ANEXO I DO TERMO DE REFERÊNCIA - REQUISITOS DE NEGÓCIO

1.Requisitos da infraestrutura computacional

1.1 A solução deverá prover uma infraestrutura hiperconvergente de alta disponibilidade em configuração de cluster para ambientes virtualizados. Não serão aceitas soluções ou funcionalidades implementadas via software ainda em fase de desenvolvimento, ou seja, aquelas que ainda não foram homologadas pelo fabricante para ambiente de produção.

1.1.1. Tanto o hardware quanto o software dessa solução deverão suportar pelo menos os seguintes hypervisors:
   1.1.1.1. Microsoft Hyper-V;
   1.1.1.2. VMware ESXi;
   1.1.1.3. Hypervisor baseado em KVM, desde que distribuído e suportado pelo fabricante da Solução Hiperconvergente.

1.1.2. A solução deve ser fornecida plenamente licenciada com qualquer dos hypervisors listados acima em sua edição mais completa.

1.1.3. No que diz respeito ao controlador de armazenamento, este deverá ser baseado em máquina virtual, executando um sistema operacional próprio desenvolvido no conceito de armazenamento definido em software. Cada servidor físico, também definido por nó em uma solução hiperconvergente, deverá hospedar um controlador de armazenamento virtual, possibilitando a criação de um cluster, apresentando ao hypervisor um sistema de arquivos único e distribuído.

1.1.4. A solução deverá suportar nós com diferentes especificações de hardware em um mesmo cluster. Adicionalmente, a solução deverá suportar nós híbridos (com HDD e SSD) e all-flash (somente SSD) no mesmo cluster.

1.1.5. A solução deverá replicar automaticamente todas as gravações para um ou mais nós do cluster, utilizando as interfaces 10 Gigabit Ethernet presente em cada um dos nós. Não serão aceitas soluções tradicionais ou convergentes baseadas em SAN.

1.1.6. O software deverá trabalhar com no mínimo fator de replicação 2 (dois), garantindo que toda gravação seja replicada de forma síncrona para outro nó do cluster, assegurando a resiliência do cluster e disponibilidade dos dados em caso de falhas.

1.1.7. A solução deverá permitir que em um cluster com 5 (cinco) ou mais nós seja possível ao administrador a inicialização do cluster com fator de replicação 3 (três), assegurando que toda operação de gravação seja replicada para 2 (dois) outros nós no cluster.

1.1.8. Quando empregados 3 (três) ou mais chassis no mesmo cluster, a solução deverá garantir que as réplicas dos dados sejam armazenadas em chassis diferentes, permitindo que um chassi inteiro falhe, sem que ocorra indisponibilidade dos dados.

1.1.9. Deve permitir escalabilidade horizontal, isso é, a adição de novos chassis e novos servidores (nós), um por vez, ao cluster através de uma console gráfica, sem a parada do ambiente de produção, aumentando como um todo a capacidade de armazenamento, processamento e memória disponibilizados ao hypervisor, além de crescer de forma linear o desempenho do cluster.

1.1.10. Deve permitir adição de nós que incrementem apenas o armazenamento do cluster de forma independente do processamento e memória.

1.1.11. Deve permitir remover nós do cluster sem parada no ambiente.

1.1.12. A fim de assegurar a máxima performance, toda operação de gravação de uma determinada máquina virtual deverá acontecer primariamente nos discos SSD daquele nó que está hospedando a máquina virtual. Caso o disco SSD local esteja com alta taxa de ocupação, a operação de gravação deverá ser redirecionada para um disco SSD pertencente a outro nó do cluster.

1.1.13. A solução deverá se utilizar de um mecanismo para mover os dados não acessados para os discos rígidos pertencentes ao cluster, deixando os discos SSD para dados acessados com frequência. Caso o dado volte a ser requisitado, o mesmo deverá ser migrado para o cache unificado descrito anteriormente.

1.1.14. A solução deverá garantir replicação síncrona de todos os dados gravados localmente para outros servidores que compõem o cluster, cada qual com seu respectivo sistema de armazenamento local com garantia de que a promoção e a demoção dos dados ocorram simultaneamente nos servidores do cluster.
1.1.15. As controladoras de armazenamento virtual deverão manter os dados distribuídos uniformemente através de todos os discos SSD e rígidos conectados aos nós pertencentes ao cluster. A distribuição dos dados deverá ser um processo automático agendado pelo software ou disparado assim que uma determinada porcentagem de utilização do discos daquele nó for atingida.
1.1.16. A solução deverá manter os dados das máquinas virtuais no armazenamento local do próprio nó, caso essa VM se movimente de um servidor a outro os dados devem ser movidos em segundo plano, para esse novo servidor, buscando o melhor desempenho possível.
1.1.17. O sistema operacional em execução em cada um dos nós deve suportar atualizações do tipo um clique, possibilitando a atualização de todos os nós do cluster de forma simples e automatizada, eliminando a intervenção manual do administrador e necessidade de parada completa do ambiente.
1.1.18. Deve implementar, via software, compressão inline (durante o processo de gravação).
1.1.19. Deve implementar, via software, desduplicação de dados.
1.1.20. Deve implementar compressão pós-processada, sendo que após uma operação de escrita, exista um atraso em minutos para iniciar o processo de compressão. O atraso deverá ser configurável pelo administrador do sistema.
1.1.21. Para permitir um melhor aproveitamento dos recursos de armazenamento do cluster, implementar método de proteção de dados Erasure Coding, no qual os dados são divididos em fragmentos, estendidos e codificados com pedaços de dados redundantes e armazenados em diferentes nós.
1.1.22. A solução deve suportar snapshots por máquina virtual nativamente independente do hypervisor, armazenando esses snapshots no cluster para proteção local. O snapshot realizado deve ser do tipo crash consistent, ou seja, o snapshot poderá ser feito com o ambiente em produção e irá garantir a proteção dos dados que estão gravados em disco.
1.1.23. O recurso de snapshots das máquinas virtuais em nível de storage, deve suportar um número ilimitado de snapshots, beneficiando-se de um algoritmo que redireciona a escrita para o snapshot, oferecendo mais velocidade e eficiência, sem sacrificar o desempenho do cluster.
1.1.24. Deve permitir ao usuário de uma determinada máquina virtual, restaurar arquivos armazenados em snapshots a partir da máquina virtual em execução. Essa funcionalidade deve exigir mínima intervenção manual do administrador da solução de armazenamento.
1.1.25. Com o objetivo de atender a demanda específicas de certas aplicações por acesso a armazenamento via protocolo iSCSI, permitir a apresentação de armazenamento em nível de blocos a uma dada máquina virtual.
1.1.26. A solução deve possuir console de administração WEB sem necessidade de instalação de qualquer componente adicional para essa finalidade.
1.1.27. A funcionalidade de alta disponibilidade também deve estar disponível para a interface de administração, garantindo que mesmo em caso de falhas, a interface de administração continue disponível.
1.1.28. A console WEB deve permitir integração com Active Directory da Microsoft para autenticação, ou então, utilizar autenticação local.
1.1.29. Com a finalidade de automatizar os processos de implementação, manutenção e gerenciamento do cluster, o sistema operacional em execução na solução hiperconvergente deverá oferecer REST APIs.
1.1.30. A solução deverá implementar uma interface de linha de comando completa para administração e monitoramento dos componentes do cluster.
1.1.31. Com o objetivo de proporcionar maior segurança, o sistema operacional deve oferecer uma funcionalidade de impedir o acesso ao terminal de linha de comando.
1.1.32. O gerenciador do cluster deverá enviar periodicamente informações e estatísticas automaticamente para o suporte do fabricante, funcionalidade conhecida como call-home. Este recurso tem por objetivo aplicar análises avançadas para otimizar a implementação da

solução ou atuar proativamente na identificação de problemas. Deverá ser permitido desabilitar este recurso a qualquer momento através da interface WEB.

1.1.33. A console de administração gráfica deverá disponibilizar, quando necessário, o acesso remoto do time de suporte do fabricante. Tal funcionalidade deverá estabelecer um túnel SSH reverso aos servidores do fabricante com o objetivo de permitir ao suporte, executar manutenções no software dos controladores de armazenamento virtuais. O administrador do sistema poderá habilitar ou desabilitar o acesso a qualquer momento.

1.1.34. A solução deverá possuir ferramenta de checagem interna integrada a console de gerenciamento, buscando por problemas de saúde no cluster proativamente.

1.1.35. Deverá suportar microssegmentação para prover controle granular e governança de todo o tráfego de entrada e saída de uma máquina virtual (VM) ou grupos de máquinas virtuais (VMs).

1.1.36. A microssegmentação deverá permitir a associação de políticas de rede a VMs e aplicativos ao vez de segmentos de rede específicos (por exemplo VLANs) ou identificadores (endereços IP ou MAC).

1.1.37. Deverá prover visualização de todo tráfego e relacionamentos com a descoberta automática dos fluxos entre as máquinas virtuais.

1.1.38. Deverá prover uma estrutura de segurança orientada por políticas que inspeciona o tráfego dentro do data center.

1.1.39. As políticas de segurança devem inspecionar o tráfego originado e terminado dentro de um datacenter, a fim de ajudar a eliminar a necessidade de firewalls adicionais no datacenter.

1.1.40. A estrutura deve utilizar uma abordagem centrada na carga de trabalho em vez de uma abordagem centrada na rede, permitindo examinar o tráfego de, e para as VMs, independentemente de como as configurações de rede mudam e onde residem no data center.

1.1.41. Deverá prover uma abordagem agnóstica a estrutura de rede, centrada na carga de trabalho, permitindo que a equipe de virtualização implemente essas políticas de segurança sem depender de equipes de segurança de rede.

1.1.42. As políticas de segurança deverão ser aplicadas às categorias (um agrupamento lógico de VMs) e não às próprias VMs, não importando quantas VMs são inicializadas em uma determinada categoria. O tráfego associado às VMs em uma categoria deverá ser protegido sem intervenção administrativa, em qualquer escala.

1.1.43. A interface de gerenciamento deve oferecer uma abordagem baseada em visualização para configurar políticas e monitorar o tráfego ao qual uma determinada política se aplica:

1.1.44. Política de Segurança de Aplicação: quando for necessário proteger um aplicativo especificando origens e destinos de tráfego permitidos.

1.1.45. Política de Isolamento do Ambiente: quando for necessário bloquear todo o tráfego, independentemente da direção, entre dois grupos de VMs identificados por sua categoria. VMs dentro de um grupo podem se comunicar umas com as outras.

1.1.46. Política de Quarentena: quando for necessário isolar uma VM comprometida ou infectada e, opcionalmente, desejar submetê-la à perícia.

1.1.47. Deverá garantir que seja apenas permitido o tráfego entre camadas de aplicativos ou outros limites lógicos, garantindo a proteção contra ameaças avançadas para que não sejam propagadas no ambiente virtual.

1.1.48. Deverá permitir a atualização automática durante todo o ciclo de vida da VM, eliminando a carga do gerenciamento de mudanças de políticas.

1.1.49. A Solução deve permitir categorizar as Máquinas Virtuais de forma a permitir a criação políticas de segurança com no mínimo as seguintes funções:

1.1.49.1. Isolar o tráfego de dados entre Máquinas Virtuais de Diferentes categorias

1.1.49.2. Isolar o tráfego de dados de Máquinas Virtuais específicas para modo de quarentena, tanto forense quanto restrita, de forma a prover uma rápida reação ao time de infraestrutura em caso de Máquinas Virtuais contaminadas ou pertencentes a usuários que foram desligados ou sob procedimento de custódia de dados.

1.1.49.3. Mapear o tráfego de entrada, entre as camadas e de saída de aplicações, permitindo ao administrador determinar quais servidores têm acesso de entrada na aplicação, o tipo de protocolo e o número da porta que o fluxo de dados pode ocorrer, permitir ou restringir também o fluxo de dados entre as camadas,

máquinas virtuais, pertencentes à aplicação, através da especificação do protocolo e o número da porta, realizar também o mesmo procedimento para conexões de saída das camadas da aplicação, também através da especificação de protocolo e número de porta.

1.1.50. Deve possuir integração com software de terceiros que permita o redirecionamento do tráfego das VMs para ferramentas terceiras, como por exemplo, mas não limitado a softwares de detecção e prevenção de intrusos (IDS/IPS), monitoração de performance de aplicações (APM), balanceadores de carga.

1.1.51. Conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I – Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), tanto os hardwares quanto os softwares desta solução deverão ser do mesmo fabricante ou com suporte unificado para hardware e software pelo fabricante da solução.

1.1.52. Todos os componentes de software da solução deverão ser devidamente licenciados e suportados por pelo menos 5 (cinco) anos.

1.2. Requisitos da infraestrutura de backup:

1.2.1. Deve corresponder a um sistema inteligente de armazenamento de backup em disco, que se entende como um subsistema com o propósito específico de armazenamento de backup com criptografia, compactação, desduplicação e replicação dos dados desduplicados;

1.2.2. O hardware do módulo de armazenamento de backup em disco não poderá ser compartilhado com nenhum outro software para operar.

1.2.3. Deve constar no site do fabricante (documento oficial e público) como um appliance ou sistema de armazenamento de backup em disco, em linha de produção.

1.2.4. Deve permitir a utilização de todas as funcionalidades, tecnologias e recursos especificados, sem necessidade de licenciamentos ou ônus adicionais, já licenciados para a capacidade máxima de expansão da solução.

1.2.5. Os appliances de backup devem ser agnósticos ao software de backup, sendo compatível com pelo menos dois softwares do mercado, além do software proposto para esta ocorrência;

1.2.6. Deve permitir a adição futura de ao menos mais uma controladora (nó de processamento) no mesmo conjunto de armazenamento para atuar em modo de alta-disponibilidade ativo-passivo (failover) ou ativo-ativo (load-balance) para as tarefas de backup, de forma que na eventualidade da falha de uma das controladoras (nó de processamento), as atividades de backup possam ser automaticamente redirecionadas para a outra controladora.

1.2.7. Deve possuir recursos de tolerância a falhas de, pelo menos, discos, fontes de alimentação e ventiladores.

1.2.8. Deve possuir mecanismos que protejam contra a inconsistência dos dados mesmo em casos de interrupção abrupta ou desligamento acidental.

1.2.9. Deve possuir baterias, supercapacitores ou tecnologia similar, para proteger a cache de escrita, evitando a perda de dados em eventos de falha elétrica.

1.2.10. Os appliances devem implementar mecanismos de validação da consistência dos dados desduplicados armazenados, garantindo que eles estejam íntegros durante backups, restaurações e replicações. A tecnologia deverá reparar, automaticamente, dados que não estejam consistentes com as rotinas executadas. O mecanismo deve ser nativo do equipamento, não sendo aceitos scripts para atendimento deste item.

1.2.11. Deve ser entregue com arranjos de discos rígidos do tipo RAID-6 configurado de tal modo a tolerar a falha de até 2 (dois) discos rígidos, contando com ao menos 1 disco de hot-spare para cada RAID group, para os discos destinados ao armazenamento de dados de backup.

1.2.12. Deve possuir funcionalidade de desduplicação dos dados em nível de bloco ou bytes, com capacidade de eliminação de dados redundantes para racionalizar a utilização do espaço de armazenamento. Serão aceitas soluções que efetuem a desduplicação em linha (inline) ou em paralelo. Caso possua desduplicação em linha (inline), deve fornecer todo o licenciamento e componentes para ativar essa funcionalidade em toda a volumetria útil entregue. Não serão aceitas soluções que efetuem desduplicação post-processing, requerendo janela de desduplicação, nem limitando a execução de backups, restores e replicações durante a execução do processo de desduplicação.

1.2.13. Deve suportar que a desduplicação seja realizada juntamente com as operações de backup e restauração, tornando desnecessária uma janela dedicada para sua execução.
1.2.14. Deve possuir desduplicação global, mesmo que o armazenamento esteja dividido em volumes lógicos, sendo capaz de identificar dados duplicados de backups de diferentes origens dentro de um mesmo sistema, de modo a maximizar a taxa de desduplicação e garantindo que os dados retidos sejam gravados uma única vez.
1.2.15. Deve suportar simultaneamente acessos de leitura e gravação pelos protocolos CIFS, NFS e OST.
1.2.16. Deve permitir a execução de processos de backup e restore em paralelo.
1.2.17. Deve possuir interface WEB para gerenciamento do sistema de armazenamento de backup.
1.2.18. A solução de repositório de backup deve possuir integração com o Microsoft Active Directory 2012 e superiores, para autenticação e definição de perfis de acesso. Deve ainda permitir a configuração de duplo fator de autenticação para acesso ao gerenciamento do sistema via integração com sistemas de senha descartável (senha de uso único, em inglês: One-time password - OTP), tais como Google Authenticator, Microsoft Authenticator ou similares.
1.2.19. Caso o equipamento requeira um dispositivo/sistema OTP específico que necessite de licenciamento, hardwares e/ou infraestrutura próprios – por exemplo: Common Access Card (CAC)/Personal Information Verification (PIV) cards, etc. – esses componentes (hardwares, softwares, licenças, serviços, etc.) devem ser fornecidos com a solução, para, no mínimo, 5 usuários;
1.2.20. Deve possuir funcionalidade para replicação de backups em site remoto de forma síncrona ou assíncrona entre subsistemas semelhantes do mesmo fabricante, utilizando recursos de desduplicação, permitindo reduzir o consumo do link de comunicação. Essa funcionalidade deve ser suportada pelo mesmo fabricante do subsistema e deve ser entregue licenciada para toda a capacidade fornecida.
1.2.21. Deve permitir replicar os dados através de rede IP (WAN/LAN).
1.2.22. Deve estar licenciado para replicar todo o sistema de armazenamento de backup, incluindo a capacidade de expansão.
1.2.23. Deve possuir recursos avançados de cibersegurança para prevenção de ataques cibernéticos do tipo Ransomware garantindo a proteção dos dados retidos, com as seguintes características:
1.2.24. Tal proteção deve ser do dispositivo de armazenamento ofertado e deverá funcionar de maneira automática e transparente, isto é, independentemente do software/utilitário de backup, sem depender do desenvolvimento de scripts de integração e sem requerer ações ou atividades manuais sobre o dado retido;
1.2.25. Deve garantir a inviolabilidade (imutabilidade) dos dados retidos, garantindo assim que os dados protegidos não possam ser alterados ou apagados, mesmo se o software de backup ou ambiente operacional onde ele opera ficar sob controle do atacante (hacker, malware). Tal proteção deve garantir que, mesmo nas situações em que o atacante procure expirar o conteúdo dos backups através do catálogo do software de backup, os dados retidos ainda possam ser recuperados do appliance de backup por um período de dias;
1.2.26. Não pode requerer e nem ser recomendada janela específica para a aplicação do recurso de proteção dos dados retidos, considerando o conjunto do Software de Backup envolvido e Equipamento ofertado, ou seja, a proteção deverá ser aplicada de forma imediata, assim que os dados retidos sejam desduplicados no appliance de backup;
1.2.27. Deve fazer uso do conceito de isolamento para a proteção dos dados, ou seja, os dados protegidos deverão estar invisíveis da superfície de ataque, isto é, não poderão ser acessados através da rede nem pelo software/utilitário de backup.
1.2.28. Possuir recurso de dupla autorização (Dual Authorization – Dual Auth), ou seja, alterações das configurações contra Ransomware deverão ser aprovadas por um segundo usuário;
1.2.29. Será facultada a utilização de soluções que não atendam a uma ou mais características do item referente aos recursos avançados de cibersegurança, desde que garantido a cópia/replicação dos backups fisicamente no mesmo datacenter, mas logicamente isolado (isolamento através de configurações de rede recomendadas ou software específico para essa função da solução ofertada), permitindo assim uma recuperação mais rápida. Para tal, deverá ser fornecido toda a infraestrutura e componentes necessários (armazenamento

adicional, servidores, switches, software, licenciamento, serviços, etc.) e em quantidade suficiente para proteger todos os dados retidos conforme especificações de volume de dados, retenção, crescimento vegetativo e tamanho mínimo do equipamento deste termo de referência para a proteção dos dados de backup, devendo ser fornecidos em conjunto com a solução e mantendo as condições de escalabilidade e desempenho especificadas nesse projeto;

1.2.30. Todos os componentes necessários (hardware, software, licenciamento, serviços etc.) para a proteção dos dados de backup devem ser fornecidos em conjunto com a solução e devem manter as condições de escalabilidade e desempenho especificadas nesse projeto.

1.2.31. Deve possuir recursos para monitoramento remoto pelo fabricante, tal como notificação do tipo Call-Home, para verificação proativa de componentes de hardware em situação de falha ou pré-falha.

1.2.32. Deve possuir suporte aos protocolos de monitoramento SNMP e Syslog.

1.3. Especificação dos bens e serviços que compõem a infraestrutura computacional:

DESCRIÇÃO	QTD
SERVIDOR HIPERCONVERGENTE / SOFTWARE DE GERENCIAMENTO → Cada servidor físico (nó) deverá ser fornecido com no mínimo a seguinte configuração bruta: ✓ Deve ser fornecido com 2 (dois) processadores físicos padrão x86. Cada processador deve possuir, no mínimo, 16 (dezesseis) núcleos físicos. Referência: Intel Xeon Silver 6346 ou superior. Para fins de referência, considerar-se-á superior o processador que contenha ao menos o número especificado de núcleos e "Single Thread Rating" superior ao do processador de referência no site www.cpubenchmark.net; → Deve ser fornecido com 1TB (um terabytes) de memória RAM e suportar expansão para pelo menos 2TB (dois terabytes). → Deve ser fornecido com 3,84TB (três virgula oitenta e quatro terabytes) de armazenamento bruto em discos SSD. → Deve ser fornecido com 24TB (vinte e quatro terabytes) de armazenamento bruto em discos HDD. ✓ Deve possuir pelo menos 2 (duas) portas SFP+. ✓ Deve acompanhar 1 Patch Cords CAT de no mínimo 3 metros compatível com o switch oferecido. ✓ Deve possuir 60 (sessenta) meses de garantia e suporte. → Os equipamentos e Softwares devem ser entregues com suas respectivas capacitações e transferências de conhecimento. **Software de Gerenciamento** → Deve ser disponibilizada uma ferramenta de gerência unificada, facilitando a tarefa de administração diária dos clusters localizados distantes geograficamente. A ferramenta deverá apresentar as seguintes informações consolidadas de todos os clusters registrados: ✓ Saúde dos Sistema clusters. ✓ Máquinas Virtuais. ✓ Armazenamento.	6

✓ Situação do Hardware. ✓ Dashboard de Análise de Performance. ✓ Dashboard de Alertas e Eventos. → Cada licença deverá ser fornecida com pelo menos 60 (sessenta) meses de subscrição e suporte na modalidade 24x7x365. → Deve ser implementado como uma máquina virtual adicional, integrada a console de administração local da solução de hiperconvergência. → Deve gerenciar múltiplos clusters e as máquinas virtuais, inclusive quando empregados hypervisor diferentes. → A solução deve fornecer sugestões de ajuste de configurações (CPU, memória) as máquinas virtuais baseada na utilização histórica dos recursos computacionais atribuídos a elas. → Deve possuir funcionalidade de atualização automatizada de múltiplos clusters de forma centralizada. → Deverá detectar possíveis gargalos no ambiente devido ao consumo de recursos não otimizado. → Deve possuir uma ferramenta de planejamento (Capacity Planning) disponível, de forma a permitir a análise e predição de consumo de recursos de armazenamento, CPU e memória. Caso a solução de gerenciamento centralizada não atenda este requisito, deverá ser oferecido uma ferramenta de terceiro para obter esta funcionalidade. → Solução deve possuir dashboards customizáveis. → Cada unidade compreende o licenciamento de 1 nó. → Os Softwares devem ser entregues com suas respectivas capacitações e transferências de conhecimento.	
→ Deve ser disponibilizada uma ferramenta de gerência unificada, facilitando a tarefa de administração diária dos clusters localizados distantes geograficamente. A ferramenta deverá apresentar as seguintes informações consolidadas de todos os clusters registrados: ✓ Saúde dos Sistema clusters. ✓ Máquinas Virtuais. ✓ Armazenamento. ✓ Situação do Hardware. ✓ Dashboard de Análise de Performance. ✓ Dashboard de Alertas e Eventos. → Cada licença deverá ser fornecida com pelo menos 60 (sessenta) meses de subscrição e suporte na modalidade 24x7x365. → Deve ser implementado como uma máquina virtual adicional, integrada a console de administração local da solução de hiperconvergência.	

→ Deve gerenciar múltiplos clusters e as máquinas virtuais, inclusive quando empregados hypervisor diferentes. → A solução deve fornecer sugestões de ajuste de configurações (CPU, memória) as máquinas virtuais baseado na utilização histórica dos recursos computacionais atribuídos a elas. → Deve possuir funcionalidade de atualização automatizada de múltiplos clusters de forma centralizada. → Deverá detectar possíveis gargalos no ambiente devido ao consumo de recursos não otimizado. → Deve possuir uma ferramenta de planejamento (Capacity Planning) disponível, de forma a permitir a análise e predição de consumo de recursos de armazenamento, CPU e memória. Caso a solução de gerenciamento centralizada não atenda este requisito, deverá ser oferecido uma ferramenta de terceiro para obter esta funcionalidade. → Solução deve possuir dashboards customizáveis. → Cada unidade compreende o licenciamento de 1 nó. → Os Softwares devem ser entregues com suas respectivas capacitações e transferências de conhecimento.	
APLICAÇÃO DE BACKUP → Não serão aceitas soluções do tipo comunidade, software livre, ou que possuem componentes e módulos sem suporte oficial do fabricante. → A solução ofertada deverá possuir todos os produtos na versão estável mais atual do produto, não serão aceitos produtos obsoletos ou fora de linha de produção do fabricante. → O licenciamento deve ser do tipo subscrição de direito de uso de software pelo período de 60 (sessenta) meses, por máquina virtual (virtual machine). Ao término do período de subscrição, o software deverá permanecer totalmente operacional para as funcionalidades de restore/recovery (recuperação de dados já copiados/protegidos), sem a necessidade de pagamento de quaisquer valores adicionais pelo seu uso para a restauração de cópias de segurança realizadas durante a vigência da subscrição. → Deve prover licenciamento de software baseado em assinatura ou subscrição, devendo todas as funcionalidades solicitadas neste documento estarem operacionais e disponíveis durante toda a vigência da subscrição. Não poderão ser cobrados quaisquer valores adicionais para a recuperação dos dados já protegidos - durante e após o término da vigência da subscrição. → Deve possuir suporte técnico e direito de atualização da solução pelo mesmo período de 60 (sessenta) meses de subscrição. → O licenciamento não deve possuir nenhum tipo de limite por volumetria de armazenamento de TB (terabytes), seja de backend ou frontend, em qualquer componente da solução durante a vigência da subscrição.	20

→ Deve prover licenciamento para o ambiente virtual contabilizado apenas o número de máquinas virtuais que fazem backup, independentemente das suas configurações de hardware (sockets, memória, disco, etc.), da localização lógica ou geográfica do hospedeiro em que estiver sendo executada (on-premise ou nuvem) e em qualquer ambiente de virtualização requisitado nessa especificação.

→ A licença deverá estar em uso apenas enquanto estiver executando o backup da máquina virtual. Se a máquina virtual for desassociada da política de execução de backup, a licença deverá ficar livre para uso em qualquer outra nova máquina virtual do ambiente de virtualização. Neste caso, os dados de backup da máquina virtual antiga e da nova deverão permanecer disponíveis para restauração até o término de suas respectivas políticas de retenção.

→ Cada unidade licitada deverá compreender licenciamento suficiente para 10 instâncias (máquinas virtuais, em nuvem ou físicas). Alternativamente, caso a solução ofertada não suporte licenciamento por instância, serão aceitas soluções licenciadas por socket, nesse caso, cada unidade deverá compreender licenciamento suficiente para 4 sockets.

→ Deve ser compatível nativamente com todos os hypervisors descritos nas especificações dos “Requisitos da infraestrutura computacional” deste documento.

→ Deve ser compatível com nuvem AWS.

→ Deve suportar, nos clientes de Backup/Recovery, pelo menos os sistemas operacionais:

- ✓ Microsoft Windows Server 2008 R2 e versões superiores;
- ✓ RedHat 6.5 e versões superiores;
- ✓ Ubuntu 20.04 ou superior;
- ✓ Suse Linux Enterprise 12 ou superior;
- ✓ A solução de software de backup/recovery deve nativamente, sem aplicativos de terceiros e execução de scripts, suportar compressão e desduplicação, com as seguintes características:
- ✓ Desduplicação a nível de blocos;
- ✓ Desduplicação em volumes apresentados através de das (direct attached storage) e SAN (storage area network);
- ✓ Desduplicação de dados no servidor de armazenamento (target deduplication), de forma que o servidor de backup descarte blocos repetidos de clientes, evitando assim o armazenamento de blocos redundantes.

→ Deve permitir replicação de dados entre pools de desduplicação de maneira otimizada, replicando somente as alterações.

→ Deve suportar a criptografia dos dados, com as seguintes características:

- ✓ Criptografia de dados na origem (direto no cliente ou servidor de proxy de backup), de uma forma que seja garantido que o dado trafegará criptografado na LAN (local area network) ou WAN (wide area network);
- ✓ Criptografia nos arquivos de backup;

- ✓ Módulo nativo de criptografia AES (advanced encryption standard) 256 bits.

→ Deve suportar os protocolos de rede IPv4 ou IPv6 para rotinas de backup/recovery.

→ Deve possibilitar replicação de uma origem para múltiplos destinos.

→ Deve possibilitar replicação e consolidação de dados de múltiplas origens para um destino central.

→ Deve possibilitar aplicar diferentes políticas de retenção de dados nos repositórios de origem e destino durante o processo de replicação.

→ Deve permitir o controle da banda de dados utilizada para a replicação dos dados de backup.

→ Deve possibilitar retomar a replicação do ponto onde a mesma foi interrompida, para casos de perda de comunicação entre origem e destino.

→ Deve prover recursos de desduplicação e compressão tanto no site principal como nos sites remotos. Nos sites remotos deve ainda:

→ Promover meios de recuperação rápida dos dados de catálogo e índices do servidor de backup em caso de perda ou corrompimento destas informações.

→ A solução de software de backup/recovery deve nativamente, sem aplicativos de terceiros e sem a execução de scripts:

- ✓ Possibilitar o backup e a restauração das informações em disco;
- ✓ Suportar as operações de backup e restauração em paralelo;
- ✓ Localizar um arquivo para restauração pelo nome, pesquisando no catálogo da ferramenta.
- ✓ Possuir a capacidade de efetuar backup para disco com retenções, através de políticas pré-definidas e agendadas.

→ Para um dado armazenado deve haver a possibilidade de alterar o período de retenção.

→ Deve suportar os métodos de backup full e incremental, onde:

- ✓ No método incremental, suportar modo incremental forever, ou seja, o backup deve consistir em apenas de um backup full e todos os demais incrementais até o término do período de retenção;

→ Deve possibilitar verificação e checagem automática da consistência do backup, no intuito de garantir a integridade dos dados.

→ Executar backup de bases de dados do Oracle, SQL server, MySQL e PostgreSQL de forma consistente, sem a parada do banco ou uso de scripts.

→ Deve possibilitar a integração com Microsoft Active Directory 2012 R2 e versões superiores.

→ Deve permitir a recuperação do arquivo em um momento de tempo específico.

→ Deve permitir redirecionar a restauração de uma da máquina virtual para uma pasta, datastore, hospedeiro ou rede alternativos. → Deve ser capaz e iniciar a execução da máquina virtual diretamente a partir do seu arquivo de backup, sem a necessidade de esperar o término do processo de restauração. → Deve realizar a restauração granular a nível de arquivos dentro sistema operacional cliente, sem a necessidade de se restaurar a máquina virtual inteira. → Suportar jobs simultâneos para backup de máquinas virtuais. → Permitir a integração com os serviços de nuvens (Azure, AWS e GCP) executando backup/recovery com as seguintes características: ✓ Permitir a cópia dos dados de backup de máquinas virtuais da nuvem para áreas de armazenamento on-premises; ✓ Permitir integração através de Restful API com suporte as requisições HTTP do tipo deletem, get, post e put. → Deve possuir gerenciamento das operações da infraestrutura de backup em modo gráfico, que permita o monitoramento em tempo real das rotinas de backup/recovery e status dos dispositivos e clientes de todo o ambiente. → Deve possuir dashboards com suporte a visualização de todas as rotinas de backup/recovery, com opções de gerar relatórios on-line e envio por e- mail. → Deve possuir habilidade para definir prioridades de servidores dentro de um job de backup. → Deve possuir mecanismo de auditoria para o controle de acesso, em operações realizadas através de interface gráfica ou WEB e linha de comando (interface CLI), permitindo a emissão de relatórios com, no mínimo, as seguintes informações: ✓ Data e hora da operação. ✓ Usuário que realizou a operação. ✓ Operação realizada. → Suportar a geração de relatórios gráficos customizáveis de atividades de backup/recovery, contendo: ✓ Horário de início e término dos jobs; ✓ Tempo de duração dos jobs; ✓ Todos os jobs em execução; ✓ Status (situação) de execução dos jobs; ✓ Relação e porcentagem de jobs executados por status, como por exemplo: com sucesso e com falhas; ✓ Logs dos jobs; ✓ Volume de dados na origem e no destino, total e por job, por período de tempo, por localidade e por host (físico ou virtual); ✓ Tendência de crescimento; ✓ Dados históricos de, no mínimo, 24 (vinte e quatro) meses; → Deve permitir a exportação dos relatórios nos formatos HTML, CSV ou PDF.	

→ Deve possuir mecanismos que evitem o impacto da solução de proteção, reduzindo o desempenho das atividades de backup quando um limite configurado for atingido, evitando a sobrecarga nos sistemas de armazenamento do ambiente virtualizado. → Deve possibilitar, por meios de logs e alertas, a análise de causa raiz de problemas de backup/recovery. → Os Softwares devem ser entregues com suas respectivas capacitações e transferências de conhecimento.	
APPLIANCE DE BACKUP → Deve ser composto por hardware e software do mesmo fabricante. Não serão aceitas soluções montadas especificamente para esse certame, composições de soluções em regime de OEM, nem equipamentos usados, remanufaturados, de demonstração ou gateways. → Não serão aceitas soluções definidas por Software (Virtual Appliance). → Deve ser fornecido com discos rígidos hot-pluggable e hot-swappable, permitindo substituição sem necessidade interrupção do funcionamento da solução. → Deve permitir montagem em rack padrão 19" e deve ser fornecido com todos os trilhos, cabos, conectores, manuais de operação e quaisquer outros componentes que sejam necessários à instalação, customização e plena operação. → Deve possuir capacidade de 70 TB (setenta terabytes) de capacidade total para uso, sem considerar taxa de desduplicação, compressão, perdas com formatação e área necessária para o sistema do equipamento); → A infraestrutura de backup (conjunto de um ou mais appliances) deve suportar a expansão de sua capacidade para, no mínimo, 500TB (quinhentos terabytes) de capacidade líquida (sem considerar taxas de desduplicação, compressão, perdas com formatação e área necessária para o sistema do equipamento). Esta ampliação de capacidade poderá ser realizada através de discos adicionais, ou unidades de expansão, para o mesmo conjunto de armazenamento, mantendo a característica de desduplicação global da solução; → Deve possuir pelo menos 2 (duas) portas SFP+ → Deve acompanhar 2 cabos DAC de pelo menos 3 (três) metros compatíveis com o switch Fortinet existente. → Deve possuir pelo menos 1 (uma) porta Gigabit Ethernet padrão 1000Base-T dedicada gerenciamento. → Deve acompanhar 1 Patch Cords CAT6 de no mínimo 3 metros compatível com o switch oferecido. → Deve possuir taxa de transferência de, no mínimo, 5 TB/hora (cinco terabytes por hora) para operações de backup e de restauração caso a desduplicação seja do tipo paralelo, com utilização de cache em disco. Se a solução possuir desduplicação em linha, a taxa de transferência da solução deve ser de, no mínimo, 15 TB/hora (vinte e um terabytes por hora) para operações de backup, sem utilizar a desduplicação na origem para esse cálculo.	2

→ Deve possuir criptografia utilizando no mínimo AES128-SHA ou 256-SHA baseada em hardware. Caso a criptografia seja baseada em software, o desempenho (taxa de transferência) do sistema deve ser 30% maior ao requisitado no item anterior, sem utilizar desduplicação na origem para esse cálculo. Todas as licenças e componentes necessários a essa função devem ser fornecidos em conjunto com a solução. → A CONTRATADA deverá fornecer, mediante contrato de garantia de 60 (sessenta) meses, juntamente com a solução de armazenamento de backup o acesso expresso ao 2º nível de suporte do fabricante (nível onde o analista de suporte é qualificado para atuar diretamente no problema, sem necessidade de triagem prévia). O analista de suporte do fabricante deve, adicionalmente, realizar durante todo o período de garantia as seguintes atividades: atualização da solução de armazenamento de backup, verificações proativas junto ao CONTRATANTE, esclarecimento de dúvidas e apoio em atividades de revisão e alteração de configurações do dia a dia. → Os equipamentos devem ser entregues com suas respectivas capacitações e transferências de conhecimento.	
INSTALAÇÃO DE SERVIDOR HIPERCONVERGENTE → Deverá ser feita a montagem em rack padrão 19", alimentação elétrica e conexão do equipamento à rede de dados. → O serviço de instalação consiste na colocação do equipamento em pleno funcionamento, em conformidade com o disposto nesta especificação técnica, no Edital e seus Anexos e em perfeitas condições de operação, de forma integrada ao ambiente de infraestrutura de informática da Contratante e deve contemplar, no mínimo, o seguinte: ✓ Montagem em rack padrão 19" indicado pela contratante, alimentação elétrica e conexão do equipamento à rede de dados. ✓ Conexão e configuração do(s) nó(s) nos equipamentos de rede do Contratante; ✓ Atualização de softwares, firmwares e drives que compõem a solução; ✓ Instalação, configuração e aplicação das licenças aplicáveis; ✓ Configuração do call-home; ✓ Documentação do ambiente configurado e instalado. → A ativação e configuração da solução deve ser realizada segundo as boas práticas do fabricante, disponibilizando o ambiente de virtualização (hiperconvergência) em condições de pleno funcionamento. → Não compreende a migração das aplicações eventualmente existentes em outra infraestrutura. → Os equipamentos e Softwares devem ser entregues com suas respectivas capacitações e transferências de conhecimento.	6
INSTALAÇÃO DE APPLIANCE DE BACKUP → Deverá ser feita a montagem em rack padrão 19", alimentação elétrica e conexão do equipamento à rede de dados. → O serviço de instalação consiste na colocação do equipamento em pleno funcionamento, em conformidade com o disposto nesta especificação técnica, no Edital e seus Anexos e em perfeitas condições de operação, de forma integrada ao	2

ambiente de infraestrutura de informática da Contratante e deve contemplar, no mínimo, o seguinte: ✓ Montagem em rack padrão 19” indicado pela contratante, alimentação elétrica e conexão do equipamento à rede de dados. ✓ Conexão e configuração do(s) nó(s) nos equipamentos de rede do Contratante; ✓ Atualização de softwares, firmwares e drives que compõem a solução; ✓ Instalação, configuração e aplicação das licenças aplicáveis; ✓ Documentação do ambiente configurado e instalado. → A ativação e configuração da solução deve ser realizada segundo as boas práticas do fabricante, disponibilizando o ambiente de backup em condições de pleno funcionamento.	

1.4 Requisitos dos serviços de instalação para os itens

1.4.1 As atividades de instalação deverão ser realizadas dentro do horário comercial.

1.4.2 A implantação deverá abranger a configuração de quaisquer funcionalidades suportadas pelo equipamento / software – desde que especificadas neste TR. Estas informações serão documentadas no termo de abertura do projeto a ser documentado pela CONTRATADA após alinhamento do escopo de trabalho entre CONTRATADA e CONTRATANTE.

1.4.3 Todo o processo de instalação e configuração realizado deverá ser documentado pela CONTRATADA sob a forma de relatório.

1.4.4 A instalação física compreenderá a desembalagem e montagem de todos os componentes que integram a especificação dos dispositivos, a instalação física em ambiente interno ou externo, conexão à rede de dados e alimentação elétrica dos equipamentos.

1.4.5 A configuração compreenderá a realização dos ajustes de hardware e software necessários ao funcionamento dos dispositivos a fim de apresentarem a melhor performance de funcionamento possível.

1.4.6 A migração das aplicações não será parte do escopo de instalação, porém, a CONTRATADA deverá dar instruções e o suporte necessário à equipe da CONTRATANTE para a migração.

1.4.7 Deverão ser feitas todas as atualizações de firmware ou qualquer outro software componente da solução, para a versão mais atualizada disponível ou a última compatível com as demais soluções deste lote e considerada estável.

1.4.8 Deverão ser habilitadas todas as licenças que porventura sejam adquiridas e recursos do equipamento que serão utilizados no projeto.