

Ao
Governo do Distrito Federal
Secretaria de Estado de Economia do Distrito Federal

Pregão Eletrônico nº 028/2021 - COLIC/SCG/SECONT/SEEC-DF
Processo nº 00040-00028133/2020-53

Objeto: Sistema de Registro de Preços para eventual contratação de empresa para fornecimento de atualização de licenciamento do software Commvault Backup & Recovery com suporte técnico por de 36 (Trinta e Seis) meses, e fornecimento de Appliance de Backup de curta retenção com instalação, configuração e Serviços de Assistência Técnica para o Appliance de Backup por 36 (trinta e seis) meses, de acordo com as condições constantes deste instrumento e seus Anexos.

PROPOSTA

A empresa Servix Informática Ltda., inscrita no CNPJ sob o nº 01.134.191/0002-28, estabelecida na SIG, Quadra 04, Lote 125, Bloco A, Salas 01 e 02, Zona Industrial, Brasília – DF, telefone (11) 3525-3400 e e-mail editais@servix.com, neste ato representada pelo seu Sócio – Diretor o Sr. Fabiano Theis Nascimento, portador do documento de identidade RG nº 15.219.699-7, expedido pela SSP/SP, e inscrito no CPF sob o nº 117.670.268-89, apresenta sua proposta para a execução do objeto nas condições que seguem.

GRUPO 01					
Item	Descrição	Quant.	Unidade	Valor Unitário	Valor Total
01	Renovação e aquisição de quantitativo excedente com Suporte técnico do fabricante para o software Commvault Backup & Recovery for Virtualized Environments, Per VM	4.402	Virtual Machine	R\$ 1.815,00	R\$ 7.989.630,00
02	Renovação e aquisição de quantitativo excedente com Suporte técnico do fabricante para o software Commvault Backup & Recovery for Non-Virtual and File, Per Front-End TB	2.461	Front-End Terabyte	R\$ 3.750,00	R\$ 9.228.750,00
03	Aquisição de Appliance de Proteção de Dados de Curta Retenção	2	Und.	R\$ 2.368.845,00	R\$ 4.737.690,00
04	Aquisição de software para Appliance de Proteção de Dados de Curta Retenção.	2	Und.	R\$ 1.001.965,00	R\$ 2.003.930,00
Valor Total				R\$23.960.000,00	

BRASÍLIA

SIG, Quadra 4, Bloco A
Ed. Capital Financial Center - Sala 01-02
Brasília - DF – CEP: 70610-440
T +55 61 3031.2960

servix.com

D4Sign 084cfa61-c575-4029-ae52-ecfbf2ecc073 - Para confirmar as assinaturas acesse <https://secure.d4sign.com.br/verificar>
Documento assinado eletronicamente, conforme MP 2.200-2/01, Art. 10º, §2.

Valor total da proposta: R\$23.960.000,00 (Vinte e três milhões, novecentos e sessenta mil reais).

Nos valores desta proposta estão computados todos os custos necessários para o atendimento do objeto desta licitação, tais como: quantidade de pessoal alocado na execução do contrato, materiais, equipamentos, impostos, encargos trabalhistas, previdenciários, fiscais, comerciais, taxas, seguros, transporte, garantia e quaisquer outros que incidam ou venham a incidir sobre os serviços contratados.

Validade da proposta: 60 (sessenta) dias corridos, contados da data de abertura da licitação.

Declaro que os serviços contratados serão executados nas especificações e condições estabelecidas no edital e seus anexos.

Declaro que não possui, em nossa cadeia produtiva, empregados executando trabalho degradante ou forçado.

A execução dos serviços contratados será iniciada na forma e condições estabelecidas no Termo de Referência.

Brasília, 07 de janeiro de 2025.

fabiano.theis@servix.com

Assinado
FABIANO THEIS
NASCIMENTO
11767026889
D4Sign



Servix Informática Ltda.
Fabiano Theis Nascimento
Sócio-Diretor

PROPOSTA TÉCNICA

7. DOS REQUISITOS DA CONTRATAÇÃO

7.1. A tabela abaixo detalha os itens da contratação, que estão agrupados em grupo único:

Componentes da Solução	
Grupo	Bem/Serviço
1	Item 1 - Renovação e aquisição de quantitativo excedente com Suporte técnico do fabricante para o software Commvault Backup & Recovery for Virtualized Environments, Per VM
	Item 2 - Renovação e aquisição de quantitativo excedente com Suporte técnico do fabricante para o software Commvault Backup & Recovery for Non-Virtual and File, Per Front-End TB
	Item 3 - Aquisição de Appliance de Proteção de Dados de Curta Retenção
	Item 4 - Aquisição de software para Appliance de Proteção de Dados de Curta Retenção

7.2 Requisitos específicos do Item 1 - Renovação e aquisição de quantitativo excedente com Suporte técnico do fabricante para o software Commvault Backup & Recovery for Virtualized Environments, Per VM e Item 2 - Renovação e aquisição de quantitativo excedente com Suporte técnico do fabricante para o software Commvault Backup & Recovery for Non-Virtual and File, Per Front-End TB

7.2.1. A CONTRATADA irá garantir o quantitativo ideal de licenças de backup atualizadas, garantindo o suporte técnico durante toda a vigência do contrato incluindo a proteção contínua dos dados e a confiabilidade de seus serviços de TI para o Governo do Distrito Federal.

7.2.2 A CONTRATADA irá garantir backup/restore e repasse de conhecimento para a equipe técnica da SETIC, bem como, garantir o suporte técnico do fabricante visando uma operação eficiente, segura e resiliente, essencial para o funcionamento adequado da solução de backup.

7.2.3. A abertura de chamados técnicos, será realizada diretamente com o fabricante de software de proteção de dados.

7.2.4. A solução será capaz de proteger um montante 4.402 Máquinas Virtuais em ambientes virtualizados e de 2.461 TB de Front-End para ambientes físicos.

7.2.5. Será capaz de detectar máquinas virtuais novas criadas em jobs e incluí-las automaticamente no Job de Backup.

7.2.6. Permitirá atualização e suporte do fabricante da solução por 36 meses.

7.2.7. A Interface de gerenciamento será acessível a qualquer Sistema Operacional, independente do S.O. que hospeda esse serviço (Windows, Linux); ou ao menos com a separação entre estrutura de backup da Central de Serviços e estrutura de backup das Unidades remotas.

7.2.8 Deverá ser capaz de efetuar download e instalação de atualizações, de forma automática, no servidor de backup e clientes.

7.2.9. Possuirá ambiente de gestão de backup/restore por interface gráfica e linha de comando.

7.2.10. Permitirá a autenticação de usuários por meio do LDAP ao ambiente de gestão de backup/restore.

7.2.11. Será capaz de realizar backup em disco de Storage, fitas magnéticas/bibliotecas de fitas, em Appliance de Backup e em ambiente de nuvem, independente de fabricantes e modelos de equipamentos.

7.2.12. Será capaz de execução de agendamento de jobs de backup, parametrizadas por políticas de Backup. com parâmetros de agendamento e periodicidade de realização, período de retenção das cópias, backup full, diferencial, incremental, com gestão em interface gráfica.

7.2.13. Possuirá uma arquitetura em múltiplas camadas permitindo desempenho e escalabilidade horizontal:

1. Camada de gerência;
2. Camada do serviço de mídia/unidade de disco de retenção dos dados;
3. Camada de clientes/agentes multiplataforma de backups.

7.2.14. Possuirá catálogo ou banco de dados centralizado contendo as informações sobre todos os dados e mídias onde os backups foram armazenados, esse banco de dados ou catálogo será próprio e fornecido em conjunto com o produto.

7.2.15. Possuirá mecanismo de verificação e checagem de consistência da base de dados no intuito de garantir a integridade dos dados.

7.2.16. Possuirá console única de gerenciamento do ambiente de servidores físicos e virtuais.

7.2.17. Possuirá mecanismo de reconstrução do catálogo ou banco de dados centralizado em caso de perda do mesmo, sem a necessidade de recatálogo as imagens de backup.

7.2.18. Suportará servidor e gerência de backup nas plataformas Linux e Windows.

7.2.19. Permitirá a configuração de servidores de gerência de catálogo em cluster para promover a alta disponibilidade dos serviços de gerenciamento. A implementação do cluster será possível para ao menos uma das plataformas a seguir:

1. Red Hat Enterprise Linux;
2. Oracle Linux ou
3. Windows Server.

7.2.20. Permitirá o backup e restore de arquivos abertos, garantindo a integridade do backup.

7.2.21. Será capaz de gerenciar múltiplos e diferentes dispositivos de backup (bibliotecas de fitas, drives de backup, dispositivos de disco com e sem deduplicação), conectados localmente (Direct Attached) ou compartilhados entre múltiplos servidores da camada de mídia via SAN (Storage Area Network).

7.2.22. Possuirá a capacidade de escrever múltiplos fluxos de dados provenientes de servidores distintos (multiplexação), divididos em blocos de tamanhos constantes em um único dispositivo físico de gravação.

7.2.23. Possuirá a capacidade de dividir o fluxo de dados proveniente de um servidor em vários dispositivos de gravação (multiple streams).

7.2.24. Possuirá a capacidade de reiniciar backups e restores a partir do ponto de falha, após a ocorrência da mesma.

7.2.25. Possuirá mecanismo de instalação e atualização de clientes e agentes de backup de forma remota, através da interface de gerenciamento, permitindo a instalação de múltiplos clientes de backup simultaneamente.

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

7.2.27. Permitirá a programação de tarefas de backup automatizadas em que sejam definidos prazos de retenção dos arquivos.

7.2.28. Possuirá função para definição de prioridades de execução de Jobs de backup.

7.2.29. Permitirá a programação de jobs de backup automatizadas em que sejam definidos prazos de retenção das imagens.

7.2.30. Possuirá a função de Backup sintético que permite a criação de uma única imagem de backup a partir de um backup full e qualquer quantidade de backups incrementais. O restore será efetuado da nova imagem full sintética.

7.2.31. Possuirá políticas de ciclo de vida nativas, gerenciar camadas de armazenamento e transferir automaticamente os dados de backup entre camadas através do seu ciclo de vida.

7.2.32. Permitirá a realização do backup completo de servidor para recuperação de desastres.

7.2.33. Permitirá restaurar o backup de recuperação de desastres para hardware diferente do original - para ambiente Windows.

7.2.34. Permitirá o controle da banda de tráfego de rede durante a execução do backup e/ou do restore.

7.2.35. Suportará a proteção dos dados de aplicações de big data Hadoop e AHV (Nutanix Acropolis Hypervisor) e bancos de dados NoSQL (Apache HBase e MongoDB).

7.2.36. Será capaz de recuperar dados para servidores diferentes do equipamento de origem.

7.2.37. Será capaz de utilizar qualquer tecnologia utilizada pela Solução de Armazenamento como destino dos backups seja armazenamento diretamente anexado (DAS), armazenamento em rede NAS ou rede SAN.

7.2.38. Possuirá a função de Disk Staging, ou seja, que permita o envio dos dados para disco e posteriormente do disco para outro tipo de mídia (disco ou fita).

7.2.39. Permitirá que Logical Unit Numbers (LUNs) sejam apresentadas aos servidores da camada de mídia como destino para realização de backups.

7.2.40. Realizará backup e restore de file systems montados em dispositivos Network-Attached Storage (NAS) através do suporte ao protocolo NDMP versão 4 ou superiores.

7.2.41. Permitirá integração do controle de acesso com sistemas de diretório Active Directory ou Open LDAP.

7.2.42. Permitirá a replicação de imagens de um servidor de gerência para outro ambiente, possibilitando a inserção das informações de catálogo da imagem de origem para o catálogo do destino, de forma automática e sem a necessidade de licenciamento adicional.

7.2.43. Implementará monitoramento e administração remotos da solução de backup a partir de qualquer servidor ou estação de trabalho Windows.

7.2.44. A Solução de Backup permitirá operações de Backup e Restore através de rede local (LAN_based e Storage Area Network (SAN_based ou LAN_free).

7.2.45. Permitirá a verificação da integridade do conteúdo das fitas por software.

7.2.46. Permitirá liberação das fitas magnéticas quando todos os arquivos contidos nas mesmas tenham suas datas de retenção expiradas.

7.2.47. As fitas liberadas ficarão disponíveis automaticamente para uso de outras tarefas de backup.

7.2.48. A Solução de Backup irá, a partir de uma única interface, gerenciar operações de Backup e Restore de diferentes sistemas operacionais (clientes), bem como operações de recuperação bare metal.

7.2.49. Permitirá a criação de imagens de servidores físicos, Linux e Windows, para recuperação de desastres (funcionalidade conhecida como bare metal restore de forma nativa, i.e., sem a utilização de software de terceiros).

7.2.50. Para servidores Windows, será possível a recuperação das imagens de recuperação de desastres mesmo em um hardware diferente do original ou em ambiente virtual.

7.2.51. Permitirá a verificação da integridade dos dados armazenados através de algoritmos de checksum e/ou autocorreção.

7.2.52. Permitirá escolher se a criptografia será realizada no agente, com o tráfego de dados via rede já criptografado ou no servidor de backup.

7.2.53. Possuirá capacidade nativa de efetuar criptografia dos backups em no mínimo 256 bits nos Clientes de Backup e em dispositivos de mídia que suportem criptografia.

7.2.54. Possuirá a capacidade de gerenciar software de snapshot de storages de outros fabricantes, tais como Dell EMC, Netapp, HPE, Hitachi, Nutanix e Pure com o intuito de automatizar o processo de agendamento de cópias "snapshot" e montagem no servidor de backup "off-host".

7.2.55. A Solução de Backup irá permitir a integração com a funcionalidade de cópias instantâneas (Snapshot) de subsistemas de armazenamento em disco (storage).

7.2.56. Possuirá integração para gerência de Snapshots.

7.2.57. Permitirá a criação e gerenciamento de Snapshots através da ferramenta de administração da Solução de Backup.

7.2.58. Possibilitará o registro dos Snapshots na base relacional de catálogos da Solução de Backup de forma a possibilitar a realização de buscas.

7.2.59. Controlará o período pelo qual os Snapshots serão válidos, realizando a expiração automática de um Snapshot assim que o período de retenção configurado seja atingido.

7.2.60. Possuirá a funcionalidade de proteção contínua de dados (CDP) para todo o ambiente VMware com no mínimo os seguintes requisitos:

1. Não irá impactar as VMs durante a execução da proteção contínua de dados (CDP);
2. Protegerá continuamente os dados das VMs do ambiente VMware e fornecer replicação de baixo RPO (até 30 minutos) por meio de interface de administração java ou web.

7.2.61. Oferecerá suporte para backup com acelerador para armazenamento baseado em disco de deduplicação, além de restauração de arquivo único sem agente.

7.2.62. Suportará API e RBAC para a proteção contínua dos dados.

7.2.63. Possibilitará enviar notificações, quando configurado, dos eventos por e-mail.

7.2.64. Possuirá a funcionalidade de backup com duplicação dos dados simultânea entre mídias distintas para envio a cofre.

7.2.65. Possuirá mecanismo de auditoria, permitindo a emissão de relatórios onde constem, no mínimo, a data e hora da operação, Usuário que realizou a operação, Ação realizada (em caso de modificação de configurações, informar qual a configuração anterior e a modificação realizada).

7.2.66. Proverá monitoramento via interface gráfica e em tempo real dos Jobs sendo executados, incluindo visão de nível hierárquico dos jobs.

7.2.67. Suportará operações de backup e restore em paralelo.

7.2.68. Permitirá encadear Jobs para que um só comece após outro ter terminado.

7.2.69. Permitirá a orquestração de sistemas virtuais de forma automatizada para recuperação de desastres com no mínimo:

1. Permitirá a recuperação de desastres orquestrada, automatizada e em escala para o próprio data center, ambientes híbridos e multicloud.

2. Permitirá a recuperar sistemas locais na nuvem com visibilidade direta e integrado ao software de backup.

3. Permitirá a recuperação automatizada e orquestrada para solução em nuvem e local com APIs para otimizar o tempo e os recursos.

4. Proverá meios automáticos de garantir a consistência do backup a nível de aplicação, ou seja, será capaz de automatizar a restauração de uma máquina virtual e executar ações de testes previamente programadas para aquela determinada aplicação de forma a garantir que o backup está consistente.

5. Terá a capacidade de testar a consistência do backup, emitindo relatório de auditoria para garantir a capacidade de recuperação seguintes parâmetros: sistema operacional, aplicação e máquina virtual.

7.2.70. Permitirá a recuperação granular de desastres, ou seja, é possível realizar o failover e migração de máquinas virtuais, aplicações individuais, um serviço composto por múltiplos componentes e até mesmo do site inteiro.

7.2.71. Automatizará operações de resiliência incluindo: testes de recuperação/simulação, migrações, failover e failback.

7.2.72. Possuirá funcionalidade para simulação de desastres, ou seja, permitirá a verificação de uma operação de failover para o site secundário sem afetar o ambiente de produção no site principal.

7.2.73. Permitirá a criação de planos de continuidade customizados para execução automatizada de uma sequência de passos para recuperação de desastres.

7.2.74. Permitirá que seja configurado a execução de scripts customizados no plano de continuidade.

7.2.75. Replicará VMs no local para alta disponibilidade ou off-site para disaster recovery.

7.2.76. Suportará a orquestração de failover e failback das máquinas virtuais replicadas.

7.2.77. Permitirá a restauração do ambiente VMWare em grande escala caso o ambiente VMWare de produção tenha sido comprometido.

7.2.78. Permitirá e estará licenciado o envio de dados deduplicados para a nuvem.

7.2.79. Possibilitará a replicação para armazenamento seguro imutável, WORM (Write Once Read Many), com imagens automaticamente prontas para recuperação.

7.2.80. Suportará armazenamento seguro imutável, WORM (Write Once Read Many), para evitar que seus dados sejam criptografados, modificados ou excluídos. E todos os dados salvos nessas instâncias serão protegidos com as seguintes medidas de segurança:

1. Garantirá a funcionalidade WORM (Write Once Read Many) em todos os tipos de dados existentes no ambiente da CONTRATANTE, incluindo ambiente de servidores físicos, virtuais, nuvem e ambiente Oracle;
2. Garantirá a proteção das imagens de backup para que elas sejam somente leitura e não possa ser modificada, corrompida ou criptografada após o backup;
3. Garantirá a propriedade da imagem de backup e não ser possível excluir antes da expiração dos dados;
4. Possuirá e implementará o fator duplo de autenticação - 2FA para o console de administração gráfica e linha de comando por meio do provedor de identidade baseado em SAML ou cartões inteligentes CAC / PIV ou certificados de usuário ou de forma nativa;
5. Possuirá detecção de anomalias próximo a tempo real no site principal à medida que os backups são criados, e através de uso de inteligência artificial para alertar sobre ataques "ransomware" ou outro tipo de ataques cibernéticos, evitando assim que dados comprometidos sejam replicados.

7.2.81. Possuirá mecanismos de proteção contra ransomware, devendo, mas não se limitando a:

1. Suportará imutabilidade de dados para plataforma que utilizem protocolo S3;
2. Deverá possuir detecção de anomalias nos dados em tempo de execução de backup.

7.2.82. Deverá suportar replicação de dados de Backup entre Clouds Públicas e privadas. Todos os recursos necessários de licenciamento serão devidamente fornecidos, de modo a contemplar as funcionalidades de imutabilidade, proteção de dados em nuvem, proteção contra ransomware, detecção de anomalias, e demais funcionalidades descritas no presente termo.

7.2.83. Detecção e alerta sobre mudanças inesperadas nos dados de backup, com no mínimo os seguintes metadados, atributos ou recursos da tarefa de backup:

1. Tamanho da imagem de backup;
2. Número de arquivos de backup;
3. Dados que são transferidos em KB;
4. Taxa de desduplicação;
5. Tempo de conclusão do trabalho de backup;
6. Fará uso de tecnologia de Inteligência Artificial e aprendizagem de máquina para detecção de anomalias.

7.2.84. Possuirá a capacidade de relatar anomalias como um falso positivo através do cálculo de parâmetro com base nos dados históricos disponíveis após uma determinada frequência oferecendo maior flexibilidade e reduzindo a quantidade de falsos positivos.

7.2.85. Qualquer desvio incomum nesses atributos de trabalho de backup será considerado uma possível anomalia notificando por meio de console WEB e REST-API.

7.2.86. Possuirá suporte a backup e restore de máquinas virtuais Vmware 6.5 ou superior através de vStorage API com as seguintes características:

1. Permitirá a recuperação granular de arquivos/aplicações através da execução de um único backup;
2. Permitirá o descobrimento automático das máquinas virtuais nos ambientes VMware, com capacidade de realizar filtros avançados com critérios que incluam pelo menos:
 - Nome da máquina virtual;
 - Sistema Operacional;
 - DataStore (VMware);
 - vApp;
 - vSAN;
 - Tag name.

7.2 87. Suportará VMware CBT para backup incrementais rápidos.

7.2 88. Possuirá a capacidade de balanceamento de carga automática dos backups através de múltiplos backups hosts.

7.2 89. Permitirá restaurar e iniciar a execução de uma máquina virtual instantaneamente, diretamente a partir do seu repositório de backup, sem a necessidade de manter réplicas ou snapshots disponíveis para o processo de recuperação instantânea.

7.2.90. Permitirá realizar restauração, através de um único backup, de Máquina virtual completa ou arquivos de dentro da máquina virtual para ambientes Windows e Linux, sem a necessidade de instalação de agentes nas VMs de origem e destino.

7.2.91. Possuirá a capacidade de restaurar a VM de origem em um ponto no tempo enviando apenas a diferença dos blocos entre a VM de origem e imagem de backup para ambiente VMware através da integração com o VADP.

7.2.92. Permitirá a visualização, monitoração e recuperação de máquinas virtuais através de plugin integrado ao vCenter ou vSphere 6.5 Web Client ou superior.

7.2.93. Possuirá capacidade de realizar backup de maneira off-host, sem a necessidade de instalação de agentes nas máquinas virtuais.

7.2.94. Será possível recuperar uma máquina virtual várias vezes de pontos de recuperação diferentes.

7.2.95. Possuirá a capacidade de realizar backup de maneira Full, Incremental ou Diferencial sem a necessidade de instalação de agentes nas máquinas virtuais.

7.2.96. Suportará ambientes configurados com Cluster Shared Volumes.

7.2.97. Implementará a proteção de dados do ambiente Nutanix AHV nativo na mesma solução e não sendo permitido uma instalação separada para a proteção dos dados do ambiente Nutanix AHV, ou seja, possuirá uma instalação única da solução de proteção de dados para os ambientes físicos, virtuais, Oracle e Nutanix AHV.

7.2 98. Permitirá executar backup ad hoc fora da programação de backup.

7.2 99. Permitirá controlar os recursos AHV do Nutanix durante as operações de backup, controlando o número de backups que podem ser executados em um recurso Nutanix AHV.

7.2.100. Possuirá assistente de recuperação da através de interface java ou web.

7.2.101. Permitirá restaurar todo o AHV VM para o mesmo ou para um cluster AHV diferente.

7.2.102. Permitirá a restauração de arquivos e pastas individuais de AHV VM protegida para qualquer host de destino. O host de destino pode ser uma máquina virtual hospedada em AHV ou outros hipervisores ou até mesmo uma máquina física

7.2.103. Suportará os seguintes bancos de dados, utilizando agente específico:

1. Microsoft SQL Server versões 2012, 2014, 2016, 2017 e 2019;

2. Oracle/Oracle RActive versões 11g, 12c, 18c, 19c e 21c.;

3. Microsoft Exchange 2013, 2016 e 2019;

4. Microsoft Sharepoint 2013, 2016 e 2019;

5. MySQL 5 e 8;

6. PostgreSQL 10, 11, 12, 13, 14, 15 e 16;

7. Microsoft Active Directory.

7.2 104. Possuirá funcionalidade de acesso instantâneo para banco de dados Oracle, diretamente do repositório de backup.

7.2 105. Suportará DAG (DataBase Availability Groups) do MS Exchange.

7.2.106. Suportará backup do Information Store de Microsoft Exchange, com possibilidade de restore granular, ou seja, de e-mails únicos, itens de calendário e também de caixa postal de algum usuário.

7.2.107. Suportará backup do Microsoft Active Directory, com possibilidade de restore granular, ou seja, restauração de todo um diretório, de objetos selecionados e até de atributos individuais.

7.2 108. Suportará backup completo do Sharepoint, com possibilidade de recuperação de uma ou mais databases, documentos individuais, sites, subsites, listas e itens/documentos individuais.

7.2.109. Permitirá o backup e restauração nativamente de aplicativos Kubernetes com no mínimo as seguintes características:

1. Suportará aplicativos Kubernetes integrado com o software de backup;
 2. Permitirá backup e restauração de aplicativos Kubernetes na forma de namespaces;
 3. Configuração do cluster Kubernetes e gerenciamento seguro de credenciais;
 4. Descoberta automática e sob demanda de ativos do Kubernetes;
 5. RBAC na granularidade do cluster e nível de namespace;
 6. Backups baseados em plano de proteção em nível de namespace;
 7. Opções de recuperação versáteis, como namespace completo, um recurso personalizado individual ou um volume persistente individual;
 8. Gerenciamento do ciclo de vida da imagem com retenção e limpeza personalizáveis;
 9. Limitação de recursos por cluster do Kubernetes.
- 7.2.110. Possuirá descoberta inteligente e automática de ativos.
- 7.2.111. Permitirá executar backups baseados em snapshot sem a utilização de agentes.
- 7.2.112. Suportará controle de fluxo de recursos e recuperação de local alternativo.
- 7.2.113. Requisitos de deduplicação por software
- 7.2.114. Possuirá capacidade de realizar deduplicação de dados na camada no cliente, servidor de backup e appliances de deduplicação. A solução permitirá a deduplicação de qualquer capacidade (de acordo com o volume identificado e licenciado) e em qualquer forma de deduplicação (cliente, servidor de backup e appliances) nativamente, não sendo aceitos composições de produtos.
- 7.2.115. Suportará deduplicação de blocos na origem (client-side), de forma que o cliente envie apenas novos blocos de dados criados e/ou modificados a partir do último backup full.
- 7.2.116. Suportará deduplicação de blocos de tamanho fixo ou variável.
- 7.2.117. A solução de backup será capaz de gerenciar a réplica do backup deduplicado entre appliances de deduplicação.
- 7.2.118. Possuirá a capacidade de deduplicação global de dados no nível de segmentos ou blocos de dados repetidos, entre ambientes físicos e virtuais, mesmo em localidades remotas.
- 7.2.119. Permitirá o envio de dados deduplicados para a nuvem.
- 7.2.120. Possuirá algoritmo hash de deduplicação SHA-2.
- 7.2.121. Possuirá a capacidade de deduplicação de dados no nível de segmentos ou blocos de dados repetidos de ambientes Oracle.
- 7.2.122. Suportará deduplicação de blocos na origem (client-side), para ambientes Oracle.
- 7.2.123. Permitirá ativar o recurso de deduplicação em volumes apresentados via SAN, DAS ou iSCSI para servidores Windows e Linux.
- 7.2.124. Possuirá a capacidade de Replicação de Dados entre “pools” de deduplicação de maneira otimizada, enviando somente blocos únicos.
- 7.2.125. Possuirá a capacidade de realizar balanceamento de carga automático entre servidores ou appliances de deduplicação.
- 7.2.126. Possibilitará a distribuição automática de carga entre os servidores que executarão o serviço de proteção de dados, ou seja, os dados oriundos dos clientes de backup serão distribuídos de forma automática entre os servidores de backup da solução. Em caso de falha de um dos servidores de backup, o cliente automaticamente irá encaminhar seus dados através de outro servidor de backup ativo. Esta funcionalidade será nativa do produto, não sendo admitidas soluções baseadas em softwares de cluster de terceiros.
- 7.2.127. Possuirá a capacidade de criptografar os dados armazenados de forma deduplicada.
- 7.2.128. As políticas de ciclo de vida da informação permitirá a replicação das imagens de backup de forma otimizada, fazendo o uso da tecnologia de deduplicação de dados da solução no mesmo site ou entre sites distintos.
- 7.2.129. Fará uso de tecnologia de replicação dos dados (não somente os dados protegidos – imagens de backup – mas também do catálogo do software de backup necessário para a recuperação do dado) do site principal para o site de desastre, de forma que em um evento de desastre, os sites sejam independentes no processo de recuperação.

7.2.130. Possuirá tecnologia de deduplicação de dados inline por padrão.

7.2.131. Permitirá que depois de um backup full inicial, os backups subsequentes sejam feitos apenas através do envio das diferenças deduplicadas e que esses backups sejam consolidados como se fosse um backup full com a última data de envio.

7.2.132. Possuirá a funcionalidade de backup com duplicação dos dados simultânea entre mídias distintas para envio a cofre.

7.2.133. Possuirá a capacidade de proteção da base de hashes de deduplicação com cópia externa.

7.2.134. Possuirá tecnologia de deduplicação de dados, ou seja, não armazenar mais de uma vez dados que sejam duplicados.

7.2.135. A funcionalidade de deduplicação de dados será executada em linha com a ingestão dos dados, ou seja, acontecerá antes dos dados serem gravados nos discos, eliminando a necessidade de armazenamento intermediário para cache dos dados.

7.2.136. A deduplicação será global, ou seja, identificará dados duplicados tanto do mesmo servidor-cliente de origem do backup como outros servidores-cliente armazenados no mesmo Appliance de backup, armazenando na solução somente blocos de dados únicos.

7.2.137. Permitirá o envio de dados deduplicados para a nuvem.

7.2.138. Permitirá suporte à replicação dos dados no formato deduplicado, com controle e atualização do catálogo do aplicativo de backup.

7.2.139. Os repositórios de backup para salvaguarda de dados de longa retenção serão de responsabilidade do CONTRATANTE.

7.2.140. Proverá relatórios gerenciais de backup com no mínimo as seguintes informações:

1. Backups com sucesso;
2. Backups com falha;
3. Volumetria de backup realizado;
4. Restores com sucesso;
5. Restores com falha;
6. Volumetria de restore realizado;
7. Clientes de backup configurados;
8. Ocupação no destino de backup;
9. Licenciamento e capacidade;
10. Interface Web De Gerenciamento.

7.2.141. Possuirá interface web para gerenciamento, monitoramento, emissão de alertas, emissão de relatórios sobre operações de backup e restore e emissão de relatórios, com as seguintes características:

1. Relatórios sobre capacidade e tendência de crescimento do ambiente;
2. Se houver múltiplos ambientes de backup, com independência operacional e localizados em diferentes Data Centers, possuirá nativamente uma única interface web deverá ser capaz de monitorar e agregar informações de diversos Servidores da Camada de Gerenciamento para emissão dos relatórios;
3. Relatórios para verificar o nível de serviço, ou seja, visualização de que aplicações estão com políticas de backup ativadas e executadas periodicamente;
4. Permitirá exportar relatórios;
5. Base de dados de relatórios para suportar armazenamento de dados históricos superior a 30 dias.

7.3. Requisitos específicos do ITEM 3 e 4: Appliance de Backup para curta retenção

7.3.1. Possuirá, no mínimo, 450TB (Quatrocentos e cinquenta Terabytes) de capacidade líquida utilizável, considerando base 2 (1 TB igual a 1024 gigabytes) em Erasure Coding (4+2), sem considerar ganhos com deduplicação e compressão de dados, baseado em discos de no mínimo 16TB HDD ou superiores.

7.3.2. Implantará taxa de ingestão de dados de, no mínimo, 12 TB/hora considerando deduplicação no destino (server-side) ou 90 TB/hora com deduplicação na origem (client-side).

7.3.3 Cada Appliance suportará taxa de ingestão de dados de, no mínimo 50 TB/hora. Será admitida a composição de até dois equipamentos do mesmo modelo e versão, visando atingir a taxa de ingestão.

7.3.4. Caso a solução a ser ofertada faça uso de servidores para movimentação de dados, estes serão entregues junto com a solução.

7.3.5. Será novo, sem uso e constar no site do fabricante como homologado e suportado pelo software de proteção de dados, garantindo total integração entre o hardware e o software de Backup, a fim de manter o desempenho e estabilidade desejada do ambiente.

7.3.6. Permitirá a utilização de todas as funcionalidades, tecnologias e recursos especificados, de maneira perpétua, irrestrita e sem necessidade de licenciamentos ou ônus adicionais.

7.3.7. Será composto, de processamento, portas de conectividade e armazenamento integrado, dedicado única e exclusivamente, à execução das atividades ingestão, desduplicação e replicação dos dados.

7.3.8. Possuirá interface de administração GUI e CLI.

7.3.9. Possuirá mecanismo de proteção dos dados armazenados, seja através de RAID (Redundant Array of Independent Disks) ou Erasure Coding de forma a suportar a falha simultânea de no mínimo dois discos quaisquer, sem interrupção do serviço. A solução será dimensionada e configurada para suportar a perda de qualquer componente sem impacto para o serviço.

7.3.10. Possuirá discos Hot Spare para o appliance e gavetas de expansão de disco da solução, sem necessidade de intervenção prévia manual.

7.3.11. Permitirá a substituição dos componentes redundantes sem interrupção do serviço (hot swapping).

7.3.12. Possuirá ao menos 512GB de memória RAM, permitindo expansão de memória RAM. Não serão aceitas como memória a utilização de tecnologias Flash, SSD ou qualquer outra tecnologia de extensão de cache.

7.3.13. Permitirá expansão à no mínimo 600 TB (seiscentos Terabytes) de capacidade utilizável considerando base 2 (1 TB igual a 1024 gigabytes), apenas com adição de nós, sem considerar ganhos com desduplicação e compressão de dados.

7.3.14. Possuirá no mínimo: 4 (quatro) portas 1GbE (um gigabit ethernet), 4 (quatro) portas 10GbE SFP (dez gigabits ethernet fibra) e 4 (quatro) portas de 16Gb FC (Fibre Channel) para interconexão e integração com os servidores clientes, com garantia de conexão com a estrutura de rede da SEEC, por meio de cabos fibra multimodo GBICS de 1GbE (um gigabit ethernet), cabos fibra multimodo GBICS de 10GbE SFP (dez gigabits ethernet fibra), cabos com especificação de multimodo FC GBICS de 16Gb FC (Fibre Channel), de forma a atender a seguinte composição de portas por site:

1. 3x 1Gbps (RJ45?) para gerencia;
2. 12x 10 Gbps (SPF+) para dados/backend;
3. 6x SAN 16 Gbps para fita.

7.3.15. A replicação de dados de backup entre appliances ocorrerá através de otimizador WAN embutido para economia de largura de banda do link.

7.3.16. Possibilitará a replicação dos dados em disco para outro servidor ou outro dispositivo de mesma natureza. A replicação será assíncrona e ocorrer em horário pré-determinado.

7.3.17. Possuirá licença para replicação dos dados armazenados no dispositivo de armazenamento para outro dispositivo de mesma natureza em formato desduplicados.

7.3.18. Os componentes de FAN e power supply serão redundantes.

7.3.19. O produto do backup estará disponível para restauração diretamente no RMAN, utilizando os dados disponíveis no disco do appliance.

7.3.20. Permitirá que a os dados copiados diretamente do RMAN sejam duplicados em cópias complementares para fita, disco com ou sem desduplicação.

7.3.21. Permitirá replicar os dados através de rede IP (WAN/LAN).

7.3.22. Suportará os protocolos IPv4 e IPv6.

7.3.23. Possuirá autosuporte do tipo call home para seus componentes de hardware e software, tais como: CPU, disco, fonte, ventiladores, temperatura, capacidade de utilização, firmware, entre outros.

7.3.24. Permitirá sua instalação em rack padrão 19”.

7.3.25. Possuirá alimentação elétrica por fontes internas ao equipamento, redundantes e hot-swappable, com faixa de operação de tensão de entrada compreendida, no mínimo, entre 200V a 240V, monofásica (P+N+T), com seleção automática ou manual por meio de chave seletora de tensão, devendo obedecer ao padrão IEC 320 C13-C14 ou similar que utilize plugues no padrão C14.

7.3.26. Proverá software de gerenciamento, administração e configuração do sistema de forma local ou remota., que permitam também a análise de desempenho e implementação das políticas de segurança física, lógica, e de acesso de usuários.

7.3.27. Possuirá todos os acessórios necessários para a plena configuração, operacionalização, utilização e gerenciamento do equipamento, sem necessidade de aquisições futuras de licenças ou softwares de ativação.

7.3.28. Os softwares, drives e firmwares necessários estarão em suas últimas versões.

7.3.29. Não serão aceitas soluções compostas por componentes de fabricantes diferentes.

7.3.30. Sobre a deduplicação

7.3.31. Possuirá tecnologia de deduplicação de dados, ou seja, não armazenar mais de uma vez dados que sejam duplicados.

7.3.32. A deduplicação segmentará automaticamente os dados em blocos de tamanho fixo ou variável.

7.3.33. A funcionalidade de deduplicação de dados será executada em linha com a ingestão dos dados, ou seja, acontecerá antes dos dados serem gravados nos discos, eliminando a necessidade de armazenamento intermediário para cache dos dados.

7.3.34. A deduplicação será global, ou seja, identificará dados duplicados tanto do mesmo servidor-cliente de origem do backup como outros servidores-cliente armazenados no mesmo appliance de backup, armazenando na solução somente blocos de dados únicos.

7.3.35. Permitirá o envio de dados deduplicados para a nuvem.

7.3.36. Permitirá suporte à replicação dos dados no formato deduplicado, com controle e atualização do catálogo do aplicativo de backup.

7.3.37. Os repositórios de backup para salvaguarda de dados de longa retenção serão de responsabilidade do CONTRATANTE.

7.3.38. Serão aceitos somente hardwares compatíveis e homologados pelo fabricante de software de proteção de dados. As especificações técnicas como processador, memória RAM, discos, etc. seguirão as melhores práticas conforme demonstrado na documentação oficial de arquitetura de referência.

7.3.39. Sobre os serviços de garantia e suporte técnico para o Appliance de Backup

7.3.39.1. Prazo da garantia e suporte: 36 (trinta e seis) meses.

7.3.39.2. Será prestada assistência técnica aos equipamentos fornecidos, sem custo adicional, no período de vigência da garantia.

7.3.39.3. Os serviços serão prestados pela CONTRATADA ou por representante indicada pela CONTRATADA ou pelo fabricante da solução, sem prejuízo a responsabilidade integral da CONTRATADA quanto ao atendimento dos níveis de serviço.

7.3.39.4. Entende-se por Serviços de assistência técnica para o Appliance de Backup toda atividade do tipo “corretiva” não periódica que variavelmente poderá ocorrer, durante todo o período de vigência. A mesma possui suas causas em falhas e erros no Hardware e trata da correção dos problemas atuais e não iminentes de fabricação dos mesmos. Esta Garantia e Suporte incluem os procedimentos destinados a recolocar em perfeito estado de operação os serviços e produtos ofertados, tais como desinstalação, reconfiguração ou reinstalação decorrente de falhas de fabricação no hardware, fornecimento de peças de reposição, substituição de hardware defeituoso por defeito de fabricação, atualização da versão de drivers e

firmwares, correção de defeitos de fabricação, ajustes e reparos necessários, de acordo com os manuais e as normas técnicas específicas para os recursos utilizados.

7.3.39.5 A CONTRATADA fornecerá e aplicará pacotes de correção oficiais do fabricante, em data e horário a serem definidos pela CONTRATANTE, sempre que forem encontradas falhas de laboratório (bugs) ou falhas comprovadas de segurança em firmware dos aparelhos que integrem os appliances do contrato. O atendimento deste requisito está condicionado a liberação pelo fabricante dos pacotes de correção e/ou novas versões de software.

7.3.39.6. É facultado a CONTRATADA a execução, ao seu planejamento e disponibilidade, de Garantia e Suporte do tipo “preventiva” que pela sua natureza reduza a incidência de problemas que possam gerar Garantia e Suporte do tipo “corretiva”. As manutenções do tipo “preventiva” não podem gerar custos a CONTRATANTE.

7.3.39.7 A manutenção técnica do tipo “corretiva” será realizada sempre que solicitada pelo CONTRATANTE por meio da abertura de chamado técnico diretamente à empresa CONTRATADA (ou a outra informada pela CONTRATADA) via telefone (com número do tipo “0800” caso a Central de Atendimento esteja fora de Brasília-DF) ou Internet ou e-mail ou outra forma de contato.

7.3.39.8. A CONTRATADA disponibilizará a central atendimento 8 horas por dia, 5 dias da semana (de segunda a sexta-feira, exceto feriados) e equipe com conhecimentos sólidos no funcionamento e operação da solução de gestão.

7.3.39.9. Os Serviços de assistência técnica para o Appliance de Backup incluirão:

1. Solução de problemas relativos à indisponibilidade da solução decorrentes de problemas de fabricação e desenvolvimento;
2. Solução de falhas ou defeitos no funcionamento, incluindo a instalação de arquivos para correção dos erros;
3. Esclarecimento de dúvidas sobre o funcionamento e operação da solução;
4. Instalação de novas versões ou atualizações e patches;

7.3.39.10. Os serviços de assistência técnica para o Appliance de Backup disponibilizarão os seguintes tipos de atendimento:

1. Nível I - Atendimento Telefônico (Help Desk): chamados abertos através de ligação telefônica ou e-mail ou outra forma de contato, em regime de 8x5: 8 horas por dia, 5 dias da semana (de segunda a sexta-feira, exceto feriado). Esse serviço deve atender demandas dos usuários referentes ao funcionamento da solução, que decorram de problemas de funcionamento.
2. Nível II - Atendimento Remoto: atendimento remoto de chamados de suporte técnico através de tecnologia disponibilizada pela CONTRATANTE, mediante prévia autorização e seguindo os padrões de segurança da CONTRATANTE, objetivando análise e solução remota dos problemas apresentados.
3. Nível III - Atendimento Presencial (On-Site): atendimentos técnicos realizados nas dependências do CONTRATANTE, através de visita de técnico especializado, com a finalidade de resolver demandas abertas no Help Desk e não solucionadas pelo Atendimento Telefônico e/ou Remoto.

7.3.39.11. Toda Garantia e Suporte serão solicitados inicialmente via Help Desk (Nível I), ficando a transferência do atendimento para o Atendimento Remoto (Nível II) condicionado à autorização da CONTRATANTE.

7.3.39.12. Toda Garantia e Suporte solicitados inicialmente via Help Desk (Nível I), serão transferidos para o Atendimento Presencial (Nível III) quando o atendimento do Help Desk não for suficiente para solução do problema sem a intervenção presencial de um técnico.

7.3.39.13. Os prazos para a prestação dos serviços garantirão a observância ao atendimento do seguinte Acordo de Níveis de Serviços (ANS) e sua SEVERIDADE:

· SEVERIDADE URGENTE – Solução totalmente inoperante.

1. Prazo máximo de início de atendimento de até 08 horas úteis contadas a partir do horário de abertura do chamado.
2. Prazo máximo de resolução do problema de até 48 horas úteis contadas a partir do início do atendimento.

- SEVERIDADE IMPORTANTE – Solução parcialmente inoperante – Necessidade de suporte na solução com a necessidade de interrupção de funcionamento da solução.

1. Prazo máximo de início de atendimento de até 24 horas úteis contadas a partir do horário de abertura do chamado.

2. Prazo máximo de resolução do problema de até 72 horas úteis contadas a partir do início do atendimento.

- SEVERIDADE NORMAL – Solução não inoperante, mas com problema de funcionamento – Necessidade de suporte na solução sem a necessidade de interrupção de funcionamento da solução.

1. Prazo máximo de início de atendimento de até 24 horas úteis contadas a partir do horário de abertura do chamado.

2. Prazo máximo de resolução do problema de até 96 horas úteis contadas a partir do início do atendimento.

- SEVERIDADE EXTERNA – Solução inoperante, de forma parcial ou total, fruto de falha de elemento de hardware e/ou software não fornecido pela CONTRATADA.

1. Neste caso, ficam suspensos todos os prazos de atendimento até que a CONTRATANTE resolva os problemas externos que provocam a inoperância da solução. Após a CONTRATANTE disponibilizar o ambiente de forma estável para a reativação da solução, a CONTRATADA realizará avaliação da extensão do dano a solução e as partes definirão em comum acordo o prazo para a reativação da solução.

- SEVERIDADE INFORMAÇÃO – Solicitações de informações diversas ou dúvidas sobre a solução.

1. Prazo máximo de resposta de até 10 dias úteis, contados a partir da data de abertura da ocorrência

2. Um chamado técnico somente poderá ser fechado após a confirmação do responsável da CONTRATANTE e o término de atendimento dar-se-á com a disponibilidade do recurso para uso em perfeitas condições de funcionamento no local onde o mesmo está instalado.

3. Na abertura de chamados técnicos, serão fornecidas informações, como Número de série (quando aplicável), anormalidade observada, nome do responsável pela solicitação do serviço e versão do software utilizada e severidade do chamado.

4. A severidade do chamado poderá ser reavaliada quando verificado que a mesma foi erroneamente aplicada, passando a contar no momento da reavaliação os novos prazos de atendimento e solução.

5. A CONTRATADA poderá solicitar a prorrogação de qualquer dos prazos para conclusão de atendimentos de chamados, desde que o faça antes do seu vencimento e devidamente justificado.

6. No caso de necessidade de substituição integral do equipamento, a CONTRATADA deve realizar a troca da unidade com defeito em até 45 dias.

Proposta Comercial e Técnica Ajustada pdf

Código do documento 084cfa61-c575-4029-ae52-ecfbf2ecc073



Assinaturas



FABIANO THEIS NASCIMENTO:11767026889

Certificado Digital

fabiano.theis@servix.com

Assinou

Eventos do documento

07 Jan 2025, 11:30:47

Documento 084cfa61-c575-4029-ae52-ecfbf2ecc073 **criado** por JEFFERSON MATOS SILVA (13d0a009-9190-4be7-8f54-fe0c81a20280). Email:jefferson.matos@servix.com. - DATE_ATOM: 2025-01-07T11:30:47-03:00

07 Jan 2025, 11:34:10

Assinaturas **iniciadas** por JEFFERSON MATOS SILVA (13d0a009-9190-4be7-8f54-fe0c81a20280). Email: jefferson.matos@servix.com. - DATE_ATOM: 2025-01-07T11:34:10-03:00

07 Jan 2025, 11:35:03

ASSINATURA COM CERTIFICADO DIGITAL ICP-BRASIL - FABIANO THEIS NASCIMENTO:11767026889 **Assinou**
Email: fabiano.theis@servix.com. IP: 187.11.122.18 (187-11-122-18.dsl.telesp.net.br porta: 6028). Dados do Certificado: CN=FABIANO THEIS NASCIMENTO:11767026889, OU=(em branco), OU=RFB e-CPF A1, OU=Secretaria da Receita Federal do Brasil - RFB, OU=23087030000182, OU=VideoConferencia, O=ICP-Brasil, C=BR. - DATE_ATOM: 2025-01-07T11:35:03-03:00

Hash do documento original

(SHA256):25f602915367bf697d24c0ca54e082927de65f5d316e777f180a81ef4c824189

(SHA512):e8b08d807ffa4c91eb05b3af719976c4c0880bc50cf481a09861a2d14d10766e4a95e8078b591dfdd734bb96784037f49d23889d9d6deec127108f4ebc9a6bee

Esse log pertence **única e exclusivamente** aos documentos de HASH acima

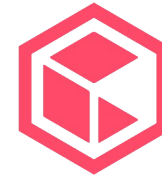


Esse documento está assinado e certificado pela D4Sign

Integridade certificada no padrão ICP-BRASIL

Assinaturas eletrônicas e físicas têm igual validade legal, conforme **MP 2.200-2/2001** e **Lei 14.063/2020**.

COMMVAULT®



Certificate of Completion

This is to certify that

Douglas Barros

*has completed
the course*

Professional Advanced 11.26.2 Self-Paced eLearning

Completion Date

10/11/2023


Joseph C. Ilvento, Chief Learning Officer



Commvault Solutions Architect

ISSUED TO

Douglas Barros



Issued on: 11 JUL 2022 | Issued by: Commvault
Verify: <https://www.credly.com/go/MepqjdUx>