

## ANEXO I - ESPECIFICAÇÕES TÉCNICAS

A. Todos os requisitos especificados, independentemente do verbo utilizado, deverão estar disponíveis e completamente funcionais, exceto quando explicitamente mencionado o contrário.

B. A CONTRATANTE reserva-se o direito de diligenciar, após apresentação da proposta, o fornecedor e/ou fabricante para comprovação das informações prestadas na proposta.

C. Parceiros de solução de Backup do Fabricante Veeam podem valer-se do licenciamento perpétuo da CGU, que atualmente conta com 270 licenças do *tipo Veeam Availability Suite Perpetual Universal License*, desde que a solução ofertada seja compatível com todos os requisitos descritos nesta Especificação Técnica.

D. A solução ofertada para atendimento dos itens 1 a 6 deverá pertencer ao mesmo Fabricante de software. Não serão aceitas composições de softwares de fabricantes distintos para o atendimento das especificações técnicas deste edital.

E. 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.

F. A licitante deverá apresentar, para os requisitos descritos em 1.1, 5.1 e seus subitens, comprovação de que a solução proposta atende aos requisitos. A comprovação deverá ser feita por meio da indicação de documentação pública e oficial do fabricante (eletrônica ou impressa) e da numeração da página (ou localização no texto) onde a equipe técnica da CGU possa confirmar tais argumentos. Na Tabela 1, deverá ser especificado um documento para cada ÍNDICE, e na coluna COMPROVAÇÃO, dos requisitos com esta exigência, deverá ser especificado o ÍNDICE do documento da Tabela 1 e a NUMERAÇÃO DA PÁGINA (ou localização no texto do documento) para comprovação.

**Tabela 1**

ÍNDICE	DOCUMENTO (anexo impresso ou sítio da internet)
A	
B	
C	
D	
E	
F	
G	

H	
I	
J	

G. A solução ofertada deve atender a todos os requisitos técnicos descritos abaixo:

SUBITEM	REQUISITOS DA SOLUÇÃO DE BACKUP/RECOVERY PARA MÁQUINAS VIRTUAIS / BKP ON-PREMISES	COMPROVAÇÃO (ÍNDICE E PÁGINA)
1.1.	<b>Compatibilidade</b> A solução de <i>software</i> de <i>backup/recovery</i> deverá:	
1.1.1.	Ser compatível nativamente com todos os ambientes de virtualização abaixo:	
1.1.1.1.	<i>VMWare VCenter Server Appliance (VCSA)</i> e <i>VSphere Esxi</i> versões 8 e versões superiores.	
1.1.1.2.	<i>Microsoft Hyper-V 2019 R2 Standalone</i> e versões superiores.	
1.1.1.3	Nutanix AHV (Acropolis Hypervisor) versão 6.5 e superiores	
1.1.1.4.	Nuvem da <i>Amazon Web Services (AWS) EC2</i> e <i>Microsoft Azure VM</i> .	
1.1.2.	Ser compatível nativamente com todas as aplicações abaixo:	
1.1.2.1.	<i>Microsoft Active Directory 2019 R2</i> e versões superiores.	

1.1.2.2.	<i>Microsoft Exchange 2019 e versões superiores.</i>	
1.1.2.3.	<i>Microsoft FileServer FailoverCluster 2016 e versões superiores.</i>	
1.1.2.4.	<i>Microsoft SQL Server 2016 e versões superiores.</i>	
1.1.3.	Suportar, nos clientes de <i>backup/recovery</i> , os sistemas operacionais:	
1.1.3.1.	<i>Microsoft Windows Server 2012 R2 e versões superiores.</i>	
1.1.3.2.	<i>Centos Linux 7 e versões superiores.</i>	
1.1.3.2.1.	Para Centos Linux versão 7.x, será aceito backup da forma tradicional a nível de sistema de arquivos.	
1.1.4.	Suportar, nos clientes para <i>backup/recovery</i> , os sistemas de arquivos do tipo: <i>EXT3, EXT4, NTFS, XFS, ReFS.</i>	
1.1.5.	Suportar, nos clientes de <i>backup/recovery</i> , o <i>backup</i> de partições de rede montadas no sistema operacional com o protocolo NFS ( <i>Network File System</i> ).	
1.1.6.	Possuir compatibilidade, declarada pelo seu fabricante (no <i>website</i> ou por carta do fabricante), com os seguintes equipamentos de armazenamento:	
1.1.6.1	Storage Dell Powerstore 5200T.	
1.1.6.2	Storage Hitachi Vantara VSP E590.	
1.1.6.3	Fitoteca: IBM TS4300.	
1.1.7.	Deverá suportar armazenamento de backups em Object Storage, sendo compatível com Amazon S3 e Microsoft Azure Blob Storage. Deverá também possibilitar a restauração granular de dados contidos nos backups armazenados nesses repositórios.	

1.1.8.	Deverá suportar armazenamento de backups em Object Storage nas camadas de arquivamento (frias), incluindo Amazon S3 Glacier e Microsoft Azure Archive Storage.	
1.2.	<b>ARQUITETURA</b> A solução de <i>software</i> de <i>backup/recovery</i> nativamente, sem aplicativos de terceiros e execução de scripts, deverá:	
1.2.1.	Permitir a instalação de quantos servidores de mídia e de gerenciamento de backup forem necessários para a configuração do ambiente da CONTRATANTE, seguindo as melhores práticas propostas pelo fabricante, sem custo adicional.	
1.2.2.	Suportar compressão e deduplicação, com as seguintes características:	
1.2.2.1.	Suportar deduplicação a nível de blocos.	
1.2.2.2.	Suportar deduplicação em volumes apresentados através de DAS ( <i>Direct Attached Storage</i> ), SAN ( <i>Storage Area Network</i> ) e em compartilhamento de rede NAS, via protocolos SMB e NFS.	
1.2.2.3.	Suportar deduplicação de dados no servidor de armazenamento ( <i>target deduplication</i> ), de forma que o servidor de backup descarte blocos repetidos de clientes, evitando assim o armazenamento de blocos redundantes.	
1.2.2.4.	Suportar deduplicação de dados na origem ( <i>source deduplication</i> ), de forma que sejam enviados apenas novos blocos de dados criados e/ou modificados a partir da última cópia de segurança.	
1.2.2.5.	Permitir replicação de dados entre pools de deduplicação de maneira otimizada, replicando somente blocos únicos.	
1.2.3.	Suportar a Criptografia dos dados, com as seguintes características:	
1.2.3.1.	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 ( <i>Local Area Network</i> ) ou WAN ( <i>Wide Area Network</i> ).	

1.2.3.2.	Criptografia de dados no destino (servidor de <i>backup</i> ).	
1.2.3.3.	Módulo nativo de criptografia AES ( <i>Advanced Encryption Standard</i> ) 256 bits.	
1.2.3.4.	Deve suportar criptografia em trânsito (in Flight) visando proteger o conteúdo do backup durante o transporte dos dados.	
1.2.4.	Possuir suporte aos protocolos de rede IPv4 e IPv6 para rotinas de <i>backup/recovery</i> .	
1.2.5.	A solução deve suportar o backup de dados de dispositivos de <i>Storage NAS (Network Attached Storage)</i> via protocolo NDMP ( <i>Network Data Management Protocol</i> ).	
1.2.6.	Suportar qualquer tecnologia utilizada na infraestrutura de armazenamento como destino do <i>backup</i> – DAS, NAS e SAN, sem prejuízos das demais funcionalidades suportadas pelo <i>software</i> .	
1.2.7.	Paralelizar a gravação de dados de um cliente de backup em diferentes caminhos pertencentes à vários dispositivos de armazenamento (funcionalidade conhecida como <i>multistreaming</i> ).	
1.2.8.	Permitir a gravação serial e simultânea de vários <i>streams</i> de backup, provenientes de clientes distintos, em um único caminho pertencente à um dispositivo de armazenamento (funcionalidade conhecida como multiplexação).	
1.2.9.	Possibilidade de exportar o conteúdo de backup para mídia removível, possibilitando o transporte físico de dados até o destino.	
1.2.9.	Ser flexível e escalável, permitindo sua instalação, configuração e uso em sites remotos interligados ao site principal através da WAN ou através de LAN.	
1.2.10.1.	Suportar a replicação dos dados de backup armazenados em disco e fita para diversos sites remotos, permitindo ainda que a restauração dos dados seja feita através das cópias armazenadas remotamente.	

1.2.10.1.1.	Possibilidade de replicação de uma origem para múltiplos destinos.	
1.2.10.1.2.	Possibilidade de replicação e consolidação de dados de múltiplas origens para um destino central.	
1.2.10.1.3.	Possibilidade de aplicar diferentes políticas de retenção de dados nos repositórios de origem e destino durante o processo de replicação.	
1.2.10.1.4.	Permitir o controle da banda de dados utilizada para a replicação dos dados de backup.	
1.2.10.1.5.	Possibilidade de retomar a replicação do ponto onde a mesma foi interrompida, para casos de perda de comunicação entre origem e destino.	
1.2.10.2.	Prover recursos de deduplicação e compressão tanto no site principal como nos sites remotos.	
1.2.10.3.	Nos sites remotos:	
1.2.10.3.1.	Ser gerenciada através da mesma console única do site principal.	
1.2.10.3.2.	Suportar o armazenamento local de dados.	
1.2.10.3.3.	Suportar deduplicação de blocos localmente, de forma que o cliente ou servidor de proxy envie, em LAN e WAN, apenas os blocos de dados modificados para o site principal.	
1.2.11.	Para backups em fitas:	
1.2.11.1.	Permitir a movimentação de dados entre fitas.	
1.2.11.2.	Suportar meios de otimização do consumo de fita, através do agrupamento de dados que estão espalhados em diversas fitas com baixa porcentagem de utilização, movendo esses dados para uma nova fita ou através de políticas que garantam uma melhor consolidação de backups e permitam a cópia dos backups deduplicados e comprimidos para a fita, sem a necessidade de reidratação dos dados.	

1.2.11.3.	Deverá permitir cópias adicionais do backup principal com funcionalidade de clonagem de fitas.	
1.2.12.	Promover meios de recuperação rápida dos dados de catálogo e índices do servidor de backup em caso de perda ou corrompimento destas informações.	
1.3.	<b>FUNCIONALIDADES</b> A solução de software de <i>backup/recovery</i> nativamente, sem aplicativos de terceiros e sem a execução de scripts, deverá:	
1.3.1.	Possibilitar o <i>backup</i> e a restauração das informações em disco e fita.	
1.3.1.1.	Suportar as operações de <i>backup</i> e restauração em paralelo.	
1.3.1.2.	Localizar um arquivo para restauração pelo nome, pesquisando no catálogo da ferramenta.	
1.3.2.	Possuir a capacidade de efetuar <i>backup</i> para disco e fita com retenções, através de políticas pré-definidas e agendadas.	
1.3.2.1.	Para um dado armazenado deve haver a possibilidade de alterar o período de retenção.	
1.3.2.2.	Permitir a política de retenção GFS ( <i>Granfather-Father-Son</i> ) para <i>archives</i> de periodicidade: mensal e anual.	
1.3.3.	Possuir a função de <i>Disk Staging</i> , visando permitir a gravação de dados em disco e, posteriormente, do disco para outro tipo de mídia (disco e fita).	
1.3.3.1.	Possuir políticas de ciclo de vida das camadas de armazenamento (disco e fita) responsáveis por transferir automaticamente os dados de backup entre as camadas através do seu ciclo de vida de forma temporal ou por utilização de espaço de armazenamento.	
1.3.4.	Suportar os métodos de <i>backup</i> : <i>Full</i> e <i>Incremental</i> .	

1.3.4.1.	No método <i>Incremental</i> , suportar modo <i>Incremental Forever</i> , ou seja, o backup deve consistir em apenas de um <i>backup Full</i> e todos os demais incrementais até o término do período de retenção.	
1.3.4.2.	Suportar a funcionalidade de <i>Synthetic Full Backup</i> , que permite a consolidação de um novo <i>backup Full</i> a partir dos backups já existentes ( <i>Full</i> inicial + incrementais), sem a necessidade de executar no cliente um novo <i>backup Full</i> .	
1.3.4.3.	Permitir a geração de cópias de longa retenção <i>full</i> , tanto no modo ativo - executando um novo <i>backup Full no cliente</i> - quanto no modo sintético - utilizando os <i>backups</i> já salvos anteriormente.	
1.3.4.4.	Permitir atribuir uma política de retenção para estas cópias.	
1.3.4.5.	Permitir o agendamento para geração automática destas cópias.	
1.3.5.	Possibilitar verificação e checagem automática da consistência do <i>backup</i> , no intuito de garantir a integridade dos dados.	
1.3.6.	A solução de backup deverá prover mecanismos que garantam a imutabilidade dos dados de backup no armazenamento, impedindo sua exclusão ou modificação, inclusive por administradores, durante o período de retenção.	
1.3.6.1.	Essa proteção poderá ser implementada por meio de funcionalidades de software (como Ransomware Protection, Compliance Lock, entre outras) ou por integração com recursos nativos do armazenamento (como object lock, WORM, ou snapshots imutáveis).	
1.3.7	Deverá suportar a análise dos dados de backup e determinar se existe algum comprometimento por malware ou ransomware	
1.4.	<p style="text-align: center;"><b>INTEGRAÇÃO</b></p> <p>A solução de software de <i>backup/recovery</i> nativamente, sem aplicativos de terceiros e sem a necessidade de criação de <i>scripts</i>, deverá:</p>	



1.4.1.	Permitir a integração nativa com o <i>Microsoft Exchange 2019 on- premises</i> (local) e versões superiores.	
1.4.1.1.	Suportar a arquitetura DAG ( <i>Database Availability Group</i> ) do <i>Exchange</i> .	
1.4.1.2.	Permitir a restauração granular a nível de mensagem direto na caixa de correio do usuário.	
1.4.1.3.	Permitir a recuperação da mensagem em um momento do tempo específico.	
1.4.1.4.	Gerar logs com as informações: o que foi restaurado, quem restaurou e para onde foi restaurado.	
1.4.2.	Permitir a integração com o <i>Microsoft SQL Server 2016</i> e versões superiores.	
1.4.2.1.	Executar <i>backup/recovery</i> de bases de dados do <i>SQL Server</i> de forma “online”, ou seja, sem a parada do banco.	
1.4.2.2.	Executar <i>backup</i> de <i>logs</i> transacionais, possibilitando a criação de rotina de backup para que ocorra em intervalos mínimos de 1 (uma) hora.	
1.4.2.3.	Permitir a configuração que após o <i>backup</i> dos <i>logs</i> transacionais os mesmos sejam mantidos ou deletados.	
1.4.2.4.	Permitir a recuperação granular a nível individual de Banco de dados, no mesmo servidor e em servidor remoto.	
1.4.2.5.	Permitir a recuperação do Banco de dados em um momento de tempo específico.	
1.4.3.	Permitir a integração com <i>Microsoft Active Directory 2019 R2</i> e versões superiores.	

1.4.3.1.	Permitir a restauração granular a nível de objeto, por exemplo, objetos de usuário.	
1.4.4.	Permitir a integração com <i>Microsoft Windows FileServer FailoverCluster 2016</i> e versões superiores.	
1.4.4.1.	Deve integrar-se à tecnologia <i>VSS (Volume Shadowcopy Service)</i> do <i>Windows</i> para realizar cópias e assegurar a consistência de qualquer aplicação que disponha de um <i>VSS Writer</i> em estado funcional, quando da execução do backup.	
1.4.4.2.	Permitir a recuperação do Arquivo em um momento de tempo específico.	
1.4.5.	Permitir a integração com ambiente virtual <i>VMWare VCenter Server Appliance 8</i> e superiores e deverá executar <i>backup/recovery</i> com as seguintes características:	
1.4.5.1.	Permitir a conexão com o <i>VCenter</i> e a exploração (descoberta) automática das máquinas virtuais.	
1.4.5.2.	Realizar o <i>backup/recovery</i> de Máquinas Virtual sem a necessidade de instalação de agente.	
1.4.5.3.	Realizar o armazenamento de <i>backup</i> das Máquinas Virtuais de maneira desduplicada.	
1.4.5.3.1.	Ser compatível com a funcionalidade <i>VMWare VSphere CBT (Changed Block Tracking)</i> , ou seja, em vez de verificar todo o arquivo <i>VMFS (Virtual Machine File System)</i> deverá consultar a <i>API (Application Programming Interface)</i> do <i>VMWare</i> para descobrir somente os blocos que foram alterados desde o último backup.	
1.4.5.4.	Permitir a inclusão automática de máquinas virtuais sem <i>backup</i> em seleções de <i>backup</i> anteriores.	
1.4.5.5.	Permitir o <i>backup</i> das Máquinas Virtuais através de <i>Snapshot</i> executados diretamente nos <i>Storages</i> especificados no subitem 1.1.6.1,	

	1.1.6.2.	
1.4.5.6.	Realizar a restauração da imagem completa da Máquina Virtual dentro do VMWare.	
1.4.5.7.	Permitir redirecionar a restauração de uma da Máquina Virtual para uma pasta, <i>datastore</i> , hospedeiro ou rede alternativos.	
1.4.5.7.1.	Ser capaz e iniciar a execução da Máquina Virtual diretamente a partir do seu arquivo de <i>backup</i> , sem a necessidade de esperar o término do processo de restauração.	
1.4.5.8.	Realizar a restauração granular a nível de arquivos dentro sistema operacional cliente, sem a necessidade de se restaurar a Máquina Virtual inteira.	
1.4.5.9.	Permitir a instanciação sob demanda de uma ou mais Máquinas Virtuais, que estejam salvas em <i>backup</i> , em ambiente virtual de laboratório com as seguintes características:	
1.4.5.9.1.	Manter todas as configurações originais de rede das Máquinas Virtuais sem ocasionar nenhum conflito com o ambiente de produção, ou seja, deverá ser um ambiente de rede isolado.	
1.4.5.9.2.	Permitir a comunicação de rede entre as Máquinas Virtuais dentro deste ambiente isolado.	
1.4.5.9.3.	A solução deverá prover automaticamente uma Máquina Virtual com a função de proxy de rede, que permita a configuração de uma comunicação da rede isolada com o ambiente de rede de produção de uma forma segura.	
1.4.5.9.4.	Prover meios automáticos de garantir a consistência do <i>backup</i> a nível de aplicação, ou seja, ser 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 <i>backup</i> está consistente.	

1.4.5.10.	Suportar <i>jobs</i> simultâneos para backup de Máquinas Virtuais.	
1.4.6.	Permitir a integração com os ambientes virtuais Microsoft Hyper-V 2019 R2 Standalone e versões superiores, Nutanix 6.5 e versões superiores, possibilitando a execução de backup/recovery com as seguintes características:	
1.4.6.1.	Permitir a conexão com o hospedeiro (Hyper-V e Nutanix) e a exploração (descoberta) automática das máquinas virtuais.	
1.4.6.2.	Realizar o backup/recovery de Máquinas Virtual sem a necessidade de instalação de agente.	
1.4.6.3.	Realizar o armazenamento de backup das Máquinas Virtuais de maneira desduplicada.	
1.4.6.4.	Realizar a restauração da imagem completa da Máquina Virtual dentro do mesmo ou de outro Hospedeiro do virtualizador.	
1.4.6.5.	Realizar a restauração granular a nível de arquivos dentro sistema operacional, sem a necessidade de se restaurar a Máquina Virtual inteira.	
1.4.7.	Permitir a integração com a <i>nuvem AWS EC2</i> e deverá executar <i>backup/recovery</i> com as seguintes características:	
1.4.7.1.	Permitir o <i>backup/restore</i> de Máquinas Virtuais na AWS para áreas de armazenamento AWS S3.	
1.4.7.2.	Permitir o direcionamento dos dados de <i>backup</i> de Máquinas Virtuais da nuvem para áreas de armazenamento <i>on-premises</i> da CGU.	
1.4.7.3.	Permitir a restauração do backup de Máquinas Virtuais, criadas no ambiente <i>on-premises</i> a partir do <i>VMWare</i> e <i>Hyper-V</i> , direto na a AWS EC2.	
1.4.7.4.	Permitir a movimentação dos dados de <i>backup</i> do ambiente <i>on- premises</i> da CGU para áreas de armazenamento na AWS.	

1.5.	<b>DO GERENCIAMENTO E CONFIGURAÇÃO</b> O software de <i>backup/recovery</i> deverá:	
1.5.1.	Possuir módulo de gerenciamento central com interface gráfica (ou web) e linha de comando (interface CLI) responsáveis pela administração de todas as operações de <i>backup/recovery</i> , configurações, gerenciamento, monitoração, criação/atualização de políticas do ambiente e rotinas associadas à proteção de dados de todos os sites.	
1.5.2.	Suportar a instalação do módulo de gerenciamento e da base de dados do catálogo de metadados nos sistemas operacionais Microsoft Windows ou Linux.	
1.5.3.	Possuir gerenciamento das operações da infraestrutura de backup em modo gráfico, que permita o monitoramento em tempo real das rotinas de <i>backup/recovery</i> e status dos dispositivos e clientes de todo o ambiente.	
1.5.4.	Possuir <i>dashboards</i> com suporte a visualização de todas as rotinas de <i>backup/recovery</i> , com opções de gerar relatórios on-line e envio por e-mail.	
1.5.5.	Permitir que as tarefas abaixo sejam realizadas pela interface gráfica central, sem a necessidade de scripts e sem a necessidade de acessar a interface do cliente:	
1.5.5.1.	Instalar e aplicar <i>patches/upgrades</i> de agentes remotamente.	
1.5.5.2.	Configurar backup de clientes de forma remota, ou seja, toda a configuração do backup que o cliente irá executar deve ser feita na própria console central, sem a necessidade de ter que configurar localmente o cliente.	
1.5.5.3.	Executar a restauração de backup de forma remota, ou seja, na console central seleciona-se o <i>backup</i> , com as integrações descritas no subitem 1.4., e para onde será realizada a restauração remota.	

1.5.6.	Suportar em uma mesma operação ( <i>schedule</i> ) de <i>backup</i> a implementação de diferentes clientes e tipos de integração, podendo ser utilizada a agregação de duas ou mais tarefas ( <i>jobs</i> ) ou funcionalidade equivalente.	
1.5.7.	Possuir habilidade para definir prioridades de servidores dentro de um <i>job</i> de <i>backup</i> .	
1.5.8.	Possuir recursos avançados de agendamento de rotinas de backup, para datas específicas, dias da semana recorrentes, dia do mês recorrente. Primeiro, segundo terceiro e último dia do mês. Ser capaz de filtrar por mês e dia da semana.	
1.5.9.	Possuir agendamento de rotinas de backup, sem a utilização de utilitários de agendamento de servidores. O agendamento deve ser controlado pelo gerenciador de <i>backup/recovery</i> .	
1.5.10.	Prover integração com <i>Microsoft Active Directory (AD) 2019</i> e versões superiores para autenticação da Console de Gerência.	
1.5.10.1.	Suportar a criação de perfis de usuários/grupos do AD com diferentes níveis de acesso à interface de gerenciamento para as atividades de administração e operação do <i>software</i> .	
1.5.11.	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:	
1.5.11.1.	Data e hora da operação.	
1.5.11.2.	Usuário que realizou a operação.	
1.5.11.3.	Operação realizada.	
1.5.12.	O software de backup deve incluir o recurso de dupla aprovação, exigindo a autenticação e autorização de um segundo usuário administrador para concluir a alteração/exclusão de parâmetros críticos.	

1.5.13.	Permitir o envio automático de alertas por e-mail e SNMP ( <i>Simple Network Management Protocol</i> ) através de <i>traps</i> ou consultas, com o objetivo de reportar eventos ocorridos nas operações do software de <i>backup/recovery</i> .	
1.5.14.	A solução deve oferecer notificações sobre problemas, bem como sobre realização de backups, por meio de logs, e-mail e mensagens na console.	
1.6.	<b>RELATÓRIOS E MONITORAMENTOS</b> O software de <i>backup/recovery</i> deverá, nativamente, ser capaz de emitir relatórios com informações completas, conforme subitens:	
1.6.1.	Permitir acesso aos relatórios através de interface gráfica ou web.	
1.6.2.	Suportar a geração de relatórios gráficos customizáveis de atividades de <i>backup/recovery</i> , contendo:	
1.6.2.1.	Horário de início e término dos <i>jobs</i> ;	
1.6.2.2.	Tempo de duração dos <i>jobs</i> ;	
1.6.2.3.	Todos os <i>jobs</i> em execução;	
1.6.2.4.	Status (situação) de execução dos <i>jobs</i> ;	
1.6.2.5.	Relação e porcentagem de <i>jobs</i> executados por status, como por exemplo: com sucesso e com falhas;	
1.6.2.6.	Logs dos <i>jobs</i> ;	
1.6.2.7.	Volume de dados na origem e no destino, total e por <i>job</i> , por período, por localidade e por host (físico ou virtual);	
1.6.2.8.	Tendência de crescimento;	
1.6.2.9.	Dados históricos de, no mínimo, 24 (vinte e quatro) meses.	

1.6.2.10.	Relatórios sobre o consumo de licenças;	
1.6.3.	Suportar a geração de relatórios gráficos customizáveis de atividades de backups, contendo:	
1.6.3.1.	Identificação da ocupação nos destinos de backups: espaço utilizado em disco e quantidade de fitas ocupadas;	
1.6.3.2.	Porcentagem de ganhos com redução de dados.	
1.6.4.	Suportar a geração de relatórios gráficos customizáveis de atividades de <i>backups</i> , contendo contexto de:	
1.6.4.1.	Aplicativos;	
1.6.4.2.	Domínios de armazenamento;	
1.6.4.3.	Janela de <i>backup</i> .	
1.6.5.	Permitir a geração de relatórios baseados na utilização de recursos, identificando restrições associadas a aplicativos específicos.	
1.6.6.	Permitir a geração de relatórios baseados em alertas pré-definidos, com o objetivo de reportar eventos ocorridos do ambiente operacional de <i>backup/recovery</i> .	
1.6.7.	Permitir a exportação dos relatórios nos formatos html, csv ou pdf.	
1.6.8.	Prover monitoramento, através de interface gráfica ou web, em tempo real, de <i>jobs</i> sendo executados.	
1.6.9.	Possibilitar, por meios de logs e alertas, a análise de causa raiz de problemas de <i>backup/recovery</i> .	



SUBITEM	REQUISITOS DE LICENCIAMENTO - BACKUP ON-PREMISES
2.1.	<b>DISPOSIÇÕES GERAIS</b> A solução de software de <i>backup/recovery</i> deverá:
2.1.1.	Prover licenciamento para até 350 (trezentos e cinquenta) Máquinas Virtuais.
2.1.2.	Prover licenciamento de <i>software</i> perpétuo, ou seja, não poderá perder nenhuma funcionalidade operacional e não poderão ser cobrados quaisquer valores adicionais pelo seu uso completo - durante e após o término do CONTRATO.
2.1.3.	Prover licenciamento de software sem qualquer limite de volumetria de armazenamento em terabytes (TB), seja no backend ou frontend, para todos os componentes da solução, durante e após o término do contrato.
2.1.3.1	Nos casos de backup diretamente de NAS e de máquinas físicas, a solução deverá contemplar licenciamento suficiente para, no mínimo, 20TB de dados para cada uma dessas modalidades.
2.1.4.	Prover licenciamento para o ambiente virtual contabilizando apenas o número de Máquinas Virtuais que fazem backup, independentemente das suas especificações de hardware ( <i>sockets</i> , memória, disco, etc.), da localização física ou lógica do host de execução (DF, regionais ou nuvem), e em qualquer ambiente de virtualização descrito no Anexo I.
2.1.5.	A licença deverá estar em uso apenas enquanto estiver executando o backup da Máquina Virtual.
2.1.6.	Se a Máquina Virtual for desassociada da política de execução de backup, a licença deverá estar livre para uso em qualquer outra nova Máquina Virtual do ambiente de virtualização descrito no Anexo I.
2.1.7.	No caso do subitem anterior, os dados de <i>backup</i> da Máquina Virtual antiga e da nova deverão permanecer disponíveis para restauração até o término de suas respectivas políticas de retenção.
2.1.8.	Caso seja necessário a instalação de algum agente da solução de software por causa de alguma peculiaridade da Máquina Virtual, por exemplo, por causa de discos RDM ou de suas aplicações, conforme subitem 1.4. do Anexo I, todos os agentes deverão estar incluídos neste licenciamento, sem nenhum tipo de cobrança adicional para a CONTRATANTE.

2.1.9.	Todas as máquinas virtuais necessárias para o funcionamento da solução deverão estar contabilizadas no licenciamento provido pela solução, não sendo debitada das quantidades contratadas.
2.1.10.	Prover licenciamento que englobe todas as funcionalidades e requisitos elencados neste Termo de Referência, independentemente de qualquer quantidade de utilização do referido serviço, sem nenhum tipo de cobrança adicional para a CONTRATANTE.
2.1.11.	O licenciamento e os softwares deverão estar registrados em nome da CONTRATANTE.
2.1.12.	A solução ofertada deve incluir todos os produtos na versão estável mais recente, não sendo aceitos produtos obsoletos ou fora de linha de produção.
2.1.13.	A solução ofertada não deve ser do tipo comunidade, software livre, nem possuir componentes ou módulos sem suporte oficial do fabricante.
2.1.14.	O detalhamento dos termos e condições requeridos para prestação do serviço de suporte estão descritos no Anexo II.

SUBITEM	REQUISITOS PARA O SERVIÇO DE IMPLANTAÇÃO / BACKUP ON-PREMISES
3.1.	<p style="text-align: center;"><b>DISPOSIÇÕES GERAIS</b></p> <p>Serviço consiste na instalação e configuração de todos os componentes adquiridos</p>
3.1.1.	A CONTRATANTE fornecerá ambiente físico e virtualizado para a execução dos componentes de software fornecidos, seguindo recomendações de dimensionamento indicadas pelo fabricante, com os seguintes detalhes:
3.1.1.1.	2 (duas) máquinas físicas no DF podendo ser Windows 2016 (ou superior) ou Centos 7 (ou superior), com acesso via SAN a 2 (duas) Fitotecas IBM TS4300 localizadas uma no edifício Sede e outra no Bloco-A.
3.1.1.2.	Espaço em Storage NL-SAS para área de staging de dados em disco.
3.1.1.2.1.	O Storage não possui deduplicação de hardware, toda a deduplicação deverá ser executada pelo software.
3.1.1.3.	Máquinas Virtuais para instalação dos módulos do software Windows 2016 (ou superior) ou Centos 7 (ou superior) no ambiente de virtualização VMWare 8 em Brasília/DF.

3.1.1.4.	01 (uma) Máquina Virtual Windows 2016 (ou superior) ou Centos 7 (ou superior) no ambiente de virtualização Microsoft Hyper-V 2019 R2 em cada Regional para função de proxy, se necessário.
3.1.2.	Todas as máquinas necessárias para o funcionamento da solução deverão estar contabilizadas no licenciamento provido pela solução, não sendo debitada das quantidades contratadas.
3.1.3.	Qualquer necessidade de licenciamento de banco de dados para o funcionamento da solução de backup, durante todo o período do contrato, deverá ser fornecida pela contratada, sem nenhum ônus adicional para a CONTRATANTE.
3.1.4.	A CONTRATADA deverá fazer a instalação e configuração do novo backup em todos os clientes do ambiente e de acordo com a política de backup fornecida pela CONTRATANTE.
3.1.5.	A migração de um cliente para nova solução deverá ser executada em uma janela de até 24 (vinte e quatro) horas, ou seja, a diferença máxima entre a última execução do backup na solução antiga e o primeiro backup da solução nova deverá ser de até 24 (vinte e quatro) horas.
3.1.6.	As atividades serão realizadas remotamente em horário comercial, ficando a cargo da CONTRATADA fornecer um meio seguro para o acesso.
3.1.7.	O serviço de implantação deverá ser executado por profissional(ais) com experiência e certificação no produto ou por profissionais do próprio fabricante da solução.
3.1.7.1.	A experiência será comprovada por Declaração ou Atestado de Capacidade Técnico Operacional, conforme modelo do ANEXO VI – MODELO DE ATESTADO DE CAPACIDADE TÉCNICA, fornecido por pessoa jurídica de direito público ou privado, que comprove que o profissional ou a empresa prestou, satisfatoriamente, serviços de instalação e configuração, compatíveis com o objeto da presente licitação, contendo informações que permitam estabelecer, por proximidade de características técnicas, comparação entre o objeto deste Edital e o serviço prestado.
3.1.5.2.	Deverá ser entregue comprovação da capacitação e experiência em até 10 (dez) dias úteis antes do início da execução do serviço.
3.2.	<b>PLANO DE IMPLANTAÇÃO</b>
3.2.1.	Deve ser entregue pela CONTRATADA em até 15 (quinze) dias úteis após a Assinatura do Contrato.
3.2.2.	Deve prever cronograma com todas as tarefas de implantação, suas dependências e os

	seus responsáveis, não podendo este cronograma superar um prazo de 20 (vinte) dias úteis.
3.2.3.	Deve prever diagrama de arquitetura, demonstrando os componentes da solução e os relacionamentos entre eles.
3.2.4.	Deve contemplar a elaboração de Plano de Testes.
3.2.5.	Deve contemplar, no mínimo, os seguintes aspectos:
3.2.5.1.	Lista completa dos requisitos necessários para implantação da solução no ambiente da CONTRATANTE.
3.2.5.2.	Plano de Instalação e configuração de todos os servidores (principais e proxies) e conexões de rede LAN, SAN e WAN necessários, para contemplar a arquitetura do backup da CGU na Sede (DF), Bloco-A (DF) e Regionais (demais estados).
3.2.5.3.	Plano de Implementação da política de <i>Backup</i> , entregue pela CONTRATANTE, com as suas retenções e os clientes a que pertencem a cada uma delas.
3.2.5.4.	<i>Sizing</i> (dimensionamento) em TB da área de armazenamento (em cada nível, disco e fita) necessário para implementação do <i>backup</i> de acordo com o tamanho do ambiente e a política de <i>backup</i> definidas pela CONTRATANTE.
3.2.5.5.	Definição da política de <i>staging</i> de forma a acomodar devidamente as políticas de retenção da CONTRATANTE.
3.2.5.6.	Plano de implantação para a nova solução de <i>backup/recovery</i> do <i>Microsoft Active Directory</i> .
3.2.5.7.	Plano de migração para a nova solução de <i>backup/recovery</i> de Máquinas Virtuais do <i>VMWare</i> .
3.2.5.8.	Plano de <i>backup/recovery</i> de Máquinas Virtuais na nuvem da AWS.
3.2.5.8.	Plano de implantação de <i>backup</i> de <i>Storage NAS</i> através do protocolo NDMP.
3.2.5.10.	Plano de migração para a nova solução de <i>backup/recovery</i> do <i>Microsoft Exchange</i> .
3.2.5.11.	Plano de migração para a nova solução de <i>backup/recovery</i> de Bancos de Dados <i>Microsoft SQL Server</i> .
3.2.5.12.	Plano de migração para a nova solução de <i>backup/recovery</i> de FileServers no Hyper-V (nas Unidades Regionais) e no Microsoft Failover Cluster em disco RDM no VMWare (na Sede).

3.2.5.13.	Plano de migração para a nova solução de <i>backup/recovery</i> no site de DR.
3.2.14.	Plano de monitoramento com os principais itens a serem monitorados em toda arquitetura da solução.
3.2.5.15.	Atualização de <i>softwares</i> para a versão mais recente que seja considerada estável pelo fabricante.
3.2.5.16.	Orientações e sugestões de eventuais ajustes nos equipamentos da CGU que serão integrados à solução, de acordo de melhores práticas.

SUBITEM	REQUISITOS PARA O SERVIÇO DE REPASSE DE CONHECIMENTO / BACKUP ON-PREMISES E BACKUP DO MICROSOFT 365
4.1.	DISPOSIÇÕES GERAIS
4.1.2.	O serviço de Repasse de Conhecimento deve ser realizado no modo online, com abordagem prática voltada a todos os requisitos funcionais da solução contratada.
4.1.3.	O processo de Repasse de Conhecimentos deverá ser ministrado de forma a garantir que todos os conhecimentos necessários para operação, gerência e manutenção da solução sejam ministrados com a carga horária adequada.
4.1.4.	Deverá ser ministrado em até 30 (trinta) dias úteis após a Assinatura do Contrato.
4.1.4.1.	A critério da CONTRATANTE, essa data pode ser adiada.
4.1.5.	O curso deverá ser ministrado para 1 turma, composta por 04 (quatro) alunos oficiais e até 4 (quatro) alunos na condição de ouvintes.
4.1.7.	O horário para a realização do curso deverá ser aprovado previamente pela CONTRATANTE devendo ser, preferencialmente, realizado entre 08 e 18 hr.
4.1.8.	Caso necessário, o material didático, meios audiovisuais e toda infraestrutura física necessária para realização do curso serão providos pela CONTRATADA.
4.1.9.	Deverá ser do tipo hands-on com conteúdo teórico e laboratórios práticos para assimilação do conteúdo. Devendo contemplar o uso prático da solução e o desenvolvimento de estudos de caso.
4.1.10.	O curso deverá ser ministrado em língua portuguesa.
4.1.11.	A CONTRATANTE não assumirá os custos de licenças e/ou softwares extras, assim como outros custos relativos a esta capacitação. Todos os custos devem ser previstos

	pela CONTRATADA da solução na elaboração de suas propostas.
4.1.12.	Ao término do processo de Repasse de Conhecimentos, a CONTRATADA deverá realizar uma avaliação de satisfação em relação ao curso, como conteúdo, instalações, material didático e de aplicação à prática profissional, bem como do(s) instrutor(es).
4.1.12.1.	Esta avaliação utilizará modelo fornecido pela CONTRATANTE – ANEXO III do Termo de Referência.
4.1.12.2.	Caso o curso seja considerado insatisfatório, a CONTRATADA deverá realizar um novo Repasse de Conhecimentos, com a finalidade de atender as demandas não supridas inicialmente.
4.1.3.	Um relatório contendo a avaliação de satisfação dos alunos deverá ser enviado à CONTRATANTE.
<b>4.2.</b>	<b>DO INSTRUTOR</b>
4.2.1.	Deve ser executado por profissional(ais) com experiência e certificação oficial do fabricante na solução ofertada.
4.2.1.1.	A comprovação de experiência e certificação do(s) profissional(ais) deverá ser entregue em até 10 (dez) dias úteis antes do início do Repasse de Conhecimento.
<b>4.3.</b>	<b>DOS TÓPICOS A SEREM ABORDADOS (Backup On-premises)</b>
4.3.1.	Arquitetura da Solução de backup/recovery.
4.3.2.	Apresentação das funcionalidades através da console central de gerenciamento.
4.3.3.	Operações básicas de backup/recovery.
4.3.4.	Desduplicação e compressão.
4.3.5.	Backups remotos e replicação.
4.3.6.	Estratégias de Disaster /Recovery.
4.3.7.	Backup/Recovery Exchange.
4.3.8.	Backup/Recovery Active Directory.
4.3.9.	Backup/Recovery Microsoft SQL Server.
4.3.10.	Backup/Recovery VMWare.
4.3.11.	Backup/Recovery Microsoft Hyper-V.

4.3.12.	Backup/Recovery na AWS EC2 com S3 e Glacier.
4.3.13.	Montagem de Ambiente virtual de laboratório a partir de backups de máquinas virtuais.
4.3.4.	Relatórios de compliance do backup do ambiente.
4.3.5.	Monitoramento da solução.
<b>4.4.</b>	<b>DOS TÓPICOS A SEREM ABORDADOS (Backup Microsoft 365)</b>
4.4.1.	Arquitetura da solução de backup para ambientes Microsoft 365.
4.4.2.	Integração com o Entra ID (Azure AD) e autenticação segura (OAuth/MFA).
4.4.3.	Backup/Recovery do Exchange Online (e-mails, calendários, contatos, etc.).
4.4.4.	Backup/Recovery do SharePoint Online.
4.4.5.	Backup/Recovery do OneDrive for Business.
4.4.6.	Backup/Recovery do Microsoft Teams (incluindo chats, canais, arquivos e wikis).
4.4.7.	Retenção e recuperação granular de itens (e-mail individual, arquivo, site, etc.).
4.4.8.	Políticas de retenção, exclusão e conformidade.
4.4.9.	Relatórios de compliance e auditoria.
4.4.10.	Console de gerenciamento centralizado para ambiente Microsoft 365.
4.4.11.	Monitoramento, alertas e notificações específicas para o backup Microsoft 365.

## SOLUÇÃO DE BACKUP/RECOVERY PARA MICROSOFT 365

SUBITEM	REQUISITOS DA SOLUÇÃO DE BACKUP/RECOVERY PARA MICROSOFT 365	COMPROVAÇÃO (ÍNDICE E PÁGINA)
<b>5.1.</b>	<b>LICENCIAMENTO E MODELO DE SERVIÇO</b>	
5.1.1.	A solução proposta deverá ser capaz de fazer backup e recuperar dados no Microsoft 365, sendo o licenciamento para até 3200 (três mil e duzentos) usuários.	
5.1.2.	O licenciamento e os softwares deverão estar registrados em nome da CONTRATANTE.	

5.1.3.	A solução ofertada deve incluir todos os produtos na versão estável mais recente, não sendo aceitos produtos obsoletos ou fora de linha de produção.	
5.1.4.	A solução ofertada não deve ser do tipo comunidade, software livre, nem possuir componentes ou módulos sem suporte oficial do fabricante.	
5.1.5.	Para fins de licenciamento, deverão ser considerados apenas os usuários ativos e com licença atribuída no Microsoft 365. Contas que não exigem licenciamento no Microsoft 365 — como Shared Mailbox, Room Mailbox e GroupMailbox — não deverão ser contabilizadas para fins de licenciamento da solução de backup, mas deverão ser incluídas na proteção oferecida pela solução.	
5.1.6.	O licenciamento da solução ofertada não deverá impor restrições quanto à volumetria de armazenamento, seja em front-end ou back-end.	
5.1.7.	O licenciamento de software deve ser baseado em assinatura ou subscrição, devendo todas as funcionalidades solicitadas estarem operacionais e disponíveis durante toda a vigência do CONTRATO. Não poderão ser cobrados quaisquer valores adicionais para a recuperação dos dados já protegidos, durante e após o término do CONTRATO.	
5.1.8.	A CONTRATADA deverá disponibilizar para a CGU acesso ao site oficial do fabricante da solução, possibilitando o gerenciamento das licenças adquiridas, acesso a base de conhecimento, fórum de discussão, documentações técnicas e abertura de chamados.	
5.1.10.	Não deve haver qualquer tipo de restrição ou limite, imposto pelo licenciamento da solução, com relação à quantidade de dados que poderão sofrer backup ou restauração por dia, semana, mês ou ano.	
5.1.11.	Deverão ser informados na proposta todos os part numbers de software e serviços que compõem a solução ofertada. O modelo ofertado deve estar em linha de produção, na data de entrega da proposta.	
5.1.12.	O detalhamento dos termos e condições requeridos para prestação do serviço de suporte estão descritos no Anexo II.	



<b>5.2.</b>	<b>ARQUITETURA DA SOLUÇÃO</b>	
5.2.1.	O FABRICANTE será responsável pelo pleno funcionamento da “Infraestrutura Tecnológica” onde se encontrará hospedada a solução, devendo se responsabilizar por envidar todos os esforços necessários para garantir a disponibilidade, integridade e segurança do ambiente.	
5.2.2.	A solução deverá ser oferecida no modelo SaaS (Software como Serviço), não necessitando de nenhuma infraestrutura local ou IaaS (Infraestrutura como Serviço) para seu pleno funcionamento.	
5.2.3.	Deverá suportar salvaguardar os dados em Cloud.	
5.2.4.	Deverá ser realizado, no mínimo, uma cópia de segurança dos dados em datacenter seguro, de forma a garantir os dados em caso de desastre.	
5.2.5.	Deverá possuir um SLA do tipo 3, ou seja, 99,9% de tempo de atividade, garantindo a disponibilidade e integridade de todos os dados armazenados.	
5.2.6.	Deverá ser comprovada, através de documentações oficiais, a segurança física e lógica dos data centers, assim como a garantia da privacidade dos dados.	
5.2.7.	A CGU poderá solicitar, a qualquer tempo, a comprovação por parte da CONTRATADA que os dados estão sendo mantidos em ambiente seguro.	
5.2.8.	A CONTRATADA deverá permitir a exportação e o expurgo total dos dados armazenados em seu ambiente, possibilitando que a CGU possa transferir via rede (internet) ou copiar (via dispositivo físico) seus dados para um ambiente de sua preferência.	
5.2.9.	Não serão aceitas soluções que simplesmente façam a exportação dos dados no formato PST ou download de pasta arquivos sem manter a consistência das cadeias de backup.	
<b>5.3.</b>	<b>INTEGRAÇÃO E SEGURANÇA</b>	
5.3.1.	Deverá possuir integração com o Entra ID (antigo Azure AD), ou similar de outras clouds públicas.	

5.3.2.	Suportar controle de acesso com single sign-on via AD FS, Entra ID, ou similar de outras clouds públicas.	
5.3.3.	Suportar Single-Tenant Architecture para salvaguarda dos dados de backup da Contratante.	
5.3.4.	Deverá permitir a adição de contas de backup auxiliares da organização, por meio de grupos de segurança pré-configurados do Microsoft 365.	
5.3.5.	Toda comunicação entre a plataforma Microsoft 365, a solução de backup e sua interface deverá ocorrer de forma segura, utilizando protocolos criptografados e autenticação	
5.3.6.	Deverá oferecer criptografia AES de 256 bits para dados armazenados (em repouso) e em trânsito, com suporte a gerenciamento seguro de chaves.	
5.3.7.	Deverá prover segurança de acesso à console com restrição de IPs ou com o uso de duplo fator de autenticação.	
5.3.8.	Deverá ter suporte a autenticação multifator (MFA) para execução segura dos processos de backup e restauração.	
<b>5.4.</b>	<b>FUNCIONALIDADES GERAIS</b>	
5.4.1.	Deverá ser capaz de realizar, de forma integrada e centralizada, o backup e recuperação de dados para, no mínimo, as seguintes funcionalidades do Microsoft 365:	
5.4.1.1.	E-mail: caixa postal inteira, e-mails individuais, arquivos, calendário, contatos, tarefas e caixas postais compartilhadas.	
5.4.1.2.	SharePoint: sites completos e arquivos.	
5.4.1.3.	OneDrive for Business: pastas completas e arquivos.	
5.4.2.	Teams: Equipes, Canais, Posts, arquivos e conversas.	
5.4.2.	Deverá permitir, no mínimo, as seguintes formas de restauração dos dados:	
5.4.2.1.	Recuperação para o local de origem.	
5.4.2.2.	Fazer download dos arquivos.	
5.4.2.3.	Recuperação para novo local.	
5.4.3.	Deverá ter a capacidade de realizar a restauração granular e total dos dados.	

5.4.4.	Deverá ser capaz de executar backups incrementais do Exchange Online, SharePoint Online e OneDrive, reduzindo as janelas de backup do Microsoft 365.	
5.4.5.	Deverá permitir enviar notificações sobre os resultados das tarefas de backup por e-mail ou disponibilizadas em uma central de notificações.	
5.4.6.	Deverá ter a capacidade de recuperar uma caixa de correio inteira ou selecionar individualmente quaisquer itens e recuperá-los para qualquer caixa de correio existente, ou exportá-los para arquivos .PST ou .EML.	
5.4.7.	Deverá permitir o cadastro de grupos e usuários, possibilitando a associação dos mesmos a diferentes perfis de acesso para administração da solução.	
5.4.8.	Deverá prover controle de acesso baseado em função, sendo possível configurar e controlar os acessos de vários tipos de usuários e perfis.	
5.4.9.	Deverá suportar múltiplas operações nas aplicações que compõem o Microsoft 365, permitindo atividades de backup e restauração simultâneas.	
5.4.10.	Deverá possibilitar a retenção com base na data de criação dos itens em seu local original ou baseadas na data de execução dos backups.	
5.4.11.	Deverá reter as imagens (backup) por todo período de subscrição sem custo adicional.	
5.4.12.	Deverá ser possível aplicar períodos de retenção imutáveis.	
5.4.13.	Deverá suportar RBAC - Role Based Access.	
5.4.14.	Deverá suportar imutabilidade dos dados em cloud Storage.	
5.5.	<b>GERENCIAMENTO E MONITORAMENTO</b>	
5.5.1.	Deverá possuir uma console de gerenciamento acessível via web browser.	
5.5.2.	Deverá múltiplas operações nas aplicações que compõem o Microsoft 365, permitindo atividades de backup e restauração simultâneas.	
5.5.3.	Deverá possuir dashboard para exibição dos resultados dos Jobs de backup executados/em execução.	

5.5.4	Deverá permitir a busca de arquivos a partir de uma interface guiada, sem a necessidade de prévia restauração dos dados.	
5.5.5	Deverá permitir a busca de arquivos, sem a necessidade de saber o seu local ou a hora que foi excluído.	
5.5.6.	Deverá gerar relatórios detalhados sobre:	
5.5.6.1.	Status dos backups realizados, incluindo sucesso, falhas e detalhes de execução.	
5.5.6.2.	Utilização das licenças, permitindo monitoramento do uso das licenças contratadas.	
5.5.6.3.	Estado da proteção das caixas do Microsoft 365, fornecendo visibilidade sobre a integridade e cobertura dos dados.	
5.5.6.4.	visibilidade sobre o consumo de armazenamento.	
5.5.7.	Deverá permitir o envio de alertas por e-mail ou integração com sistemas de monitoramento disponíveis no mercado, via SNMP (Simple Network Management Protocol) ou API (Application Programming Interface).	
5.5.8.	Deverá disponibilizar logs de auditoria para as operações dos usuários realizadas na plataforma com, no mínimo, as seguintes informações:	
5.5.8.1.	b) Arquivos baixados (download);	
5.5.8.2.	c) Arquivos pré-visualizados;	
5.5.8.3.	e) Arquivos recuperados;	
5.5.8.4.	f) Data e horário das atividades.	
5.6.	<b>AGENDAMENTO E POLÍTICAS DE BACKUP</b>	
5.6.1.	Deverá possibilitar a criação de Jobs de backup, permitindo a sua execução por meio de agendamento personalizado ou agendamento fixo (pré-definido), admitindo a inclusão ou exclusão de diferentes objetos de acordo com as necessidades da organização.	
5.6.2.	Para o caso de execução de Jobs de backup com agendamento fixo, a solução deverá suportar, no mínimo, as seguintes periodicidades: a cada 8 (ou 12), 18 e 24 horas.	
5.6.3.	A implementação deve permitir a configuração ou geração de políticas de retenção.	

5.6.4.	Os backups deverão acontecer sem interromper ou comprometer a performance dos serviços presentes no ambiente do Microsoft 365, preservando sempre a integridade dos dados.	
5.6.5.	Deverá adicionar os usuários novos nas políticas de backups programados automaticamente, dentro da quantidade de licenças contratadas.	

SUBITEM	REQUISITOS PARA O SERVIÇO DE IMPLANTAÇÃO DA SOLUÇÃO DE BACKUP/RECOVERY PARA MICROSOFT 365.
<b>6.1.</b>	<b>DISPOSIÇÕES GERAIS</b> Serviço consiste na instalação e configuração de todos os componentes adquiridos.
6.1.1.	O serviço deverá conter a implementação da solução SaaS, incluindo configuração do ambiente para atividades de operação, administração e gerenciamento.
6.1.2.	A solução deverá ser configurada de modo a garantir total operabilidade com o ambiente computacional da CGU e ser otimizada para usufruir das melhores condições em termos de desempenho e disponibilidade.
6.1.3.	A CONTRATADA será responsável pelo fornecimento, instalação e configuração de qualquer equipamento ou software adicional, que julgar necessário, para a devida prestação do Serviço de Implantação da Solução.
6.1.4.	Demais tarefas relacionadas à solução ofertada, que porventura não estejam previstas, mas que sejam necessárias para o seu correto funcionamento, deverão ser executadas pela CONTRATADA, sem custo adicional para a CONTRATANTE.
	O processo de configuração da solução deverá ser acompanhado pela equipe técnica indicada pela CGU.
6.1.5.	As atividades serão realizadas remotamente em horário comercial, ficando a cargo da CONTRATADA fornecer um meio seguro para o acesso.
6.1.6.	O serviço de implantação deverá ser executado por profissional(ais) com experiência e certificação no produto ou por profissionais do próprio fabricante da solução.
6.1.6.1.	A experiência será comprovada por Declaração ou Atestado de Capacidade Técnico Operacional, conforme modelo do ANEXO VI – MODELO DE ATESTADO DE CAPACIDADE TÉCNICA, fornecido por pessoa jurídica de direito público ou privado, que comprove que o profissional ou a empresa prestou, satisfatoriamente, serviços de instalação e configuração, compatíveis com o objeto da presente licitação, contendo informações que permitam estabelecer, por proximidade de características técnicas, comparação entre o objeto deste Edital e o serviço prestado.

6.1.6.2.	Deverá ser entregue comprovação da capacitação e experiência em até 10 (dez) dias úteis antes do início da execução do serviço.
<b>6.2.</b>	<b>DO PLANO DE IMPLANTAÇÃO</b>
6.2.1.	Deverá ser entregue pela CONTRATADA em até 15 (quinze) dias úteis após a Assinatura do Contrato.
6.2.2.	Deverá prever diagrama de arquitetura, demonstrando os componentes da solução e os relacionamentos entre eles.
6.2.3.	Deverá contemplar a elaboração de Plano de Testes.
6.2.4.	Deverá prever cronograma com todas as tarefas de implantação, suas dependências e os seus responsáveis, não podendo este cronograma superar um prazo de 20 (vinte) dias úteis.
6.2.5.	Para configuração da solução de backup, a CONTRATADA deverá executar, no mínimo, as seguintes atividades básicas:
6.2.5.1.	Configuração inicial do ambiente de acordo com as recomendações do fabricante e integração com o tenant 365 da CGU;
6.2.5.2.	Configuração de usuários e integração com Entra ID;
6.2.5.3.	Configuração das políticas de backup;
6.2.5.4.	Configuração das proteções de segurança;
6.2.5.5.	Criar Jobs de backup separados para cada aplicação do pacote Microsoft 365: Exchange, SharePoint, OneDrive e Teams;
6.2.5.6.	Criar políticas de retenção para os diferentes Jobs de backup criados;
6.2.5.7.	Configurar os repositórios para armazenamento dos dados;
6.2.5.8.	Configurar os perfis e os usuários para autenticação na solução;
6.2.5.9.	Configurar e-mails para envio de alertas e relatórios relativos à solução;
6.2.5.10.	Adequar a solução às melhores práticas orientadas pelo fabricante;
6.2.5.11.	Realizar testes de backup e restore de dados;
6.2.5.12.	Validação e entrega da solução junto à equipe técnica da CGU.
6.2.6.	Além das atividades básicas relacionadas acima, a CONTRATADA deverá realizar, junto à CGU, o levantamento detalhado dos requisitos a serem considerados para configuração da solução, que se dará por meio do plano de implantação.



## ANEXO II – SUPORTE TÉCNICO

### DO SUPORTE TÉCNICO

1. Durante a vigência do contrato de suporte referente aos itens 1., 2., 3., e 6. – a CONTRATADA deverá fornecer atendimento técnico de forma remota ou *on-site* (local) observando os parâmetros a seguir:
  - 1.1. Deverão ser providos canais de atendimento do fabricante para que a CONTRATANTE realize diretamente a abertura de chamados por telefone, e-mail ou por *website* na internet disponíveis 24 (vinte e quatro) horas x 07 (sete) dias por semana x 365 (trezentos e sessenta e cinco) dias por ano.
  - 1.2. O atendimento do suporte técnico deverá estar disponível, no mínimo, 12 (doze) horas por dia (8h as 18h), 05 (cinco) dias por semana (de segunda a sexta-feira).
  - 1.3. O suporte técnico deve ser prestado por analistas técnicos do fabricante, que deverão analisar os problemas reportados pela CONTRATANTE e trabalhar para resolvê-los em conjunto com o corpo técnico da CONTRATANTE.
    - 1.3.1. O suporte técnico do fabricante deverá ser prestado em português ou deverá ser oferecido um tradutor.
  - 1.4. Deverá disponibilizar número ilimitado de chamados.
  - 1.5. Deverá estar disponível para possibilidade de acesso remoto no ambiente da CONTRATADA durante a execução do suporte.
  - 1.6. Deverá disponibilizar acesso a todas atualizações do software, correções, atualizações de segurança e novas versões estáveis dos produtos.
  - 1.7. Deverá dar direito a acesso a ferramentas de autosserviço no site do fabricante que permita pesquisa em base de conhecimento do fabricante para diagnóstico e sugestões de solução do problema quando possível.
  - 1.8. A CONTRATADA deverá cumprir prazos máximos para resposta aos acionamentos (Tabela 1), de acordo com o nível de severidade de cada chamado:
    - 1.8.1. **Severidade ALTA:** Esse nível de severidade é aplicado quando a solução de backup/recovery central, regional ou na nuvem se encontra totalmente indisponível. Há uma falha no software que deixe indisponíveis seus



recursos (serviço parado). Há impacto em diversos clientes de backup de serviços de produção que afete operações de backup/recovery críticas da CONTRATANTE.

1.8.2. **Severidade MÉDIA:** Esse nível de severidade é aplicado quando há falha, simultânea ou não, do uso da solução de backup/recovery, quando um dos componentes da solução se encontra parcialmente indisponível ou com degradação de tempo de resposta no acesso ao software, módulos ou recursos.

1.8.3. **Severidade BAIXA:** Esse nível de severidade é aplicado quando a solução de *backup/recovery* se encontra disponível, mas há ocorrência de alarmes, bem como quando é necessário realizar consultas sobre problemas ou dúvidas gerais sobre a solução. A correção pode ser feita de forma agendada, em um momento futuro.

Modalidade de abertura	Evento	Prazos para os níveis de severidade		
		1 – ALTA	2 - MÉDIA	3 – BAIXA
Website, E-mail ou Telefone.	Início de atendimento.	Em até <b>2h</b> após a abertura do chamado.	Em até <b>4h</b> após a abertura do chamado.	Em até <b>24h</b> após a abertura do chamado.
Website, E-mail ou Telefone.	Final de atendimento.	Em até <b>12h</b> úteis após a abertura do chamado.	Em até <b>24h</b> úteis após a abertura do chamado.	-

1.9. Será considerado para efeitos dos níveis exigidos:

1.9.1. **Prazo de início de atendimento:** tempo decorrido entre a abertura do chamado efetuada pela equipe técnica da CGU à CONTRATADA e a primeira tentativa de atendimento feita pelo técnico do Fabricante, respeitando os limites de dias e horários do subitem 1.3.

1.9.2. **Prazo de final de atendimento:** tempo decorrido entre a abertura do chamado efetuada pela equipe técnica da CGU à CONTRATADA e a implantação da solução do problema ou de uma solução de contorno para o problema apresentado, respeitando os limites de dias e horários do subitem 1.2

- 1.10. O nível de severidade será informado pela CONTRATANTE no momento da abertura de cada chamado.
- 1.11. O nível de severidade poderá ser reclassificado a critério da CONTRATANTE. O nível de severidade de um acionamento poderá ser reclassificado no decorrer do atendimento e conforme a disponibilidade de recursos dos módulos e componentes da solução.
- 1.12. Todas as solicitações de suporte técnico devem ser registradas pela CONTRATADA, para acompanhamento e controle da execução do serviço.
- 1.13. A CONTRATADA apresentará à CGU, ao término de cada atendimento, um relatório de atendimento técnico contendo dados sobre a intervenção na solução.
- 1.14. A CONTRATADA também fornecerá atendimento técnico por meio de visitas à sede da CGU, para eventuais demandas que as tentativas por solução remota (por meio de contato telefônico, correio eletrônico ou acesso remoto) não solucionaram o problema. Sempre que demandada neste sentido, a CONTRATADA alocará recursos para atendimento *on-site*, mediante prévio agendamento, para possibilitar a estruturação da visita já com a solução esquematizada. O relatório de visita deverá ser assinado pelo servidor da CONTRATANTE que solicitou o atendimento técnico.

### ANEXO III – MODELO DE AVALIAÇÃO DE TREINAMENTO

Tópicos a serem avaliados	Critérios a serem avaliados	Média de Avaliação por Categoria	Média Geral
Em relação ao curso	Coerência entre o proposto e o realizado	Média das notas igual ou superior a 3.	Média das notas igual ou superior a 3,5.
	Material entregue no primeiro dia de treinamento?		
	Cumprimento do conteúdo programático		
	Aderência dos exercícios de laboratório ao conteúdo proposto		
Em relação ao Material Didático	Conteúdo contempla toda a ementa do Curso	Média das notas igual ou superior a 3.	
	Qualidade de Impressão		
	Clareza		
	Corretude		
	Coerência com a versão da ferramenta/equipamento.		
Em relação ao Instrutor	Clareza e Didática	Média das notas igual ou superior a 3.	
	Estímulo à participação do grupo		
	Esclarecimento de dúvidas		
	Foco na apresentação do tema		
	Administração do tempo previsto		
	Domínio do tema		
Em relação às instalações	POD	Média das notas igual ou superior a 3.	
	Equipamentos Disponibilizados		
	Sala de Aula		

As notas utilizadas no formulário para avaliação de cada critério do curso deverão ser as seguintes:

- 1 - Muito Insatisfeito
- 2 - Insatisfeito
- 3 - Indiferente
- 4 - Satisfeito

## 5 - Muito Satisfeito

Após o recebimento da planilha contendo as notas dos participantes do treinamento, deve-se adotar os seguintes critérios para o cômputo da nota:

- As notas dos ouvintes devem ser descartadas;
- Calcular a média ponderada das notas.
  - Equipes diretamente envolvidas tem peso 2
  - Equipes convidadas, peso 1.
- Quanto às médias:
  - A média de cada um dos grupos (Curso, Material e Instrutor) tem que ser superior a 3;
  - A média geral deve ser superior a 3,5.

## ANEXO IV - MODELO DE TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO

### TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO

CONTRATO Nº \_\_\_\_\_ /201X

A <PESSOA JURÍDICA OU FÍSICA CONTRATADA> doravante referida simplesmente como **CONTRATADA**, inscrita no CNPJ/MF sob o número <NÚMERO DO CNPJ>, com endereço <ENDEREÇO>, neste ato representada pelo <VÍNCULO DO SIGNÁRIO COM A CONTRATADA>, <NOME DO SIGNATÁRIO>, nos termos do <CONTRATO OU TERMO ADITIVO EM QUE FOI PACTUADO O SIGILO>, compromete-se a observar o presente TERMO DE COMPROMISSO, firmado perante a **UNIÃO**, por meio do **CONTROLADORIA-GERAL DA UNIÃO**, doravante referido simplesmente como **CGU**, em conformidade com as cláusulas que seguem:

#### CLÁUSULA PRIMEIRA - DO OBJETO

O objeto deste TERMO DE COMPROMISSO é a necessária e adequada proteção às informações controladas de propriedade exclusiva da CGU fornecidas à CONTRATADA para que possa desenvolver as atividades contempladas especificamente no Contrato nº \_\_\_\_/\_\_\_\_.

**Subcláusula Primeira** - A CONTRATADA reconhece que, em razão da prestação de serviços à CGU, tem acesso a informações que pertencem à CGU, que devem ser tratadas como controladas.

#### CLÁUSULA SEGUNDA - DAS INFORMAÇÕES CONFIDENCIAIS

O termo “informações controladas de propriedade exclusiva da CGU” abrange toda informação, por qualquer modo apresentada ou observada, tangível ou intangível, podendo incluir, mas não se limitando a: técnicas, projetos, especificações, desenhos, cópias, diagramas, fórmulas, modelos, amostras, fluxogramas, croquis, fotografias, plantas, programas de computador, discos, disquetes, pen drives, fitas, contratos, planos de negócios, processos, projetos, conceitos de produto, especificações, amostras de ideia, clientes, nomes de revendedores e/ou distribuidores, preços e custos, definições e informações mercadológicas, invenções e ideias, outras informações técnicas, financeiras ou comerciais, entre outras a que, diretamente ou através de seus empregados, prepostos ou prestadores de serviço, venha a CONTRATADA ter acesso durante ou em razão da execução do contrato celebrado.

**Subcláusula Primeira** - Em caso de dúvida acerca da natureza confidencial de determinada informação, a CONTRATADA deverá mantê-la sob sigilo até que seja

autorizada expressamente pelo representante legal da CGU, referido no Contrato, a tratá-la diferentemente. Em hipótese alguma, a ausência de manifestação expressa da CGU poderá ser interpretada como liberação de qualquer dos compromissos ora assumidos.

### **CLÁUSULA TERCEIRA - DAS OBRIGAÇÕES**

A CONTRATADA compromete-se a não reproduzir nem dar conhecimento a terceiros, sem a anuência formal e expressa da CGU, das informações controladas reveladas.

**Subcláusula Primeira** – As informações de caráter técnico observadas ou informadas durante a execução do contrato que impactem especificamente os produtos ou serviços fornecidos e prestados pela CONTRATADA poderão ser utilizadas por essa para a melhoria de seus produtos, reparos ou mesmo compartilhados com outros clientes sem a necessidade de autorização prévia da CGU. Em nenhum momento o nome da CGU ou outra fonte poderá ser vinculada ou distribuída conjuntamente com a informação dos produtos da CONTRATADA.

**Subcláusula Segunda** - A CONTRATADA compromete-se a não utilizar, bem como a não permitir que seus diretores, consultores, prestadores de serviços, empregados e/ou prepostos utilizem, de forma diversa da prevista no contrato de prestação de serviços à CGU, as informações controladas reveladas.

**Subcláusula Terceira** - A CONTRATADA deverá cuidar para que as informações reveladas fiquem limitadas ao conhecimento dos diretores, consultores, prestadores de serviços, empregados e/ou prepostos que estejam diretamente envolvidos nas discussões, análises, reuniões e demais atividades relativas à prestação de serviços à CGU, devendo cientificá-los da existência deste Termo e da natureza confidencial das informações controladas reveladas.

**Subcláusula Quarta** - A CONTRATADA possuirá ou firmará acordos por escrito com seus diretores, consultores, prestadores de serviços, empregados e/ou prepostos cujos termos sejam suficientes a garantir o cumprimento de todas as disposições do presente Termo.

**Subcláusula Quinta** - A CONTRATADA obriga-se a informar imediatamente à CGU qualquer violação das regras de sigilo estabelecidas neste Termo que tenha tomado conhecimento ou ocorrido por sua ação ou omissão, independentemente da existência de dolo.

### **CLÁUSULA QUARTA - DO DESCUMPRIMENTO**

A quebra do sigilo das informações controladas reveladas, devidamente comprovada, sem autorização expressa da CGU, possibilitará a imediata rescisão de qualquer contrato firmado entre a CGU e a CONTRATADA sem qualquer ônus para a CGU. Nesse caso, a CONTRATADA estará sujeita, por ação ou omissão, ao pagamento ou

recomposição de todas as perdas e danos sofridos pela CGU, inclusive os de ordem moral, bem como as responsabilidades civil e criminal respectivas, as quais serão apuradas em regular processo judicial ou administrativo.

#### **CLÁUSULA QUINTA - DO RETORNO DAS INFORMAÇÕES**

A CONTRATADA devolverá imediatamente à CGU, ao término do Contrato, todo e qualquer material de propriedade desta, inclusive registro de documentos de qualquer natureza que tenham sido criados, usados ou mantidos sob seu controle ou posse, bem como de seus empregados, prepostos ou prestadores de serviço, assumindo o compromisso de não utilizar qualquer informação considerada confidencial, nos termos do presente TERMO DE CONFIDENCIALIDADE, a que teve acesso em decorrência do vínculo contratual com a CGU.

#### **CLÁUSULA SEXTA - DA VIGÊNCIA**

O presente Termo tem natureza irrevogável e irretratável, permanecendo em vigor a partir de sua assinatura e enquanto perdurar a natureza sigilosa ou restrita da informação, inclusive após a cessação da razão que ensejou o acesso à informação.

#### **CLÁUSULA SÉTIMA - DAS DISPOSIÇÕES FINAIS**

Os casos omissos neste TERMO DE COMPROMISSO, assim como as dúvidas surgidas em decorrência da sua execução, serão resolvidos pela CGU.

Por estarem de acordo, a CONTRATADA, por meio de seu representante, firma o presente TERMO DE COMPROMISSO, lavrando em duas vias de igual teor e forma.

Brasília, DF, \_\_\_\_\_ de \_\_\_\_\_ de \_\_\_\_\_.

**<REPRESENTANTE DA CONTRATADA>**

**<VÍNCULO DO REPRESENTANTE COM A CONTRATADA>**

RG:

CPF:

DE ACORDO:

(integrantes da equipe técnica da CONTRATADA)

\_\_\_\_\_  
Nome:

\_\_\_\_\_  
Nome:

RG:

RG:





## ANEXO V – MODELO DE TERMO DE CIÊNCIA

### TERMO DE CIÊNCIA

#### INTRODUÇÃO

Visa obter o comprometimento formal dos empregados da contratada diretamente envolvidos no projeto sobre o conhecimento da declaração de manutenção de sigilo e das normas de segurança vigentes na Instituição.

#### IDENTIFICAÇÃO

Contrato N°:			
Objeto:			
Contratante:	Controladoria-Geral da União		
Gestor do		Matr.:	
Contratada:		CNPJ:	
Preposto da		CPF:	

Por este instrumento, os funcionários abaixo-assinados declaram ter ciência e conhecer o teor do Termo de Compromisso de Manutenção de Sigilo e as normas de segurança vigentes na Contratante:

- a) [Portaria CGU nº 587/2021](#): Institui a Política de Segurança da Informação da Controladoria-Geral da União;
- b) [Norma Complementar nº 05/2017](#): Estabelece as diretrizes para o uso dos recursos de Tecnologia da Informação e Comunicação no âmbito da CGU; e
- c) [Código de Conduta da CGU](#);

#### CIÊNCIA

#### CONTRATADA – Empregados

\_\_\_\_\_  
<Nome>  
Matrícula: <Matr.>

\_\_\_\_\_  
<Nome>  
Matrícula: <Matr.>

\_\_\_\_\_  
<Nome>  
Matrícula: <Matr.>

\_\_\_\_\_  
<Nome>  
Matrícula: <Matr.>

\_\_\_\_\_  
**<Nome>**  
Matrícula: **<Matr.>**

\_\_\_\_\_  
**<Nome>**  
Matrícula: **<Matr.>**

\_\_\_\_\_, \_\_\_\_ de \_\_\_\_\_  
de 20\_\_\_\_.

## **ANEXO VI – MODELO DE ATESTADO DE CAPACIDADE TÉCNICA**

O(a) Sr(a) [nome do(a) responsável], CPF [número do CPF do responsável], cargo [cargo que ocupa], na [Nome (Razão Social) da Empresa Contratante], CNPJ [número do CNPJ da Contratante], endereço [endereço completo], atesta, sob as penas da Lei, que o Sr.(a) [Nome do profissional ou Razão Social da Empresa Individual CPF/CNPJ [número do CPF do profissional ou CNPJ da empresa individual], prestou os serviços de [nome do(s) serviço(s)] de solução de backup, marca [marca da solução] e modelo [modelo da solução], com [quantidade de horas] horas, tendo prestado os referidos serviços de forma satisfatória, no período de [dd/mm/aaaa] a [dd/mm/aaaa].

---

[Local e data da emissão do Atestado]

---

[Assinatura do responsável pela emissão do Atestado, com nome, cargo, telefone e e-mail institucional para contato.