) | 38,15 |
| 60.2 (full do mês 60, semana 2) | 38,21 |
| 60.3 (full do mês 60, semana 3) | 38,28 |
| 60.4 (full do mês 60, semana 4) | 38,34 |
| | |
| **Backups incrementais** | |
| | |
| **Quantidade** | **Volume** |
| 26 | 0,23 |

6.30. Calculando o volume armazenado para 24 meses, que será o tempo de retenção dos backups dos arquivos que estão na nuvem, os dados obtidos são os seguintes:

| **ONE DRIVE** | |
|---|---|
| Front-end armazenado (somatório do último backup full e incrementais do mês corrente) | 38,57 |
| Volumetria sem redução de dados (somatório dos backups realizados a partir do mês 37 e incrementais do mês corrente) | 963,26 |
| Volumetria com redução de dados (90% / 10:1) | 96,33 |

6.31. Os cálculos do Exchange ficaram da seguinte forma:

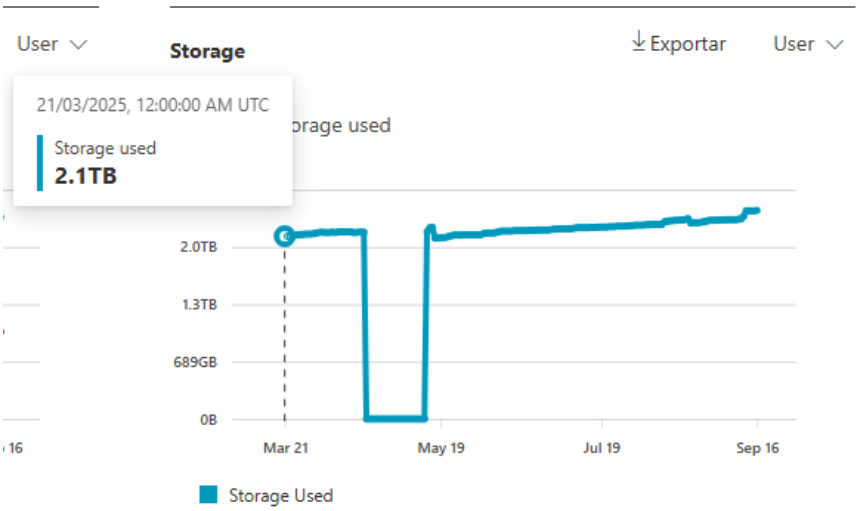



Figura 7 – Espaço em disco utilizado em 21/03/2025

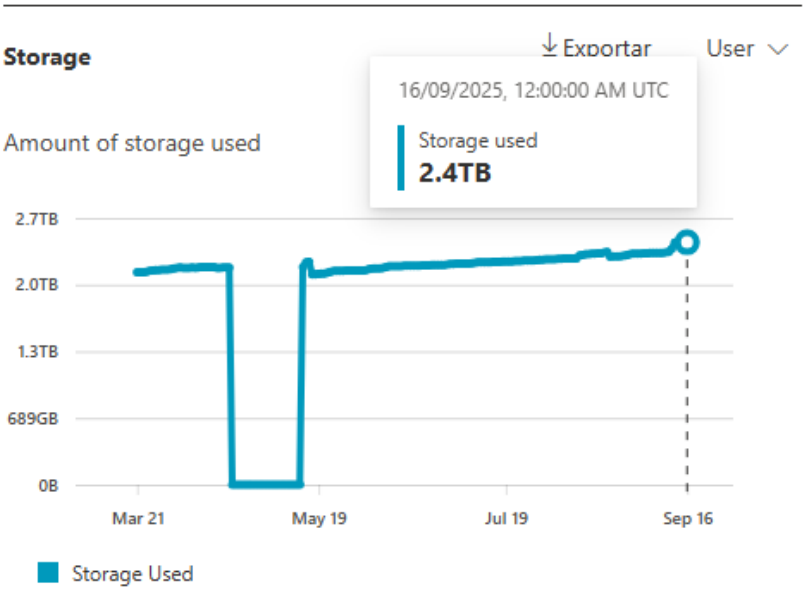



Figura 8 – Espaço em disco utilizado em 16/09/2025

| EXCHANGE | |
|---|---|
| | |
| Espaço utilizado em 16/09/2025 | 2,4 |
| Variação mensal | 0,05 |
| Incremento diário | 0,0017 |
| | |
| **Backups full** | |
| | |
| **Mês** | **Volume salvo em backup** |
| 1 | 2,4 |
| 2 | 2,45 |
| 3 | 2,50 |
| 4 | 2,55 |
| 5 | 2,60 |
| 6 | 2,65 |
| 7 | 2,70 |
| 8 | 2,75 |
| 9 | 2,80 |
| 10 | 2,85 |
| 11 | 2,9 |
| 12 | 2,95 |
| 13 | 3,00 |
| 14 | 3,05 |
| 15 | 3,10 |
| 16 | 3,15 |
| 17 | 3,20 |
| 18 | 3,25 |
| 19 | 3,30 |
| 20 | 3,35 |
| 21 | 3,4 |
| 22 | 3,45 |
| 23 | 3,50 |
| 24 | 3,55 |
| 25 | 3,60 |
| 26 | 3,65 |
| 27 | 3,70 |
| 28 | 3,75 |
| 29 | 3,80 |
| 30 | 3,85 |
| 31 | 3,9 |
| 32 | 3,95 |
| 33 | 4,00 |
| 34 | 4,05 |

| | |
|---|---|
| 35 | 4,10 |
| 36 | 4,15 |
| 37 | 4,20 |
| 38 | 4,25 |
| 39 | 4,30 |
| 40 | 4,35 |
| 41 | 4,4 |
| 42 | 4,45 |
| 43 | 4,50 |
| 44 | 4,55 |
| 45 | 4,60 |
| 46 | 4,65 |
| 47 | 4,70 |
| 48 | 4,75 |
| 49 | 4,80 |
| 50 | 4,85 |
| 51 | 4,9 |
| 52 | 4,95 |
| 53 | 5,00 |
| 54 | 5,05 |
| 55 | 5,10 |
| 56 | 5,15 |
| 57 | 5,20 |
| 58 | 5,25 |
| 59 | 5,30 |
| 60.1 (full do mês 60, semana 1) | 5,31 |
| 60.2 (full do mês 60, semana 2) | 5,32 |
| 60.3 (full do mês 60, semana 3) | 5,34 |
| 60.4 (full do mês 60, semana 4) | 5,35 |
| | |
| **Backups incrementais** | |
| **Quantidade** | **Volume** |
| 26 | 0,04 |

6.32. Analisando a variação mensal apresentada no relatório, o cálculo ficou da seguinte maneira:

6.33. Cálculo do volume armazenado para 24 meses:

| EXCHANGE | |
|---|---|
| Front-end armazenado (somatório do último backup full e incrementais do mês corrente) | 5,39 |
| Volumetria sem redução de dados (somatório dos backups realizados a partir do mês 37 e incrementais do mês corrente) | 130,62 |
| Volumetria com redução de dados (90% / 10:1) | 13,06 |

6.34. Por fim, com relação ao SharePoint, os dados são os seguintes:

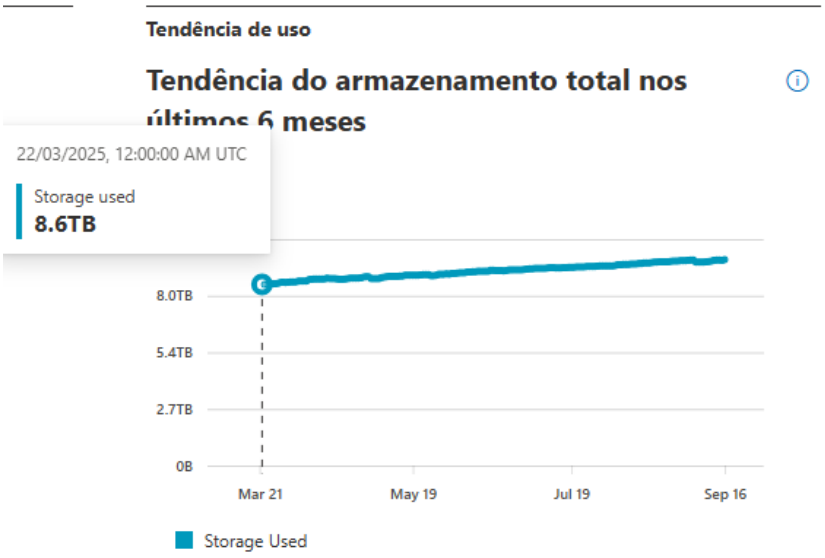



Figura 9 – Espaço em disco utilizado em 22/03/2025

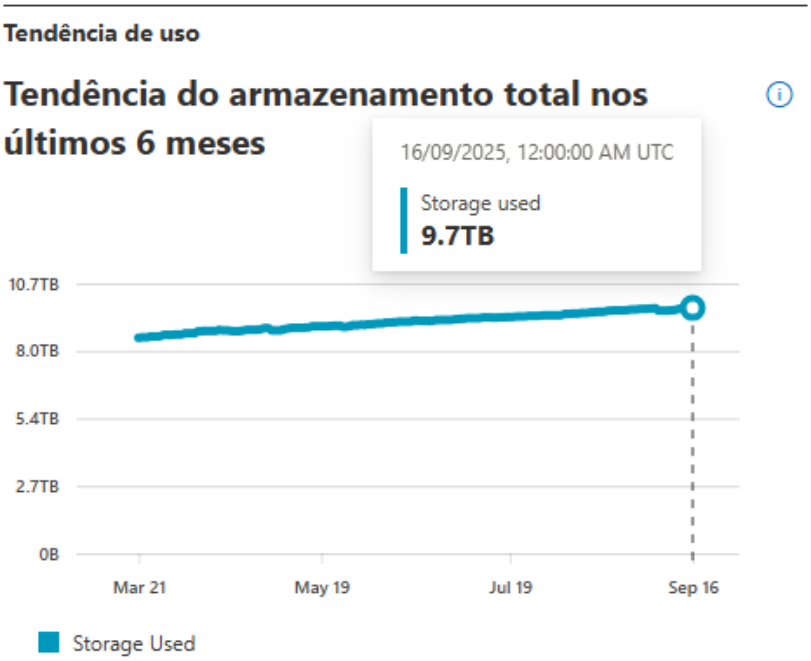



Figura 10 – Espaço em disco utilizado em 16/09/2025

6.35. Analisando os dados, seguem os valores:

| SHAREPOINT | |
|---|---|
| | |
| Espaço utilizado em 16/09/2025 | 9,7 |
| Variação mensal | 0,18 |
| Incremento diário | 0,0060 |
| | |
| **Backups full** | |
| | |
| **Mês** | **Volume salvo em backup** |
| 1 | 9,7 |
| 2 | 9,88 |
| 3 | 10,06 |
| 4 | 10,24 |
| 5 | 10,42 |
| 6 | 10,6 |
| 7 | 10,78 |
| 8 | 10,96 |
| 9 | 11,14 |
| 10 | 11,32 |
| 11 | 11,5 |
| 12 | 11,68 |

| | |
|---|---|
| 13 | 11,86 |
| 14 | 12,04 |
| 15 | 12,22 |
| 16 | 12,4 |
| 17 | 12,58 |
| 18 | 12,76 |
| 19 | 12,94 |
| 20 | 13,12 |
| 21 | 13,3 |
| 22 | 13,48 |
| 23 | 13,66 |
| 24 | 13,84 |
| 25 | 14,02 |
| 26 | 14,2 |
| 27 | 14,38 |
| 28 | 14,56 |
| 29 | 14,74 |
| 30 | 14,92 |
| 31 | 15,1 |
| 32 | 15,28 |
| 33 | 15,46 |
| 34 | 15,64 |
| 35 | 15,82 |
| 36 | 16 |
| 37 | 16,18 |
| 38 | 16,36 |
| 39 | 16,54 |
| 40 | 16,72 |
| 41 | 16,9 |
| 42 | 17,08 |
| 43 | 17,26 |
| 44 | 17,44 |
| 45 | 17,62 |
| 46 | 17,8 |
| 47 | 17,98 |
| 48 | 18,16 |
| 49 | 18,34 |
| 50 | 18,52 |
| 51 | 18,7 |
| 52 | 18,88 |
| 53 | 19,06 |
| 54 | 19,24 |
| 55 | 19,42 |

| | |
|---|---|
| 56 | 19,6 |
| 57 | 19,78 |
| 58 | 19,96 |
| 59 | 20,14 |
| 60.1 (full do mês 60, semana 1) | 20,19 |
| 60.2 (full do mês 60, semana 2) | 20,23 |
| 60.3 (full do mês 60, semana 3) | 20,28 |
| 60.4 (full do mês 60, semana 4) | 20,32 |
| | |
| **Backups incrementais** | |
| | |
| **Quantidade** | **Volume** |
| 26 | 0,16 |

6.36. Para 24 meses:

| **SHAREPOINT** | |
|---|---|
| Front-end armazenado (somatório do último backup full e incrementais do mês corrente) | 20,48 |
| Volumetria sem redução de dados (somatório dos backups realizados a partir do mês 37 e incrementais do mês corrente) | 498,85 |
| Volumetria com redução de dados (90% / 10:1) | 49,88 |

6.37. Para o ambiente em nuvem do Tribunal, optou-se por uma taxa de redução de dados mais conservadora. Para a definição da taxa a ser utilizada para o projeto, vários pontos foram analisados, em especial a taxa atual obtida no backup local e documentos de fabricantes de referência no mercado. Segundo informações contidas no e-DOC 2912009D, o valor padrão para o HPE StoreOnce seria uma taxa de 20:1 (95% de redução); para Dell PowerProtect, o menor valor encontrado foi 15:1 (93,67% de redução); ExaGrid apresenta valores de 10:1 a 50:1, sendo a média 20:1. Assim, percebe-se que há taxas bastante agressivas de redução de dados.

6.38. Porém, com relação aos dados que estão na nuvem Microsoft, escolheu-se a taxa de 10:1 (90% de redução), por conta dos tipos de dados que são armazenados na estrutura.

6.39. Tanto o OneDrive for Business quanto o SharePoint Online servem para armazenar arquivos corporativos e colaborativos. Os tipos de dados mais comuns incluem:

6.39.1. Documentos Office (Word, Excel, PowerPoint) – Arquivos .docx, .xlsx, .pptx largamente

utilizados. Esses formatos modernos já são compactados internamente (pacotes Open XML baseados em ZIP) e muitas vezes incorporam imagens ou mídia internas comprimidas.

6.39.2. Arquivos PDF – Relatórios, formulários digitalizados e documentos oficiais em PDF estão entre os tipos mais frequentes em bibliotecas do SharePoint. PDFs também costumam usar compressão interna (por exemplo, compactação de imagens ou texto).

6.39.3. Imagens – Fotos e gráficos nos formatos JPEG, PNG, GIF etc. são muito comuns no Microsoft 365, seja como arquivos armazenados ou embutidos em documentos. Esses formatos já aplicam compressão.

6.39.4. Vídeos e áudios – Em menor proporção, pode haver mídias como vídeos MP4 (por exemplo, gravações de reuniões do Teams armazenadas em SharePoint/OneDrive) e arquivos de áudio. Arquivos de mídia tendem a ser grandes, porém já vêm altamente comprimidos.

6.39.5. Outros – Arquivos de texto simples, código-fonte, arquivos ZIP, e possivelmente arquivos de banco de dados ou backups exportados (menos comuns). Arquivos ZIP e semelhantes são por definição dados pré-comprimidos.

6.40. Do ponto de vista da deduplicação, essa característica é importante. Dados pré-comprimidos ou multimídia normalmente não deduplicam bem, pois não apresentam sequências redundantes óbvias: formatos como ZIP, JPEG, MP4 etc. removem redundâncias internamente e deixam poucos padrões repetidos para o mecanismo de deduplicação aproveitar. A própria Dell EMC, em seu programa de garantia de deduplicação9, exclui arquivos multimídia e dados pré-comprimidos do cálculo de eficiência, justamente porque esses tipos costumam ter baixo ganho de dedupe. Em outras palavras, um conjunto de arquivos Office, PDFs e imagens todos diferentes entre si não irá, em um único backup, encolher muito além do que já foi compactado – possivelmente apenas ~1.2x a 2x com compressão adicional, se tanto.

6.41. Por outro lado, OneDrive e SharePoint frequentemente também contêm dados duplicados entre usuários ou sites. Por exemplo, um modelo de documento do Word pode ser copiado por vários funcionários, ou um mesmo PDF (como uma política interna) armazenado em várias pastas compartilhadas. Nesses casos, embora os arquivos estejam compactados, a deduplicação de nível de bloco no appliance consegue identificar blocos binários idênticos entre os arquivos duplicados e armazená-los apenas uma vez. Assim, arquivos idênticos ou muito semelhantes presentes em locais diferentes serão bons candidatos à deduplicação. Porém, fora esses casos de arquivos

[9] < https://www.delltechnologies.com/asset/en-us/products/storage/briefs-summaries/data-protection-deduplication-guarantee-terms-and-conditions-brief.pdf>. Acessado em 07/07/2025.

duplicados, a redundância dentro do dataset do OneDrive/SharePoint tende a advir mais do histórico de backup (mesmo arquivo em backups de dias diferentes) do que de similaridade entre arquivos distintos – este último é limitado por cada arquivo ser único e comprimido.

6.42. No Exchange Online, os dados consistem principalmente em e-mails e seus anexos. Esse ambiente costuma oferecer muito mais redundância intrínseca para a deduplicação explorar, por vários motivos:

6.42.1. Usuários diferentes podem ter cópias do mesmo e-mail (por exemplo, mensagens enviadas a toda a equipe, ou threads de resposta com todo o histórico incluído). Assim, trechos de texto repetidos (como rodapés padrão, disclaimers legais, ou o histórico de respostas) aparecem em múltiplas caixas de correio. A nível de backup, isso significa blocos de dados idênticos presentes em diversos locais.

6.42.2. Mais significativamente, anexos de e-mail duplicados geram grandes oportunidades de dedupe. Se um arquivo de 5 MB é enviado para 50 pessoas, o sistema de e-mail normalmente armazenará 50 cópias separadas. Cada backup completo da plataforma salvaria esses 250 MB no total. Com deduplicação, apenas uma única cópia de cada anexo idêntico precisa ser armazenada, referenciando-a para todos os destinatários. Isso representa, neste exemplo, uma eliminação de 49 cópias redundantes – um fator de 50:1 apenas para esse anexo. De forma geral, é comum um anexo popular (por exemplo, um memorando em PDF) aparecer dezenas ou centenas de vezes em um backup de e-mails, o que resulta em taxas de deduplicação altíssimas localmente para esses itens. O caso típico citado na literatura é 100 instâncias de um anexo de 1 MB em caixas diferentes; sem dedupe seriam 100 MB, mas com dedupe armazena-se ~1 MB, uma razão de ~100:1[10].

6.43. O conteúdo textual dos e-mails, embora não ocupe tanto espaço quanto os anexos, também contribui para a deduplicação. Muitas mensagens corporativas contêm rodapés padronizados (ex: assinaturas, avisos de confidencialidade) repetidos em cada envio. Além disso, em conversas de e-mail, as respostas carregam todo o fio da conversa, duplicando várias vezes o mesmo texto à medida que a thread cresce. Quando se faz backup de todas as caixas de correio, essa redundância textual pode ser eliminada pelo mecanismo de dedupe de bloco, reduzindo ainda mais o armazenamento necessário.

6.44. Em resumo, os backups de e-mail (Exchange) tendem a deduplicar muito bem devido à grande quantidade de dados repetidos (mesmos anexos e conteúdos) entre usuários e mensagens.

[10] https://pt.wikipedia.org/wiki/Desduplica%C3%A7%C3%A3o_de_dados. Acessado em 07/07/2025.

6.45. Para avaliar se é razoável esperar ao menos 10:1 (dez vezes de redução) nos backups dos dados do OneDrive, SharePoint e Exchange, é preciso considerar como a deduplicação trabalha e os fatores que influenciam sua eficácia:

6.45.1. Redundância de dados: A deduplicação identifica padrões de bytes repetidos para armazená-los uma única vez. Se os dados possuem muita repetição, o potencial de dedupe é alto; se cada fragmento é único, o ganho é próximo de zero. Nos exemplos, notou-se que muitos arquivos armazenados (Office, PDF, imagens) já vêm compactados e com pouca redundância interna. Assim, dentro de um único backup inicial do OneDrive/SharePoint, pode não haver tantas repetições óbvias entre arquivos diferentes. Taxas baixas (2:1, 3:1) são comuns no primeiro backup completo de um dataset heterogêneo, pois a única redundância vem de arquivos eventualmente duplicados ou padrões comuns muito genéricos. Por outro lado, em e-mails há bastante redundância de anexos e textos repetidos, o que puxa a eficiência para cima.

6.45.2. Retenção e backups incrementais ao longo do tempo: Esse é o fator crucial. A verdadeira força da deduplicação em backups está em armazenar apenas as mudanças entre backups sucessivos, já que a maioria dos dados permanece igual de um dia para o outro. Quando se mantêm vários pontos de recuperação (vários dias/semanas de backup), a maior parte dos dados de cada novo backup já foi vista em backups anteriores – e o appliance então armazena apenas referências. Com o passar do tempo, a taxa de deduplicação acumulada cresce substancialmente, conforme o “dicionário” de segmentos duplicados vai se enriquecendo. Não por acaso, muitas empresas retêm 4 a 12 semanas de backups em disco, e deduplicadores costumam atingir em torno de 15:1 nesse intervalo de retenção típico11. Esse valor de 15:1 quer dizer ~93% de economia – 10:1 (90% de economia) situa-se bem dentro desse patamar esperado, desde que haja algumas semanas de retenção.

6.46. Assim, acredita-se, com base em referências do mercado de backup, que a taxa de 10:1 de deduplicação (guardar 10 TB lógicos em 1 TB físico) é realista em backups de OneDrive, SharePoint e Exchange, desde que se tenha retenção de múltiplos backups ao longo do tempo e uso consolidado de deduplicação global no destino, o que será o caso do Tribunal.

6.47. Além do espaço calculado, julga-se prudente acrescentar ao appliance 20% a mais de espaço, para cobrir eventuais novos sistemas e dados a serem salvos durante a execução contratual. Dessa forma, o espaço líquido do appliance de backup será de, no mínimo, 215 TB, considerando-se o

11 https://i.dell.com/sites/csdocuments/Shared-Content_data-Sheets_Documents/en/uk/demystifying-deduplication.pdf. Acessado em 07/07/2025.

somatório dos volumes que serão armazenados, com redução de dados.

6.48. Ressalta-se que serão necessários dois appliances com essa capacidade, pois um ficará no datacenter principal do Tribunal e o outro receberá as replicações do backup, no ambiente de recuperação de desastres.

6.49. Com relação ao licenciamento do software de backup deve-se considerar os seguintes fatores:

6.49.1. Para o ambiente on-premise, backup e restore, irrestrito, dos dados de, no mínimo, 167 máquinas virtuais. Atualmente, o Tribunal possui 131 máquinas virtuais em execução e todas elas passarão pelas rotinas de backup. Em média, cria-se uma máquina virtual a cada dois meses, perfazendo seis novas máquinas virtuais por ano. Ao final dos 60 meses de suporte e garantia, estima-se um acréscimo de 30 novas máquinas virtuais. Para suportar eventuais novos serviços não abarcados no planejamento, julga-se prudente acrescentar 20% ao número de máquinas virtuais que podem ser criadas, resultado em 36. Assim, o total de máquinas virtuais a serem licenciadas será de 131 + 36, isto é, 167.

6.49.2. Caso o modelo de licenciamento da solução não seja por máquina virtual, e sim por front-end, deve-se considerar o seguinte volume de dados que será armazenado:

6.49.2.1. Front-end armazenado: 215 TB (179,03 TB de estimativa + 20% de margem de segurança para eventuais novos dados a serem salvaguardados).

6.49.3. Para o ambiente em nuvem do Microsoft 365, caso o modelo de licenciamento seja por licença de usuário, deve-se considerar para fins de cobertura das capacidades de backup e restore:

6.49.3.1. M365 E3: 1.100 licenças;

6.49.3.2. O365 E1: 180 licenças.

6.49.4. Caso o modelo de licenciamento da solução seja por front-end:

**6.49.4.1. One Drive:**

6.49.4.1.1. Front-end armazenado: 46,28 TB (38,57 TB de estimativa + 20% de margem de segurança para eventuais novos dados a serem salvaguardados).

**6.49.4.2. Exchange:**

6.49.4.2.1. Front-end armazenado: 6,46 TB (5,39 TB de estimativa + 20% de margem de segurança para eventuais novos dados a serem salvaguardados).

**6.49.4.3. SharePoint:**

6.49.4.3.1. Front-end armazenado: 24,57 TB (20,48 TB de estimativa + 20% de margem de segurança para eventuais novos dados a serem salvaguardados).

## 7. DO PARCELAMENTO DA CONTRATAÇÃO

7.1. Ocorrerá apenas uma contratação desse objeto, dentro do mesmo ciclo do Plano Anual de contratação vigente.

7.2. Considerando os aspectos técnicos da solução os itens 1 ao 3 foram agrupados em lote único.

7.3. O objeto da presente contratação é composto por atividades interdependentes, compreendendo aquisição de equipamentos, instalação, configuração, software de backup, e treinamento na solução, composta por software de backup local e appliances (Item 1), software de backup local para ambiente em nuvem Microsoft O365/M365 (Item 2), treinamento na solução (Item 3). A solução deverá ter garantia e suporte por 60 meses.

7.4. O não parcelamento do Lote tem potencial de trazer uma maior economia para a contratação, pois a eventual contratada poderia diluir seus custos fixos de alocação de pessoal no contrato para a prestação de ambos os serviços e melhor aproveitamento de tempo ocioso. Na hipótese inviável de parcelamento, cada empresa seria obrigada a alocar profissionais diferentes, o que provavelmente aumentaria o custo individual de cada contrato. Não obstante, ressalte-se que o parcelamento e absolutamente inviável para a presente solução.

7.5. Além disso, se resguardará a ampla participação de licitantes, por haver considerável número de empresas que já realizam o objeto da contratação de forma única.

7.6. Por fim, não trará restrição no mercado potencial de contratação de empresas com capacidade para a execução dos serviços na totalidade do objeto a ser licitado, conforme já comprovado no Estudo Técnico Preliminar (ETP), que bem atende aos termos previstos na Súmula TCU nº 247.

## 8. DA ESTIMATIVA DO VALOR DA CONTRATAÇÃO

8.1. Abaixo está a pesquisa de preços realizada para o projeto, aplicando-se as quantidades necessárias:

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Pregão Eletrônico** | | | 90142/2024 | | | | | | |
| | | | **Lote/Item** | | | | | | | | | |
| 1 | 1 | BACKUP/APPLIAC E | | 7.367.508,00 | 4.030.393,76 | 5.584.630,40 | 5.660.844,05 | 5.584.630,40 | 2.792.315,20 | 8.376.945,60 | 5.584.630,40 | 5.584.630,40 |
| **ITEM** | **QTD** | **DESCRIÇÃO** | **EMPRESAS** | UNITECH | O2Sistem | | **MÉDIA** | **MEDIANA** | **INEXEQUÍVEL** | **EXORBITANTE** | **Valor Unitário Estimado (R$)** | **Valor Total Estimado (R$)** |
| | | | **UASG** | | | 530001 | | | | | | |
| | | | **Pregão Eletrônico** | | | 90014/2024 | | | | | | |
| | | | **Lote/Item** | | | | | | | | | |
| 2 | 1 | BACKUP NUVEM | | 1.731.210,00 | 1.198.822,40 | 1.721.600,00 | 1.550.544,13 | 1.721.600,00 | 860.800,00 | 2.582.400,00 | 1.550.544,13 | 1.550.544,13 |
| **ITEM** | **QTD** | **DESCRIÇÃO** | | | | | **MÉDIA** | **MEDIANA** | **INEXEQUÍVEL** | **EXORBITANTE** | **Valor Unitário Estimado (R$)** | **Valor Total Estimado (R$)** |
| | | | **UASG** | 195006 | 925400 | 927131 | | | | | | |
| | | | **Pregão Eletrônico** | 90142/2024 | 93756/2024 | 90015/2024 | | | | | | |
| | | | **Lote/Item** | | | | | | | | | |
| 3 | 1 | TREINAMENTO | | 8.398,95 | 9.000,00 | 5.775,00 | 7.724,65 | 8.398,95 | 4.199,48 | 12.598,43 | 7.724,65 | 7.724,65 |
| | | | | | | | | | | | **VALOR ESTIMADO DA CONTRATAÇÃO (R$)** | **7.142.899,18** |

8.2. O valor total estimado da presente contratação, portanto, será de **R$ 7.142.899,18** (sete milhões, cento e quarenta e dois mil, oitocentos e noventa e nove reais e dezoito centavos).

## 9. CONTRATAÇÕES CORRELATAS

9.1. Contratações correlatas já ocorreram em diversos órgãos e entidades da Administração Pública brasileira, como:

9.1.1. UASG 50001_PE 90087-2024

9.1.2. UASG 70022_PE 90030-2024

9.1.3. UASG 70023_PE 90006-2025

9.1.4. UASG 153031_PE 90134-2024

9.1.5. UASG 154054_PE 90004-2025

9.1.6. UASG 195006_PE 90142-2024

9.1.7. UASG 530001_PE 90014-2024

9.1.8. UASG 925007_PE 90058-2024

9.1.9. UASG 925153_PE 90002-2024

9.1.10. UASG 925400_PE 93756-2024

9.1.11. UASG 926426_PE 90013-2024

9.1.12. UASG 926919_PE 90006-2024

9.1.13. UASG 927131_PE 90015-2024

## 10. DAS PROVIDÊNCIAS ADMINISTRATIVAS A SEREM TOMADAS ANTES DA CONTRATAÇÃO

10.1. **CAPACITAÇÃO DE SERVIDORES OU DE EMPREGADOS PARA FISCALIZAÇÃO E GESTÃO CONTRATUAL**

10.1.1. Não aplicável.

10.2. **PREVISÃO DE INDICADORES PARA A GESTÃO DO CONTRATO**

10.2.1. Após a instalação e configuração dos equipamentos, estes deverão funcionar 24/7, e serão acompanhados pelos profissionais lotados nesta Corte, devendo eventuais problemas apresentados serem solucionados dentro de prazo estipulado no Edital.

10.3. **ORGANIZAÇÃO DE EQUIPES E COMISSÕES**

10.3.1. Não aplicável.

10.4. **DISPONIBILIZAÇÃO DE ESPAÇO**

10.4.1. Não aplicável.

10.5. **DISPONIBILIZAÇÃO DE ESTRUTURA LOGÍSTICA**

10.5.1. Não aplicável.

10.6. **PREVISÃO DE HORÁRIOS ESPECIAIS PARA EXECUÇÃO**

10.6.1. Os horários serão definidos pela equipe da GEINT.

## 11. RESULTADOS PRETENDIDOS

11.1. Um dos resultados esperado é o aumento do desempenho e da confiabilidade: as soluções modernas oferecem taxas de backup e recuperação superiores a 50 TB/h, o que garante atendimento às janelas de backup mesmo diante do crescimento exponencial dos dados. Além disso, a nova solução deverá fornecer recuperação rápida em casos de falha ou desastre, com mecanismos de imutabilidade, air gap e criptografia, elevando o nível de proteção contra ataques de ransomware e acessos não autorizados.

11.2. Adicionalmente, a solução contratada permitirá escalabilidade contínua, crescendo conforme a demanda, sem necessidade de substituições disruptivas, e garantirá integração nativa com ambientes em nuvem para retenção de longo prazo e estratégias de recuperação em desastres. Como resultado, espera-se maior resiliência operacional, redução de riscos e maior aderência às boas práticas de governança de TI, assegurando a disponibilidade e integridade dos dados institucionais em qualquer cenário.

11.3. ECONOMICIDADE

11.3.1. Redução no consumo de armazenamento: a tecnologia de deduplicação e compressão pode reduz em mais de 90% o volume efetivo de dados armazenados. Essa economia evita a necessidade de adquirir discos adicionais ou ampliar a infraestrutura de forma prematura.

11.3.2. Otimização de espaço físico e energia elétrica: menor quantidade de equipamentos, gavetas ou até mesmo discos resulta em redução do consumo energético e de refrigeração, além de, em alguns casos, liberar espaço em rack do datacenter.

11.3.3. Redução de danos à imagem do Tribunal por indisponibilidade: com velocidades de recuperação altas, o impacto de indisponibilidades é reduzido, evitando prejuízos associados a paralisações prolongadas.

11.3.4. Proteção contra ransomware e fraudes: funcionalidades de imutabilidade, air gap e time-lock evitam, em boa parte dos ataques, a necessidade de gastos emergenciais com resgate ou reconstrução de dados, assegurando a continuidade do negócio.

3.2. **APROVEITAMENTO DE RECURSOS**

3.2.1. Humanos

3.2.1.1. A equipe de infraestrutura irá coordenar a instalação dos equipamentos, junto à CONTRATADA, que realizará a instalação e configuração dos equipamentos.

3.2.2. Materiais

3.2.2.1. Serão usados os racks do TCDF para instalação dos equipamentos.

3.2.3. Financeiros

3.2.3.1. Não Aplicável.

## 12. REQUISITOS DE SUSTENTABILIDADE AMBIENTAL

### 3.3. IMPACTOS AMBIENTAIS

3.3.1. Não Aplicável.

### 3.4. LOGÍSTICA REVERSA

3.4.1. Não Aplicável.

### 3.5. RECICLAGEM

3.5.1. Não Aplicável.

## 13. CONCLUSÕES E CONSIDERAÇÕES FINAIS

13.1. Diante do exposto, a aquisição de uma nova solução de backup mostra-se estratégica para assegurar a continuidade dos serviços, a integridade e a disponibilidade das informações do Tribunal, ao mesmo tempo em que promove ganhos de desempenho, escalabilidade e segurança contra incidentes cibernéticos. A consolidação em uma plataforma moderna permitirá redução de custos operacionais e de infraestrutura, maior eficiência na utilização dos recursos, integração com ambientes de nuvem e capacidade de atender ao crescimento futuro da demanda sem substituições disruptivas. Assim, a contratação representa não apenas um avanço tecnológico, mas também uma decisão pautada na economicidade, na resiliência e na governança de TI, alinhada às melhores práticas de mercado e às necessidades críticas do TCDF.

13.2. Por todo o exposto, apresenta-se o presente Estudo Técnico Preliminar (ETP) em acordo com o disposto nos dispositivos legais e regulamentares aplicáveis ao caso. Sendo que, os integrantes requisitante e técnico aprovam o seu teor e atestam a viabilidade da contratação – seja pelos preços aplicados na presente contratação apresentado, seja pelas questões técnicas e econômicas aplicadas ao presente caso, de forma que procedemos a assinatura por meio eletrônico.

**Ednaldo Ramos de Souza**
Secretário de Tecnologia da Informação
**INTEGRANTE REQUISITANTE**
**(CHEFIA)**

**Leonardo Ramos Paz**
Gerente de Infraestrutura Tecnológica
**INTEGRANTE REQUISITANTE**
**(ÁREA TÉCNICA)**

**Sérgio Ricardo Brazão**
Gerente de Recursos de Terceiros
**INTEGRANTE TÉCNICO**
**(ÁREA ADMINISTRATIVA)**

**Miguel Kojiio Nobre**
Auditor de Controle Externo – Área Especializada: Sistemas de TI
**INTEGRANTE TÉCNICO**
**(ÁREA TÉCNICA)**

**Oswaldo Junqueira Vaz Júnior**
Supervisor de Planejamento da Contratação
**INTEGRANTE ADMINISTRATIVO**
**(ÁREA ADMINISTRATIVA)**

# ANEXO I – ANÁLISE DE RISCOS

Cumprindo com o disposto na Instrução Normativa SGD/ME nº 94/2022, serão analisados os riscos inerentes a três situações distintas relacionadas a este processo de contratação, originando os subsequentes eventos:

1. Fases do planejamento da contratação

1.1. Equívocos na descrição do objeto.
1.2. Elaboração falha da estimativa.
1.3. Erros materiais/formais no Termo de Referência.
1.4. Descontinuidade dos equipamentos.

2. Fases da seleção do fornecedor:

2.1. Morosidade no processo licitatório.
2.2. Impropriedades no processo licitatório.
2.3. Fracasso do processo licitatório.

3. Fases da contratação:

3.1. Não assinatura do contrato.
3.2. Atraso no fornecimento do objeto.
3.3. Equipamentos não possuem funcionalidades exigidas.
3.4. Inexecução total do contrato.
3.5. Inexecução parcial do contrato.

DESCRIÇÃO DAS PROBABILIDADES E IMPACTOS

**Tabela 1 -** risco de ocorrência de eventos.

| Probabilidade (Risco referencial) | OBSERVAÇÕES |
|---|---|
| Alta | A probabilidade de ocorrer é grande. |
| Média | As chances de ocorrer ou não são equivalentes. |
| Baixa | A probabilidade de ocorrer é pequena. |

**Tabela 2 -** avaliação do impacto.

| Impacto | OBSERVAÇÕES |
|---|---|
| Muito grande | Perda do recurso orçamentário; má aplicação de recursos públicos; indisponibilidade de todos os serviços ou perda de dados. |
| Grande | Perda do processo licitatório; degradação crítica do desempenho, indisponibilidade ou falhas graves em vários serviços, em algum(ns) serviço(s) essencial(is) ou equipamentos. |
| Moderado | Degradação moderada do desempenho ou falhas contornáveis de alguns serviços ou equipamentos, em um serviço essencial ou equipamentos. |
| Pequeno | Degradação leve do desempenho ou falhas contornáveis em serviços ou equipamentos não essenciais. |
| Muito pequeno | Degradação leve do desempenho em um serviço não essencial ou no fornecimento de produtos ou equipamentos. |

**TRIBUNAL DE CONTAS DO DISTRITO FEDERAL – TCDF**
**Secretaria de Tecnologia da Informação - STI**
Supervisão de Planejamento da Contratação - SPC

## ANÁLISE QUALITATIVA DOS RISCOS

FASES DO PLANEJAMENTO DA CONTRATAÇÃO

**Tabela 3** – Equívocos na descrição do objeto

| **RISCO - EQUÍVOCOS NA DESCRIÇÃO DO OBJETO** | | |
|---|---|---|
| (X) PLANEJAMENTO DA CONTRATAÇÃO<br>( ) SELEÇÃO DO FORNECEDOR<br>( ) CONTRATAÇÃO | | |
| **PROBABILIDADE** | ( ) ALTA ( ) MÉDIA ( X ) BAIXA | |
| **IMPACTO** | ( ) MUITO GRANDE (X) GRANDE ( ) MODERADO ( ) PEQUENO ( ) MUITO PEQUENO | |
| **DANO – CONSEQUÊNCIA** | | |
| 1 | Atraso na realização da contratação pleiteada. | |
| 2 | Obsolescência de equipamentos ou serviços descontinuados. | |
| **ITEM** | **AÇÃO PREVENTIVA** | **RESPONSÁVEL** |
| 1 | Realização de pesquisa intensa no mercado. | Integrante Requisitante<br>Integrante Técnico |
| **ITEM** | **AÇÃO DE CONTINGÊNCIA** | **RESPONSÁVEL** |
| 1 | Análise das impugnações dos Editais para as devidas corretivas. | Integrante Requisitante<br>Integrante Técnico |
| 2 | Pesquisa no mercado. | |
| **CAUSAS (FONTE + VULNERABILIDADES)** | | |
| 1 | Pessoal - Não observância dos requisitos mínimos do equipamento ou serviço. | |
| 2 | Pessoal - Ausência de pesquisa no mercado potencial das melhores práticas e produtos. | |
| 3 | Processo - Ausência de um Manual de Produtos e Serviços de Tecnologia da Informação. | |

**Tabela 4** – Elaboração falha da estimativa.

| **RISCO - ELABORAÇÃO FALHA DA ESTIMATIVA** | | |
|---|---|---|
| (X) PLANEJAMENTO DA CONTRATAÇÃO<br>( ) SELEÇÃO DO FORNECEDOR<br>( ) CONTRATAÇÃO | | |
| **PROBABILIDADE** | ( ) ALTA ( X ) MÉDIA ( ) BAIXA | |
| **IMPACTO** | ( ) MUITO GRANDE ( X ) GRANDE ( ) MODERADO ( ) PEQUENO ( ) MUITO PEQUENO | |
| **DANO – CONSEQUÊNCIA** | | |
| 1 | Atraso na realização da contratação pleiteada. | |
| 2 | Contratação superfaturada | |
| 3 | Atraso na realização da elaboração da estimativa. | |
| **ITEM** | **AÇÃO PREVENTIVA** | **RESPONSÁVEL** |
| 1 | Pesquisa, análise e estudo de preços praticados no mercado. | Integrante Requisitante<br>Integrante Técnico |
| 2 | Constar preços públicos na estimativa de produtos e serviços de Tecnologia da Informação a serem contratados. | |
| **ITEM** | **AÇÃO DE CONTINGÊNCIA** | **RESPONSÁVEL** |
| 1 | Análise das impugnações dos Editais e as devidas corretivas. | Integrante Requisitante<br>Integrante Técnico |
| 2 | Pesquisa no mercado, quanto aos preços praticados. | |
| **CAUSAS (FONTE + VULNERABILIDADES)** | | |

| | |
|---|---|
| 1 | Pessoal - Não atendimento do mínimo de 3 (três) orçamentos para estimativa. |
| 2 | Processo - Ausência de preços públicos |
| 3 | Processo - Ausência de um Catálogo de fornecedores vinculado ao Manual de Produtos e Serviços de TI |

**Tabela 5** – Erros materiais/formais no Termo de Referência.

| **RISCO - ERROS MATERIAIS/FORMAIS NO TERMO DE REFERÊNCIA** | | |
|---|---|---|
| (X) PLANEJAMENTO DA CONTRATAÇÃO<br>( ) SELEÇÃO DO FORNECEDOR<br>( ) CONTRATAÇÃO | | |
| **PROBABILIDADE** | ( ) ALTA ( ) MÉDIA ( X ) BAIXA | |
| **IMPACTO** | ( ) MUITO GRANDE (X) GRANDE ( ) MODERADO ( ) PEQUENO ( ) MUITO PEQUENO | |
| **DANO – CONSEQUÊNCIA** | | |
| 1 | Retrabalho e atraso na realização da contratação pleiteada. | |
| 2 | Atraso na realização da contratação pleiteada. | |
| **ITEM** | **AÇÃO PREVENTIVA** | **RESPONSÁVEL** |
| 1 | Estabelecer no Termo de Referência / Projeto Básico que haja suporte técnico e manutenção para os equipamentos adquiridos | Integrante Requisitante<br>Integrante Técnico<br>Integrante Administrativo |
| 2 | Realização de interações com os demais setores do TCDF para elaboração dos Termos de Referência e Projetos Básico e demais documentos necessários ao processo. | |
| **ITEM** | **AÇÃO DE CONTINGÊNCIA** | **RESPONSÁVEL** |
| 1 | Análise das impugnações dos Editais e as devidas corretivas. | Integrante Requisitante<br>Integrante Técnico |
| **CAUSAS (FONTE + VULNERABILIDADES)** | | |
| 1 | Pessoal - Não atendimento a estrutura formalizada dos documentos | |
| 2 | Processo - Elaboração do Termo de Referência e Projeto Básico sem interação com outros setores. | |

**Tabela 6** – Descontinuidade dos Equipamentos.

| **RISCO – DESCONTINUIDADE DOS EQUIPAMENTOS** | | |
|---|---|---|
| (X) PLANEJAMENTO DA CONTRATAÇÃO<br>( ) SELEÇÃO DO FORNECEDOR<br>( ) CONTRATAÇÃO | | |
| **PROBABILIDADE** | ( ) ALTA ( X ) MÉDIA ( ) BAIXA | |
| **IMPACTO** | ( ) MUITO GRANDE ( X ) GRANDE ( ) MODERADO ( ) PEQUENO ( ) MUITO PEQUENO | |
| **DANO – CONSEQUÊNCIA** | | |
| 1 | Possível atraso em atualizações. | |
| 2 | Possível obsolescência de software. | |
| **ITEM** | **AÇÃO PREVENTIVA** | **RESPONSÁVEL** |
| 1 | Estabelecer no Termo de Referência / Projeto Básico que haja suporte técnico e manutenção para os equipamentos adquiridos enquanto durar o contrato. | Integrante Requisitante<br>Integrante Técnico<br>Integrante Administrativo |
| **ITEM** | **AÇÃO DE CONTINGÊNCIA** | **RESPONSÁVEL** |
| 1 | Manter o uso do equipamento, mas sem as últimas novidades implementadas em versões em linha de produção. | Integrante Requisitante<br>Integrante Técnico |
| **CAUSAS (FONTE + VULNERABILIDADES)** | | |
| 1 | Pessoal – Pesquisa de mercado para conhecer as famílias e tempo de vida dos equipamentos disponíveis | |
| 2 | Processo - Elaboração do Termo de Referência sem informar do suporte enquanto durar o contrato. | |

## FASES DA SELEÇÃO DO FORNECEDOR

**Tabela 7** – Morosidade no processo licitatório.

| **RISCO - MOROSIDADE NO PROCESSO LICITATÓRIO** | | |
|---|---|---|
| ( ) PLANEJAMENTO DA CONTRATAÇÃO<br>(X) SELEÇÃO DO FORNECEDOR<br>( ) CONTRATAÇÃO | | |
| **PROBABILIDADE** | ( ) ALTA ( X ) MÉDIA ( ) BAIXA | |
| **IMPACTO** | ( ) MUITO GRANDE ( X ) GRANDE ( ) MODERADO ( ) PEQUENO ( ) MUITO PEQUENO | |
| **DANO – CONSEQUÊNCIA** | | |
| 1 | Atraso na realização da contratação pleiteada. | |
| **ITEM** | **AÇÃO PREVENTIVA** | **RESPONSÁVEL** |
| 1 | Acionar as áreas envolvidas na contratação quando se verificar demora demasiada em determinada fase. | Ocupantes de cargos com poder de decisão. |
| 2 | Estabelecer normativamente os prazos para a entrega de documentos. | Integrante Requisitante<br>Integrante Técnico<br>Integrante Administrativo |
| 3 | Cumprir a Portaria TCDF nº 381/1997. | |
| **ITEM** | **AÇÃO DE CONTINGÊNCIA** | **RESPONSÁVEL** |
| 1 | Atender com celeridade as demandas da Licitação. | Integrante Requisitante<br>Integrante Técnico<br>Integrante Administrativo |
| **CAUSAS (FONTE + VULNERABILIDADES)** | | |
| 1 | Processo - Ausência de prazos definidos na fase externa do processo administrativo de contratação em TI. | |
| 2 | Processo - Ausência dos fluxogramas dos processos de contratação em TI | |

**Tabela 8** – Impropriedades no processo licitatório.

| **RISCO - IMPROPRIEDADES NO PROCESSO LICITATÓRIO** | | |
|---|---|---|
| ( ) PLANEJAMENTO DA CONTRATAÇÃO<br>(X) SELEÇÃO DO FORNECEDOR<br>( ) CONTRATAÇÃO | | |
| **PROBABILIDADE** | ( ) ALTA ( ) MÉDIA ( X ) BAIXA | |
| **IMPACTO** | (X) MUITO GRANDE ( ) GRANDE ( ) MODERADO ( ) PEQUENO ( ) MUITO PEQUENO | |
| **DANO – CONSEQUÊNCIA** | | |
| 1 | Retrabalho e atraso na realização da contratação pleiteada. | |
| **ITEM** | **AÇÃO PREVENTIVA** | **RESPONSÁVEL** |
| 1 | Seguir a legislação relacionada às contratações em geral e contratações de bens e serviços de TI. | Integrante Requisitante<br>Integrante Técnico<br>Integrante Administrativo |
| 2 | Atender as recomendações do Controle Interno | Integrante Requisitante |
| 3 | Agir com transparência e velar pela aplicação dos princípios norteadores da Administração Pública. | Integrante Requisitante<br>Integrante Técnico<br>Integrante Administrativo |
| 4 | Cumprir a Portaria TCDF nº 381/1997. | Integrante Requisitante<br>Integrante Técnico<br>Integrante Administrativo |
| **ITEM** | **AÇÃO DE CONTINGÊNCIA** | **RESPONSÁVEL** |
| 1 | Atender com celeridade as demandas da Licitação. | Integrante Requisitante |

| | | |
|---|---|---|
| | | Integrante Técnico<br>Integrante Administrativo |
| **CAUSAS (FONTE + VULNERABILIDADES)** | | |
| 1 | Pessoal - Inobservância das legislações e princípios relacionados às contratações em TI. | |
| 2 | Processo - Falta de controle das recomendações do Controle Interno | |

**Tabela 9** – Fracasso no processo licitatório.

| **RISCO - FRACASSO NO PROCESSO LICITATÓRIO** | | |
|---|---|---|
| ( ) PLANEJAMENTO DA CONTRATAÇÃO<br>(X) SELEÇÃO DO FORNECEDOR<br>( ) CONTRATAÇÃO | | |
| **PROBABILIDADE** | ( ) ALTA ( ) MÉDIA (X) BAIXA | |
| **IMPACTO** | (X) MUITO GRANDE ( ) GRANDE ( ) MODERADO ( ) PEQUENO ( ) MUITO PEQUENO | |
| **DANO – CONSEQUÊNCIA** | | |
| 1 | Retrabalho para novo procedimento licitatório. | |
| 2 | Anulação do processo de contratação pleiteada | |
| **ITEM** | **AÇÃO PREVENTIVA** | **RESPONSÁVEL** |
| 1 | Seguir a legislação relacionada às contratações em geral e contratações de bens e serviços de tecnologia da informação. | Integrante Requisitante<br>Integrante Técnico<br>Integrante Administrativo |
| 2 | Proceder à especificação dos itens de forma que a maior quantidade possível de licitantes possa participar do certame. | Integrante Requisitante<br>Integrante Técnico |
| 3 | Seguir o trâmite administrativo para aprovação de documentos referentes à contratação. | Integrante Requisitante<br>Integrante Técnico<br>Integrante Administrativo |
| **ITEM** | **AÇÃO DE CONTINGÊNCIA** | **RESPONSÁVEL** |
| 1 | Atender com celeridade as demandas da Licitação. | Integrante Requisitante<br>Integrante Técnico<br>Integrante Administrativo |
| 2 | Correção da documentação pertinente, estimativa e outros documentos necessários ao processo. | Integrante Requisitante<br>Integrante Técnico<br>Integrante Administrativo |
| **CAUSAS (FONTE + VULNERABILIDADES)** | | |
| 1 | Pessoal - Inobservância de preços públicos e requisitos mínimos necessários. | |
| 2 | Pessoal - Especificações limitadas dos produtos e serviços do mercado. | |
| 3 | Pessoal - Documentação elaborada sem observância das normas | |

## FASES DA CONTRATAÇÃO

**Tabela 10** – Não assinatura do contrato.

| **RISCO - NÃO ASSINATURA DO CONTRATO** | |
|---|---|
| ( ) PLANEJAMENTO DA CONTRATAÇÃO<br>( ) SELEÇÃO DO FORNECEDOR<br>(X) CONTRATAÇÃO | |
| **PROBABILIDADE** | ( ) ALTA ( ) MÉDIA ( X ) BAIXA |

| | | |
|---|---|---|
| **IMPACTO** | (X) MUITO GRANDE ( ) GRANDE ( ) MODERADO ( ) PEQUENO ( ) MUITO PEQUENO | |
| **DANO – CONSEQUÊNCIA** | | |
| 1 | Atraso na realização da contratação pleiteada. | |
| 2 | Revogação da contratação | |
| **ITEM** | **AÇÃO PREVENTIVA** | **RESPONSÁVEL** |
| 1 | Convocar, dentro do prazo e condições estabelecidas, o interessado para assinar o termo de contrato. | Ocupantes de cargos com poder de decisão |
| 2 | Elaborar e promover a gestão orçamentária e financeira por meio de um plano de despesas orçamentárias anuais da STI | Ocupantes de cargos com poder de decisão<br>Integrante Requisitante |
| **ITEM** | **AÇÃO DE CONTINGÊNCIA** | **RESPONSÁVEL** |
| 1 | Convocar, dentro do prazo e condições estabelecidas, os licitantes remanescentes para manifestar o interesse e assinar o termo de contrato. | Ocupantes de cargos com poder de decisão |
| 2 | Realizar a gestão orçamentária e financeira junta as instâncias necessárias para realização de despesas. | Ocupantes de cargos com poder de decisão |
| **CAUSAS (FONTE + VULNERABILIDADES)** | | |
| 1 | Fator externo - Desistência do fornecedor em atender as demandas | |
| 2 | Fator externo - Falta de recurso orçamentário e financeiro para atendimento da contratação | |

**Tabela 11** – Atraso no fornecimento do objeto.

| | | |
|---|---|---|
| **RISCO - ATRASO NO FORNECIMENTO DO OBJETO** | | |
| ( ) PLANEJAMENTO DA CONTRATAÇÃO<br>( ) SELEÇÃO DO FORNECEDOR<br>(X) CONTRATAÇÃO | | |
| **PROBABILIDADE** | ( ) ALTA ( X ) MÉDIA ( ) BAIXA | |
| **IMPACTO** | ( ) MUITO GRANDE ( ) GRANDE ( X ) MODERADO ( ) PEQUENO ( ) MUITO PEQUENO | |
| **DANO – CONSEQUÊNCIA** | | |
| 1 | Contratação com início postergado | |
| 2 | Paralisação de serviços ou inutilização de equipamentos. | |
| 3 | Provimento extemporâneo dos setores demandantes | |
| 4 | Impossibilidade de o fornecedor efetivar as entregas | |
| **ITEM** | **AÇÃO PREVENTIVA** | **RESPONSÁVEL** |
| 1 | Estabelecer um prazo razoável para entrega dos objetos licitados. | Integrante Técnico<br>Integrante Requisitante |
| 2 | Estabelecer penalizações por atrasos, na forma prevista no instrumento convocatório ou no contrato. | Integrante Administrativo<br>Ocupantes de cargos com poder de decisão |
| 3 | Realizar um estudo técnico preliminar sobre a estrutura tecnológica do TCDF. | Integrante Técnico<br>Integrante Requisitante |
| 4 | Cumprir a Portaria TCDF nº 381/1997. | Integrante Requisitante<br>Integrante Técnico<br>Integrante Administrativo |
| **ITEM** | **AÇÃO DE CONTINGÊNCIA** | **RESPONSÁVEL** |
| 1 | Aplicar penalizações por atrasos, na forma prevista no instrumento convocatório ou no contrato | Integrante Requisitante<br>Ocupantes de cargos com poder de decisão. |

| | | |
|---|---|---|
| 2 | Efetivar ações junto aos fornecedores para entrega dos equipamentos e início dos serviços. | Integrante Requisitante<br>Integrante Técnico |
| 3 | Agilizar as adaptações da estrutura para entrega dos produtos e início dos serviços. | Integrante Requisitante<br>Integrante Técnico |
| **CAUSAS (FONTE + VULNERABILIDADES)** | | |
| 1 | Processo - Falta de controle nos trâmites da contratação | |
| 2 | Pessoal - Falta de controle na entrega dos produtos ou execução do serviço | |
| 3 | Processo - Falta de cronograma de contratação | |
| 4 | Estrutura Física - Parque tecnológico não preparado para recepcionar as contratações | |

**Tabela 12** – Equipamentos não possuem funcionalidades exigidas.

| **RISCO - EQUIPAMENTOS NÃO POSSUEM FUNCIONALIDADES EXIGIDAS.** | | |
|---|---|---|
| ( ) PLANEJAMENTO DA CONTRATAÇÃO<br>( ) SELEÇÃO DO FORNECEDOR<br>(X) CONTRATAÇÃO | | |
| **PROBABILIDADE** | ( ) ALTA ( ) MÉDIA ( X ) BAIXA | |
| **IMPACTO** | ( ) MUITO GRANDE (X) GRANDE ( ) MODERADO ( ) PEQUENO ( ) MUITO PEQUENO | |
| **DANO – CONSEQUÊNCIA** | | |
| 1 | Não provimento adequado do TCDF | |
| 2 | Contratações Ineficazes | |
| **ITEM** | **AÇÃO PREVENTIVA** | **RESPONSÁVEL** |
| 1 | Realizar os estudos técnicos preliminares com profundidade e técnica devida para obter e atender às necessidades do TCDF. | Integrante Requisitante<br>Integrante Técnico |
| 2 | Realizar reuniões com as áreas interessadas a fim de obter suas necessidades. | Integrante Requisitante |
| **ITEM** | **AÇÃO DE CONTINGÊNCIA** | **RESPONSÁVEL** |
| 1 | Adaptar os equipamentos e os serviços do TCDF, com os meios disponibilizados. | Integrante Requisitante<br>Integrante Técnico |
| 2 | Iniciar os Estudos Estratégicos de Tecnologia da Informação | Ocupantes de cargos com poder de decisão |
| **CAUSAS (FONTE + VULNERABILIDADES)** | | |
| 1 | Pessoal - Inexistência de pesquisa e estudo sobre demandas | |
| 2 | Pessoal - Ausência de Estudos Estratégicos de TI | |

**Tabela 13** – Inexecução total do contrato.

| **RISCO - INEXECUÇÃO TOTAL DO CONTRATO** | |
|---|---|
| ( ) PLANEJAMENTO DA CONTRATAÇÃO<br>( ) SELEÇÃO DO FORNECEDOR<br>(X) CONTRATAÇÃO | |
| **PROBABILIDADE** | ( ) ALTA ( ) MÉDIA (X) BAIXA |
| **IMPACTO** | (X) MUITO GRANDE ( ) GRANDE ( ) MODERADO ( ) PEQUENO ( ) MUITO PEQUENO |
| **DANO – CONSEQUÊNCIA** | |

| | | |
|---|---|---|
| 1 | Impossibilidade de celebração contratual | |
| **ITEM** | **AÇÃO PREVENTIVA** | **RESPONSÁVEL** |
| 1 | Atentar aos requisitos de habilitação, quando da elaboração da documentação (Projeto Básico/Termo de Referência) | Integrante Requisitante<br>Integrante Técnico<br>Integrante Administrativo |
| 2 | Pesquisar o histórico contratual das licitantes contratadas. | Integrante Requisitante |
| **ITEM** | **AÇÃO DE CONTINGÊNCIA** | **RESPONSÁVEL** |
| 1 | Aplicar penalizações, na forma prevista no instrumento convocatório ou no contrato. | Integrante Requisitante<br>Ocupantes de cargos com poder de decisão. |
| 2 | Convocar, dentro do prazo e condições estabelecidas, os licitantes remanescentes para manifestar o interesse e assinar o termo de contrato. | Ocupantes de cargos com poder de decisão |
| **CAUSAS (FONTE + VULNERABILIDADES)** | | |
| 1 | Pessoal - Inobservância dos critérios de habilitação na documentação elaborada. | |

**Tabela 14** – Inexecução parcial do contrato.

| **RISCO - INEXECUÇÃO PARCIAL DO CONTRATO** | | |
|---|---|---|
| ( ) PLANEJAMENTO DA CONTRATAÇÃO<br>( ) SELEÇÃO DO FORNECEDOR<br>(X) CONTRATAÇÃO | | |
| **PROBABILIDADE** | ( ) ALTA ( ) MÉDIA (X) BAIXA | |
| **IMPACTO** | ( ) MUITO GRANDE (X) GRANDE ( ) MODERADO ( ) PEQUENO ( ) MUITO PEQUENO | |
| **DANO – CONSEQUÊNCIA** | | |
| 1 | Provimento extemporâneo dos setores demandantes | |
| 2 | Rescisão contratual | |
| **ITEM** | **AÇÃO PREVENTIVA** | **RESPONSÁVEL** |
| 1 | Atentar aos requisitos contratuais, quanto a inexecução parcial da contratação, quanto da execução contratual. | Integrante Requisitante<br>Integrante Técnico |
| 2 | Pesquisar o histórico contratual das licitantes contratadas, quanto a execução dos contratos realizados com a Administração Pública. | Integrante Requisitante |
| 3 | Acompanhar a execução contratual para evitar subcontratações não autorizadas. | Integrante Requisitante<br>Integrante Administrativo |
| **ITEM** | **AÇÃO DE CONTINGÊNCIA** | **RESPONSÁVEL** |
| 1 | Aplicar penalizações, na forma prevista no instrumento convocatório ou no contrato. | Integrante Requisitante<br>Ocupantes de cargos com poder de decisão. |
| 2 | Convocar, dentro do prazo e condições estabelecidas, os licitantes remanescentes para manifestar o interesse e assinar o termo de contrato, caso a rescisão contratual venha ocorrer. | Ocupantes de cargos com poder de decisão |
| **CAUSAS (FONTE + VULNERABILIDADES)** | | |
| 1 | Fator Externo - Não cumprimento de cláusulas contratuais, especificações, projetos ou prazos. | |
| 2 | Fator Externo - Subcontratação com terceiros não admitidos no Edital | |