



TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAZONAS
Av. André Araújo, S/N - Bairro Aleixo - CEP 69060-000 - Manaus - AM - www.tjam.jus.br

TERMO DE REFERÊNCIA

1. OBJETO:

- 1.1. Registro de Preço para eventual fornecimento de solução de proteção e resiliência de informação com suporte e garantia mínima de 3 anos, incluindo treinamento oficial, para utilização como estratégia de salvaguarda das informações digitais geradas pelos processos judiciais e sistemas administrativos que atendem o Tribunal de Justiça do Estado do Amazonas.
- 1.2. O serviço objeto da contratação é o previsto no Código SIASG / CATSER: 000539-8 – Prestação de Serviços de Informática.
- 1.3. Sugere-se que o critério de julgamento seja baseado no menor preço global, com uma única empresa sendo a fornecedora de todos os equipamentos, "softwares" e serviços que compõem cada lote de itens. A justificativa para tal proposição baseia-se no fato de que os itens contidos em cada grupo são complementares e dependentes entre si.

2. JUSTIFICATIVA:

- 2.1. Com vistas a atender a demanda de armazenamento seguro do crescente contingente de sistemas informatizados do Tribunal de Justiça do Estado do Amazonas - TJAM, a Secretaria de Tecnologia da Informação e Comunicação, identificou a necessidade de contratar solução corporativa de proteção e resiliência dos dados de forma a garantir a redundância e a continuidade de negócio em caso de desastres. A solução atualmente em uso não provê mecanismo ou aplicação de automação, controle, versionamento e arquivamento das máquinas virtuais ou dados contidos nelas. Por hora, são realizadas cópias manuais de algumas aplicações e arquivos em volumes compartilhados e réplicas de baixo nível existentes na plataforma hiperconvergente. Entretanto elas não são suficientes para garantir o cumprimento dos requisitos normativos e regulamentares aos quais o Egrégio Tribunal de Justiça do Estado do Amazonas está sujeito.
- 2.2. Atualmente o TJAM possui um parque computacional hiperconvergente de processamento e armazenamento de dados distribuídos em 2(duas) localidades geograficamente distantes (*datacenters*), interligadas através de comutadores de rede de alto desempenho e baixa latência com velocidades predominantes de 10Gbps, com mais de 450 (quatrocentos e cinquenta) virtuais, em torno de 180 TB de volumetria de conteúdo em uso, proteção perimetral e central de próxima geração, VMware vSphere EXSi e Acropolis Hypervisor como virtualizadores e diversas aplicações cruciais ao funcionamento orgânico do órgão como SAJ, PROJUDI, CPA/SEI, Postgres, Microsoft SQL Server entre outras.
- 2.3. Garantir a disponibilidade, integridade, confidencialidade e salvaguarda das informações é requisito básico fundamentado nas Políticas de Segurança da Informação do TJAM, nas Resoluções do CNJ e nas Normas Internacionais de Segurança da Informação, cito NBR 27001 e 27002. E estar em acordo com essas normatizações, é estar preparado para atender aos requisitos de excelência em qualidade na prestação de serviços para os clientes internos e externos do TJAM.
- 2.4. Devido à natureza, atributos e classificações as quais todas as informações geradas e processadas nesse exímio Tribunal estão sujeitas, faça-se necessário modelar uma solução de proteção de dados que seja capaz de atender com qualidade e excelência as políticas de segurança e as retenções normativas das informações judiciais que podem variar de 5 a 20 anos de proteção.
- 2.5. Utilizando as métricas de unidades de processamento (CPU), quantidade de informações de entrada (FET - Front-End Terabytes), tipo de aplicações, janela de execução, alteração mensal e período de retenção inicial o processo de modelagem da eventual solução, que atenderá as demandas de proteção e resiliência de informação pretendida por esse poder, baseou-se no melhor cenário possível para cumprir com nossas demandas e características únicas.
- 2.6. Observando os gráficos e estatísticas de área de armazenamento de informação da plataforma Nutanix, é possível identificar o FET total e a alteração mensal vegetativa que são respectivamente 180TB (máquinas virtuais e arquivos) e 2% ao mês, conforme a tabela abaixo podemos visualizar a quantidade de dados de entrada para os próximos 3 anos em TB:

1º ano	2º ano	3º anos
--------	--------	---------

211 TB	252 TB	292 TB
---------------	---------------	---------------

2.7. Para calcular o espaço necessário de arquivamento e retenção, ou seja, a área de BET (Back-End Terabytes) será necessário definir a hierarquia de mídia e a retenção esperada de cada uma delas, utilizando o valor de FET descrito acima como medida inicial. Todo o estudo de capacidade necessária, bem como as janelas de backup aceitas para definir o desempenho da arquitetura global, estão descritos em detalhes no ETPC desta contratação. No tipo de armazenamento disco pretende-se alcançar os últimos 30 dias de cópia de todo o ambiente e em fita os últimos 20 anos dos arquivos administrativos e processuais.

2.8. Avaliando as soluções de proteção e resiliência disponíveis no mercado, encontra-se um ecossistema de fabricantes que podem atender as necessidades e expectativas de negócio do TJAM. Em geral, elas devem ser modulares, licenciadas por instância de processamento virtual, podem ser integradas a equipamentos de armazenamento, suporte a diversos tipos de mídia (disco, nuvem e unidades de fita LTO) e diversas políticas de proteção, que garantam cópias de máquinas virtuais sendo executadas em VMware vSphere EXSi e Acropolis Hypervisor, bem como nos arquivos contido dentro delas, tenha técnicas de otimização de dados como compressão e deduplicação.

2.9. Não obstante, este Tribunal pretende englobar com essa contratação, todo o arcabouço necessário a estruturação dos elementos do parque de TIC para a construção de uma nuvem híbrida, incorporando a nuvem privada do próprio TJAM a um provedor público de serviços e processamento e armazenamento remoto.

2.10. Dentro das boas práticas de implementação, nossa arquitetura final será composta de distintas camadas de retenção de dados, possuindo áreas mais nobres para a restauração das informações mais recentes e repositórios com retenção estendida, tanto localmente quanto com tecnologias facilitadoras do transbordo em nuvem. Precisamos garantir que esse projeto seja base para as futuras etapas da construção de uma solução tecnológica que atua em diversos âmbitos e traz a esse órgão o grau de resiliência necessário a boa sustentação de nossos serviços.

2.11. Dessa forma essa corte de justiça necessita investir em uma solução de proteção e resiliência de informação que possua gerenciamento e orquestração de cópias de VMs e arquivos administrativos e processuais, acoplada a um appliance ou equipamento similar, tenha uma biblioteca de fita LTO, totalmente licenciada, com treinamento oficial e implantação.

2.12. Sendo assim, é totalmente factível e necessário que seja feito investimento em uma solução de proteção e resiliência das informações.

3. FUNDAMENTAÇÃO LEGAL:

3.1. A contratação para a execução dos serviços deverá obedecer, no que couber, ao disposto na Lei nº 8.666/93, de 21 de junho de 1993 e suas alterações, bem como nas seguintes normas:

- 3.1.1. Lei nº 10.520 de 17/7/2002;
- 3.1.2. Decreto 7.892/2013.
- 3.1.3 Resolução nº 25/2019/TJAM;
- 3.1.4 Decreto nº 40.674/2019;

4. REGISTRO DE PREÇOS

4.1. O objeto deste Termo de Referência será contratado mediante Sistema de Registro de Preços.

4.2. O critério de julgamento da formação do registro de preços será o de menor preço global.

5. ESPECIFICAÇÃO, CARACTERÍSTICAS e GARANTIA:

5.1. Os bens e serviços a serem adquiridos enquadram-se no conceito de bens e serviços comuns, trazidos no parágrafo único do artigo 1º. da Lei nº.10.520/2002.

5.2. O objeto deste termo terá garantia por 36 (trinta e seis) meses, cujo termo inicial é a data de emissão do Termo de Recebimento Definitivo, cujo suporte e atualização deve ser dado pelo próprio fornecedor em conjunto a cada fabricante, incluindo canal de atendimento emergencial através de telefone e e-mail.

Item	DESCRIÇÃO	UND	Quant	Quant Min
01	Licenciamento de software de proteção e resiliência de informações	Un	600	100
02.1	Unidade de armazenamento de informação – tipo 1	Un	2	1
02.2	Unidade de armazenamento de informação – tipo 2	Un	5	1
03.1	Fitoteca de armazenamento modular - base	Un	2	1

03.2	Fitoteca de armazenamento modular - expansão	Un	4	1
04	Serviço de instalação e configuração da solução	Un	100	20
05	Serviço de treinamento oficial	Un	6	3

5.3 ESPECIFICAÇÕES TÉCNICAS – CARACTERÍSTICAS DOS ITENS

5.3.1. Licenciamento de software de proteção e resiliência de informações

5.3.1.1. O licenciamento da solução de proteção e recuperação deverá ser baseado no modelo para o ambiente virtual, temporário ou por assinatura, baseando-se na quantidade de máquinas virtuais desde que não haja limitação de quantidades de uso de capacidade;

5.3.1.2. O licenciamento entregue deverá permitir a portabilidade das cargas de trabalho, garantindo proteção da informação independentemente de onde ela esteja, seja localmente, seja remotamente (em outro site, em nuvem pública, etc.);

5.3.1.3. Após o vencimento da assinatura deve existir um período mínimo de carência de 30 dias;

5.3.1.4. Para a medição do licenciamento do ambiente virtual, é a soma de todas as máquinas virtuais dos hypervisors (VMware vSphere ESXi e Acropolis Operating System), não importando a quantidade de núcleos deles, para esse licenciamento a solução não deverá ter limite de TB de entrada;

5.3.1.5. No licenciamento da solução, entendem-se que todas as funcionalidades descritas nesse termo estarão habilitadas e disponíveis para uso de forma total e irrestrita, na inteireza da capacidade licenciada, independentemente da quantidade ou tipo de agentes necessários, de acordo com a necessidade da CONTRATANTE, e, sem necessidade de aquisição de qualquer outro tipo de licença ou recurso adicional para execução de tais funcionalidades;

5.3.1.6. A solução ofertada deve estar habilitada para permitir a instalação de quantos servidores de movimentação de dados e de gerência da solução, quanto forem necessários para configuração do ambiente a ser protegido, de acordo com as melhores práticas propostas pelo fabricante;

5.3.1.7. A versão ofertada deve ser a última versão disponível, não será aceita a utilização de versões anteriores para cobrir alguma especificação técnica;

5.3.1.8. A solução ofertada deverá de maneira simples e objetiva mostrar a quantidade de licenças adquiridas e utilizadas;

5.3.1.9. Caso a solução permita o consumo acima do que foi contratada, sem nenhuma trava, não será cobrado em hipótese nenhuma essa diferença, seja no licenciamento, seja em futuras renovações ou desistência da utilização do software;

5.3.1.10. Ter suporte e garantia de 3 (três) anos, com atendimento 24 x 7 x 365 e até 2 (duas) horas para início do atendimento de chamados com prioridade mais alta, ou seja, quando o ambiente estiver em estado de indisponibilidade de uso;

5.3.1.11. Caso a solução ofertada necessite de algum banco de dados, o mesmo deverá ser fornecido devidamente licenciado sem nenhum custo extra para a CONTRATANTE.

5.3.2. Características da infraestrutura

5.3.2.1. Deve possuir arquitetura em múltiplas camadas ou arquitetura similar:

5.3.2.1.1. Servidor de gerência de proteção;

5.3.2.1.2. Servidores de movimentação de dados;

5.3.2.1.3. Clientes ou agentes de cópias.

5.3.3. O servidor de gerência de proteção deverá ter suporte para instalação no mínimo com os sistemas operacionais abaixo:

5.3.3.1.1. Microsoft Windows 2016;

5.3.3.1.2. Microsoft Windows 2019.

5.3.4. O servidor de movimentação de dados deverá ter suporte para instalação no mínimo com um dos sistemas abaixo:

5.3.4.1. Microsoft Windows 2019 ou superior;

5.3.4.2. CentOS 8.x ou superior;

5.3.4.3. Ubuntu 18.04 ou superior;

5.3.4.4. Debian 10.4 ou superior;

5.3.4.5. Suse Linux Enterprise Server 15 SP2 ou superior;

5.3.4.6. Red Hat Enterprise Linux 8.x ou superior.

5.3.5. Possuir um banco de dados ou catálogo interno, contendo informações sobre todos os arquivos e mídias onde os backups foram armazenados;

5.3.5.1. Não serão aceitas soluções que possuam catálogos distintos dentro da mesma arquitetura, ou seja,

soluções onde caso uma tarefa seja executada em um certo módulo, exista a possibilidade dos dados e metadados não refletirem no mesmo catálogo único;

5.3.5.2. Para todas as funcionalidades aqui descritas, o catálogo deverá ser único, independentemente de aplicação e servidor protegido;

5.3.6. Caso a ferramenta faça uso de um software de banco de dados para armazenamento das informações, e este requeira uma licença para uso, essa licença deve ser fornecida em conjunto com a solução;

5.3.7. Ser flexível e escalável, permitindo sua instalação, configuração e uso em sites remotos interligados ao site principal através de WAN. Além disso, a solução deve prover recursos de desduplicação na origem, desduplicação no destino, e compactação tanto no site principal como nos sites remotos na inteireza da capacidade previamente licenciada e sem necessidade de aquisição de qualquer outro tipo de licença ou recurso adicional para execução de tais operações;

5.3.7.1. As tecnologias de desduplicação e compressão de dados, devem ser independentes do tipo de repositório de armazenamento empregado na arquitetura, permitindo a ativação/desativação das tecnologias conforme o melhor cenário de implementação a ser utilizado;

5.3.8. Ter a funcionalidade para proteger localidades remotas, assegurando que a transmissão de dados através da WAN seja minimizada, provendo tanto desduplicação quanto replicação, enquanto possibilita recuperação granular de dados. A solução deve prover arquitetura flexível ao ponto de que a recuperação no escritório regional possa ser total (com todos os dados vindos do datacenter) ou parcial (com somente o envio dos dados que não estão em cache local);

5.3.8.1. Permite implementar um controle da quantidade de dados trafegados, seja limitando a quantidade de rede que a solução poderá utilizar, ou a vazão (throughput) máximo que a solução poderá utilizar para gravar no repositório.

5.4. Funcionalidades de cópia e recuperação

5.4.1. Ser capaz de realizar cópia de arquivos abertos sem que a consistência deles seja comprometida;

5.4.2. Possuir recursos avançados de agendamento de rotinas de proteção, 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;

5.4.3. Possuir a funcionalidade de paralelizar a gravação dos dados em dispositivos de armazenamento (funcionalidade conhecida como multiplexação);

5.4.4. Ser capaz de enviar alertas através de e-mail com o objetivo de reportar eventos ocorridos na operação e configuração da solução;

5.4.5. A solução deverá permitir o transporte de dados de backup em infraestrutura de objetos, como S3;

5.4.5.1. A solução deverá estar licenciada para realizar o transporte dos dados para infraestruturas de objetos em nuvem pública e privada;

5.4.5.1.1. Não se faz necessária a entrega dessa infraestrutura;

5.4.5.2. Deverá ser compatível com, no mínimo, provedores de nuvem privada e pública, como:

5.4.5.2.1. Microsoft Azure;

5.4.5.2.2. AWS;

5.4.5.2.3. Nutanix Objects;

5.4.5.2.4. Dell EMC ECS;

5.4.5.3. A solução deverá permitir a movimentação de dados para a nuvem (backup e restauração), de acordo com as políticas de backup implementadas. Não serão aceitas soluções que dependam de hardwares específicos para executar essa funcionalidade;

5.4.5.3.1. Todas as licenças necessárias à execução dessa funcionalidade deverão estar inclusas na solução;

5.4.5.4. A solução deverá permitir a construção de um repositório de armazenamento de backup com escalabilidade horizontal, garantindo uma arquitetura híbrida entre nuvem privada e nuvem pública. Deverá permitir o uso simultâneo, com o propósito de criar uma entidade virtual de armazenamento, de storages, appliances de desduplicação e arquiteturas de nuvem;

5.4.5.4.1. A solução deverá permitir que o repositório de armazenamento escalável seja composto, concomitantemente, por armazenamento direto em Windows/Linux (SAN ou DAS), compartilhamentos de rede (NAS), equipamentos específicos para deduplicação (PBBA) e armazenamento de Objetos (S3 e HTTP) em nuvem pública e privada;

5.4.5.4.2. A solução deverá permitir elencar, por características de desempenho dos repositórios, distintos níveis de armazenamento com o propósito de garantir estabilidade nos processos de backup e restauração de dados;

5.4.5.4.3. A solução deverá permitir a escolha do armazenamento contínuo das imagens de backup, de modo que um ciclo de backup possa estar presente em um único elemento da infraestrutura compartilhada

(integralmente em um appliance de deduplicação), bem como em múltiplos elementos da infraestrutura compartilhada (backups completos em um appliance de deduplicação e backups incrementais em compartilhamentos NAS);

5.4.5.4.4. A solução deverá validar diariamente, de modo automático, o estado dos distintos elementos de armazenamento que compõem o repositório compartilhado. A solução deverá validar o status de cada elemento, informando se eles estão online ou não, se os movimentadores de dados estão estáveis e qual o espaço de armazenamento remanescente no repositório compartilhado global;

5.4.5.5. Ser capaz de enviar traps SNMP (Simple Network Management Protocol) com o objetivo de reportar eventos ocorridos na operação da solução;

5.4.5.6. A solução deverá permitir a restauração segura de imagens de backup, permitindo a criação de uma área específica, prévia à operação de recuperação, para a varredura de vírus ou malwares.

5.4.5.7. A solução deverá possuir um arquivo de configuração o qual deverá ser validado durante o processo de restauração para identificar qual software de varredura deverá ser ativado na análise de vírus ou malwares.

5.4.5.8. Deverá ser compatível com fabricantes de varredura de vírus ou malwares como Symantec, ESET e Kaspersky.

5.4.5.9. A console de gerenciamento da solução de backup deverá exibir os resultados da varredura efetuada pelo software terceiro de análise de vírus ou malwares.

5.4.6. Possuir a funcionalidade de agendamento automático de tarefas de backup;

5.4.7. Para operações de dados gravadas em disco e fita, a solução de proteção deve possuir as seguintes funcionalidades:

5.4.7.1. Para um mesmo dado armazenado deve haver a possibilidade de configuração de diferentes períodos de retenção;

5.4.7.2. Para um dado armazenado deve haver a possibilidade de estender o período de retenção.

5.4.7.3. Implementar a execução de cópias completas sintéticas ou similar, podendo implementar através de cópias do tipo eternamente incremental (Forever Incremental);

5.4.7.3.1. Uma cópia completa sintética é gerada através de uma outra cópia completa tradicional (não sintetizada) anterior e de cópias incrementais ou diferenciais subsequentes ou de um backup incremental cumulativo. A cópia sintetizada deverá ser capaz de restaurar arquivos e diretórios da mesma maneira que um cliente faz a restauração de uma cópia tradicional;

5.4.7.4. Permitir a gravação de cópias do tipo Disco-Para-Disco-Para-Unidade de Fita;

5.4.7.5. Ser compatível com bibliotecas auto-carregadoras de cartuchos de fitas magnéticas;

5.4.7.6. Possuir a funcionalidade de criar múltiplas cópias de backups armazenados, com a opção de recuperação dos dados de forma automática através da cópia secundária se a cópia primária não estiver mais disponível.

5.5. Funcionalidades da console de gerenciamento, integração e alta-disponibilidade

5.5.1. Possuir interface que seja capaz de gerenciar e executar operações de proteção e recuperação dos sistemas operacionais Windows, Unix e Linux; ambientes de virtualização VMware e Acropolis Operating System; aplicações como Microsoft Active Directory e banco de dados Microsoft SQL Server, Oracle (Windows e Linux) e Oracle RAC (em Linux);

5.5.2. O acesso administrativo ao console do servidor de gerenciamento da solução poderá ser feito através de ferramenta disponibilizada no próprio software (console gráfico) ou através de navegador Web;

5.5.3. Suportar cópia de segurança dos arquivos de catálogo e configuração, para promover recuperação dos serviços de gerenciamento no evento de falhas;

5.5.4. Suportar unificação de autenticação (single sign on - SSO), permitindo a integração com o Microsoft Active Directory. A funcionalidade de integração com o Active Directory deverá permitir a definição granular das permissões administrativas aos recursos, objetos e servidores definidos na configuração do software;

5.5.5. A base de dados para armazenamento do catálogo deverá possuir mecanismo de proteção (backup) das informações armazenadas no catálogo e funcionalidades de recuperação rápida do catálogo em caso de desastre.

5.6. Suporte à Criptografia:

5.6.1. Implementar criptografia de dados na origem (cliente ou proxy de backup), de uma forma que seja garantido que o dado que trafegará na rede local ou na rede WAN seja criptografado;

5.6.2. Criptografia de dados no destino (servidor de backup);

5.6.3. Implementar no mínimo chaves de criptografia de 256 bits para cifrar os dados;

5.6.4. Implementar pares de chaves de criptografia de 4096 bits para recuperação de desastres;

5.7. Suportar protocolos IPv4 e IPv6 para rotinas de backup;

5.8. Integração com as seguintes aplicações para cópia e restauração

5.8.1. Realizar proteção e recuperação dos seguintes sistemas operacionais, aplicações, banco de dados e ambientes de virtualização:

- 5.8.1.1. Microsoft Windows 7 SP1, 8.1, 10, Server 2008 R2 SP1, 2012, 2012 R2, 2016 e 2019;
- 5.8.1.2. Oracle Linux 6.x ou superiores;
- 5.8.1.3. Red Hat Enterprise Linux 6.x ou superiores;
- 5.8.1.4. Ubuntu 16.x ou superiores;
- 5.8.1.5. Debian 8.x ou superiores;
- 5.8.1.6. Microsoft Active Directory 2012 ou superiores;
- 5.8.1.7. Microsoft SQL Server 2012 ou superiores;
- 5.8.1.8. Oracle 11g R2 ou superiores (Linux ou Windows);
- 5.8.1.9. MySQL 5.6.x ou superiores;
- 5.8.1.10. PostgreSQL 9.4 ou superiores;
- 5.8.1.11. VMware ESX/ESXi 6.0 ou superiores;
- 5.8.1.12. Nutanix 5.10 ou superiores.

5.9. Suporte ao Active Directory

5.9.1. Executar cópia em tempo de execução do Microsoft Active Directory;

- 5.9.1.1. Possibilitar as seguintes opções de recuperação:
- 5.9.1.2. Recuperação de um objeto;
- 5.9.1.3. Recuperação de um atributo;
- 5.9.1.4. Recuperação de um atributo deletado de um objeto.

5.10. Suporte a Oracle e Oracle RAC

5.10.1. Deverá executar proteção e recuperação de base de dados Oracle e Oracle RAC com as seguintes características nativas ou não:

- 5.10.1.1. Executar proteção e recuperação das bases de dados do Oracle/Oracle RAC via RMAN e sem parada do banco;
- 5.10.1.2. Executar arquivamento do registro de eventos (log) possibilitando a criação de rotina de cópia para que ocorra com intervalos de 1 (uma) hora;
- 5.10.1.3. Permitir a cópia do arquivamento de transações (archives logs) baseados na quantidade de arquivamento (archives);
- 5.10.1.4. Permitir a configuração que após a cópia dos registros de transações (archives logs) os mesmos sejam mantidos ou deletados;
- 5.10.1.5. Além da proteção do Banco, a solução deverá proteger a área de catálogo, control file e sp file.
- 5.10.1.6. Possibilitar a recuperação com as seguintes características:
- 5.10.1.7. Recuperação completa da Base de dados no mesmo servidor
- 5.10.1.8. Recuperação completa da Base de dados em outro servidor
- 5.10.1.9. Recuperação de um datafile específico
- 5.10.1.10. Recuperação granular no nível de tabela
- 5.10.1.11. Recuperação em um momento do tempo específico;

5.11. Suporte a Microsoft SQL Server

5.11.1. Executar proteção e recuperação de base dos dados Microsoft SQL Server com as seguintes características nativas ou não:

- 5.11.1.1. Executar proteção e recuperação de bases de dados Microsoft SQL Server sem parada do banco;
- 5.11.1.2. Executar cópia de registro de transações (transaction log) possibilitando a criação de rotina de cópia para que ocorra com intervalos de 1 (uma) hora;
- 5.11.1.3. Permitir a configuração que após a cópia dos registros de transações (transaction log) os mesmos sejam mantidos ou deletados;
- 5.11.1.4. A solução deverá possibilitar a recuperação com as seguintes características:
- 5.11.1.5. Recuperação completa da base de dados no mesmo servidor
- 5.11.1.6. Recuperação completa da base de dados em outro servidor
- 5.11.1.7. Recuperação de uma base específica
- 5.11.1.8. Recuperação granular no nível de tabela
- 5.11.1.9. Recuperação em um momento do tempo específico;

5.12. Suporte a PostgreSQL

5.12.1. Executar proteção e recuperação de base de dados PostgreSQL Server com as seguintes características nativas ou não:

- 5.12.1.1. Cópia em tempo de execução do banco de dados;

- 5.12.1.2. Permitir a recuperação completa;
 - 5.12.1.3. Restaurar a base de dados ou seus arquivos no mesmo servidor em caminho diferente;
 - 5.12.1.4. Restaurar uma instância ou seus arquivos em um outro servidor.
- 5.13. Suporte a MySQL
- 5.13.1. Executar proteção e recuperação de base de dados MySQL Server com as seguintes características nativas ou não:
 - 5.13.1.1. Cópia em tempo de execução do banco de dados;
 - 5.13.1.2. Permitir a recuperação completa;
 - 5.13.1.3. Restaurar a base de dados ou seus arquivos no mesmo servidor;
 - 5.13.1.4. Restaurar uma instância ou seus arquivos em um outro servidor.
- 5.14. Suporte ao ambiente virtual (VMware e Acropolis Hypervisor)
- 5.14.1. Executar proteção e recuperação do Ambiente Virtual com as seguintes características:
 - 5.14.1.1. Realizar recuperação da imagem completa da máquina virtual (ambientes VMware e Acropolis Hypervisor) e também de arquivos de maneira granular sem a necessidade de scripts, área temporária ou montagem dos arquivos vmdk, vhd;
 - 5.14.1.2. No caso da restauração granular, não há necessidade de se restaurar a Guest VM inteira;
 - 5.14.1.3. Permitir redirecionar a restauração de uma máquina virtual hospedada para uma pasta alternativa, outro volume de armazenamento;
 - 5.14.1.4. Incluir automaticamente máquinas virtuais novas criadas dentro de seleções de cópias anteriores;
 - 5.14.1.5. Permitir cópia completa (Full) e incremental para os servidores virtuais;
 - 5.14.1.6. Ser capaz de realizar cópias e restauração de servidores virtuais Linux e Windows, sejam elas estado de consistência ou aplicação;
 - 5.14.1.7. Permitir que as tarefas de cópias e restauração sejam realizadas via interface gráfica;
 - 5.14.1.8. O backup dos servidores virtuais deverá ser armazenado de maneira desduplicada;
 - 5.14.1.9. Permitir orquestração de cópias de baixo nível da camada de armazenamento (Snapshot) de máquinas virtuais ou Domínios de Proteção no Nutanix AHV, com a retenção desses dados armazenados diretamente no cluster AHV.
 - 5.14.1.10. Permitir a restauração granular de arquivos ou sistemas de arquivos a partir de cópias em disco. Em caso de backup armazenado em disco a recuperação granular poderá ser feito utilizando-se cópias que possam estar desduplicados;
 - 5.14.1.11. Possui capacidade de realizar a replicação de máquinas virtuais VMware localmente e remotamente em outro Cluster, realizando clones ou snapshots com proteção contínua dos dados por máquina virtual:
 - 5.14.1.11.1. Deverá suportar a replicação remota a fim de replicar os dados das máquinas virtuais entre soluções de armazenamento distintas, inclusive de diferentes fabricantes;
 - 5.14.1.11.2. Suportar a orquestração de failover e failback das máquinas virtuais replicadas;
 - 5.14.1.12. Permitir a execução de uma máquina virtual diretamente de uma imagem de backup desduplicada e comprimida;
 - 5.14.1.12.1. Essa funcionalidade deverá permitir sua execução de modo agnóstico ao servidor e repositório de backup utilizado, seja para vSphere ou para Acropolis;
 - 5.14.1.12.1.1. Deverá permitir que a solução de virtualização empregada possa movimentar a máquina virtual para o ambiente de produção, posteriormente;
 - 5.14.1.12.1.2. A máquina virtual iniciada não deverá alterar os dados de backup existentes, ficando a encargo da solução tratar a área de armazenamento temporária da máquina;
 - 5.14.1.12.1.3. Permitir que uma máquina virtual Acropolis seja restaurada como máquina virtual VMware diretamente da imagem de backup;
 - 5.14.1.13. A solução deverá permitir a criação de uma área de testes isolada, compatível com VMware ou Acropolis, para depurar máquinas virtuais, testar upgrades de software e instalar novas aplicações nas máquinas virtuais;
 - 5.14.1.13.1. Quaisquer atualizações realizadas somente deverão ser aplicadas nas máquinas após a restauração completa dos dados no ambiente de produção;
 - 5.14.1.13.2. Ações executadas no ambiente isolados deverão ocorrer em infraestrutura temporária, sendo descartadas ou rotacionadas caso a máquina não venha a ser restaurada;
 - 5.15. Funcionalidade de desduplicação de cópia e arquivamento
 - 5.15.1. Permitir uso da tecnologia de desduplicação de dados para toda a capacidade existente, não existindo limitações devido a licença empregada, eliminando blocos repetidos, para cópias e arquivamento em disco e movimentação de dados desduplicados, independentemente de quantitativo de dispositivos de

armazenamento que compõem a infraestrutura da CONTRATANTE.

5.15.2. Implementar deduplicação a nível de blocos, não sendo aceita a técnica de Single-Instance Storage;

5.15.3. Implementar deduplicação de blocos na origem (client-side deduplication), de forma que o cliente envie apenas novos blocos de dados criados e/ou modificados a partir da última cópia total completa;

5.15.4. Implementar deduplicação de blocos no destino (target-side deduplication), de forma que seja responsabilidade do servidor de transporte executar a tecnologia;

5.15.5. Implementar deduplicação de dados em tarefas de cópia;

5.15.6. Implementar deduplicação e compressão em uma mesma tarefa.

5.15.7. Implementar deduplicação em infraestrutura de armazenamento local (DAS) e vida rede (SAN e NAS);

5.15.8. A tecnologia de deduplicação não deverá possuir limites quanto a quantidade de dados que serão lidos (front-end), nem limites para a quantidade de dados que serão escritos (back-end);

5.16. Reportes e alertas

5.16.1. Vir disponível com os seguintes relatórios e reportes:

5.16.1.1. Histórico de rotinas de proteção concluídos nas últimas 24 horas, nos últimos 30 dias e nos últimos 6 meses;

5.16.1.2. Histórico de recuperações efetuadas nas últimas 24 horas, nos últimos 30 dias e nos últimos 6 meses;

5.16.1.3. Reportes de rotinas de backup concluídos com sucesso, com erro ou não concluídos;

5.16.1.4. Taxa de deduplicação por rotina de backup;

5.16.1.5. Possuir relatórios com as seguintes características:

5.16.1.5.1. Horário de início e término de uma rotina de backup;

5.16.1.5.2. Tempo de duração de uma rotina de backup;

5.16.1.5.3. Status do backup (situação):

5.16.1.5.3.1. Relação dos objetos incluídos na rotina de backup;

5.16.1.5.3.2. Horário de início e término do backup de cada objeto;

5.16.1.5.3.3. Tempo de duração do backup de cada objeto;

5.16.1.5.3.4. Volume de dados na origem durante a rotina de backup;

5.16.1.5.3.5. Volume de dados trafegados durante a rotina de backup;

5.16.1.5.3.6. Volume de dados com compressão e deduplicação;

5.16.1.5.3.7. Taxa de deduplicação de dados;

5.16.1.5.3.8. Taxa de compressão de dados;

5.16.1.6. A solução ofertada deverá enviar os seguintes alertas via e-mail:

5.16.1.7. Rotina de backup finalizada com sucesso;

5.16.1.8. Rotina de backup finalizada com erro;

5.16.1.9. Rotina de backup com problema;

5.16.1.10. Alerta para utilização de licenciamento.

5.17. Unidade de armazenamento de informação

5.17.1. Características Gerais

5.17.1.1. Ser homologada pelo software de proteção ofertada;

5.17.1.2. Prover infraestrutura de armazenamento, voltados para a proteção de dados do ambiente de hiperconvergência ou nuvem privada;

5.17.1.3. Corresponder a um módulo de armazenamento de backup em disco, com o propósito específico de ingestão dos dados de backup com compactação, deduplicação e replicação (local e remota/nuvem) dos dados deduplicados;

5.17.1.4. Ser novo, de primeiro uso e estar em linha de fabricação na data da abertura da licitação. Não serão aceitos equipamentos usados, remanufaturados, de demonstração ou gateways;

5.17.1.5. Constar no site do fabricante (documento oficial e público) como um sistema de armazenamento de backup em disco, em linha de produção;

5.17.1.6. Não serão aceitas soluções definidas por Software (Virtual Appliance);

5.17.1.7. O hardware do módulo de armazenamento de cópias em disco não poderá ser compartilhado com nenhum outro software para operar;

5.17.1.8. Ser do tipo agnóstico, ou seja, possuir compatibilidade com diversas soluções de software de proteção. Não serão aceitas soluções proprietárias ("lock in") ou seja, aqueles que só funcionam com um software de backup específico;

5.17.1.8.1. Deverá possuir compatibilidade com softwares e aplicações de backup comuns de mercado, como, no mínimo, Arcserve, Backup Exec, Commvault, DellEMC Networker, Hycu, IBM TSM,

Oracle RMAN, Microsoft SQL, NetBackup e Veeam;

5.17.1.9. Estar licenciada para toda sua capacidade e funcionalidade, incluindo replicação;

5.17.1.10. Permitir o particionamento lógico da área de armazenamento, sem prejuízo às características de deduplicação solicitadas neste certame;

5.17.1.11. Todos os valores de capacidade de armazenamento devem ser calculados considerando o sistema de cálculo BASE 2, ou seja, 1 Terabyte (TB) é igual a 1024 Gigabytes (GB);

5.17.1.12. Possuir recursos de tolerância a falhas de, pelo menos, discos, fontes de alimentação e ventiladores. Os discos rígidos deverão ser hot-pluggable e hot-swappable permitindo substituição sem necessidade interrupção do funcionamento da solução;

5.17.1.13. Possuir mecanismos que protejam contra a inconsistência dos dados mesmo em casos de interrupção abrupta ou desligamento acidental;

5.17.1.14. Ser entregue com arranjos de discos rígidos do tipo RAID-6 configurado de tal modo a tolerar a falha de até 2 (dois) discos rígidos, para os discos destinados ao armazenamento de dados de backup;

5.17.1.14.1. Deverá possuir, no mínimo, 1 (um) disco configurado como hot-spare;

5.17.1.15. Possuir funcionalidade de deduplicação dos dados em nível de bytes ou blocos, com capacidade de eliminação de dados redundantes para racionalizar a utilização do espaço de armazenamento;

5.17.1.16. Implementar deduplicação global para o módulo de armazenamento de backup em disco, considerando todos os dados retidos, sendo capaz de identificar dados duplicados de backups de diferentes origens dentro de um mesmo conjunto de armazenamento de modo a maximizar a taxa de deduplicação e garantindo que os dados sejam gravados uma única vez;

5.17.1.17. Suportar simultaneamente acessos de leitura e gravação pelos protocolos CIFS e NFS;

5.17.1.18. Suportar a implementação do OpenStorage Technology;

5.17.1.19. Permitir a criação de backups sintéticos completos, do software de proteção ofertado, internamente no appliance;

5.17.1.20. Permitir a execução de processos de backup e restore em paralelo;

5.17.1.21. Deverá implementar tecnologia que detém dos serviços de movimentação de dados compatível com o Software de Proteção ofertado, removendo a necessidade de utilização de servidores gateways, servidores intermediários, servidores auxiliares ou similares para o emprego de tais serviços;

5.17.1.21.1. Caso o appliance não implemente internamente os serviços de movimentação de dados do software de proteção ofertado, será aceita a entrega de servidor físico adicional com recurso suficiente para comportar o tráfego de, ao menos, 170 TB (cento e setenta terabytes líquidos) de dados protegidos durante uma janela de 10 (dez) horas;

5.17.1.22. Integração entre o software de proteção ofertado e o módulo de armazenamento:

5.17.1.22.1. O módulo de armazenamento deverá permitir a inicialização de máquinas virtuais, através do software ofertado, diretamente da sua área de armazenamento, desde que o virtualizador suporte a funcionalidade;

5.17.1.22.2. Deverá permitir a restauração de máquinas virtuais, arquivos únicos e objetos/arquivos específicos de aplicações diretamente do repositório de armazenamento;

5.17.1.23. Possuir funcionalidade para replicação de cópias em equipamento similar e do mesmo fabricante de forma assíncrona, utilizando recursos de deduplicação e reduzindo consumo do link de comunicação, através de rede IP (WAN/LAN);

5.17.1.24. Possuir arquitetura baseada em camadas que permita a proteção contra “ransomware attack”, independente do software de backup.

5.17.1.24.1. Entende-se por equipamento multi-camadas àqueles onde as camadas de armazenamento são nativas (não podem ser criadas ou removidas) e onde pelo menos uma das camadas não pode ser acessada diretamente pelo software de backup para escrita. Além disso, deve possuir pelo menos uma camada isolada do acesso externo com funcionalidade de atraso de deleção, onde os dados retidos ao longo do tempo devem ser armazenados no formato imutável e não podem ser imediatamente deletados por comando do software de backup.

5.17.1.24.1.1. Tal atraso de deleção deve ser configurável em dias, proporcionado ao menos o atraso por 15 dias.

5.17.1.24.1.2. Para desativação ou modificação desse recurso deve ser possível requerer escalação e duplo fator de autenticação.

5.17.1.24.2. Caso a solução ofertada não possua arquitetura multi-camadas e não possua todas as características solicitadas no item anterior, deve ser entregue com um segundo equipamento (para cada unidade contratada no certame), possuindo as mesmas características do equipamento primário, juntamente com um mecanismo que realize o filtro da replicação de dados entre eles para isolar os dados replicados do repositório primário e impedir a propagação do ataque de ransomware no momento da sincronização entre os sistemas

(Air-Gap, Atraso de Sincronismo). Todos os componentes para o funcionamento dessa proteção devem ser fornecidos com a solução.

5.17.1.25. O appliance deverá possuir baterias, supercapacitores ou tecnologia similar, para proteger a cache de escrita, evitando a perda de dados em eventos de falha elétrica;

5.17.1.26. O appliance deverá implementar mecanismos de validação da consistência dos dados desduplicados armazenados, garantindo que eles estejam íntegros durante backups, restaurações e replicações. A tecnologia deverá reparar, automaticamente, dados que não estejam consistentes com as rotinas executadas;

5.17.1.27. Deverá possuir integração com Microsoft Active Directory para autenticação de usuários quanto ao acesso a interface de gerência da solução;

5.17.1.28. Deverá permitir a implementação de topologias de replicação, como 1 para 1, 1 para N e o cascadeamento de equipamentos. A solução deverá permitir a criação de topologias de nuvem privada e híbrida;

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

5.17.1.30. Ser montado em rack padrão 19" e deve ser entregue com todos os trilhos, cabos, conectores, manuais de operação e quaisquer outros componentes que sejam necessários à instalação, customização e plena operação;

5.17.1.31. Ter suporte e garantia de 3 (três) anos, com atendimento 24 x 7 x 365 e até 2 (duas) para início do atendimento de chamados com prioridade mais alta, ou seja, quando o equipamento estiver em estado de indisponibilidade de uso. É troca de peça no próximo dia útil;

5.17.1.31.1. Permitir abertura de chamados diretamente com a equipe do fabricante de engenharia nível 2 (técnicos especializados para atuar na investigação do problema, sugestão de ajustes e correção, coleta e avaliação de logs). Além disso, esse engenheiro deve estar disponível para implementar atualizações e correções, revisar as configurações do ambiente e sugerir ajustes de acordo com melhores práticas, mesmo sem a ocorrência de problemas ou indisponibilidade na solução.

5.18. Unidade de armazenamento de informação - tipo 1

5.18.1. Possuir 149 TB (cento e quarenta e nove terabytes) de área útil;

5.18.2. Possuir alguma das seguintes arquiteturas para o módulo de armazenamento:

5.18.2.1. Scale-up: Soluções com arquitetura tradicional (crescimento vertical) baseada em uma ou duas controladoras interconectadas a um ou mais gabinetes de discos, onde a ampliação do armazenamento é realizada com a adição de gavetas de disco e está limitada à capacidade das controladoras e a desduplicação é do tipo em linha (in-line) e global para o volume de armazenamento gerenciado por essas controladoras. Nesse caso a solução:

5.18.2.1.1. Entregar duas controladoras, no mínimo no modelo ativo-passivo, com discos sólidos (SSD) para aceleração de desduplicação e reconstrução de dados (rehidratação);

5.18.2.1.2. Deverá possuir interfaces de rede redundantes e dedicadas a interconexão de alta disponibilidade da solução, empregando interfaces 10G Ethernet SFP+, incluindo transceivers Short-Range e fibras OM4, multi-modo, de 1.0m;

5.18.2.1.3. Permitir desempenho de, no mínimo, 25 TB/h (vinte e cinco terabytes por hora) para tarefas de backup. O desempenho deve ser possível sem considerar desduplicação na origem, compressão ou componentes de software e hardware externos;

5.18.2.1.4. Deve permitir desduplicação global quando associado a, pelo menos, dois outros equipamentos similares do mesmo fabricante, com objetivo de constituir uma única área de armazenamento lógica. Se não possuir essa capacidade, deve ser fornecido com área de armazenamento 37,5% maior, considerando um ganho futuro de 1,6:1;

5.18.2.1.5. Deverá ser entregue habilitado para desduplicar sua máxima capacidade suportada.

5.18.2.2. Scale-out: Soluções com arquitetura hiperconvergente (crescimento horizontal), que possuem em seu módulo computacional processador, memória, interfaces de rede e discos associados e permita a agregação de vários módulos em um mesmo cluster onde a ampliação do armazenamento é realizada com a simples adição de módulos e a desduplicação é global entre eles. Nesse caso a solução:

5.18.2.3. Permitir desempenho de, no mínimo, 13 TB/h (treze terabytes por hora) para tarefas de backup e restore, sem contabilizar o uso externo de softwares e hardwares;

5.18.2.4. Permitir desduplicação global quando associado a, pelo menos, dois outros módulos similares do mesmo fabricante, com objetivo de constituir uma única área de armazenamento lógica;

5.18.2.5. Deverá ser entregue habilitado para desduplicar sua máxima capacidade suportada.

5.18.3. Ser fornecido com portas Ethernet de 10Gbps do tipo SFP+, com suas respectivas GBICS, na quantidade suficiente para que o desempenho especificado seja alcançado;

5.18.4. Deverá possuir, no mínimo, 16 (dezesesseis) núcleos de processamento, com o dobro de threads, por

controladora entregue;

5.18.5. Deverá ser entregue com o máximo de memória suportado pelo equipamento, conforme divulgado em documentação oficial da fabricante;

5.18.6. A solução deverá ser escalável a, no mínimo, 1000 TB (mil terabytes líquidos), seja através da adição de gavetas de discos ou de equipamentos similares em uma arquitetura scale-out;

5.18.7. A solução deverá estar licenciada para receber imagens de backup desduplicadas na origem;

5.18.8. Ter pelo menos 1 (um) Porta IPMI, 2 (Duas) Portas 1GB Ethernet e 2 (Duas) portas 10GB SFP+.

5.19. Unidade de armazenamento de informação - tipo 2

5.19.1. Possuir 62 TB (sessenta e dois terabytes) de área útil;

5.19.2. Possuir alguma das seguintes arquiteturas para o módulo de backup:

5.19.2.1. Scale-up: Soluções com arquitetura tradicional (crescimento vertical) baseada em uma ou duas controladoras interconectadas a um ou mais gabinetes de discos, onde a ampliação do armazenamento é realizada com a adição de gavetas de disco e está limitada à capacidade das controladoras e a desduplicação é do tipo em linha (in-line) e global para o volume de armazenamento gerenciado por essas controladoras. Nesse caso a solução:

5.19.2.1.1. Entregar duas controladoras, no mínimo no modelo ativo-passivo, com discos sólidos (SSD) para aceleração de desduplicação e reconstrução de dados (rehidratação);

5.19.2.1.2. Deverá possuir interfaces de rede redundantes e dedicadas a interconexão de alta disponibilidade da solução, empregando interfaces 10G Ethernet SFP+, incluindo transceivers Short-Range e fibras OM4, multi-modo, de 1.0m;

5.19.2.1.3. Permitir desempenho de, no mínimo, 10 TB/h (dez terabytes por hora) para tarefas de backup. O desempenho deve ser possível sem considerar desduplicação na origem, compressão ou componentes de software e hardware externos;

5.19.2.1.4. Permitir desduplicação global quando associado a, pelo menos, dois outros equipamentos similares do mesmo fabricante, com objetivo de constituir uma única área de armazenamento lógica. Se não possuir essa capacidade, deve ser fornecido com área de armazenamento 37,5% maior, considerando um ganho futuro de 1,6:1;

5.19.2.1.5. Deverá ser entregue habilitado para desduplicar sua máxima capacidade suportada.

5.19.2.2. Scale-out: Soluções com arquitetura hiperconvergente (crescimento horizontal), que possuem em seu módulo computacional processador, memória, interfaces de rede e discos associados e permita a agregação de vários módulos em um mesmo cluster onde a ampliação do armazenamento é realizada com a simples adição de módulos e a desduplicação é global entre eles. Nesse caso a solução:

5.19.2.2.1. Permitir desempenho de, no mínimo, 5,5 TB/h (cinco e meio terabytes por hora) para tarefas de backup e restore, sem contabilizar o uso externo de softwares e hardwares;

5.19.2.2.2. Permitir desduplicação global quando associado a, pelo menos, dois outros módulos similares do mesmo fabricante, com objetivo de constituir uma única área de armazenamento lógica.

5.19.2.2.3. Deverá ser entregue habilitado para desduplicar sua máxima capacidade suportada.

5.19.2.3. Ser fornecido com portas Ethernet de 10Gbps do tipo SFP+, com suas respectivas GBICS, na quantidade suficiente para que o desempenho especificado seja alcançado;

5.19.2.4. Deverá possuir, no mínimo, 6 (seis) núcleos de processamento, com o dobro de threads, por controladora entregue;

5.19.2.5. Deverá ser entregue com o máximo de memória suportado pelo equipamento, conforme divulgado em documentação oficial da fabricante;

5.19.2.6. A solução deverá ser escalável a, no mínimo, 500 TB (quinhentos terabytes líquidos), seja através da adição de gavetas de discos ou de equipamentos similares em uma arquitetura scale-out;

5.19.2.7. A solução deverá estar licenciada para receber imagens de backup desduplicadas na origem;

5.19.2.8. Deve ter pelo menos 1 (um) Porta IPMI, 2 (Duas) Portas 1GB Ethernet e 2 (Duas) portas 10GB SFP+.

5.20. Fitoteca de armazenamento modular

5.20.1. Características Gerais

5.20.1.1. Ser composto por todos os equipamentos e acessórios necessários para plena instalação e funcionamento;

5.20.1.2. Ser do mesmo fabricante dos equipamentos ofertados para solução de software de proteção, ou estar homologado por ele, estando presente na lista de compatibilidade de hardware desses equipamentos;

5.20.1.3. Gabinete para rack, com tamanho máximo de 3U, acompanhado de:

5.20.1.3.1. Cabo de alimentação compatível com as PDU's do Rack;

5.20.1.3.2. Trilhos e demais elementos de fixação necessários para a instalação em rack de 19 polegadas, do próprio fabricante dos equipamentos;

- 5.20.1.3.3. Possuir fonte de alimentação redundante 110/220Vac;
- 5.20.1.3.4. Ser modular permitindo expandir a capacidade de drives e slots através de módulos de expansão para no mínimo 21 unidades de operação e 272 slots;
- 5.20.1.3.5. Ter suporte e garantia de 3 (três) anos, com atendimento 24 x 7 x 365 e até 2 (duas) horas para início do atendimento de chamados com prioridade mais alta, ou seja, quando o equipamento estiver em estado de indisponibilidade de uso. É troca de peça no próximo dia útil.
- 5.20.1.3.6. Ter acesso direto ao engenheiro de nível 2 do fabricante nomeado para a CONTRATANTE, que possibilite a execução das seguintes atividades durante toda a vigência da garantia, sem limite de quantidade:
 - 5.20.1.3.6.1. Atualização de software e/ou aplicação de correções;
 - 5.20.1.3.6.2. Revisão do ambiente para validação das configurações e, se necessário, realizar os ajustes com as melhores práticas indicadas;
 - 5.20.1.3.6.3. Abertura de chamados de suporte direto com engenheiro de nível 2, sem necessidade de triagem de nível 1;
 - 5.20.1.3.6.4. Reinstalações ou reconfigurações que se fizerem necessárias, mesmo que não sejam decorrentes de problemas de suporte.
- 5.21. Fitoteca de Armazenamento – base
 - 5.21.1. Suportar múltiplos caminhos e particionamento lógico;
 - 5.21.2. Suportar funcionalidade de alta disponibilidade de caminhos que garanta o uso de um caminho de comunicação redundante quando o caminho principal falha;
 - 5.21.3. Suportar até 3 unidades LTO 6, 7 ou 8;
 - 5.21.4. Ser entregue com 1 unidade LTO-7 (Linear Tape-Open geração 7), com capacidade de gravação mínima de 6TB em cada cartucho, sem o uso de compressão;
 - 5.21.5. Ser acompanhada por no mínimo 2 (duas) portas SAS de 6 Gb;
 - 5.21.6. Ter compatibilidade de leitura e escrita com o padrão LTO-6, e de leitura com o padrão LTO-5;
 - 5.21.7. Cada unidade de leitura e gravação deverá possuir taxa de transferência de no mínimo 300 Mbps, sem o uso de compressão;
 - 5.21.8. Cada unidade deverá ser acompanhada por no mínimo 2 (dois) cabos Mini-SAS para SAS de 1,5 m;
 - 5.21.9. O equipamento deverá ser do tipo “library”, com capacidade de armazenamento mínima para 40 (quarenta) cartuchos LTO-7;
 - 5.21.10. Contar com interface Ethernet dedicada para gerenciamento, através de redes TCP/IP, compatível com os protocolos HTTP e SNMP;
 - 5.21.11. Possuir dispositivo que permita a identificação dos cartuchos por código de barras;
 - 5.21.12. Estar acompanhado de 35 (trinta e cinco) cartuchos normais de fita, no padrão LTO-7, e quatro cartuchos de limpeza;
 - 5.21.13. Os cartuchos já devem ser acompanhados das respectivas etiquetas de código de barras;
 - 5.21.14. Ser compatível, e estar homologado, com os sistemas operacionais:
 - 5.21.14.1. Microsoft Windows Server 2016 ou superior;
 - 5.21.14.2. Red Hat Enterprise Linux 7.6 ou superior;
 - 5.21.14.3. SUSE Linux Enterprise Server (SLES) 15 ou superior.
 - 5.21.15. Vir acompanhado também da unidade de controle, que deve possuir no mínimo:
 - 5.21.15.1. Sistema operacional base licenciado, Microsoft Windows Server 2016 ou superior. Não serão aceitos softwares que não possuam suporte da fabricante;
 - 5.21.15.1.1. O sistema operacional deverá ser instalado em SSD redundante, configurado em RAID-1 e com, ao menos, 80 GiB de área de armazenamento líquida total;
 - 5.21.15.2. Entregue com redundância de CPU, com no mínimo 8 cores e hyperthread. Deverão ser da última geração de processadores ofertados pela fabricante do mesmo;
 - 5.21.15.3. Suporte a CPUs com memória base de 2.400, 2.666 e 2.933 MHz;
 - 5.21.15.4. Entregue com 32 GB de memória RAM;
 - 5.21.15.4.1. O servidor ofertado deverá suportar uma quantidade idêntica de DIMMs de memória por processador instalado, não sendo aceitas ofertas onde os processadores podem ser configurados com quantidades distintas de DIMMs por soquete;
 - 5.21.15.5. Entregue com 2 (duas) interfaces de rede de 10Gbps e cabos passivos de conexão direta e 5,0m;
 - 5.21.15.6. Respeitando as seguintes características de armazenamento:
 - 5.21.15.6.1. Placa de hardware RAID com 2GB de cache;
 - 5.21.15.6.2. Suporte aos níveis RAID 0, 1, 10, 5, 50, 6, 60;
 - 5.21.15.6.3. Suporte a discos HDD, SSD e SED;

- 5.21.15.6.4. Com 2 (duas) interfaces Mini-SAS de 12Gb/s;
 - 5.21.15.6.4.1. Deverá possuir, no mínimo, um slot extra para expansão de HBAs;
- 5.21.15.7. Respeitando as seguintes características de gerenciamento:
 - 5.21.15.7.1. Controlar o consumo energético do módulo;
 - 5.21.15.7.2. Permitir o gerenciamento remoto da solução;
 - 5.21.15.7.3. Permitir o gerenciamento IPMI-over-LAN;
 - 5.21.15.7.4. Permitir o mapeamento de imagens através de compartilhamentos HTTPS, SFTP, CIFS e NFS;
 - 5.21.15.7.5. Permitir o uso concomitante da interface de gerência por, no mínimo, 6 (seis) usuários;
 - 5.21.15.7.6. Permitir o controle de consumo de banda de rede;
- 5.21.15.8. Possuir fontes e ventiladores hot-swap e redundantes, com tensão bivolt;
- 5.22. Fitoteca de Armazenamento – Expansão
 - 5.22.1. Suportar até 3 unidades LTO 6, 7 ou 8;
 - 5.22.2. Possuir 1 unidade LTO-7 (Linear Tape-Open geração 7), com capacidade de gravação mínima de 6TB em cada cartucho, sem o uso de compressão;
 - 5.22.3. Cada unidade LTO-7 deverá possuir conectividade SAS, de no mínimo, 6Gb com 2 portas por unidade LTO;
 - 5.22.4. Cada unidade deverá ser acompanhada por no mínimo 2 (dois) cabos Mini-SAS para SAS de 1,5 m;
 - 5.22.5. Ter compatibilidade de leitura e escrita com o padrão LTO-6, e de leitura com o padrão LTO-5;
 - 5.22.6. Cada unidade de leitura e gravação deverá possuir taxa de transferência de no mínimo 300 Mbps, sem o uso de compressão;
 - 5.22.7. O equipamento deverá ser do tipo “Expansion module”, com capacidade de armazenamento mínima para 40 cartuchos LTO-7;
 - 5.22.8. Estar acompanhado de 35 (trinta e cinco) cartuchos normais de fita, no padrão LTO-7;
 - 5.22.9. Ter suporte e garantia de 3 (três) anos, com atendimento 24 x 7 x 365 e até 2 (duas) para início do atendimento de chamados com prioridade mais alta, ou seja, quando o equipamento estiver em estado de indisponibilidade de uso. É troca de peça no próximo dia útil;
 - 5.22.90. Os cartuchos já devem ser acompanhados das respectivas etiquetas de código de barras.
- 5.23. Serviço instalação e configuração
 - 5.23.1. Desenvolver documentação mínima de projeto que inclua cronograma, recursos e plano de implantação;
 - 5.23.2. A CONTRATADA deverá definir a quantidade de esforço em horas, para escopo desejado pela CONTRATANTE;
 - 5.23.3. Conforme acordados entre as partes, as atividades podem ser executadas remotamente ou fisicamente;
 - 5.23.4. A CONTRATANTE deverá aprovar o plano de execução apresentado pela executora;
 - 5.23.5. A aprovação poderá ocorrer por email ou outros meios oficiais utilizados pelo órgão;
 - 5.23.6. As atividades previstas são:
 - 5.23.6.1. Instalação física dos equipamentos;
 - 5.23.6.2. Inicialização dos equipamentos;
 - 5.23.6.3. Atualização com as versões mínimas recomendados pelo fabricante;
 - 5.23.6.4. Configuração de movimentadores de dados;
 - 5.23.6.5. Configuração de entidades intermediárias;
 - 5.23.6.6. Configuração de unidade de fita;
 - 5.23.6.7. Configuração de agentes;
 - 5.23.6.8. Configuração de políticas de proteção e cópia;
 - 5.23.6.9. Configuração de relatórios;
 - 5.23.6.10. Configuração de repositórios;
 - 5.23.6.11. Aplicação de políticas e cópias de auto-proteção;
 - 5.23.6.12. Configuração de rotinas de alertas;
 - 5.23.6.13. Avaliação de desempenho;
 - 5.23.6.14. Realização de ajustes de desempenho;
 - 5.23.6.15. Execução de plano de testes;
 - 5.23.6.16. Documentação da solução implantada
 - 5.23.7. Acompanhar localmente ou remotamente durante 8 (horas), após implantação no decorrer de 5 dias.
- 5.24. Serviço de capacitação
 - 5.24.1. Ser ofertado treinamento oficial focado na administração do serviço de proteção e recuperação;
 - 5.24.2. Ser ofertado antes do início dos trabalhos de instalação, configuração e migração da solução

ofertada; de forma que os analistas do Tribunal de Justiça do Amazonas possam acompanhar todo o trabalho de implantação da solução com o embasamento técnico necessário para entender as atividades a serem executadas pela CONTRATADA;

5.24.3. O treinamento não poderá ser completamente teórico, devendo incluir laboratórios e simulações em ambiente propício a treinamento;

5.24.4. Ser ofertado treinamento oficial do fabricante conforme previsto no item Em relação ao software de backup minimamente deverá possuir conteúdo programático contendo administração, operação e gerência com carga horária mínima de 24 horas:

5.24.4.1. Conceitos, arquitetura, topologia e componentes da solução fornecida;

5.24.4.2. Definição de políticas, agendamento, parâmetros de desduplicação e de execução dos backups / restores via Rede Local;

5.24.4.3. Realização de cópias de segurança manuais;

5.24.4.4. Procedimentos de restauração de backups pelo cliente e pelo servidor;

5.24.4.5. Gerenciamento de “backup” e “restore” de catálogo;

5.24.4.6. Utilização de scripts pré e pós “backup”;

5.24.4.7. Definição e execução de “backup” e “restore” do Microsoft Exchange, inclusive recuperação de caixas postais individuais;

5.24.4.8. Definição e execução de “backup” e “restore” do SQL Server, inclusive recuperação de bases de dados;

5.24.4.9. Definição e execução de “backup” e “restore” do Oracle;

5.24.4.10. Resolução de problemas do ambiente de “backup”: definição e avaliação de “logs”, detecção de problemas de comunicação, problemas de unidades de fitas, ajustes do sistema, detecção de problemas em servidores e clientes por meio de utilitários do sistema, mensagens de erro mais comuns e respectivos procedimentos corretivos.

5.24.5. O treinamento deverá ser ministrado em local informado pela CONTRATANTE, juntamente com a disponibilidade de projetor, quadro branco e outros itens essenciais a realização dessa atividade;

5.24.6. O treinamento deverá capacitar à equipe do TJAM a operar, configurar, administrar e resolver problemas usuais na solução ofertada, englobando todos os componentes da solução;

5.24.7. O treinamento será ministrado a 6 (seis) participantes. A composição das turmas será de responsabilidade da CONTRATANTE;

5.24.8. Ter duração mínima de 40/60 (quarenta / sessenta) horas. Para treinamentos oficiais com duração inferior a 40 horas, deverá ser complementado com atividades “hands-on” e passagem de conhecimento, específicos ao ambiente computacional da CONTRATANTE;

5.24.9. Em relação a unidade de backup em disco deverá ser realizado a transferência de conhecimento pelo fabricante ou não, presencial ou formato EAD, devendo abranger todas as funcionalidades, componentes e ferramentas, em seus aspectos mais relevantes e, em especial, envolvendo aqueles relacionados ao ambiente computacional, tomando como base o seguinte escopo:

5.24.9.1. Conceitos básicos e componentes da solução;

5.24.9.2. Configuração dos repositórios no sistema de armazenamento de cópias de proteção;

5.24.9.3. Configuração de replicação de dados;

5.24.9.4. Monitoramento e gestão da ferramenta.

5.24.10. A CONTRATADA se responsabiliza em fornecer, sem custo adicional, todo o material didático impresso ou eletrônico na língua portuguesa (Brasil) ou língua inglesa a todos participantes para acompanhamento do treinamento;

5.24.11. Os dias e horários de execução dos treinamentos serão acordados juntamente com a CONTRATANTE;

5.24.12. Ao final do treinamento deverá ser emitido certificado de participação a cada participante, especificando conteúdo abrangido e carga horária do treinamento.

6. ESTIMATIVA DE QUANTIDADES A SEREM ADQUIRIDAS PELO ÓRGÃO GERENCIADOR E ÓRGÃOS PARTICIPANTES

6.1. O quantitativo total registrado deverá ser utilizado pelo órgão gerenciador e órgãos participantes, se houver, de maneira remanejada, de tal forma que o total aderido (gestor + participantes) não ultrapasse o quantitativo total registrado.

7. ESTIMATIVA DE QUANTIDADES A SEREM ADQUIRIDAS POR ÓRGÃOS NÃO PARTICIPANTES

7.1. As aquisições ou contratações adicionais, consoante o Decreto Estadual nº. 40.674/19, observarão os seguintes limites:

- I - Considerando o Decreto nº 9.488/2018, não poderá exceder a 50% (cinquenta por cento) do quantitativo do item registrado na ata de registro de preços; e
- II - O somatório das adesões não poderá ultrapassar o limite de 2 (duas) vezes o quantitativo de cada item registrado na ata de registro de preços.

8. FORMA DE FORNECIMENTO

8.1. O fornecimento dos Materiais e Serviços decorrentes do Registro de Preços devem ser entregues de forma Integral ao Tribunal de Justiça do Estado do Amazonas.

9. VALOR ESTIMADO DA CONTRATAÇÃO

9.1. A estimativa de custo dos bens e/ou serviços a serem adquiridos ou prestados, constantes deste Termo de Referência, será discriminada na planilha de valor estimado, de competência da Divisão de Compras e Operações.

10. NECESSIDADE DE CONTRATO

10.1. Para a execução dos serviços objeto desse Termo de Referência faz-se necessária a formalização do Contrato Administrativo, nos termos do artigo 54 e seguintes da Lei nº 8.666/1993.

10.2. O contrato deverá ter vigência de 36 (trinta e seis) meses, a contar da data de assinatura.

11. SUBCONTRATAÇÃO

11.1. Será permitida a subcontratação do objeto deste Termo de Referência de Forma Parcial, apenas para os Serviços que se referem a Garantia e Assistência Técnica.

12. CATÁLOGOS E/OU AMOSTRAS

12.1. Apresentar documentos que sejam de acesso público cuja a origem seja exclusivamente do fabricante dos produtos, a exemplo: catálogos, manuais, ficha de especificação técnica, ou informações obtidas em sites oficiais do fabricante através da Internet. A documentação técnica apresentada deverá corroborar a proposta, comprovando características técnicas que os equipamentos e softwares atendam a este Termo de Referência.

12.2. Não há necessidade de apresentar amostra de nenhum item.

13. QUALIFICAÇÃO TÉCNICA

13.1. As empresas interessadas deverão apresentar Atestado de Capacidade Técnica, emitido por entidade pública ou privada, comprovando o fornecimento satisfatório de material e serviço similar ao solicitado. Os atestados de capacidade técnica deverão demonstrar, ao menos, o fornecimento dos seguintes quantitativos mínimos para os itens destacados no termo de referência:

13.1.1. Para o item 01, 20% da quantidade registrada. Caso a licitante tenha comercializado produtos similares com licenciamento distinto, serão aceitas, ao menos, 12 licenças de software por processador físico ou 34 licenças de FETB.

13.1.2. Para os itens 02 e 03, a licitante deverá demonstrar que já comercializou, ao menos, 02 unidades de repositório de backup em disco, conforme as especificações exigidas e similares.

13.1.3. Para os demais itens, a licitante deverá demonstrar que já executou serviços de instalação, migração, configuração, garantia e suporte de infraestrutura ou software de backup.

13.3. Deverá ser comprovada a execução de treinamento, repasse de conhecimento ou fornecimento de treinamento oficial de fabricante de infraestrutura ou backup;

13.4. Será aceito o somatório de atestados de capacidade técnica para atingir os quantitativos solicitados.

13.5. Serão aceitos atestados com tempos de garantia diferentes daquele a ser contratado, todavia os artefatos deverão corroborar o atendimento integral aos produtos e serviços solicitados.

14. OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATANTE:

14.1. Caberá ao Tribunal de Justiça do Estado do Amazonas:

14.1.1. Efetuar os pagamentos nas condições e preços pactuados;

14.1.2. Fiscalizar a prestação do serviço;

14.1.3. Comunicar à entidade, sempre por escrito, as solicitações e quaisquer alterações ocorridas;

14.1.4. Notificar à entidade, por escrito, qualquer ocorrência considerada irregular, bem como quaisquer insatisfações ou imperfeições observadas no fornecimento do material, fixando prazos para as devidas correções, aplicando, conforme o caso, eventuais multas;

- 14.1.5. Prestar os esclarecimentos solicitados pela entidade, atinentes ao objeto desta Licitação;
- 14.1.6. Atestar as faturas correspondentes, por intermédio da fiscalização.

15. OBRIGAÇÕES RESPONSABILIDADES DA CONTRATADA:

15.1 Caberão à contratada, a partir da contratação, o cumprimento das seguintes obrigações:

- 15.1.1. Assumir inteira e total responsabilidade técnica pela qualidade dos materiais fornecidos.
- 15.1.2. Fornecer os materiais em estrita conformidade com as especificações constantes na especificação técnica e no prazo estabelecido;
- 15.1.3. Nomear um profissional como responsável técnico e representante da CONTRATADA para ser o interlocutor junto à CONTRATANTE sobre o objeto deste contrato.

16. FISCALIZAÇÃO E ACOMPANHAMENTO

16.1 A fiscalização e o acompanhamento da prestação do serviço ou fornecimento do material será realizada pelo setor DVITIC/SETIC do Tribunal de Justiça do Estado do Amazonas. São obrigações da fiscalização contratual:

- 16.1.1. Acompanhar a execução do contrato, fiscalizando o cumprimento das condições estabelecidas no Termo de Referência, no edital de licitação e na proposta de preço;
- 16.1.2. Anotar em registro próprio todas as ocorrências relacionadas com a execução do contrato, determinando o que for necessário à regularização das faltas ou defeitos observados;
- 16.1.3. Atestar a(s) Nota(s) Fiscal(is) apresentada(s) pela contratada, comprovando a prestação do serviço de maneira adequada e satisfatória.

17. LOCAL E PRAZO DE ENTREGA OU APLICAÇÃO:

- 17.1. Os objetos deste termo deverão ser entregues à Divisão de Tecnologia da Informação e Comunicação a do TJAM, sito a Avenida André Araújo s/n, Prédio Desembargador Arnaldo Péres - Bairro Aleixo – CEP 69.060-000.
- 17.2. O prazo a ser fixado para a entrega do objeto deverá ser de 30 (trinta) dias corridos, a partir do recebimento da Nota de Empenho.
- 17.3. O material poderá ser recusado se não atender às especificações solicitadas;
- 17.4. Ocorrendo a hipótese prevista no item acima, o fornecedor deverá providenciar, em prazo máximo de 10 (dez) dias corridos, os ajustes necessários para a adequação do material, contados a partir da comunicação do Tribunal de Justiça do Estado do Amazonas quando do não aceite.

18. DO RECEBIMENTO PROVISÓRIO E DEFINITIVO

18.1. O prazo a ser fixado para a entrega deverá ser de no máximo 30 (trinta) dias corridos, a partir da homologação/adesão. O recebimento do serviço será feito em duas etapas:

- 18.1.1. Provisoriamente, para efeito de verificação da estabilidade, vazão e confiabilidade do serviço contratado, durante 10 (dez) dias corridos;
- 18.1.2. Definitivamente, no prazo de até 30 (trinta) dias corridos, contados do recebimento provisório, através do grupo de infraestrutura e telecomunicações da DVTIC que procederá ao recebimento, verificando e atestando que o serviço entregue atende completamente as especificações, em conformidade com o exigido neste Termo de Referência.
- 18.2. Os serviços poderão ser recusados se não atenderem às especificações dispostas no Termo de Referência e na proposta de preço.
- 18.3. Ocorrendo a hipótese prevista no item acima, a contratada deverá providenciar a substituição do material ou reparação do serviço no prazo máximo de 10 (dez) dias corridos, contados a partir da comunicação do Tribunal de Justiça do Estado do Amazonas acerca do não aceite.

19. DO PAGAMENTO:

- 19.1. O pagamento será efetuado de forma definitiva em uma única fatura pela Divisão de Orçamento e Finanças do TJAM, de acordo com a legislação vigente, após recebimento da Nota Fiscal ou Fatura, conferida e atestada pelo setor requisitante, comprovando a prestação do serviço ou o fornecimento do material de maneira satisfatória.
- 19.2. Poderão ser solicitados para o pagamento: Nota Fiscal, de acordo com a legislação vigente; provas de regularidade perante o Fundo de Garantia por Tempo de Serviço (Certidão de Regularidade do FGTS), perante o Instituto Nacional do Seguro Social (Certidão Negativa de Débito do INSS), perante a Fazenda Federal (Certidão Conjunta Negativa de Débitos relativos aos TRIBUTOS FEDERAIS e à DÍVIDA ATIVA DA

UNIÃO), perante a Fazenda Estadual (Certidão Negativa de DÉBITO DO ESTADO), perante a Fazenda Municipal (Certidão Negativa de DÉBITO MUNICIPAL), e perante a Justiça do Trabalho.

19.3. Constatada qualquer incorreção na Nota Fiscal, bem como qualquer outra circunstância que desaconselhe o seu pagamento, o prazo para pagamento fluirá a partir da respectiva regularização.

20. LOCAL DE ENTREGA

20.1 O objeto deste termo deverá ser entregue na Sala da SETIC/DVITIC na Sede do Tribunal de Justiça do Estado do Amazonas, Edifício Desdor. Arnaldo Péres, situado na Avenida André Araújo, s/n, Aleixo, CEP 69060-000, Manaus – AM.

21. VISTORIA TÉCNICA

21.1. Para o correto dimensionamento, elaboração de sua proposta e conhecimento da ambiente, o licitante PODERÁ realizar a vistoria nas instalações do local de onde serão executados os serviços, acompanhado por servidor designado para esse fim, em dia útil, de segunda a sexta-feira, das 08 horas às 11 horas e das 14 horas às 16 horas, devendo o agendamento ser efetuado previamente pelo telefone 92 2129-6779 ou através do e-mail ti@tjam.jus.br após confirmação do órgão licitante, ou presencialmente no endereço: Av. André Araújo, S/N - Aleixo, Manaus - AM, 69060-000 – Prédio Desembargador Arnaldo Péres.

21.2. O prazo para vistoria iniciar-se-á no dia útil seguinte ao da publicação do Edital, estendendo-se até o segundo dia útil anterior à data prevista para a abertura da sessão pública.

21.3. Para a vistoria, o licitante, ou o seu representante, deverá estar devidamente identificado.

21.4. A Licitante poderá optar por não realizar a visita técnica, mas, deverá, obrigatoriamente, apresentar junto a sua documentação de habilitação uma declaração de conhecimento prévio da área onde serão executados o fornecimento e instalação dos equipamentos. Dessa forma, caso venha ser a vencedora, não poderá alegar em nenhuma hipótese o desconhecimento dos locais da realização do fornecimento e instalação dos materiais e suas peculiaridades como justificativa para se eximir das obrigações assumidas em consequência do presente certame.

22. PRAZO DE GARANTIA E ASSISTÊNCIA TÉCNICA

22.1. Com relação aos serviços de Garantia e Assistência Técnica:

22.1.1. A contratada deverá prestar serviços de garantia e assistência técnica, os quais deverão ser providos pelos fabricantes dos produtos ofertados, pelo período de vigência do contrato;

22.1.2. Manutenção corretiva de "hardware" dos produtos fornecidos, incluindo a reparação de eventuais falhas, mediante a substituição de peças e componentes por outros de mesma especificação, novos de primeiro uso e originais, de acordo com os manuais e normas técnicas específicas para os mesmos;

22.1.3. Atualizações corretivas e evolutivas de "software" e "firmware", incluindo pequenas atualizações de "release", reparos de pequenos defeitos ("bug fixing" e "patches");

22.1.4. Ajustes e configurações conforme manuais e normas técnicas do fabricante;

22.1.5. Demais procedimentos destinados a recolocar os equipamentos em perfeito estado de funcionamento;

22.1.6. Assistência técnica especializada para investigar, diagnosticar e resolver incidentes e problemas relativos aos produtos fornecidos;

22.1.7. Os serviços de garantia por 36 (trinta e seis) meses, para todos os componentes de "hardware" e de "software" ofertados na respectiva proposta, deverão ser comprovados pelo fabricante do equipamento por meio de "site", portal ou documentação;

22.1.8. Os serviços de garantia e de assistência técnica deverão ser prestados pelo fabricante da solução no regime de 24 (vinte e quatro) horas dia durante os 7 (sete) dias da semana (24 x 7), sem qualquer ônus adicional ao contratante;

22.1.9. A troca de peças deverá ser realizada no próximo dia ;

22.1.10. A contratada deverá disponibilizar canal de atendimento para abertura de chamados técnicos, por meio de número de telefone fixo ou número local (nas cidades onde se encontrarem instalados os equipamentos), ou ainda, poderá ser disponibilizado serviço de abertura de chamado via "site" ou "e-mail";

22.1.11. Para cada chamado técnico, a contratada deverá informar um número de controle (protocolo) para registro, bem como manter histórico de ações e atividades realizadas;

22.1.12. Os chamados técnicos serão classificados por criticidade, de acordo com o impacto no ambiente computacional do contratante, conforme prioridades enumeradas a seguir:

22.1.13. Prioridade Alta: Sistema indisponível ou com severa degradação de desempenho;

22.1.14. Prioridade Média: Sistema disponível, com mau funcionamento, que importe baixa degradação de desempenho ou comprometimento em um de seus elementos que importe em risco para a disponibilidade do sistema;

- 22.1.15. Prioridade Baixa: Sistema disponível, sem impacto em seu desempenho ou disponibilidade; consultas gerais sobre instalação, administração, configuração, otimização, "troubleshooting" ou utilização.
- 22.1.16. O nível de severidade será informado pelo contratante no momento da abertura do chamado.
- 22.1.17. O contratante poderá escalar os chamados para níveis mais altos ou baixos, de acordo com a criticidade do problema. Nesse caso, os prazos de atendimento e de solução, bem como os prazos e percentuais de multa, serão automaticamente ajustados para o novo nível de prioridade.
- 22.1.18. Os serviços de assistência técnica em garantia deverão atender, respectivamente, os seguintes prazos de atendimento inicial e de solução do incidente:
- 22.1.19. Os chamados de "Prioridade Alta" deverão ser atendidos em até 2 (duas) horas, com resolução do chamado ou solução de contorno em até 6 (seis) horas;
- 22.1.20. Os chamados de "Prioridade Média" deverão ser atendidos em até 8 (oito) horas com resolução do chamado ou solução de contorno em até 24 (vinte e quatro) horas;
- 22.1.21. Os chamados de "Prioridade Baixa" deverão ser atendidos em até 24 (vinte e quatro) com resolução do chamado ou solução de contorno em até 96 (noventa e seis) horas;
- 22.1.22. O prazo de atendimento começará a ser contado a partir da hora do acionamento do suporte via central de atendimento da contratada;
- 22.1.23. Entende-se por início de atendimento a hora de chegada do técnico de suporte ao local onde está o produto ou sua intervenção remota;
- 22.1.24. Entende-se por término do atendimento ou chamado atendido a ocorrência de um dos eventos abaixo relacionados:
- 22.1.25. Solução definitiva;
- 22.1.26. Solução de contorno e escalonamento do chamado para um nível de menor severidade, mediante prévia aprovação do contratante;
- 22.1.27. O encerramento do chamado será dado por servidor da equipe técnica do contratante na conclusão dos serviços, após a disponibilização da solução para uso em perfeitas condições de funcionamento no local onde está instalada;
- 22.1.28. Caberá aos técnicos do fabricante ou da empresa autorizada pelo fabricante identificar os componentes, peças e materiais responsáveis pelo mau funcionamento dos produtos fornecidos;
- 22.1.29. Em caso de falhas irreversíveis de "hardware" ou impossibilidade de solução pela assistência técnica, a contratada deverá providenciar a troca por equipamento idêntico ou superior;
- 22.1.30. Casos em que se tornará obrigatória a substituição de equipamentos pela contratada;
- 22.1.31. Falha de componente de "hardware" que interrompa o perfeito funcionamento do equipamento;
- 22.1.32. Por questão de segurança, os equipamentos e "software" nunca deverão ser removidos das dependências do contratante sem a remoção de dados ou regras sigilosas;
- 22.1.33. No caso de troca do produto por defeito, não haverá qualquer ônus adicional para o contratante;
- 22.1.34. Relativamente à manutenção corretiva de "hardware" e "software";
- 22.1.35. Os componentes danificados deverão ser substituídos, entregues, instalados e configurados, de modo a deixar o equipamento em perfeitas condições de uso e com todas as funcionalidades operacionais, nas dependências do contratante, nos prazos de solução estabelecidos acima, sem a cobrança de quaisquer custos adicionais (frete, seguro, etc.);
- 22.1.36. Concluída a manutenção, a contratada fornecerá ao contratante, documento em que conste a identificação do chamado técnico, data e hora de início e término da assistência técnica, descrição dos serviços executados, indicação da peça e/ou componente eventualmente substituído, assim como relato referente às condições inadequadas ao funcionamento do equipamento ou sua má utilização, fazendo constar a causa e as medidas para a sua correção;
- 22.1.37. Durante todo o período de garantia, a contratada atualizará ou disponibilizará para "download", sem ônus adicionais para o contratante, os componentes de "softwares" necessários ao perfeito funcionamento dos produtos fornecidos, fornecendo as novas versões ou "releases" lançados. Os componentes de "softwares" tratados neste item incluem assinaturas, "software" de gerenciamento, "firmwares" de BIOS e "drivers";
- 22.1.38. Qualquer manutenção e/ou intervenção por solicitação da contratada ou do fabricante, mesmo não implicando em inoperância do sistema ou alteração de suas características, deverá ser agendada e acordada previamente com o contratante;
- 22.1.39. Os serviços deverão ser prestados por equipe técnica qualificada pelo fabricante do sistema;
- 22.1.40. A contratada não poderá impor qualquer limitação de quantitativo de chamados, seja diário, mensal, anual, ou de tempo de duração dos chamados, durante o período de prestação dos serviços.
- 22.1.41. O contratante poderá acompanhar os chamados técnicos abertos pela contratada junto ao fabricante;
- 22.1.42. Será admitida a subcontratação dos serviços de garantia e assistência técnica, desde que previamente autorizada por escrito pelo contratante, por empresa comprovadamente autorizada pelo fabricante dos

equipamentos;

Manaus, 11 de fevereiro de 2022.

(Assinado Digitalmente)

Washington Alves da

Cunha Neto

Assessor

SETIC

(Assinado Digitalmente)

Breno Figueiredo Corado

Secretario de Tecnologia da Informação

e Comunicação

SETIC

(Assinado Digitalmente)

Rodrigo Camelo de Oliveira

Diretor de Infraestrutura de Tecnologia da

Informação e Comunicação

SETIC



Documento assinado eletronicamente por **RODRIGO CAMELO DE OLIVEIRA, Diretor(a)**, em 11/02/2022, às 13:54, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **WASHINGTON NETO, Coordenador(a)**, em 11/02/2022, às 14:07, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **BRENO FIGUEIREDO CORADO, Secretário(a)**, em 11/02/2022, às 14:22, conforme art. 1º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida no site https://sei.tjam.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0455129** e o código CRC **55409971**.