Contribuições a consulta Pública de Backup JF1

1- Homologação da Solução

Considerando a gravidade, complexidade e importância da solução a ser adquirida. Sugerimos a apreciação do time na possibilidade da faculdade de realizar um processo de avaliação/homologação da solução proposta pelo arrematante. Neste caso, fica a JF-1 resguardada de uma avaliação criteriosa e consequente validação de solução proposta afim de garantir maior confiabilidade e mitigar possíveis falhas e consequentemente dano de custos, tempo e financeiro ao erário no processo de implantação.

Analisando os pontos críticos do processo, segue abaixo sugestão para refletir tal exigência:

Homologação/Amostra da Solução

O TRF-1 poderá, caso julgue necessário, realizar a homologação técnica da solução, seguindo os seguintes os itens da tabela abaixo:

Itens a serem comprovados com homologação	**Forma de Homologação**	
	Bancada	Documentação
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:		X
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. Executa deduplicação de dados e também é responsável pela execução da restauração de dados;		X
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.		X
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);		X
1.2.3. O armazenamento em fitas deverá suportar tecnologia de fitas LTO:		X
1.2.3.1. Deve possuir compatibilidade a partir do padrão LTO3 (para fins de migração de ambiente legado);		X
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;		X

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;		X
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;	X	
1.2.7. A solução deve permitir a integração com Microsoft Active Directory 2012 e superiores, permitindo a autenticação de usuário do domínio;	X	
1.2.8. A solução ofertada deverá estar na versão de software mais recente do fabricante.		X
1.3.1. A solução deverá suportar o backup e restauração de dados de, no mínimo:	X	
1.3.1.1. VMware:	X	
1.3.1.1.1. Máquinas virtuais inteiras ou de forma granular;	X	
1.3.1.1.2. Discos de máquinas virtuais provisionados com modo de compatibilidade RDM virtual;	X	
1.3.1.2. Microsoft:	X	
1.3.1.2.1. Dados de servidores de arquivos;	X	
1.3.1.2.2. Sistemas de arquivos que estejam utilizando a tecnologia DFS;	X	
1.3.1.2.3. Objetos do Active Directory de forma granular;	X	
1.3.1.2.4. Deve suportar cópia de dados de Exchange e DAG (DataBaseAvailabilityGroups) - inclusive granularmente;	X	
1.3.1.3. Dados de Bancos de dados Oracle:	X	
1.3.1.3.1. Versão 12.1.0.2 - por meio de integração com RMAN;	X	
1.3.1.4. Storages:	X	
1.3.1.4.1. Compartilhamentos CIFS e NFS;	X	

1.3.1.4.2. Volumes internos por meio do protocolo NDMP;	X	
1.3.1.5. Dados de sistemas de arquivos diversos, no mínimo: NTFS, EXT3, EXT4 e XFS, de forma granular;	X	
1.3.1.6. Caixas de e-mail e objetos do Microsoft Exchange, de forma granular;	X	
1.3.2. A solução deverá permitir a restauração de dados em local diverso ao local de origem do backup efetuado;	X	
1.3.3. Deverá realizar criptografia de dados, com as seguintes características mínimas:	X	
1.3.3.1. Criptografia de dados de cópias de backup em mídias externas (fitas LTO) ou discos de armazenamento de cópias seguras;	X	
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.	X	
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 solução.	X	
1.3.4.1. As tarefas de backup e restauração devem ser realizadas por meio desta interface gráfica, sem a obrigatoriedade de utilização de scripts;	X	
1.3.5. Deve possuir mecanismo de auto salvamento e reconstrução do catálogo (base de dados) centralizado, em caso de perda do mesmo:	X	
1.3.5.1. A reconstrução do catálogo, poderá ser realizada a partir dos repositórios de fita e/ou disco;	X	
1.3.6. A solução deverá implementar funcionalidade configurável de deduplicação na origem (cliente) ou no destino (servidor/mídia);	X	
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;	X	
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;	X	
1.3.9. A solução deverá implementar agendador 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;	X	

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);	X	
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);	X	
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;	X	
1.3.13. Deve viabilizar backups e restaurações via rede de dados (LAN);	X	
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;	X	
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;	X	
1.3.16. Deve permitir a criação de listas de exclusão configuráveis - por cliente - dos apontamentos de backup a serem salvos;	X	
1.3.17. Deve permitir a criação de tarefas que serão executadas antes e/ou depois da execução dos jobs de backup/restauração;	X	
1.3.18. Deverá suportar a execução de, no mínimo, os seguintes tipos de backup: completo (full), incremental e diferencial ou cumulativo;	X	
1.3.19. Deverá suportar a configuração de, no mínimo, os seguintes tipos de frequência de execução de backup: Diária, semanal, mensal e anual;	X	
1.3.20. Deverá suportar a configuração de retenções de, pelo menos, até 5 (cinco) anos;		X
1.3.21. Deverá armazenar dados históricos de gerenciamento e de execução de cópias seguras (jobs de backup) por, no mínimo, 12 (doze) meses;		X

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;	X	
1.3.22.1. Deve possibilitar a configuração e determinação de retenções para cada local de armazenamento;	X	
1.3.22.2. Deve possuir funcionalidade de criar múltiplas cópias de backups;	X	
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;	X	
1.3.23. A solução deverá implementar deduplicação 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;	X	
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;	X	
1.3.24. A solução deve ser capaz de gerenciar as fitas magnéticas contidas na fitoteca ou fitas armazenadas off-site:	X	
1.3.24.1. Deve possibilitar a migração de dados entre fitas magnéticas;	X	
1.3.24.2. Deve possibilitar a verificação da integridade do conteúdo das fitas.	X	
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;	X	
1.4.2. O gerenciamento centralizado deverá prover integração com o Microsoft Active Directory para fins de autenticação de usuários;	X	
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;	X	
1.4.4. Deverá implementar permissionamento baseado em perfil de grupo de usuários:	X	

1.4.4.1. Possuir capacidade de estabelecer níveis de acesso diferenciados e configuráveis para atividades de administração e operação da solução;	X	
1.4.5. Deve permitir a emissão de relatórios agendados e envio dos mesmos via protocolo SMTP, para caixas de e-mail;	X	
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;	X	
1.4.7. Deve permitir exportação de relatórios, no mínimo, nos formatos .CSV e .PDF;	X	
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;	X	
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.	X	
1.5. Compatibilidades tecnológicas		
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”;		X
1.5.2. Deverá ser compatível com ambiente de virtualização VMware vCenter 6.7;		X
1.5.3. Deve ser compatível com sistemas operacionais Windows Server 2016 e superiores;		X
1.5.4. Deve ser compatível com sistemas operacionais Linux CentOS, Red Hat 7.0 e superiores;		X
1.5.5. Deve ser compatível com sistemas operacionais Oracle Linux 7 e superiores;		X
1.5.6. Deve ser compatível com servidores físicos DELL PowerEdge R720, R730, R820, R630 e R640;		X
1.5.7. Deve ser compatível com servidores Huawei CH 242 DDR4;		X

1.5.8. Deve ser compatível com servidores físicos HPE Proliant DL360 Gen 10;		X
1.5.9. Deve ser compatível com storagesHuaweiOceanStor 5600 v3 e 5300 v5;		X
1.5.10. Deve ser compatível com storages EMC VNX 5600 e 5800;		X
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;		X
1.5.12. Deve ser compatível com as seguintes fitotecas:		X
1.5.12.1. IBM TS4300 e TS4500;		X
1.5.12.2. Quantum scalar i40 e i80;		X
1.5.12.3. TandbergExabyte Magnum 224 e T40;		X
1.5.12.4. QualStar XLS;		X
1.5.12.5. DELL PowerVault TL2000.		X
4.2 Serviços de Migração (deverá ser homologado a solução proposta e o sucesso em amostra de dado no ambinete para ser migrado respeitando todos os subitens do item 4.2)		X

A CONTRATADA deverá apresentar todo oPlano de Migração da solução ofertada nos ambientes operacionais da CONTRATANTEque deverá ser seguido para homologação da parte dos serviços de migração;

A homologação será realizada na SEDE do TRF1 em Brasília;

A homologação será analisada pelo TRF1 com o objetivo de aferir o atendimento às Especificações Básicas apresentadas;

O TRF1 poderá rejeitar a homologação, independentemente da informação contida na proposta, caso verifique nos testes de homologação que o serviço não seja capaz de cumprir às especificações exigidas;

A entrega e instalação das licenças e infraestrutura (para serviços de migração) necessárias à homologação deverá ocorrer em até 30 (trinta) dias contados a partir da solicitação formal do TRF1;

Após a devida instalação e adequação do ambiente lógico e físico, a LICITANTE terá até 15 (quinze) dias úteis para comprovar o funcionamento e atendimento à especificação técnica;

No caso de não atendimento de algum item deste edital, a LICITANTE terá um único prazo de até 2 (dois) dias úteis para regularizar e comprovar o funcionamento;

A homologação do serviço ofertado deverá ser realizada sem custo para o TRF1;

A LICITANTE que for reprovada na homologação não terá direito a qualquer indenização;

Será emitido um relatório descrevendo os exames realizados e contendo a aprovação ou não da homologação.

O acompanhamento da homologação, por parte dos INTERESSADOS, poderá ser realizado mediante, por e-mail, junto ao RESPONSÁVEL, que divulgará aos interessados a informação de horário, local do procedimento e as condições do acompanhamento da análise

Homologação da migração:

Deverá ser migrada as imagens de backup (dados em fitas LTO) dos ambientes a seguir para a solução ofertada como requisito de aceitação:

• Controlador de domínio	Windows Server 2012 R2
• Servidor de Arquivos	Windows Server 2008 R2
• Banco de dados Oracle 12.1.0.2	RedHat 6.6
• Banco de dados Oracle 12.1.0.2	Oracle Linux 6.7
• virtualização VMware	ESXi 6.0
• virtualização VMware	ESXi 6.7
• Banco de dados PostgreeSQL	RedHat 7.4

Deverá após a migração das imagens de backup (dados em fitas LTO) dos ambientes acima, executar a restauração do backup para homologar se os backups estão íntegros.

Deverá respeitar as configurações de retenções dos dados, conforme aplicado no ambiente em produção atualmente;

Deverá ser realizada sem perda de dados e deve-se manter a política de retenção, salvo se, expressamente, autorizado pela equipe técnica do CONTRATANTE;

2- Qualificação Técnica

Sobre a Minuta de qualificação técnica destacamos o fato de o texto exigido ser muito específico o que acaba limitando uma maior participação de empresas, mesmo que aptas, restringindo uma competitividade maior no certame.

Sabemos da necessidade de buscar uma compatibilidade entre capacidade dos licitantes e o escopo envolvido no projeto. Com essa premissa gostaríamos de propor um pleito mais compatível, trazendo maior competitividade e mantendo a segurança da competência e capacidade da empresa na execução do objeto.

Primeiramente, destacamos que o edital permite diferentes tipos de licenciamentos para atender a solução. Ressaltamos também que a capacidade de entregar uma solução de backup pode ser constatada em projetos diversos onde algumas características são suficientes para comprovar a capacidade de execução.

Um exemplo desse fato seria projetos de backup de entrega de appliances. A complexidade desses projetos é por vezes maior que aqueles que contemplam servidores comuns. Outros casos podem ser citados como projetos com licenciamento de frontEnd e/ou instancia de VMs. Na maioria dos casos, a tratativa dos dados a serem protegidos são agnósticos ao seu tipo. Por último, salientamos saudável a possibilidade do somatório de atestados, visto que uma empresa consegue aumentar sua expertise com base no volume e granularidade de clientes atendidos.

Logo, com base nessas premissas e no intuito de maior aderência a qualificação técnica e o escopo do edital, sugerimos:

- Ter fornecido e prestado suporte técnico em soluções de *backup* institucionais (proteção de dados), em ambiente computacional que totalize o mínimo de 03 (três) servidores de *backup* e o mínimo de 50 (cinquenta) clientes de *backup* em cópias seguras, ou30TB de dados de origem, ou 02 Appliances de backups com capacidade mínima de proteção de 200 TB de dados;
- Deve-se comprovar a prestação de serviços relacionados a soluções de *backup* (proteção de dados), por, no mínimo, 12 (doze) meses consecutivos;

Especificamente para o serviço de Instalação e Migração, quando a solução fornecida for distinta à implantada na JF1 (Netbackup):

- Serviço de migração de dados de soluções de backup institucional entre plataformas distintas. Considerar e comprovar a migração mínima de volumetria de 300 (trezentos) TB em fitas de backup do tipo LTO, entre soluções distintas

3 – Migração de dados

Estabelece o item 4.2.9: “Cabe à CONTRATADA o provimento de toda infraestrutura necessária para 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”.

O item 4.2.9.3, consigna que : “Os serviços de migraçãonãopoderão acarretar impactos nos ambientes tecnológicos em produção na JF1.”

Nesse diapasão, é correto entender que os serviços de migração não poderão fazer uso, ainda que compartilhado, da infraestrutura que será disponibilizada consoante item 4.1.7. Logo sugerimos a inserção de texto explícito e esclarecedor;

4.2.9.4 Os serviços de migração não poderão fazer uso, ainda que compartilhado, da infraestrutura que será disponibilizada consoante item 4.1.7.