	ESTUDO TÉCNICO PRELIMINAR	Código:
		FOR-DILOG-002-xx (V.00)

1. OBJETO

Aquisição de Solução de Backup.

2. NECESSIDADE DA CONTRATAÇÃO

Com vistas a atender a demanda de armazenamento seguro do crescente contingente de sistemas informatizados do Tribunal de Justiça do Estado do Acre- TJAC, a Diretoria de Tecnologia da Informação, identificou a necessidade de contratar solução corporativa de proteção e resiliência dos dados de forma de mitigar a chances de perda de informação em caso de incidente cibernético e para garantir a continuidade de negócio. **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 nas plataformas de armazenamento hoje existentes. Entretanto elas não são suficientes para garantir o cumprimento dos requisitos normativos e regulamentares aos quais o Egrégio Tribunal de Justiça do Estado do Acre está sujeito. Atualmente utilizamos um *software* chamado *Symantec Backup Exec*, que é um *software* que está bastante desatualizado, em torno de 10 anos de utilização, não corresponde a nossa necessidade atual de eficiência, sincronismo, replicação e homologação de *backups*, o que põe em risco nossos sistemas em caso de recuperação de algum incidente de segurança ou desastre. **Além disso um *backup* eficiente, em última instância, é a principal ferramenta que resguarda os dados em caso de ataques de *ransomware,* como ocorrido recentemente no STJ e TJRS. Nenhuma outra medida, do ponto de vista da segurança da informação, é tão importante quanto *backup* para resguardar os dados em caso de sequestro de dados, conforme explanado na informação (1255562).**

3. DESCRIÇÃO DE REQUISITOS.

3.1. Atender às solicitações nos prazos estipulados.

3.2. Aceitar o controle de qualidade realizado por laboratório oficial.

3.3. Responder por todos os ônus referentes ao fornecimento ora contratado, tais como fretes, impostos, seguros, encargos trabalhistas, previdenciários, fiscais e comerciais, decorrentes do objeto e apresentar os respectivos comprovantes, quando solicitados pelo TJAC e Diretores de Secretaria do interior.

3.4. Entregar o material durante o expediente das Comarcas do interior ou em horários alternativos, previamente acordados com os Diretores de Secretaria.

3.5. Reparar ou indenizar, dentro do prazo estipulado pela autoridade competente, todas e quaisquer avarias ou danos causados aos bens do contratante, ou de terceiros, decorrentes de ação ou omissão de seus empregados e fornecedores.

3.6. Substituir, no prazo máximo de até 02 (duas) horas, a contar da data da notificação, os produtos entregues, caso se apresentem impróprios para consumo.

3.7. Providenciar para que seus empregados cumpram as normas internas relativas à segurança do contratante.

3.8. Manter durante todo o período de vigência do contrato, todas as condições que ensejaram a sua habilitação na licitação e contratação.

3.9. Não subcontratar ou transferir a outrem, no todo ou em parte, o objeto da contratação definida neste Termo de Referência, sem prévia anuência do Contratante. Caso ocorra a subcontratação, mesmo que autorizada pelo Contratante, este não se responsabilizará por qualquer obrigação ou encargo do subcontratado.

3.10. Fornecer os materiais descritos nos respectivos grupos, com rapidez e eficiência.

3.11. Cumprir o objeto do contrato estritamente de acordo com as normas que regulamentam o objeto da contratação.

3.12. O atraso na prestação de serviços pela CONTRATADA aplicar-se-á em multas e sansões administrativas previstas no contrato.

4. ANÁLISE DE MERCADO

De acordo com as propostas apresentadas nos eventos 1268606, 1268608 e 1268609

5. DESCRIÇÃO DA SOLUÇÃO

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 Acre.

6. ESTIMATIVA DAS QUANTIDADES A SEREM CONTRATADAS

ITEM	DESCRIÇÃO	UND	QTD AQUISIÇÃO IMEDIATA	QTD PARA REGISTRO
01	Licenciamento de software de proteção e resiliência de informações	Un	300	600
02	Unidade de armazenamento de informação – tipo 1	Un	0	2
03	Unidade de armazenamento de informação – tipo 2	Un	2	5
04	Fitoteca de armazenamento modular - base	Un	1	2
05	Fitoteca de armazenamento modular - expansão	Un	0	4
06	Serviço de instalação e configuração da solução	Un	0	100
07	Serviço de treinamento oficial	Un	3	6

7. ESTIMATIVA DO VALOR DA CONTRATAÇÃO

De acordo com o Mapa de Preços fornecido pela GECON (1270414)â��

8. ALINHAMENTO AO PLANO INSTITUCIONAL

a) Cumprir o Plano de Continuidade de Serviços essenciais de TIC constante na Resolução 370/2020 do CNJ, conforme Caput IV, Art. 34, Art. 36, *in verbis:*

> " - Art. 34. Os itens de infraestrutura tecnológica deverão atender as especificações, temporalidade de uso e obsolescência a serem regulados em instrumentos aplicáveis e específicos.
>
> - Art. 36. Cada órgão deverá elaborar Plano de Gestão de Continuidade de Negócios ou de Serviços no qual estabeleça estratégias e planos de ação que garantam o funcionamento dos serviços essenciais quando na ocorrência de falhas."

b) O objetivo da aquisição encontra respaldo no Planejamento Estratégico de TI (PETIC), estando inserido especificamente no Plano de Continuidade de Serviços de TI.
c) O presente projeto faz parte do conjunto de ações de TI que serão desenvolvidas pela Diretoria de Tecnologia da Informação e está previsto no Plano de Aquisições e Contratações de TI.

9. RESULTADOS PRETENDIDOS

Ser capaz de realizar cópia de arquivos abertos sem que a consistência deles seja comprometida;
9.1 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;
9.2 Possuir a funcionalidade de paralelizar a gravação dos dados em dispositivos de armazenamento (funcionalidade conhecida como multiplexação);
9.3 Ser capaz de enviar alertas através de e-mail com o objetivo de reportar eventos ocorridos na operação e configuração da solução;
9.4 A solução deverá permitir o transporte de dados de backup em infraestrutura de objetos, como S3;
9.5 Solução deverá estar licenciada para realizar o transporte dos dados para infraestruturas de objetos em nuvem pública e privada;
9.6 Não se faz necessária a entrega dessa infraestrutura;
9.7 Deverá ser compatível com, no mínimo, provedores de nuvem privada e pública, como:
9.8 Microsoft Azure;
9.9 AWS;
9.10 Nutanix Objects;
9.11 Dell EMC ECS;
9.12 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;
9.13 Todas as licenças necessárias à execução dessa funcionalidade deverão estar inclusas na solução;
9.14 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;
9.15 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;
9.16 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;
9.17 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 desduplicação), bem como em múltiplos elementos da infraestrutura compartilhada (backups completos em um appliance de deduplicação e backups incrementais em compartilhamentos NAS);
9.18 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;
9.19 Ser capaz de enviar traps SNMP (Simple Network Management Protocol) com o objetivo de reportar eventos ocorridos na operação da solução;

9.20 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.
9.21 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.
9.22 Deverá ser compatível com fabricantes de varredura de vírus ou malwares como Kaspersky.
9.23 A console de gerenciamento da solução de backup deverá exibir os resultados da varredura efetuada pelo software terceiro de análise de vírus ou malwares.
9.24 Possuir a funcionalidade de agendamento automático de tarefas de backup;
9.25 Para operações de dados gravadas em disco e fita, a solução de proteção deve possuir as seguintes funcionalidades:
9.26 Para um mesmo dado armazenado deve haver a possibilidade de configuração de diferentes períodos de retenção;
9.27 Para um dado armazenado deve haver a possibilidade de estender o período de retenção.
9.28 Implementar a execução de cópias completas sintéticas ou similar, podendo implementar através de cópias do tipo eternamente incremental (Forever Incremental);
9.29 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;
9.30 Permitir a gravação de cópias do tipo Disco-Para-Disco-Para-Unidade de Fita;
9.31 Ser compatível com bibliotecas auto-carregadoras de cartuchos de fitas magnéticas;
9.32 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.

9.1 Funcionalidades da console de gerenciamento, integração e alta-disponibilidade

9.1.1 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; aplicações como Microsoft Active Directory e banco de dados Microsoft SQL Server, Oracle (Windows e Linux) e Oracle RAC (em Linux);
9.1.2 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;
9.1.3 Suportar cópia de segurança dos arquivos de catálogo e configuração, para promover recuperação dos serviços de gerenciamento no evento de falhas;
9.1.4 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;
9.1.5 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.

9.2 Suporte à Criptografia:

9.2.1 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;
9.2.2 Criptografia de dados no destino (servidor de backup);
9.2.3 Implementar no mínimo chaves de criptografia de 256 bits para cifrar os dados;
9.2.4 Implementar pares de chaves de criptografia de 4096 bits para recuperação de desastres;

9.3 Suportar protocolos IPv4 e IPv6 para rotinas de backup;

9.4 Integração com as seguintes aplicações para cópia e restauração

9.4.1 Realizar proteção e recuperação dos seguintes sistemas operacionais, aplicações, banco de dados e ambientes de virtualização:
9.4.2 Microsoft Windows 7 SP1, 8.1, 10, 11, Server 2008 R2 SP1, 2012, 2012 R2, 2016 e 2019;
9.4.3 Oracle Linux 6.x ou superiores;
9.4.4 Red Hat Enterprise Linux 6.x ou superiores;
9.4.5 Ubuntu 16.x ou superiores;
9.4.6 Debian 8.x ou superiores;
9.4.7 Microsoft Active Directory 2012 ou superiores;
9.4.8 Microsoft SQL Server 2012 ou superiores;
9.4.9 Oracle 11g R2 ou superiores (Linux ou Windows);
9.4.10 MySQL 5.6.x ou superiores;
9.4.11 PostgreSQL 9.4 ou superiores;
9.4.12 VMware ESX/ESXi 6.0 ou superiores;
9.4.13 Nutanix 5.10 ou superiores.

9.5 Suporte ao Active Directory

9.5.1 Executar cópia em tempo de execução do Microsoft Active Directory;
9.5.2 Possibilitar as seguintes opções de recuperação:

9.5.3 Recuperação de um objeto;
9.5.4 Recuperação de um atributo;
9.5.5 Recuperação de um atributo deletado de um objeto.

9.6 Suporte a Oracle e Oracle RAC

9.6.1 Deverá executar proteção e recuperação de base da dados Oracle e Oracle RAC com as seguintes características nativas ou não:
9.6.1.1 Executar proteção e recuperação das bases de dados do Oracle/Oracle RAC via RMAN e sem parada do banco;
9.6.1.2 Executar arquivamento do registro de eventos (log) possibilitando a criação de rotina de cópia para que ocorra com intervalos de 1 (uma) hora;
9.6.1.3 Permitir a cópia do arquivamento de transações (archives logs) baseados na quantidade de arquivamento (archives);
9.6.1.4 Permitir a configuração que após a cópia dos registros de transações (archives logs) os mesmos sejam mantidos ou deletados;
9.6.1.5 Além da proteção do Banco, a solução deverá proteger a área de catálogo, control file e sp
9.6.1.6 Possibilitar a recuperação com as seguintes características:
9.6.1.7 Recuperação completa da Base de dados no mesmo servidor
9.6.1.8 Recuperação completa da Base de dados em outro servidor
9.6.1.9 Recuperação de um datafile específico
9.6.1.10 Recuperação granular no nível de tabela
9.6.1.11. Recuperação em um momento do tempo específico;

9.7 Suporte a Microsoft SQL Server

9.7.1. Executar proteção e recuperação de base dos dados Microsoft SQL Server com as seguintes características nativas ou não:
9.7.1.1. Executar proteção e recuperação de bases de dados Microsoft SQL Server sem parada do banco;
9.7.1.2. Executar cópia de registro de transações (transaction log) possibilitando a criação de rotina de cópia para que ocorra com intervalos de 1 (uma) hora;
9.71.3. Permitir a configuração que após a cópia dos registros de transações (transaction log) os mesmos sejam mantidos ou deletados;
9.7.1.4. A solução deverá possibilitar a recuperação com as seguintes características:
9.7.1.5. Recuperação completa da base de dados no mesmo servidor
9.7.1.6. Recuperação completa da base de dados em outro servidor
9.7.1.7. Recuperação de uma base específica
9.7.1.8. Recuperação granular no nível de tabela
9.7.1.9. Recuperação em um momento do tempo específico;

9.8. Suporte a PostgreSQL

9.8.1. Executar proteção e recuperação de base da dados PostgreSQL Server com as seguintes características nativas ou não:
9.8.1.1. Cópia em tempo de execução do banco de dados;
9.8.1.2. Permitir a recuperação completa;
9.8.1.3. Restaurar a base de dados ou seus arquivos no mesmo servidor em caminho diferente;
9.8.1.4. Restaurar uma instância ou seus arquivos em um outro servidor.

9.9. Suporte a MySQL

9.9.1. Executar proteção e recuperação de base da dados MySQL Server com as seguintes características nativas ou não:
9.9.1.1. Cópia em tempo de execução do banco de dados;
9.9.1.2. Permitir a recuperação completa;
9.9.1.3. Restaurar a base de dados ou seus arquivos no mesmo servidor;
9.9.1.4. Restaurar uma instância ou seus arquivos em um outro servidor.

9.10. Suporte ao ambiente virtual (VMware e Acropolis Hypervisor)

9.10.1. Executar proteção e recuperação do Ambiente Virtual com as seguintes características:
9.10.1.1. 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;
9.10.1.2. No caso da restauração granular, não há necessidade de se restaurar a Guest VM inteira;
9.10.1.3. Permitir redirecionar a restauração de uma máquina virtual hospedada para uma pasta alternativa, outro volume de armazenamento;
9.10.1.4. Incluir automaticamente máquinas virtuais novas criadas dentro de seleções de cópias anteriores;
9.10.1.5. Permitir cópia completa (Full) e incremental para os servidores virtuais;
9.10.1.6. Ser capaz de realizar cópias e restauração de servidores virtuais Linux e Windows, sejam elas estado de consistência ou aplicação;

9.10.1.7. Permitir que as tarefas de cópias e restauração sejam realizadas via interface gráfica;
9.10.1.8. O backup dos servidores virtuais deverá ser armazenado de maneira desduplicada;
9.10.1.9. 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.
9.10.1.10. 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;
9.10.1.11. 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:
9.10.1.11.1. Deverá suportar a replicação remota a fim de replicar os dados das máquinas virtuais entre soluções de armazenamento distintas, inclusive de diferentes fabricantes;
9.10.1.11.2. Suportar a orquestração de failover e failback das máquinas virtuais replicadas;
9.10.1.12. Permitir a execução de uma máquina virtual diretamente de uma imagem de backup desduplicada e comprimida;
9.10.1.12.1. Essa funcionalidade deverá permitir sua execução de modo agnóstico ao servidor e repositório de backup utilizado, seja para vSphere ou para Acropolis;
9.10.1.12.1.1. Deverá permitir que a solução de virtualização empregada possa movimentar a máquina virtual para o ambiente de produção, posteriormente;
9.10.1.12.1.2. 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;
9.10.1.12.1.3. Permitir que uma máquina virtual Acropolis seja restaurada como máquina virtual VMware diretamente da imagem de backup;
9.10.1.13. 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;
9.10.1.13.1. Quaisquer atualizações realizadas somente deverão ser aplicadas nas máquinas após a restauração completa dos dados no ambiente de produção;
9.10.1.13.2. Ações executadas no ambiente isolados deverão ocorrer em infraestrutura temporária, sendo descartadas ou rotacionadas caso a máquina não venha a ser restaurada;

9.11. Funcionalidade de desduplicação de cópia e arquivamento

9.11.1. 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.
9.11.2. Implementar desduplicação a nível de blocos, não sendo aceita a técnica de Single-Instance Storage;
9.11.3. Implementar desduplicação 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;
9.11.4. Implementar desduplicação de blocos no destino (target-side deduplication), de forma que seja responsabilidade do servidor de transporte executar a tecnologia;
9.11.5. Implementar desduplicação de dados em tarefas de cópia;
9.11.6. Implementar desduplicação e compressão em uma mesma tarefa.
9.11.7. Implementar desduplicação em infraestrutura de armazenamento local (DAS) e vida rede (SAN e NAS);
9.11.8. A tecnologia de desduplicação 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);

9.12. Reportes e alertas

9.12.1. Vir disponível com os seguintes relatórios e reportes:
9.12.1.1. Histórico de rotinas de proteção concluídos nas últimas 24 horas, nos últimos 30 dias e nos últimos 6 meses;
9.12.1.2. Histórico de recuperações efetuadas nas últimas 24 horas, nos últimos 30 dias e nos últimos 6 meses;
9.12.1.3. Reportes de rotinas de backup concluídos com sucesso, com erro ou não concluídos;
9.12.1.4. Taxa de desduplicação por rotina de backup;
9.12.1.5. Possuir relatórios com as seguintes características:
9.12.1.5.1. Horário de início e término de uma rotina de backup;
9.12.1.5.2. Tempo de duração de uma rotina de backup;
9.12.1.5.3. Status do backup (situação):
9.12.1.5.3.1. Relação dos objetos incluídos na rotina de backup;
9.12.1.5.3.2. Horário de início e término do backup de cada objeto;
9.12.1.5.3.3. Tempo de duração do backup de cada objeto;
9.12.1.5.3.4. Volume de dados na origem durante a rotina de backup;
9.12.1.5.3.5. Volume de dados trafegados durante a rotina de backup;
9.12.1.5.3.6. Volume de dados com compressão e desduplicação;
9.12.1.5.3.7. Taxa de desduplicação de dados;

9.12.1.5.3.8. Taxa de compressão de dados;
9.12.1.6. A solução ofertada deverá enviar os seguintes alertas via e-mail:
9.12.1.7. Rotina de backup finalizada com sucesso;
9.12.1.8. Rotina de backup finalizada com erro;
9.12.1.9. Rotina de backup com problema;
9.12.1.10. Alerta para utilização de licenciamento

9.13. Unidade de armazenamento de informação

9.13.1. Características Gerais
9.13.1.1. Ser homologada pelo software de proteção ofertada;
9.13.1.2. Prover infraestrutura de armazenamento, voltados para a proteção de dados do ambiente de hiper convergência, nuvem privada ou arquitetura em 3 camadas;
9.13.1.3. Corresponder a um módulo de armazenamento de backup em disco, com o propósito específico de ingestão dos dados de backup com compactação, desduplicação e replicação (local e remota/nuvem) dos dados desduplicados;
9.13.1.4. 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;
9.13.1.5. Constar no site do fabricante (documento oficial e público) como um sistema de armazenamento de backup em disco, em linha de produção;
9.13.1.6. Não serão aceitas soluções definidas por Software (Virtual Appliance);
9.13.1.7. O hardware do módulo de armazenamento de cópias em disco não poderá ser compartilhado com nenhum outro software para operar;
9.13.1.8. 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;
9.13.1.8.1. 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;
9.13.1.9. Estar licenciada para toda sua capacidade e funcionalidade, incluindo replicação;
9.13.1.10. Permitir o particionamento lógico da área de armazenamento, sem prejuízo às características de desduplicação solicitadas neste certame;
9.13.1.11. 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);
9.13.1.12. 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;
9.13.1.13. Possuir mecanismos que protejam contra a inconsistência dos dados mesmo em casos de interrupção abrupta ou desligamento acidental;
9.13.1.14. 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;
9.13.1.14.1. Deverá possuir, no mínimo, 1 (um) disco configurado como hot-spare;
9.13.1.15. Possuir funcionalidade de desduplicação dos dados em nível de bytes ou blocos, com capacidade de eliminação de dados redundantes para racionalizar a utilização do espaço de armazenamento;
9.13.1.16. Implementar desduplicação 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 desduplicação e garantindo que os dados sejam gravados uma única vez;
9.13.1.17. Suportar simultaneamente acessos de leitura e gravação pelos protocolos CIFS e NFS;
9.13.1.18. Suportar a implementação do OpenStorage Technology;
9.13.1.19. Permitir a criação de backups sintéticos completos, do software de proteção ofertado, internamente no appliance;
9.13.1.20. Permitir a execução de processos de backup e restore em paralelo;
9.13.1.21. 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;
9.13.1.21.1. 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;
9.13.1.22. Integração entre o software de proteção ofertado e o módulo de armazenamento:
9.13.1.22.1. 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;
9.13.1.22.2. Deverá permitir a restauração de máquinas virtuais, arquivos únicos e objetos/arquivos específicos de aplicações diretamente do repositório de armazenamento;

9.13.1.23. Possuir funcionalidade para replicação de cópias em equipamento similar e do mesmo fabricante de forma assíncrona, utilizando recursos de desduplicação e reduzindo consumo do link de comunicação, através de rede IP (WAN/LAN);
9.13.1.24. Possuir arquitetura baseada em camadas que permita a proteção contra “ransomware attack”, independente do software de backup.
9.13.1.24.1. 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.
9.13.1.24.1.1. Tal atraso de deleção deve ser configurável em dias, proporcionado ao menos o atraso por 15 dias.
9.13.1.24.1.2. Para desativação ou modificação desse recurso deve ser possível requerer escalação e duplo fator de autenticação.
9.13.1.24.2. 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.
9.13.1.25. 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;
9.13.1.26. 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;
9.13.1.27. Deverá possuir integração com Microsoft Active Directory para autenticação de usuários quanto ao acesso a interface de gerência da solução;
9.13.1.28. Deverá permitir a implementação de topologias de replicação, como 1 para 1, 1 para N e o cascateamento de equipamentos. A solução deverá permitir a criação de topologias de nuvem privada e híbrida;
9.13.1.29. 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.
9.13.1.30. 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;
9.13.1.31. 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;
9.13.1.31.1. 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.

9.14. Unidade de armazenamento de informação - tipo 1

9.14.1. Possuir 149 TB (cento e quarenta e nove terabytes) de área útil;
9.14.2. Possuir alguma das seguintes arquiteturas para o módulo de armazenamento:
9.14.2.1. Scale-up: Soluções com arquitetura tradicional (crescimento veritical) 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:
9.14.2.1.1. Entregar duas controladoras, no mínimo no modelo ativo-passivo, com discos sólidos (SSD) para aceleração de desduplicação e reconstrução de dados (rehidratação);
9.14.2.1.2. 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;
9.14.2.1.3. 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;
9.14.2.1.4. 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;
9.14.2.1.5. Deverá ser entregue habilitado para desduplicar sua máxima capacidade suportada.
9.14.2.2. 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:
9.14.2.3. 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;
9.14.2.4. 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;
9.14.2.5. Deverá ser entregue habilitado para desduplicar sua máxima capacidade suportada.
9.14.3. Ser fornecido com portas Ethernet de 10Gbps do tipo SFP+, com suas respectivas GBICS, na quantidade suficiente para que o desempenho especificado seja alcançado;
9.14.4. Deverá possuir, no mínimo, 16 (dezesseis) núcleos de processamento, com o dobro de threads, por controladora entregue;
9.14.5. Deverá ser entregue com o máximo de memória suportado pelo equipamento, conforme divulgado em documentação oficial da fabricante;
9.14.6. 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;
9.14.7. A solução deverá estar licenciada para receber imagens de backup desduplicadas na origem;
9.14.8. Ter pelo menos 1 (um) Porta IPMI, 2 (Duas) Portas 1GB Ethernet e 2 (Duais) portas 10GB SFP+.

9.15 Unidade de armazenamento de informação - tipo 2

9.15.1. Possuir 62 TB (sessenta e dois terabytes) de área útil;
9.15.2. Possuir alguma das seguintes arquiteturas para o módulo de backup:
9.15.2.1. Scale-up: Soluções com arquitetura tradicional (crescimento veritical) 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:
9.15.2.1.1. Entregar duas controladoras, no mínimo no modelo ativo-passivo, com discos sólidos (SSD) para aceleração de desduplicação e reconstrução de dados (rehidratação);
9.15.2.1.2. 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;
9.15.2.1.3. 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;
9.15.2.1.4. 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;
9.15.2.1.5. Deverá ser entregue habilitado para desduplicar sua máxima capacidade suportada.
9.15.2.2. 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:
9.15.2.2.1. 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;
9.15.2.2.2. 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.
9.15.2.2.3. Deverá ser entregue habilitado para desduplicar sua máxima capacidade suportada.
9.15.2.3. Ser fornecido com portas Ethernet de 10Gbps do tipo SFP+, com suas respectivas GBICS, na quantidade suficiente para que o desempenho especificado seja alcançado;
9.15.2.4. Deverá possuir, no mínimo, 6 (seis) núcleos de processamento, com o dobro de threads, por controladora entregue;
9.15.2.5. Deverá ser entregue com o máximo de memória suportado pelo equipamento, conforme divulgado em documentação oficial da fabricante;
9.15.2.6. 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;
9.15.2.7. A solução deverá estar licenciada para receber imagens de backup desduplicadas na origem;
9.15.2.8. Deve ter pelo menos 1 (um) Porta IPMI, 2 (Duas) Portas 1GB Ethernet e 2 (Duais) portas 10GB SFP+.

9.16. Fitoteca de armazenamento modular

9.16.1. Características Gerais
9.16.1.1. Ser composto por todos os equipamentos e acessórios necessários para plena instalação e funcionamento;
9.16.1.2. 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;
9.16.1.3. Gabinete para rack, com tamanho máximo de 3U, acompanhado de:

9.16.1.3.1. Cabo de alimentação compatível com as PDU's do Rack;
9.16.1.3.2. Trilhos e demais elementos de fixação necessários para a instalação em rack de 19 polegadas, do próprio fabricante dos equipamentos;
9.16.1.3.3. Possuir fonte de alimentação redundante 110/220Vac;
9.16.1.3.4. 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;
9.16.1.3.5. 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.
9.16.1.3.6. 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:
9.16.1.3.6.1. Atualização de software e/ou aplicação de correções;
9.16.1.3.6.2. Revisão do ambiente para validação das configurações e, se necessário, realizar os ajustes com as melhores práticas indicadas;
9.16.1.3.6.3. Abertura de chamados de suporte direto com engenheiro de nível 2, sem necessidade de triagem de nível 1;
9.16.1.3.6.4. Reinstalações ou reconfigurações que se fizerem necessárias, mesmo que não sejam decorrentes de problemas de suporte.

9.17. Fitoteca de Armazenamento – base

9.17.1. Suportar múltiplos caminhos e particionamento lógico;
9.17.2. Suportar funcionalidade de alta disponibilidade de caminhos que garanta o uso de um caminho de comunicação redundante quando o caminho principal falha;
9.17.3. Suportar até 3 unidades LTO 6, 7 ou 8;
9.17.4. 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;
9.17.5. Ser acompanhada por no mínimo 2 (duas) portas SAS de 6 Gb;
9.17.6. Ter compatibilidade de leitura e escrita com o padrão LTO-6, e de leitura com o padrão LTO-5;
9.17.7. Cada unidade de leitura e gravação deverá possuir taxa de transferência de no mínimo 300 Mbps, sem o uso de compressão;
9.17.8. Cada unidade deverá ser acompanhada por no mínimo 2 (dois) cabos Mini-SAS para SAS de 1,5 m;
9.17.9. O equipamento deverá ser do tipo "library", com capacidade de armazenamento mínima para 40 (quarenta) cartuchos LTO-7;
9.17.10. Contar com interface Ethernet dedicada para gerenciamento, através de redes TCP/IP, compatível com os protocolos HTTP e SNMP;
9.17.11. Possuir dispositivo que permita a identificação dos cartuchos por código de barras;
9.17.12. Estar acompanhado de 35 (trinta e cinco) cartuchos normais de fita, no padrão LTO-7, e quatro cartuchos de limpeza;
9.17.13. Os cartuchos já devem ser acompanhados das respectivas etiquetas de código de barras;
9.17.14. Ser compatível, e estar homologado, com os sistemas operacionais:
9.17.14.1. Microsoft Windows Server 2016 ou superior;
9.17.14.2. Red Hat Enterprise Linux 7.6 ou superior;
9.17.14.3. SUSE Linux Enterprise Server (SLES) 15 ou superior.
9.17.15. Vir acompanhado também da unidade de controle, que deve possuir no mínimo:
9.17.15.1. Sistema operacional base licenciado, Microsoft Windows Server 2016 ou superior. Não serão aceitos softwares que não possuam suporte da fabricante;
9.17.15.1.1. 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;
9.17.15.2. Entregue com redundância de CPU, com no mínimo 8 cores e hyperthread. Deverão ser da última geração de processadores ofertados pela fabricante do mesmo;
9.17.15.3. Suporte a CPUs com memória base de 2.400, 2.666 e 2.933 MHz;
9.17.15.4. Entregue com 32 GB de memória RAM;
9.17.15.4.1. 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;
9.17.15.5. Entregue com 2 (duas) interfaces de rede de 10Gbps e cabos passivos de conexão direta e 5,0m;
9.17.15.6. Respeitando as seguintes características de armazenamento:
9.17.15.6.1. Placa de hardware RAID com 2GB de cache;
9.17.15.6.2. Suporte aos níveis RAID 0, 1, 10, 5, 50, 6, 60;
9.17.15.6.3. Suporte a discos HDD, SSD e SED;
9.17.15.6.4. Com 2 (duas) interfaces Mini-SAS de 12Gb/s;
9.17.15.6.4.1. Deverá possuir, no mínimo, um slot extra para expansão de HBAs;

9.17.15.7. Respeitando as seguintes características de gerenciamento:
9.17.15.7.1. Controlar o consumo energético do módulo;
9.17.15.7.2. Permitir o gerenciamento remoto da solução;
9.17.15.7.3. Permitir o gerenciamento IPMI-over-LAN;
9.17.15.7.4. Permitir o mapeamento de imagens através de compartilhamentos HTTPS, SFTP, CIFS e NFS;
9.17.15.7.5. Permitir o uso concomitante da interface de gerência por, no mínimo, 6 (seis) usuários;
9.17.15.7.6. Permitir o controle de consumo de banda de rede;
9.17.15.8. Possuir fontes e ventiladores hot-swap e redundantes, com tensão bivolt;

9.18. Fitoteca de Armazenamento – Expansão

9.18.1.1. Suportar até 3 unidades LTO 6, 7 ou 8;
9.18.1.2. 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;
9.18.1.3. Cada unidade LTO-7 deverá possuir conectividade SAS, de no mínimo, 6Gb com 2 portas por unidade LTO;
9.18.1.4. Cada unidade deverá ser acompanhada por no mínimo 2 (dois) cabos Mini-SAS para SAS de 1,5 m;
9.18.1.5. Ter compatibilidade de leitura e escrita com o padrão LTO-6, e de leitura com o padrão LTO-5;
9.18.1.6. Cada unidade de leitura e gravação deverá possuir taxa de transferência de no mínimo 300 Mbps, sem o uso de compressão;
9.18.1.7. O equipamento deverá ser do tipo “Expansion module”, com capacidade de armazenamento mínima para 40 cartuchos LTO-7;
9.18.1.8. Estar acompanhado de 35 (trinta e cinco) cartuchos normais de fita, no padrão LTO-7;
9.18.1.9. 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;
9.18.1.10. Os cartuchos já devem ser acompanhados das respectivas etiquetas de código de barras.

9.19. Serviço instalação e configuração

9.19.1. Desenvolver documentação mínima de projeto que inclua cronograma, recursos e plano de implantação;
9.19.2. A CONTRATADA deverá definir a quantidade de esforço em horas, para escopo desejado pela CONTRATANTE;
9.19.3. Conforme acordados entre as partes, as atividades podem ser executadas remotamente ou fisicamente;
9.19.4. CONTRATANTE deverá aprovar o plano de execução apresentado pela executora;
9.19.5. A aprovação poderá ocorrer por email ou outros meios oficiais utilizados pelo órgão;
9.19.6. As atividades previstas são:
9.19.6.1. Instalação física dos equipamentos;
9.19.6.2. Inicialização dos equipamentos;
9.19.6.3. Atualização com as versões mínimas recomendados pelo fabricante;
9.19.6.4. Configuração de movimentadores de dados;
9.19.6.5. Configuração de entidades intermediárias;
9.19.6.6. Configuração de unidade de fita;
9.19.6.7. Configuração de agentes;
9.19.6.8. Configuração de políticas de proteção e cópia;
9.19.6.9. Configuração de relatórios;
9.19.6.10. Configuração de repositórios;
9.19.6.11. Aplicação de políticas e cópias de auto-proteção;
9.19.6.12. Configuração de rotinas de alertas;
9.19.6.13. Avaliação de desempenho;
9.19.6.14. Realização de ajustes de desempenho;
9.19.6.15. Execução de plano de testes;
9.19.6.16. Documentação da solução implantada
9.19.7. Acompanhar localmente ou remotamente durante 8 (horas), após implantação no decorrer de 5 dias.

9.20. Serviço de capacitação

9.20.1. Ser ofertado treinamento oficial focado na administração do serviço de proteção e recuperação;
9.20.2. 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 Acre possam acompanhar todo o trabalho de implantação da solução com o embasamento técnico necessário para entender as atividades a serem executadas pela CONTRATADA;
9.20.3. O treinamento não poderá ser completamente teórico, devendo incluir laboratórios e simulações em ambiente propício a treinamento;
9.20.4. 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:
9.20.4.1. Conceitos, arquitetura, topologia e componentes da solução fornecida;

9.20.4.2. Definição de políticas, agendamento, parâmetros de desduplicação e de execução dos backups / restores via Rede Local;
9.20.4.3. Realização de cópias de segurança manuais;
9.20.4.4. Procedimentos de restauração de backups pelo cliente e pelo servidor;
9.20.4.5. Gerenciamento de “backup” e “restore” de catálogo;
9.20.4.6. Utilização de scripts pré e pós “backup;
9.20.4.7. Definição e execução de “backup” e “restore” do Microsoft Exchange, inclusive recuperação de caixas postais individuais;
9.20.4.8. Definição e execução de “backup” e “restore” do SQL Server, inclusive recuperação de bases de dados;
9.20.4.9. Definição e execução de “backup” e “restore” do Oracle;
9.20.4.10. 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.
9.20.5. 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;
9.20.6. O treinamento deverá capacitar à equipe do TJAC a operar, configurar, administrar e resolver problemas usuais na solução ofertada, englobando todos os componentes da solução;
9.20.7. O treinamento será ministrado a 6 (seis) participantes. A composição das turmas será de responsabilidade da CONTRATANTE;
9.20.8. 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
9.20.9. 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:
9.20.9.1. Conceitos básicos e componentes da solução;
9.20.9.2. Configuração dos repositórios no sistema de armazenamento de cópias de proteção;
9.20.9.3. Configuração de replicação de dados;
9.20.9.4. Monitoramento e gestão da ferramenta.
9.20.10. 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;
9.20.11. Os dias e horários de execução dos treinamentos serão acordados juntamente com a CONTRATANTE;
9.20.12. Ao final do treinamento deverá ser emitido certificado de participação a cada participante, especificando conteúdo abrangido e carga horária do treinamento.

10. JUSTIFICATIVA PARA O PARCELAMENTO OU NÃO DA SOLUÇÃO

Não haverá necessidade de parcelamento da aquisição

11. PROVIDÊNCIAS PARA ADEQUAÇÃO DO AMBIENTE DO ÓRGÃO

Não haverá necesidade de adequações previamente a celebração do contrato. O próprio objeto da contratação prevê treinamento para utilização da solução a ser adquirida.

13. DA EQUIPE DE PLANEJAMENTO

Nome	Função	Lotação
Elson Correia de Oliveira Neto	Gerente de Segurança da Informação	GESEG/DITEC
Issac Timoteo Oliveira Junior	Supervisor Administrativo	GESEG/DITEC

12. DECLARAÇÃO DE VIABILIDADE

Com base nas informações levantadas ao longo do estudo preliminar, bem como nos registros dos contratos anteriores, a equipe de planejamento aprova o presente E.T.P.

Documento assinado eletronicamente por **Elson Correia de Oliveira Neto**, **Gerente**, em 22/08/2022, às 18:15, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Isaac Timoteo Oliveira Junior**, **Técnico(a) Judiciário(a)**, em 23/08/2022, às 07:30, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tjac.jus.br/verifica informando o código verificador **1256565** e o código CRC **F49AA118**.