ESPECIFICAÇÃO TÉCNICA
Solução de Backup Institucional
Justiça Federal da Primeira Região (JF1)

Objeto: Aquisição de solução de backup e restauração de dados com serviço de garantia, suporte técnico especializado, instalação, migração do ambiente atual e treinamento, conforme especificações do edital e anexos.

Objetivos:

- Adequar o modo de licenciamento às novas realidades dos sistemas e serviços de Tecnologia da Informação (TI) que suportam as atividades judiciais e administrativas da Justiça Federal da 1ª Região (JF1);
- Atualizar solução de backup com novas funcionalidades que atendam e suportem novas tecnologias como serviços em nuvem;
- Melhorar e resolver problemas atuais de rotinas de backup, de forma a aumentar a confiabilidade de proteção dos dados institucionais da JF1;
- Adequar os serviços de backup à nova portaria de política de backup da JF1;
- Mitigar riscos de perda de dados por desastre ou ataques cibernéticos.

Justificativa da contratação:

- A JF1, historicamente, utiliza a modalidade de licenciamento de backup por volumetria, que há algum tempo vem mostrando-se uma modalidade pouco escalável frente ao franco crescimento dos sistemas judiciais e administrativos que suportam as atividades desta corte. Dessa forma, demanda-se uma nova forma de licenciamento que seja escalável e mais econômica;
- A adoção de serviços em nuvem vem sendo uma tendência em diversos órgãos ou empresas públicas, o que aumenta os quesitos de disponibilidade e confiabilidade das informações. Dessa forma, esta contratação visa adequar a solução de backup institucional aos novos cenários que se desenham para a JF1, como a adoção de serviços de infraestrutura e armazenamento em nuvem, os quais implicam na redução de ativos e passivos de TI locais e aumentam a eficiência da prestação dos serviços de backup;
- A JF1 com seus diversos sistemas novos e legados têm enfrentado diversos problemas com relação ao backup de dados, tais como RED (Repositório Eletrônico de Documentos), e-proc, JCR (módulo do PJe para arquivos anexos dos processos), arquivos de mídia digital da ASCOM, bancos de dados Oracle/Postgres, sistemas de arquivos NAS dos storages dentre outros. Com a tecnologia e funcionalidades atuais da solução de backup da JF1 não é possível ou é inviável a resolução de forma efetiva;
- A equipe técnica não possui treinamento da atual solução e, por esse motivo, existe uma defasagem de conhecimento sobre a solução. Dessa forma, a contratação de treinamento, para a solução a ser adquirida, mitigará essa limitação e nivelará o conhecimento dos administradores e operadores de backup em toda JF1;
- O treinamento a ser adquirido terá o escopo das equipes técnicas das seções judiciárias e TRF1 por motivos de idealização da descentralização das atividades de backup às seccionais, (atividades atualmente centralizadas no TRF1);

- O serviço de migração do ambiente atual mostra-se imprescindível por motivos diversos e pelo reduzido número de colaboradores para conduzir tal atividade. O serviço de migração visa, adicionalmente, reduzir riscos de perda ou corrupção de dados durante a migração para nova solução;
- Dado o volume de dados e ambientes a serem migrados, a migração do ambiente por empresa especializada e dedicada à atividade trará redução significativa do tempo para finalização, maior estabilidade e confiabilidade a todo o processo;
- A contratação da solução de backup terá também a garantia do fabricante durante 60 (sessenta) meses para qualquer necessidade de suporte técnico a falhas ou atualizações.

AmbienteTecnológico da JF1

- Descrição da estrutura organizacional da JF1: o A JF1 abrange 13 (treze) Unidades Federativas (UF), as quais, em cada capital respectiva, existe uma Seção Judiciária que representa a justiça federal de 1º grau;
    - o Cada Seção Judiciária (ou apenas Seção), por sua vez, pode ou não ter Subseções Judiciárias (ou apenas Subseção) nos municípios da UF; o O TRF1 (localizado no Distrito Federal) representa a justiça federal de 2º grau. Este tribunal centraliza a maior parte do gerenciamento e administração das soluções de infraestrutura de TI que dão suporte à toda JF1;
    - o Cada Seção, Subseção e TRF1 possui apenas 01 (um) datacenter; o Ao todo, somam-se 94 (noventa e quatro) datacenters, sendo: 14 (quatorze) em Seções (médio porte), 79 (setenta e nove) em subseções (pequeno porte) e 01 (um) no TRF1 (grande porte).

- Descrição de conectividade WAN entre as localidades:
    - O TRF1 possui links de comunicação WAN com as Seções Judiciárias (capitais) com capacidades de banda, conforme descrito na planilha "Ambiente Tecnológico JF1"; o Da mesma forma, cada Seção possui links de comunicação WAN com suas respectivas Subseções;
    - Cada Subseção comunica-se com o TRF1, somente, através de sua respectiva Seção.

- Descrição de conectividade de internet das localidades:
- oOs acessos aos links de internet dão-se diretamente para as localidades que os possuem, conforme detalhado na planilha "Ambiente Tecnológico JF1";
    - o As Subseções que não possuem links de acesso à internet fazem seus acessos através da Seção respectiva. Caso a mesma também não possua, o acesso ocorre através do link do TRF1;
    - o As Seções que não possuem link de internet, utilizam o link de comunicação do TRF1.

- Descrição de conectividade LAN e SAN dos datacenters:
    - Todas as Seções, Subseções e TRF1 possuem dois switches core de, no mínimo, 48 (quarenta e oito) portas, conforme detalhado na planilha "Ambiente Tecnológico JF1"; o Os switches core interligam todos os servidores em uma mesma VLan de produção:

- Nas seções e TRF1, a VLan de backup é segregada logicamente da rede de produção;
- Todas as Seções, exceto a de MG, possuem switches físicos iSCSI segregados dos switches core para interligação da rede de armazenamento de produção (SAN IP);
- A Seção de MG e o TRF1 utilizam 2 (dois) switches FibreChannel (FC) para interligação da rede de armazenamento de produção (SAN FC);
- Somente o TRF1 utiliza 2 (dois) switches FC segregados para interligar a infraestrutura de backup: fitoteca, servidores de mídia e storages.

- Descrição do ambiente de virtualização:

  O ambiente de virtualização da JF1 é composto de duas principais soluções: VMware e Oracle Virtualization (OVM);

  A solução VMware é composta por 01 (um) vCenter 6.7 centralizado no TRF1, 94 (noventa e quatro) Datacenters 01 (um) por localidade, 100 (cem) clusters e 219 (duzentos e dezenove) hosts cuja distribuição encontra-se detalhada na planilha "Ambiente Tecnológico JF1";

  - Os datacenters das Subseções utilizam a modalidade de licenciamento VMWarevSphere ROBO standard 6.7;
  - Caso seja necessário qualquer tipo de provisionamento de máquina virtual em Subseção para atendimento dos requisitos deste edital, deverá ser fornecido licenciamento do mesmo tipo pela CONTRATADA, em quantidade suficiente para todo o ambiente da JF1, com garantia para o mesmo período da vigência contratual;
  - A solução OVM hospeda ambientes de banco de dados Oracle versão 12.1.0.2 e é composta por servers pools com, no mínimo, 02 (dois) servidores físicos;
  - Todas as Seções e o TRF1 possuem apenas um único ambiente OVM.

- Descrição do ambiente e rotinas de backup:
  - As infraestruturas de backup estão concentradas em algumas Subseções, em todas as Seções e no TRF1, sendo as Seções as agregadoras de backups das Subseções (centralização);
  - Não há infraestrutura de backup nas Subseções, exceto nas subseções de Juiz de Fora - MG, Uberlândia - MG e Tabatinga – AM;
  - Os quantitativos e modelos de fitotecas, servidores de mídia, fitas e drives de backup estão detalhados na planilha "Ambiente Tecnológico JF1";
  - O software de backup institucional utilizado, oficialmente, no âmbito da JF1 é o VeritasNetbackup;
  - A versão predominante do software é a 8.2, exceto pelo ambiente do TRF1 (7.6.0.4 e 8.3), Juiz de Fora (7.6.1.2), Uberlândia (7.6.0.4), Tabatinga (7.6.1.2) e SJDF (8.3);
  - As rotinas de backup utilizadas na JF1 diferenciam-se pela criticidade de cada sistema ou serviço de TI, sendo classificados como críticos ou não-críticos;
  - As frequências e retenções para cada tipo de classificação estão detalhadas natabelaabaixo:

Serviços	Frequências e Retenções			
	Diária (incremental)	Semanal (completo)	Mensal (completo)	Anual (completo)
Críticos	2 meses	4 meses	1 ano	5 anos
NãoCríticos	1 mês	2 meses	6 meses	2 anos

- As volumetrias salvaguardadas em backup, para cada tipo de classificação, estão detalhadas na planilha de "Ambiente Tecnológico JF1";
- Janelas padrões de execução de backup diárias: Entre 19h e 6h do dia subsequente, de segunda a quinta-feira;
- Janelas padrões de execução de backup de finais de semana:Entre 19h de sexta-feira até 6h de segunda-feira;
- Os masters servers de cada localidade são servidores virtuais provisionados no ambiente de VMware;
- O atual licenciamento de software utilizado na JF1 é por volumetria - (30 (trinta) Terabytes licenciados); o Atualmente existem cerca de 473 (quatrocentas e setenta e três) rotinas de backup configuradas na JF1.

Descrição da solução e composição dos Itens

- Aquisição de solução de backup, com garantia de 60 (sessenta) meses para atualização e suporte técnico especializado. Treinamento para administração e operação da solução, o qual aborde todos os aspectos necessários para execução e restauração de backups de dados, bem como resolução de problemas, gerenciamento e monitoramento de ambiente. Serviço que contemple a instalação e configurações de ambiente, migração de políticas e migração de dados (inclusive em fitas LTO); Itens a serem registrados:

Item	Subitem	Objeto	Quantitativos	Tipo
1	--	Solução de Backup	01	Unidade
2	--	Suporte técnico e Garantia de Atualização	60	Meses
3	3.1	Treinamento Telepresencial - Básico	40	Aluno
	3.2	Treinamento Telepresencial - Avançado	20	Aluno
4	--	Serviço de Instalação e configuração, migração, adequação e transferência de conhecimento	01	Unidade
5	--	OperaçãoAssistida	01	Unidade

1. Solução de Backup
   1.1. Descrição da soluçãoofertada
      1.1.1. A solução deverá ser descrita detalhadamente de forma clara, objetiva e correta. Deveabrangertoda a Justiça Federal da PrimeiraRegião (JF1);
      1.1.2. Deverá descrever o quantitativo total de licenças, seu tipo, toda a infraestrutura e topologia necessária para operação da solução;

1.1.3. Caso seja necessário o fornecimento de appliances, passivos ou qualquer tipo de hardware, os mesmos deverão ser descritos na composição da solução e deve conter os quantitativos e finalidades.

1.2. Especificaçõesgerais

1.2.1. A solução de backup deverá ser baseada em três camadas: camada de gerência e controle, camada de operação de mídia e camada de cliente, onde cada camada deverá ter suas funções específicas, conforme abaixo:

1.2.1.1. Camada de gerência e controle: É responsável por orquestrar os servidores da camada de operação de mídia na execução das rotinas de backup e restauração, além de gerenciar catálogo de metadados de mídias. Também fornece de relatórios de auditorias, análise de execução de rotinas e demais funcionalidades de gerenciamento;

1.2.1.2. Camada de operação de mídia: É responsável por executar as cópias de dados entre os clientes e as mídias de armazenamento, que podem ser fitas, disco ou armazenamento em nuvem.

1.2.1.3. Camada de cliente: É responsável pela coleta de informações sobre os clientes que terão seus dados salvos em backup, execução de rotina de deduplicação no cliente, integração do cliente com as demais camadas. Para a integração pode ser utilizado configuração de agentes ou não.

1.2.2. A solução deverá ter suporte para armazenamento de backups em mídias físicas de fitas, disco e armazenamento em infraestrutura de nuvem IaaS (Infraestructure as a Service), de forma direta e indireta (staging);

1.2.3. O armazenamento em fitas deverá suportar tecnologia de fitas LTO:

1.2.3.1. Deve possuir compatibilidade a partir do padrão LTO3 (para fins de migração de ambiente legado);

1.2.4. O armazenamento em disco deverá suportar discos de LUNs de storage do tipo bloco iSCSI e FibreChannel, além de discos virtuais virtualizados;

1.2.5. Para o armazenamento em nuvem, a solução deverá ter compatibilidade com os tipos de armazenamento das principais empresas de infraestrutura em nuvem, no mínimo: Amazon AWS, Google Cloud e Microsoft Azure;

1.2.6. A camada de gerência e controle deverá implementar mecanismos de agregação lógica de metadados de mídias, permitindo verificação de conteúdo das mesmas, tais como: Data de execução do backup, lista de dados copiados e volumetria total de dados;

1.2.7. A solução deve permitir a integração com Microsoft Active Directory 2012 e superiores, permitindo a autenticação de usuário do domínio;

1.2.8. A solução ofertada deverá estar na versão de software mais recente do fabricante.

1.3. Backup e Restauração

1.3.1. A solução deverá suportar o backup e restauração de dados de, no mínimo:

1.3.1.1. VMware:

1.3.1.1.1. Máquinas virtuais inteiras ou de forma granular;

1.3.1.1.2. Discos de máquinas virtuais provisionados com modo de compatibilidade RDM virtual;

1.3.1.2. Microsoft:

1.3.1.2.1. Dados de servidores de arquivos;

1.3.1.2.2. Sistemas de arquivos que estejam utilizando a tecnologia DFS;

1.3.1.2.3. Objetos do Active Directory de forma granular;

1.3.1.2.4. Deve suportar cópia de dados de Exchange e DAG (DataBase Availability Groups) - inclusivegranularmente;

1.3.1.3. Dados de Bancos de dados Oracle:

1.3.1.3.1. Versão 12.1.0.2 - por meio de integração com RMAN;

1.3.1.4. Storages:

1.3.1.4.1. Compartilhamentos CIFS e NFS;

1.3.1.4.2. Volumes internos por meio do protocolo NDMP;

DELL– A solução a ser proposta é compatível com diversos fabricantes do mercadodestoragesNAS, tais como Dell EMC, NetApp, HP eIBM. Para Backup de NDMP. Considerandoos equipamentos do fabricante Huawei,atendemos tal requisito mediante a criação de cópias de segurança via CIFS ou NFS. Caso seja exigida a matriz de compatibilidade para a comprovação de tal requisito, destacamos que tal fabricante (Huawei) não faz parte da mesma considerando o suporte à funcionalidade de backup NDMP.

1.3.1.5. Dados de sistemas de arquivos diversos, no mínimo: NTFS, EXT3, EXT4 e XFS, de forma granular;

1.3.1.6. Caixas de e-mail e objetos do Microsoft Exchange, de forma granular;

1.3.2. A solução deverá permitir a restauração de dados em local diverso ao local de origem do backup efetuado;

1.3.3. Deverá realizar criptografia de dados, com as seguintes característicasmínimas:

1.3.3.1. Criptografia de dados de cópias de backup em mídias externas (fitas LTO) ou discos de armazenamento de cópias seguras;

1.3.3.2. Criptografia com algoritmos mais comuns de mercado e que utilize chaves de, pelo menos, 256 (duzentos e cinquenta e seis) bits.

1.3.4. O acesso à console de gerenciamento deverá ser feito por meio de console gráfica web, cliente java ou cliente fornecido com a

1.3.4.1. solução.

As tarefas de backup e restauração devem ser realizadas por meio desta interface gráfica, sem a obrigatoriedade de utilização de scripts;

1.3.5. Deve possuir mecanismo de auto salvamento e reconstrução do catálogo (base de dados) centralizado, em caso de perda do mesmo:

1.3.5.1. A reconstrução do catálogo, poderá ser realizada a partir dos repositórios de fita e/ou disco;

1.3.6. A solução deverá implementar funcionalidade configurável de deduplicação na origem (cliente) ou no destino (servidor/mídia);

1.3.7. Replicação dados de backups entre localidades remotas, por meio de links de comunicação de dados, sem o uso de ferramentas de terceiros;

1.3.8. Execução de backups de dados de localidades remotas, distintas de onde está instalado o servidor de mídia, por meio de link de comunicação de dados;

1.3.9. A solução deverá implementaragendador de execução de rotinas de backup com base na configuração prévia de janelas (intervalo temporal) de execução e permitir a configuração de exclusão e inclusão de dias específicos nos agendamentos;

1.3.10. Deverá permitir a realização de backups do tipo sintético (backup full consolidado a partir de um backup full prévio, em conjunto com os incrementais subsequentes);

1.3.11. A solução deverá permitir a configuração de múltiplas faixas de execução de cópias paralelas para diferentes repositórios (filesystems) de um mesmo cliente (multiplestreams);

1.3.12. Deverá permitir a multiplexação de gravação de dados: cópia serial e simultânea de vários streams de backup em um único dispositivo de armazenamento;

1.3.13. Deve viabilizar backups e restaurações via rede de dados (LAN);

1.3.14. A solução deverá ser capaz e estar totalmente licenciada para execução de backups na modalidade LAN FREE (backup direto ao armazenamento, sem utilização da rede LAN – cliente SAN), tanto para clientes hospedados no ambiente de virtualização VMware, quanto para clientes não virtualizados;

DELL – Nossa solução de proteção de dados suporta LAN FREE para diversos tipo de cargas de trabalhado, inclusiveworkloadsnão virtualizados.Considerando a funcionalidade LANFREE para o ambiente VMWARE, a solução a ser proposta implementa da seguinte forma :Para esse tipo de workloads virtualizados,possuimos mecanismos nativo de redução de dados, otimizando o tráfego de rede LAN de forma bem eficiente. Tal funcionalidadeutiliza algoritmos dedesduplicação na origem,trafegando em rede somente os blocos incrementais e alterados. Tal funcionalidade somente é possível em função da integração nativa com o recurso do VMWARE CTB(ChangedBlockTracking), que identifica os setores de disco que foram alterados, transmitindo somente os blocos de dados que foram alterados no último backup ou dos blocos em uso, reduzindo significativamente o trafego na rede.

Considerando tal requisito e a impossibilidade de nossa participação, sugerimos a seguinte redação para o requisito acima:

- A solução deverá ser capaz e estar totalmente licenciada para execução de backups na modalidade LAN FREE (backup direto ao armazenamento, sem utilização da rede LAN), para ambientes

baremetalas aplicações que utilizam o hypervisorVmware, deverá suportar também métodos de desduplicação na origem e integração nativa com recurso da VMWARE CBT(ChangedBlockTracking).

1.3.15. A solução deverá ser capaz de executar backup de arquivos mesmo que estejam abertos ou em uso pelo usuário, de forma a não impactar a cópia do dado, nem a utilização do arquivo pelo usuário;

1.3.16. Deve permitir a criação de listas de exclusão configuráveis - por cliente - dos apontamentos de backup a serem salvos;

1.3.17. Deve permitir a criação de tarefas que serão executadas antes e/ou depois da execução dos jobs de backup/restauração;

1.3.18. Deverá suportar a execução de, no mínimo, os seguintes tipos de backup: completo (full), incremental e diferencial ou cumulativo;

1.3.19. Deverá suportar a configuração de, no mínimo, os seguintes tipos de frequência de execução de backup: Diária, semanal, mensal e anual;

1.3.20. Deverá suportar a configuração de retenções de, pelo menos, até 5 (cinco) anos;

1.3.21. Deverá armazenar dados históricos de gerenciamento e de execução de cópias seguras (jobs de backup) por, no mínimo, 12 (doze) meses;

1.3.22. Permitir a configuração de staging, ou seja, permitir que o dado seja copiado para uma mídia temporária e, posteriormente, ser duplicado ou movido para outra mídia de forma automática. Exemplo: Cópia para disco, inicialmente, e para fita ou nuvem posteriormente;

1.3.22.1. Deve possibilitar a configuração e determinação de retenções para cada local de armazenamento;

1.3.22.2. Deve possuir funcionalidade de criar múltiplas cópias de backups;

1.3.22.3. Deve permitir a recuperação dos dados, de forma automática, por meio da cópia secundária, em caso de indisponibilidade da cópia primária;

1.3.23. A solução deverá implementardeduplicação dos dados (na origem) a serem enviados para backup em nuvem, a fim de reduzir tráfego de dados através de links de comunicação de internet;

1.3.23.1. Se para atendimento do item anterior for necessária a utilização de equipamentos de appliance ou similar, o mesmo deverá ser fornecido totalmente licenciado e habilitado para tal funcionalidade;

1.3.24. A solução deve ser capaz de gerenciar as fitas magnéticas contidas na fitoteca ou fitas armazenadas off-site:

1.3.24.1. Deve possibilitar a migração de dados entre fitas magnéticas;

1.3.24.2. Deve possibilitar a verificação da integridade do conteúdo das fitas.

1.4. Gerenciamento e Monitoramento

1.4.1. A solução deverá ser fornecida com uma ferramenta de gerenciamento centralizado, de forma a proporcionar uma visão analítica de todo o parque computacional e infraestrutura de backup do ambiente da JF1;

DELL – Como o requisito acima não está claro o seu entendimento e considerando que o objeto a ser licitado contempla o fornecimento de uma solução de backup e não uma solução de monitoramento de todo

o parque computacional do TRF1, sugerimos a alteração do requisito acima conforme descrito abaixo :

A solução deverá ser fornecida com uma ferramenta de gerenciamento centralizado, de forma a proporcionar uma visão analítica de toda infraestrutura de backup do ambiente do JF1;

1.4.2. O gerenciamento centralizado deverá prover integração com o Microsoft Active Directory para fins de autenticação de usuários;

1.4.3. A ferramenta de gerenciamento centralizado deverá implementar relatório de auditoria que permita verificar, no mínimo, usuário, data, horário e ação efetuada em cada ambiente de backup das localidades da JF1;

1.4.4. Deverá implementarpermissionamento baseado em perfil de grupo de usuários:

1.4.4.1. Possuir capacidade de estabelecer níveis de acesso diferenciados e configuráveis para atividades de administração e operação da solução;

1.4.5. Deve permitir a emissão de relatórios agendados e envio dos mesmos via protocolo SMTP, para caixas de e-mail;

1.4.6. A configuração e confecção de relatórios deve gerar dados de estatísticas de execução de rotinas de backup, falhas de drives de gravação de fitas LTO da fitoteca, volumetria de dados em backup, número de execuções de rotinas, dados de inventário de fitas, servidores, discos e rotinas de backup;

1.4.7. Deve permitir exportação de relatórios, no mínimo, nos formatos .CSV e .PDF;

1.4.8. Deverá possibilitar a verificação do conteúdo gravado em fitas de backup sem a necessidade de montá-las nos tape drives, ou seja, utilizando apenas o catálogo da solução;

1.4.9. Funcionalidade de configuração de alertas para envio de e-mail em casos de problemas no ambiente de backup de qualquer localidade da JF1.

1.5. Compatibilidadestecnológicas

1.5.1. A solução deve ser compatível com os clientes a nível de hardware e software conforme ambiente tecnológico disposto no item “Ambiente Tecnológico da JF1” e na planilha “Ambiente Tecnológico JF1”;

1.5.2. Deverá ser compatível com ambiente de virtualização VMwarevCenter 6.7;

1.5.3. Deve ser compatível com sistemas operacionais Windows Server 2016 e superiores;

1.5.4. Deve ser compatível com sistemas operacionais Linux CentOS, RedHat 7.0 e superiores;

1.5.5. Deve ser compatível com sistemas operacionais Oracle Linux 7 e superiores;

1.5.6. Deve ser compatível com servidores físicos DELL PowerEdge R720, R730, R820, R630 e R640;

1.5.7. Deve ser compatível com servidores Huawei CH 242 DDR4;

1.5.8. Deve ser compatível com servidores físicos HPE Proliant DL360 Gen 10;

1.5.9. Deve ser compatível com storagesHuaweiOceanStor 5600 v3 e 5300 v5;

1.5.10. Deve ser compatível com storages EMC VNX 5600 e 5800; 1.5.11. Deve ser compatível com storages EMC VNXe 1600 e 3150;

1.5.12. Deve ser compatível com as seguintes fitotecas:

1.5.1.1. IBM TS4300 e TS4500;

1.5.1.2. Quantum scalar i40 e i80;

1.5.1.3. TandbergExabyte Magnum 224 e T40;

1.5.1.4. QualStar XLS;

1.5.1.5. DELL PowerVault TL2000.

1.6.

Licenciamento

1.6.1. O licenciamento da solução deverá considerar os seguintes aspectos e previsões de escalabilidade, sem custos adicionais ao CONTRATANTE, durante a vigência contratual:

1.6.1.1. Incremento do ambiente descrito (ver item sobre "AmbienteTecnológico da JF1" e planilha "Ambiente Tecnológico JF1") em, pelo menos, 100% (cem por cento), por questões de volumetria de dados de backup deduplicados, dado o crescimento de processos digitais e administrativos;

1.6.1.2. O número de máquinas virtuais pode crescer em, pelo menos, 50% (cinquenta por cento);

1.6.1.3. 1.6.1.3. O número de processadores do ambiente de virtualizaçãopoderá aumentar em até 15% (quinze por cento);

1.6.1.4. 1.6.1.4. A existência dos clientes não virtualizados descritosno item"Ambiente Tecnológico da JF1" e na planilha "Ambiente TecnológicoJF1":

1.6.1.4.1. O número de clientes não virtualizados poderá ter crescimento de 10% (dez por cento);

1.6.1.5. Backups de máquinas virtuais de subseções judiciárias (municípios) são efetuados, remotamente, pelas seções judiciárias (capitais) respectivas;

1.6.1.5.1. Caso seja necessário o provisionamento de máquina virtual no ambiente de subseção, para envio de backups à seção, deverá ser fornecido licenciamento suficiente VMware ROBO (Remote Office Branch Office) standard 6.7 para a totalidade de subseções da JF1;

1.6.1.6. Deverá estar preparado para efetuar backups em nuvem no sentido on-premise para nuvem e restaurações de dados no sentido inverso;

1.6.1.7. O fornecimento de ferramenta de gerenciamento centralizado, conforme descrito no item 1.4 e subitens;

1.6.1.8. O licenciamento deve implementar todas as funcionalidades descritas nesta especificação, de forma irrestrita e perpétua;

1.6.1.9. O licenciamento atual de VeritasNetbackup da JF1 poderá ser utilizado na composição de parte da solução, como opção de

renovação da sua garantia, para atendimento aos requisitos descritos nesta especificação.

1.6.2. O licenciamento da solução poderá ser nas modalidades: Por processador, por servidor (agente), por máquina virtual, por volumetria ou por uma composição dessas várias modalidades a fim de compor uma solução robusta, escalável e que garanta a operação do backup institucional, conforme os termos descritos nesta especificação e seus anexos:

1.6.2.1. A solução deverá ser única, implantada por localidade da JF1, de forma integrada;

1.6.2.2. Deverá conter ambiente centralizado de monitoramento, gestão e operação de backup institucional (interface gráfica unificada);

1.6.2.3. Não será permitida a oferta de solução que adote diferentes consoles, a depender do licenciamento ofertado (seja ele híbrido ou homogêneo).

A título de sugestão e considerando que tais funcionalidades são essenciais para um ambiente de backup corporativo, sugerimos a inclusão dos itens abaixo :

- ***A solução deverá ser composta por software especializado com a finalidade específica de armazenamento de backup em disco inteligente com recursos de compressão dos dados;***

- ***A desduplicação deve segmentar os dados em blocos de tamanho variável ajustado automaticamente pelo algoritmo do software;***

JUSTIFICATIVA - Bloco variável:o algoritmo possui a "inteligência" para verificar o tipo de dado e a frequência para e utilização de bloco do tamanho adequado para a amostragem e criação das "sementes", consequentemente, o resultado é uma performance e aproveitamento de espaço superiores ao bloco fixo;

- ***A solução deve possuir recurso de WORM (Write OnceReadMany) de proteção contra alteração/regravação e exclusão dos dados armazenados, permitindo somente uma única escrita e múltiplas leituras, garantindo integridade e autenticidade, deste modo a solução não deverá permitir alterar ou apagar dados protegidos, até que o tempo de retenção configurado tenha expirado.***

JUSTIFICATIVA – Evitar exclusões e alterações maliciosas no backup, a fim de garantir a integridade da informação armazenada;

- ***Deve possuir funcionalidade que permita com que usuários de desktop/laptop realizem backup e restore de forma automática ou "on-demand";***
- ***Deve permitir que restore de dados das estações desktop/laptop seja executado pelo próprio usuário, sem a necessidade de envolver o administrador do backup;***

JUSTIFICATIVA - Um dos efeitos colaterais da pandemia de corona vírus foi um aumento deusuários remotos atuando na modalidade Home Office. Sendo assim surgiu uma necessidade de proteção desses usuários trabalhando de casa.

Proteção contra Cyber Ataques

- **Um dos efeitos colaterais da pandemia de corona vírus foi um aumento no número de ataques cibernéticos. Este aumento no número de incidentes está ligado não somente ao valor das informações, mas também claramente associado à migração em massa de companhias para regimes de trabalho remoto, com funcionários em casa, o que aumenta a vulnerabilidade das redes corporativas.**

- **Toda companhia que não investe na segurança adequada de seus dados digitais está correndo o grave risco de ataques irreversíveis, que podem, além de causar perdas financeiras diretas à empresa, devido aos resgates exigidos pelos hackers para a devolução de documentos digitais, também causar prejuízos financeiros, de tempo indeterminado, incalculáveis, decorrentes dos danos causados permanentemente às informações digitais.**

- **No dia 05 de fevereiro de 2020, o Governo publicou por decreto a Estratégia Nacional de Segurança Cibernética (e-Ciber), abrangendo orientações em relação a segurança cibernética e o fortalecimento da resiliência cibernética nacional através de práticas relacionadas à segurança cibernética.**

- **A íntegra da Estratégia Nacional de Segurança da Informação, feita pelo Governo Federal, está disponível no link (https://www.in.gov.br/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419).**

A título de sugestão, sugerimos a inclusão dos itens abaixo

- ***A solução deve possuir nativamente suporte a recuperação de ataques cibernéticos que possua as seguintes características:***
- ***Possuir capacidade de se integrar com rotinas de replicação para um appliancefisicamente isolado e offline, também conhecido como "air gap", ou seja, a solução deve operar completamente offline e apartada da rede de produção, exceto ao receber atualizações da réplica dos backups de produção;***
- ***A solução deverá ser capaz de gerenciar as regras de replicação controlada garantindo a réplica segura de comunicação entre o ambiente primário (produção) e o secundário (réplica isolada);***
- ***A solução deve gerenciar os processos de proteção do equipamento de réplica para desligar portas TCP e serviços não utilizados, assim como ativar o bloqueio e imutabilidade dos dados quando necessário;.***
- ***A solução deve usar criptografia para transferir dados entre o ambiente primário (produção) e secundário (réplica isolada);***
- ***Deve gerenciar e aplicar regras de imutabilidade (WORM) nas imagens de backup consideradas livres de qualquer infecção ou corrupção;***

- ***Deverá fornecer direito de atualização contínua dos produtos licenciados, assim como novas versões e patches de atualização;***

- ***A solução deve fornecer a capacidade de manter várias cópias de dados de maneira segura.***

2. Suporte técnico e Garantia de Atualização
   - 2.1. A atualização da solução consiste no fornecimento das alterações corretivas que forem necessárias ao perfeito funcionamento dos softwares da solução contratada: bug fixing, patches, bem como alterações evolutivas representadas por novas versões (releases);
   - 2.2. A garantia da solução deverá ter vigência mínima de 60 (sessenta) meses;
   - 2.3. Durante a vigência da garantia, o fabricante deverá possibilitar a atualização da versão do licenciamento a qualquer momento;
   - 2.4. A garantia deverá dar direito ao acionamento do suporte técnico especializado do fabricante diretamente ou por intermédio da CONTRATADA;
   - 2.5. O suporte técnico especializado deverá solucionar qualquer problema de mal funcionamento e prestar orientações quanto: Às melhores práticas de configurações do fabricante, incidentes, falhas de operação, instalação e atualização de versões;
   - 2.6. Durante a vigência da garantia, o fabricante deverá conceder acesso às documentações, softwares e quaisquer tipos de conteúdo relacionado ao produto via web, por meio de portal adequado:
     - 2.6.1. O portal web do fabricante deve permitir a abertura de chamados técnicos, bem como manter o histórico de tratativas de chamados anteriores;
     - 2.6.2. O portal web do fabricante deve ter interface de gerenciamento do licenciamento adquirido, permitindo a atualização das mesmas no período contratado de garantia;
   - 2.7. A CONTRATADA e/ou o fabricante devem fornecer telefone de contato gratuito para abertura de chamados técnicos;
   - 2.8. O período disponível para abertura de chamados técnicos deverá ser 24x7 (vinte e quatro horas por dia, sete dias por semana);
   - 2.9. O atendimento de chamados técnicos pela CONTRATADA e/ou fabricante deverá ser 24x7 (vinte e quatro horas por dia, sete dias por semana), em português - Brasil, de forma ininterrupta até a solução do incidente, de forma a respeitar os limites máximos de tempo de resolução, conforme tabela a seguir:

Nível de Criticidade	Descrição do Impacto ao Negócio	PrazoMáximo de Resolução
1 - Crítico	Situação emergencial ou problema crítico que cause a indisponibilidade do ambiente de backup. Ambientes de backup não realizam nenhum tipo de backup ou restauração de dados.	10 (dez) horas
2 - Alto	Degradação do ambiente de backup ou restauração. Alguma função da solução está indisponível, intermitente ou com desempenho prejudicado frente ao usual.	02 (dois) diasúteis

3 - Médio	Degradação do ambiente de backup ou restauração, embora sem afetar a execução de rotinas. A solução apresenta algum erro de funcionamento ou divergência com as especificações requeridas.	05 (cinco) diasúteis
4 - Baixo	Projetos de melhoria, manutenção corretiva ou preventiva, com baixo impacto nas rotinas do CONTRATANTE.	10 (dez) diasúteis

2.10. O prazo, estabelecido pela tabela anterior, será contado a partir da abertura de chamado técnico;

2.11. Antes de findar o prazo fixado no subitem 2.9, a CONTRATADA poderá formalizar pedido de prorrogação cujas razões expostas serão examinadas pelo CONTRATANTE, o qual decidirá pela dilação do prazo ou aplicação das penalidades previstas no contrato;

2.12. Decorridos os prazos estipulados, sem o devido atendimento, fica o CONTRATANTE autorizado a contratar serviços emergenciais de suporte técnico e repassar os custos para a CONTRATADA, sem prejuízo à aplicação das penalidades previstas neste contrato;

2.13. Quando solicitado, a CONTRATADA deverá emitir relatório acerca do acionamento, contendo o número do chamado, a identificação do software afetado, a data e hora da abertura do chamado, a data e hora do término da reparação, o diagnóstico do problema, a solução adotada e demais informações pertinentes;

2.14. Os acionamentos efetuados até o último dia da vigência do contrato deverão ser solucionados, sem ônus adicional para a CONTRATANTE, ainda que expirado o prazo de vigência contratual;

2.15. Durante o prazo de garantia, sem quaisquer ônus adicionais para a CONTRATANTE, a própria CONTRATADA, às suas expensas, por intermédio de sua matriz, filiais, escritórios ou representantes técnicos autorizados, estará obrigada a atender às solicitações do CONTRATANTE de acordo com os prazos estabelecidos em garantia.

3. Treinamento

3.1. TreinamentoTelepresencial – Básico

3.1.1. O treinamentodeverá:

3.1.1.1. Seroficial;

3.1.1.2. Ministrado em idioma português - Brasil;

3.1.1.3. Ser apresentado na forma telepresencial (ao vivo) e

3.1.1.4. Permitir a interação dos alunos com instrutor em tempo real.

3.1.2. O treinamento deve ser realizado no período de segunda a sexta-feira (dias úteis), entre 8h (oito horas) e 18h (dezoito horas), com carga horária diária máxima de 4 (quatro) horas;

3.1.3. O treinamento deve ter carga horária mínima de **40 (quarenta) horas;**

3.1.4. O treinamento será demandado conforme a necessidade da área técnica durante a vigência do contrato;

3.1.5. A CONTRATADA deverá fornecer o material didático em mídia digital, previamente à data de início do treinamento**oficial do fabricante e desenvolvido somente para os fins de treinamento;**

3.1.6. O treinamento deverá envolver conteúdo teórico e prático, deverá abordar todas as funcionalidades da solução na sua versão mais atual, em especial:

3.1.6.1. Apresentação da arquitetura da solução e dos conceitos fundamentais;

3.1.6.2. Instalação da solução;

3.1.6.3. Configuração e gerenciamento da solução;

3.1.6.4. Operaçãocompleta da solução;

3.1.6.5. Análise de logs e problemas;

3.1.6.6. Geração e customização de relatórios, caso aplicável;

3.1.6.7. Verificação de alertas e tomada de ações.

3.1.7. O instrutor do treinamento deverá ser certificado pelo fabricante da solução contratada;

3.1.8. A CONTRATADA deverá fornecer, aos participantes do treinamento, os certificados de conclusão de curso, os quais devem conter, no mínimo:

3.1.8.1. Nome da instituição de ensino;

3.1.8.2. Nome do curso;

3.1.8.3. Nome do servidorcapacitado;

3.1.8.4. Data de início e término da capacitação;

3.1.8.5. Cargahorária;

3.1.8.6. Conteúdo programático; 3.1.8.7. Aproveitamento, se for o caso.

3.1.9. Os certificados deverão ser entregues no prazo de 05 (cinco) dias úteis contados após o término do treinamento;

3.1.10. Ao final do treinamento, os servidores participantes efetuarão uma avaliação do conteúdo ministrado. A qualidade será medida de 1 (um) a 10 (dez) pontos em cada um dos seguintes critérios:

3.1.10.1. Pontualidade;

3.1.10.2. Didática do instrutor;

3.1.10.3. Eficiência no repasse do conteúdo;

3.1.10.4. Adequação do treinamento ao conteúdo exigido no item 3.1.6;

3.1.10.5. Adequação da cargahorária.

3.1.11. Caso a média das avaliações seja inferior a 7 (sete) pontos, a CONTRATADA deverá refazer o treinamento, após as adequações necessárias, especialmente de substituição do Instrutor, e sem qualquer custo adicional para a JF1:

3.1.11.1. Neste caso, o novo treinamento também será submetido aos mesmos critérios de avaliação.

3.2. TreinamentoTelepresencial – Avançado

3.2.1. O treinamentodeverá:

3.2.1.1. Seroficial;

3.2.1.2. Ministrado em idioma português - Brasil;

3.2.1.3. Ser apresentado na forma telepresencial (ao vivo) e

3.2.1.4. Permitir a interação dos alunos com instrutor em tempo real.

3.2.2. O treinamento deve ser realizado no período de segunda a sexta-feira (dias úteis), entre 8h (oito horas) e 18h (dezoito horas), com carga horária diária máxima de 4 (quatro) horas;

3.2.3. O treinamento deve ter carga horária mínima de **40 (quarenta) horas;**

3.2.4. O treinamento será demandado conforme a necessidade da área técnica durante a vigência do contrato;

3.2.5. A CONTRATADA deverá fornecer o material didático em mídia digital, previamente à data de início do treinamento, **oficial do fabricante e desenvolvido somente para os fins de treinamento;**

3.2.6. O treinamento deverá envolver conteúdo teórico e prático, deverá abordar todas as funcionalidades avançadas da solução, na sua versão mais atual, como por exemplo:

3.2.6.1. Deduplicação de dados;

3.2.6.2. Gerenciamento de mídias;

3.2.6.3. Segurança;

3.2.6.4. Otimizações ou desempenho (performance); 3.2.6.5. Backup de aplicações específicas (Oracle, Exchange etc);

3.2.6.6. Troubleshooting.

3.2.7. O instrutor do treinamento deverá ser certificado pelo fabricante da solução contratada;

3.2.8. A CONTRATADA deverá fornecer, aos participantes do treinamento, os certificados de conclusão de curso, os quais devem conter, no mínimo:

3.2.8.1. Nome da instituição de ensino;

3.2.8.2. Nome do curso;

3.2.8.3. Nome do servidorcapacitado;

3.2.8.4. Data de início e término da capacitação;

3.2.8.5. Cargahorária;

3.2.8.6. Conteúdo programático; 3.2.8.7. Aproveitamento, se for o caso.

3.2.9. Os certificados deverão ser entregues no prazo de 05 (cinco) dias úteis contados após o término do treinamento;

3.2.10. Ao final do treinamento, os servidores participantes efetuarão uma avaliação do conteúdo ministrado. A qualidade será medida de 1 (um) a 10 (dez) pontos em cada um dos seguintes critérios:

3.2.10.1. Pontualidade;

3.2.10.2. Didática do instrutor;

3.2.10.3. Eficiência no repasse do conteúdo;

3.2.10.4. Adequação do treinamento ao conteúdo exigido no item 3.2.6;

3.2.10.5. Adequação da cargahorária.

3.2.11. Caso a média das avaliações seja inferior a 07 (sete) pontos, a CONTRATADA deverá refazer o treinamento, após as adequações necessárias, especialmente de substituição do Instrutor, e sem qualquer custo adicional para a JF1:

3.2.11.1. Neste caso, o novo treinamento também será submetido aos mesmos critérios de avaliação.

4. Serviço de instalação e configuração, migração, adequação e transferência de conhecimento
    4.1. Serviço de Instalação e Configuração:
        4.1.1. Trata-se dos serviços de instalação e configuração da solução ofertada para cada localidade da JF1;
        4.1.2. A CONTRATADA deverá submeter para aprovação por parte da CONTRATANTE, no prazo máximo de 10 (dez) dias úteis, a partir da data de emissão da ordem de serviço, Plano de Instalação e Configuração da solução ofertada nos ambientes operacionais da Contratante;
        4.1.3. O Plano de Instalação e Configuração deverá conter, no mínimo:
            4.1.3.1. Descrição da equipe do projeto de instalação, contendo nomes, contatos e papéis desenvolvidos por cada um;
            4.1.3.2. Plano de comunicação;
            4.1.3.3. Descrição das fases da instalação e configuração, atividades desenvolvidas em cada uma, metas, entregáveis e cronograma (por localidade);
            4.1.3.4. Detalhamento dos ativos necessários em cada etapa do processo;
            4.1.3.5. Análises de risco e possíveis impactos das atividades para a infraestrutura dos CPDs da JF1;
            4.1.3.6. Detalhamento da topologia e configurações propostas. Devese englobar as especificidades de clientes e políticas atualmente implantadas na JF1;
            4.1.3.7. Deverá abranger as três camadas da arquitetura de backup da solução conforme descrito no item 1.2.1: Gerência e controle, Operação de mídia e Clientes;
            4.1.3.8. Transferência de conhecimento para as equipes locais;
        4.1.4. Deverão ser observados como insumos para Elaboração do Plano de Instalação e Configuração as informações contidas sobre o ambiente tecnológico no item “Ambiente Tecnológico da JF1” e na planilha “AmbienteTecnológico JF1”;
        4.1.5. Os serviços de instalação e configuração da solução poderão ocorrer de forma local ou remota, a critério da CONTRATADA, sendo que no segundo caso a conexão deverá ocorrer a partir das instalações do TRF1, em Brasília - DF;
        4.1.6. Deve-se proceder com a instalação da solução ofertada nos ambientes operacionais da CONTRATANTE, bem como seguir as melhores práticas do fabricante e obedecer aos padrões de configurações definidos pela CONTRATANTE;
        4.1.7. A CONTRATANTE disponibilizará a infraestrutura final onde ficará hospedada a solução contratada, incluindo sistema operacional, armazenamento, servidor, fitoteca, fitas e rede;
            4.1.7.1. O disposto neste item não sobrepõe o disposto no subitem 1.1.3, assim é permitida a complementação da infraestrutura, seja a nível de software ou hardware;
        4.1.8. A aceitação do serviço de instalação e configuração da solução se dará por localidade instalada e após verificação dos aspectos abaixo:
            4.1.8.1. Acessoaoambienteinstalado;

4.1.8.2. Conformidade de licenciamento;
4.1.8.3. Conexãoestabelecida com clientes;
4.1.8.4. Conformidade de configurações de rede;
4.1.8.5. Políticas de backup criadas e em produção, em conformidade ao ambiente atual;
4.1.8.6. Conexão com fitoteca da CONTRATANTE (por localidade);
4.1.8.7. Execução com sucesso, na solução contratada, de rotinas de backup durante uma semana, excetuando os erros comprovados relativos à infraestrutura da JF1;
4.1.8.8. A partir da solução ofertada, a execução, com sucesso, de rotina de restauração de, ao menos, 03 (três) tipos de rotinas de backup, conforme escolha do CONTRATANTE.

4.2.

Serviço de Migração:

4.2.1. Trata-se do serviço de migração das cópias de segurança do ambiente atualmente em produção na JF1;
4.2.2. O serviço consiste na migração para a solução ofertada das imagens de backup (dados em fitas LTO) de cada uma das localidades da JF1, conforme detalhado na planilha "Ambiente Tecnológico JF1", com temporalidade de retenção superior a 6 (seis) meses, a partir da data de emissão da Ordem de Execução dos Serviços;
4.2.3. A quantidade de fitas existente nos ambientes operacionais do CONTRATANTE, por temporalidade, encontra-se descrita na planilha "Ambiente Tecnológico JF1";
4.2.3.1. O levantamento das mídias a serem migradas é estimativo e o levantamento real será o efetuado durante a execução contratual;
4.2.4. A CONTRATADA deverá submeter para aprovação por parte da Contratante, no prazo máximo de 10 (dez) dias úteis, a partir da data de emissão da ordem de serviço, Plano de Migração da solução ofertada nos ambientes operacionais da CONTRATANTE;
4.2.5. O Plano de Migração deverá conter, no mínimo:
4.2.5.1. Descrição da equipe do projeto de migração, contendo nomes, contatos e papéis desenvolvidos por cada um;
4.2.5.2. Plano de comunicação;
4.2.5.3. Descrição da solução tecnológica a ser utilizada paramigração, que deverá ser, integralmente, provida pela CONTRATADA;
4.2.5.4. Considerações e detalhamentos a respeito da migração de dados de filesystems tradicionais e de rotinas de aplicações específicas, como por exemplo: Oracle, VMware, Microsoft Exchange, Microsoft Active Directory etc.;
4.2.5.5. Descrição das fases da migração, atividades desenvolvidas em cada uma, metas, entregáveis e cronograma por localidade;
4.2.5.6. Detalhamento de ativos, passivos, insumos, serviços e contratos, caso aplicável, que serão utilizados durante o processo;
4.2.5.7. Análises de risco e possíveis impactos das atividades para a infraestrutura dos CPDs da JF1;

4.2.5.8. Relação de todas as mídias e dados (“imagens de backup”) que serão migrados para cada ambiente;

4.2.5.9. Cenário de testes entre ambiente atual e ambiente migrado para a nova solução de backup.

4.2.6. A aferição da efetividade dos serviços de migração ocorrerá por meio da checagem e “batimento” de informações do ambiente antigo (solução atualmente implantada no TRF1) com os dados importados (migrados) para a solução ofertada:

4.2.6.1. A aferição será de forma aleatória, conforme escolha do CONTRATANTE;

4.2.6.2. Deverá ser fornecida listagem de fitas envolvidas na migração;

4.2.6.3. Deverá ser fornecida a listagem de imagens e dados restaurados da solução em produção em cada localidade da JF1;

4.2.6.4. Deverá ser demonstrado e comprovado que a listagem disponibilizada no subitem 4.2.6.2 está, integralmente, importada para a solução ofertada pela CONTRATADA;

4.2.6.5. Deverão ser efetuados testes de restauração de arquivos, escolhidos aleatoriamente, conforme alinhamentos e definições do CONTRATADO/CONTRATANTE, a considerar o Plano de Migração definido nos itens 4.2.4 e 4.2.5.

4.2.7. Os dados levantados para serem migrados, no início do processo de migração, deverão constar no catálogo da nova solução com requisito de aceitação do serviço de migração:

4.2.7.1. Deve-se respeitar as configurações de retenções dos dados, conforme aplicado no ambiente em produção atualmente;

4.2.7.2. A migração deverá ser realizada sem perda de dados e devesemanter a mesma política de retenção, salvo se, expressamente, autorizado pela equipe técnica do CONTRATANTE;

4.2.7.3. Deve ser disponibilizada documentação que viabilize a rastreabilidade entre os dados de origem (pré-migração) e de destino (pós-migração):

4.2.7.3.1. Rastreabilidade mínima deve envolver o dado correspondente, o número de fita LTO, a data de realização backup (pré e pós-migração) e a retenção (pré e pósmigração);

4.2.8. A CONTRATADA deverá fornecer ao final da migração de cada localidade, um documento resumo com todas as ações realizadas durante a migração, bem como estatísticas relativas à migração: código das fitas envolvidas, relação de imagens, listagem de dados, total de fitas, volumetria total, tempo dispendido e vazão de dados durante o processo de restauração na solução antiga e de backup na nova solução:

4.2.8.1. Adicionalmente ao documento resumo mencionado no item 4.2.8, deve ser apresentado relatório, quinzenal, do estado e progresso de migração (também por localidade da JF1).

4.2.9. Cabe à CONTRATADA o provimento de toda infraestrutura necessáriapara realização dos serviços de migração, sejam eles servidores, fitotecas, switches, cabeamentos, fitas de backup (em casos específicos),

drives de leitura de fita, sistemas operacionais, máquinas virtuais, qualquer outro equipamento ou recurso necessário:

4.2.9.1. Os recursos envolvidos e providos para esse processo de migração, conforme consta na descrição do item 4.2.9, tem caráter temporário e não são objetos de fornecimento definitivo ao CONTRATANTE;

4.2.9.2. As fitas de backup em produção na JF1 englobam os padrões LTO 3, 4, 5 e 7 (formato tipo M) e poderão, a critério do CONTRATANTE, ser migradas para fitas de padrões superiores fornecidas pelo CONTRATANTE;

4.2.9.3. Os serviços de migração não poderão acarretar impactos nos ambientes tecnológicos em produção na JF1.

4.2.10. A infraestrutura acima descrita poderá ser instalada nas instalações do CONTRATANTE em cada uma das localidades;

4.2.11. A CONTRATADA não poderá retirar ativos ou passivos de TI da JF1, das dependências da CONTRATANTE, para execução do processo de instalação ou migração;

4.2.12. A CONTRATADA poderá utilizar infraestrutura em nuvem IaaS (Infraestructure as a Service) para o processo de migração, desde que os dados sejam integralmente acessíveis à CONTRATANTE, bem como respeitados os critérios de sigilo/confidencialidade;

4.2.13. Todos os possíveis custos de operação e armazenamento da infraestrutura em nuvem serão de total responsabilidade da CONTRATADA;

4.2.14. A CONTRATADA deve dispor de profissional capacitado e certificado em ambas soluções de backup, o qual deve estar habilitado, tecnicamente, a gerenciar e operar tanto a solução de backup em produção na JF1, bem como a solução de backup ofertada;

4.2.14.1. O profissional, citado neste item, deve atuar nos casos necessários durante o processo de migração entre soluções de

4.2.14.2. backup;

O mesmo profissional ou outro membro da CONTRATADA deverá estar habilitado e possuir conhecimentos técnicos suficientes para manipulação e configuração das fitotecas implantadas no âmbito da JF1;

4.2.15. Caso se aplique, a CONTRATADA deverá observar a melhor estratégia de transmissão de dados para nuvem, de forma a não onerar os links de internet das localidades envolvidas:

4.2.15.1. A CONTRATADA deverá adotar alternativas para diminuir o impacto no processo de migração em questão, como exemplos: a contratação de links dedicados, a carga de dados em dispositivos físicos especializados do provedor de nuvem etc.;

4.2.15.2. A CONTRATANTE poderá impor limitação de horário e banda de redes de comunicações caso os serviços de migração venham a

impactar nas atividades negociais da JF1;

4.2.15.3. Deverá ser utilizado criptografia de dados para fins de transferência dos dados - onpremise para nuvem e vice versa;

4.2.15.4. No caso de utilização de infraestrutura de comunicação do CONTRATANTE para upload de dados para nuvem, deverá ser observado o horário fora de produção, o qual se define: Entre 19h às 08h, nos dias úteis e integralmente, nos finais de semana;

4.2.15.4.1. Neste caso, a utilização de banda não poderá exceder em 80% (oitenta por cento) de utilização do canal de comunicação.

4.2.16. Após finalizado o processo de migração, a CONTRATADA deverá excluir quaisquer dados da CONTRATANTE armazenados provisoriamente, em qualquer infraestrutura paralela utilizada durante esse processo.

4.3. Serviço de Adequação:

4.3.1. Trata-se do serviço de adequação do ambiente atual em produção na JF1;

4.3.2. Caso a solução ofertada seja do mesmo fabricante da solução atualmente em produção, preterindo dos serviços de instalação e migração, os serviços estarão restritos à verificação pormenorizada do ambiente operacional atual, atualização de versão e proposição de ajustes visando adequação às melhores práticas do fabricante (destaque à implantação de recursos voltados à melhoria do desempenho e redução do tempo de realização das cópias de segurança);

4.3.2.1. Nessa hipótese a empresa terá o prazo de 20 (vinte) dias úteis, a contar da emissão da Ordem de Execução dos Serviços, para proceder os levantamentos necessários nos ambientes operacionais da CONTRATANTE;

4.3.3. Ao final desse período, deverá ser apresentado Plano de Adequação, que deverá conter, no mínimo:

4.3.3.1. Descrição da equipe do projeto, contendo nomes, contatos e papéis desenvolvidos por cada um;

4.3.3.2. Plano de comunicação;

4.3.3.3. Detalhamento das análisesrealizadas;

4.3.3.4. Detalhamento das propostas de atualização/adequação do ambiente, a destacar, em cada caso, os benefícios esperados;

4.3.3.5. Estratégia de Testes;

4.3.3.6. Cronograma de implantação;

4.3.3.7. Análises de riscos e possíveis impactos das atividades para a infraestrutura dos CPDs da JF1;

4.3.3.8. Transferência de conhecimento para as equipes locais.

4.3.4. A CONTRATADA deve dispor de profissional capacitado e certificado na solução de backup, o qual deve estar habilitado, tecnicamente, a gerenciar e operar a solução de backup em produção na JF1;

4.3.5. Os critérios para a transferência de conhecimento deverão seguir o disposto no item 4.4 e subitens.

4.4. Serviço de Transferência de Conhecimento:

4.4.1. A transferência de conhecimento às equipes locais de cada localidade, deverá ser feita por meio de reunião telepresencial e deverá contemplar:

4.4.1.1. Todas as instalações e configurações ou adequações realizadas;

4.4.1.2. Resolução de dúvidas das equipes locais com relação ao serviço, topologia, solução e decisões de adequação às melhores práticas realizadas pela CONTRATADA;

4.4.1.3. Operação básica de execução de rotinas de backup e restauração;

4.4.1.4. Configurações de políticas de backup e comunicação com clientes;

4.4.1.5. Padrões de configurações lógicas e organização de catálogo de fitas;

4.4.2. A transferência de conhecimento deverá ter duração mínima de 4 (quatro) horas, por localidade;

4.4.3. A CONTRATADA deverá entregar, ao final da instalação e configuração, de cada localidade, um documento de “as built”, o qual contém resumo de todas as instalações, configurações e topologia implementada ou adequada;

4.4.4. A transferência de conhecimento deverá estar em conformidade aos serviços de instalação e configuração ou adequação realizados em cada localidade.

4.5. ConsideraçõesGerais:

4.5.1. O prazo para finalização da instalação, configuração e migração ou adequação será de 6 (seis) meses, contados a partir da data de aceitação dos respectivos Planos por parte da CONTRATANTE;

4.5.2. A CONTRATADA deverá prestar atualizações mensais do estado da instalação, configuração, adequação e, principalmente, migração. As atualizações devem evidenciar o percentual concluído, entregáveis, problemas e quaisquer outras questões que possam estar afetando o andamento do serviço;

4.5.3. A CONTRATADA poderá solicitar extensão do prazo de migração, desde que seja, formalmente, justificada e requerida em, no mínimo, 20 (vinte) dias úteis antes de findado o respectivo prazo:

4.5.3.1. Tal solicitação estará sujeita à avaliação e aprovação da CONTRATANTE;

4.5.3.2. A extensão de prazo só será concedida por uma única vez, com prazo máximo de 60 (sessenta) dias úteis, a partir do término do prazo original.

4.5.4. A CONTRATADA assumirá total responsabilidade por qualquer dano físico ou lógico que, por ventura, possa ocorrer durante a execução da migração e que fique comprovada a imperícia ou dolo. Dessa forma, estarásujeitaàspenalidadescabíveis;

4.5.5. Deve ser apresentado, mensalmente, por localidade, até o quinto dia útil, relatório comprobatório quanto aos andamentos das execuções dos serviços de instalação e configuração, migração ou adequação.

4.5.5.1. Quanto à transferência de conhecimento, deve ser emitido relatório quando da finalização da conclusão da prestação deste serviço em igual prazo referido no item 4.6.

4.5.6. A conclusão de todos serviços deve obedecer aos requisitos mínimos, por mês, conforme segue:

4.5.6.1. Primeiro e Segundo mês: Finalizar duas localidades, por mês, e iniciar TRF1;

4.5.6.2. Do terceiro ao sexto mês: finalizar três localidades, por mês, e finalizar o TRF1.

4.6. Do Pagamento dos serviços:

4.6.1. Os serviços serão remunerados, mensalmente, após aceite definitivo dos serviços de instalação e configuração, migração, adequação e transferência de conhecimento em cada uma das localidades, conforme cenário e na proporção constante das tabelas a seguir:

Cenário 01 - Instalação e migração				
Serviço	Localidade	Porcentagem de Pagamento (por localidade)	Porcentagem de Pagamento (por serviço)	Porcentagem de Pagamento (Total)
Instalação e configuração	Seções	1,5	30	100
	TRF1	9		
Migração	Seções	2,5	45	
	TRF1	10		
Transferência de conhecimento	Seções	1,5	25	
	TRF1	4		

Cenário 02 - Adequação				
Serviço	Localidade	Porcentagem de Pagamento (por localidade)	Porcentagem de Pagamento (por serviço)	Porcentagem de Pagamento (Total)
Adequação	Seções	4	65	100
	TRF1	9		
Transferência de conhecimento	Seções	2	35	
	TRF1	7		

4.6.2. O cenário 01 corresponde à hipótese da CONTRATADA fornecer solução distinta à já implantada na JF1;

4.6.3. O cenário 02 corresponde à hipótese da CONTRATADA fornecer solução já implantada na JF1, no entanto com necessidades de adequações e/ou atualizações;

4.6.4. As localidades englobam: 14 (quatorze) Seções Judiciárias e TRF1;

4.6.5. O percentual de pagamento por cada uma dessas localidades será cabível quando da conclusão efetiva de cada tipo de serviço. Sendo:

4.6.5.1. CENÁRIO01 - Instalação e configuração: 1,5% (um e meio porcento) para cada seção judiciária e 9% (nove porcento) para o TRF1;

4.6.5.2. CENÁRIO01 - Migração: 2,5% (dois e meio porcento) para cada seção judiciária e 10% (dez porcento) para TRF1;

4.6.5.3. CENÁRIO01 - Transferência de conhecimento: 1,5% (um e meio porcento) para cada seção judiciária e 4% (quatro porcento) para o TRF1;

4.6.5.4. CENÁRIO02 - Adequação: 4% (quatro porcento) para cada seção judiciária e 9% (nove porcento) para o TRF1;

4.6.5.5. CENÁRIO02 - Transferência de conhecimento: 2% (dois porcento) para cada seção judiciária e 7% (sete porcento) para o TRF1.

5. OperaçãoAssistida
    5.1. A Operação assistida consiste no serviço de apoio técnico e operacional na solução ofertada, pelo período de 20 (vinte) dias úteis:
        5.1.1. Seráprestadoininterruptamente;
        5.1.2. Deverá ser iniciado 05 (cinco) dias úteis, após a emissão da Ordem de Serviço;
        5.1.3. Deverá ocorrer após implantação da solução e conclusão efetiva do Treinamento telepresencial - básico;
    5.2. Será prestada por profissional técnico envolvido na implantação da solução de backup ofertada para a JF1;
        5.2.1. Deverá produzir documentação específica e pontual às necessidadese ao ambiente implantado na JF1, conforme cada caso demandado pelo CONTRATANTE;
        5.2.2. As documentações demandadas e específicas do ambiente da JF1 deverão ser entregues no prazo de até 10 (dez) dias úteis, após finalizada a prestação do serviço de Operação Assistida;
        5.2.3. O formato (textual, vídeo, imagens) da documentação é de livre escolha da CONTRATADA, desde que atendidas as necessidades da CONTRATANTE;
        5.2.4. A documentação disponibilizada pela CONTRATADA será avaliada pelo CONTRATANTE e poderá ser recusada em caso de erro ou insuficiência em relação ao demandado.
            5.2.4.1. No caso de recusa do documento pelo CONTRATANTE, a documentação deverá ser reformulada pela CONTRATADA e reencaminhada, no prazo de 05 (cinco) dias úteis.
    5.3. A Operação Assistida deve auxiliar e pontuar a equipe técnica da JF1 no que diz respeito a qualquer gerenciamento, configuração ou operação da solução fornecida.