

ANEXO I DO TERMO DE REFERÊNCIA – REQUISITOS DE NEGÓCIO

1. Requisitos do Software de Backup

- 1.1. Não serão aceitas soluções do tipo comunidade, software livre, ou que possuem componentes e módulos sem suporte oficial do fabricante.
- 1.2. 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.
- 1.3. 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.
- 1.4. 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.
- 1.5. Deve possuir suporte técnico e direito de atualização da solução pelo mesmo período de 60 (sessenta) meses de subscrição.
- 1.6. 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.
- 1.7. 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 (*onpremise* ou nuvem) e em qualquer ambiente de virtualização requisitado nessa especificação.
- 1.8. 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.

1.9. Cada unidade do item licitado deverá compreender licenciamento suficiente para pelo menos 10 instâncias (máquinas virtuais, em nuvem ou físicas). Esse requisito se dá pela necessidade de realização de backup de infraestrutura em nuvem. 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 2 *sockets*.

1.10. Deve ser compatível nativamente com os *hypervisors* VMWare versão 5.5 ou posterior, Hyper-V versão 2016 ou superior, pois ambos são utilizados em nosso parque tecnológico.

1.11. A solução de backup deverá ser capaz de realizar backup de recursos do Microsoft 365 em múltiplos destinos (*on-premise* e nuvem).

1.12. Deve ser compatível com os provedores de nuvem AWS, GCP e Azure, permitindo realizar backup de instâncias desses provedores.

1.13. Deve ser compatível com os provedores de nuvem AWS, GCP e Azure, permitindo backup e *restore* nos serviços de *Object Storage* desses provedores.

1.14. Deve suportar, nos clientes de *Backup/Recovery*, pelo menos os sistemas operacionais:

1.14.1. Microsoft Windows Server 2008 R2 e versões superiores;

1.14.2. RedHat 6.5 e versões superiores;

1.14.3. Ubuntu 20.04 e versões superiores;

1.14.4. CentOS 7 e versões superiores;

1.14.5. Suse Linux Enterprise 12 e versões superiores;

1.15. A solução de software de *backup/recovery* deve nativamente, sem aplicativos de terceiros e execução de scripts isolados, suportar compressão e deduplicação, com as seguintes características:

1.15.1. Deduplicação a nível de blocos;

1.15.2. Deduplicação na origem do dado;

- 1.15.3. Desduplicação em volumes apresentados através de DAS (*Direct Attached Storage*) e SAN (*Storage Area Network*);
- 1.15.4. 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.
- 1.16. Deve permitir replicação de dados entre *pools* de desduplicação de maneira otimizada, replicando somente as alterações.
- 1.17. Deve suportar a criptografia dos dados, com as seguintes características:
 - 1.17.1. 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*);
 - 1.17.2. Criptografia nos arquivos de backup;
 - 1.17.3. Módulo nativo de criptografia AES (*Advanced Encryption Standard*) com chave de pelo menos 256 bits.
- 1.18. Deve suportar os protocolos de rede IPv4 ou IPv6 para rotinas de backup/recovery.
- 1.19. Deve possibilitar replicação de uma origem para múltiplos destinos.
- 1.20. Deve possibilitar replicação e consolidação de dados de múltiplas origens para um destino central.
- 1.21. Deve possibilitar aplicar diferentes políticas de retenção de dados nos repositórios de origem e destino durante o processo de replicação.
- 1.22. Deve permitir o controle da banda de dados utilizada para a replicação dos dados de backup.
- 1.23. Deve possibilitar retomar a replicação do ponto onde a mesma foi interrompida, para casos de perda de comunicação entre origem e destino.

- 1.24. Deve prover recursos de deduplicação e compressão tanto no site principal como nos sites remotos. Nos sites remotos deve ainda:
- 1.25. Promover meios de recuperação rápida dos dados de catálogo e índices do servidor de backup em caso de perda ou corrupção destas informações.
- 1.26. A solução de software de backup/recovery deve nativamente, sem aplicativos de terceiros e sem a execução de scripts:
 - 1.26.1. Possibilitar o backup e a restauração das informações em disco;
 - 1.26.2. Suportar as operações de backup e restauração em paralelo;
 - 1.26.3. Localizar um arquivo para restauração pelo nome, pesquisando no catálogo da ferramenta.
 - 1.26.4. Possuir a capacidade de efetuar backup para disco com retenções, através de políticas pré-definidas e agendadas.
 - 1.26.5. Para um dado armazenado deve haver a possibilidade de alterar o período de retenção.
- 1.27. Deve suportar os métodos de backup *full* e incremental, onde:
 - 1.27.1. 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;
- 1.28. Deve possibilitar verificação e checagem automática da consistência do backup, no intuito de garantir a integridade dos dados.
- 1.29. 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.
- 1.30. Deve possibilitar a integração com Microsoft Active Directory 2012 R2 e versões superiores.
- 1.31. Deve permitir a recuperação do arquivo em um momento de tempo específico.

- 1.32. Deve permitir redirecionar a restauração de uma das máquinas virtuais para uma pasta, *datastore*, hospedeiro ou rede alternativos.
- 1.33. 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.
- 1.34. Deve realizar a restauração granular a nível de arquivos dentro do sistema operacional cliente, sem a necessidade de se restaurar a máquina virtual inteira.
- 1.35. Suportar *jobs* simultâneos para backup de máquinas virtuais.
- 1.36. Permitir a integração com os serviços de provedores de nuvem (Azure, AWS e GCP) executando backup/recovery com as seguintes características:
 - 1.36.1. Permitir a cópia dos dados de backup de máquinas virtuais da nuvem para áreas de armazenamento *on-premise*;
 - 1.36.2. Permitir a cópia dos dados de backup de máquinas virtuais do ambiente on-premise (VMware e Hyper-V) para a nuvem.
- 1.37. 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.
- 1.38. 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.
- 1.39. Deve possuir habilidade para definir prioridades de servidores dentro de um *job* de backup.
- 1.40. 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:
 - 1.40.1. Data e hora da operação.
 - 1.40.2. Usuário que realizou a operação.
 - 1.40.3. Operação realizada.

- 1.41. Suportar a geração de relatórios gráficos customizáveis de atividades de backup/recovery, contendo:
 - 1.41.1. Horário de início e término dos *jobs*;
 - 1.41.2. Tempo de duração dos *jobs*;
 - 1.41.3. Todos os *jobs* em execução;
 - 1.41.4. Status (situação) de execução dos *jobs*;
 - 1.41.5. Relação e porcentagem de *jobs* executados por status, como por exemplo: com sucesso e com falhas;
 - 1.41.6. *Logs* dos *jobs*;
 - 1.41.7. Volume de dados na origem e no destino, total e por *job*, por período de tempo, por localidade e por *host* (físico ou virtual);
 - 1.41.8. Tendência de crescimento;
 - 1.41.9. Dados históricos de, no mínimo, 24 (vinte e quatro) meses;
- 1.42. Deve permitir a exportação dos relatórios nos formatos HTML, CSV ou PDF.
- 1.43. 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.
- 1.44. Deve possibilitar, por meios de *logs* e alertas, a análise de causa raiz de problemas de backup/recovery.
- 1.45. Os Softwares devem ser entregues com suas respectivas capacitações e transferências de conhecimento.
- 1.46. A solução deve ser capaz de realizar testes automatizados de *restore*, quando configurados.

2. Requisitos dos serviços de instalação para os itens

- 2.1. As atividades de instalação deverão ser realizadas dentro do horário comercial.
- 2.2. 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.
- 2.3. Todo o processo de instalação e configuração realizado deverá ser documentado pela CONTRATADA sob a forma de relatório.
- 2.4. 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, caso necessário.
- 2.5. 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.
- 2.6. 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.
- 2.7. 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.
- 2.8. Deverão ser habilitadas todas as licenças que porventura sejam adquiridas e recursos do equipamento que serão utilizados no projeto.