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. DO OBJETO

1.1. O presente Termo de Referência tem por objeto a contratação de empresa especializada para a prestação de serviços de gestão e armazenamento de documentos eletrônicos dos processos judiciais. Os serviços de gestão deverão promover o armazenamento e o rápido acesso aos documentos eletrônicos, por meio de atributos WORM (uma gravação e várias leituras) de proteção contra regravação e contra exclusão. Devendo ser executadas todas as atividades abaixo listadas:
1.1.1. Autenticação do conteúdo: todos os documentos eletrônicos oriundos do SAJ deverão ser armazenados de modo inalterável, autenticado e transparente.
1.1.2. Garantia de autenticidade e integridade: A solução deverá possuir proteção contra alteração dos documentos eletrônicos armazenados;
1.1.3. Proteção contra exclusão (controle de retenção): A solução deverá possuir nativamente controle de retenção e controles que impeça o apagar dos documentos eletrônicos enquanto estes estiverem dentro do período de retenção estabelecido. Os períodos de retenção deverão ser configurados de acordo com o tipo ou a classe do documento eletrônico;
1.1.4. Redimensionamento sem reconfiguração: A arquitetura da solução deve ser baseada em RAIN (Redundant Arrays of Independent Nodes, arrays redundantes de nós independentes), projetada para ser dimensionável e acomodar grandes volumes de conteúdo;
1.1.5. Proteção de continuidade de negócios e recuperação de desastres: A solução deve ser configurada para replicar e manter cópias dos documentos eletrônicos em site remoto, eliminando a possibilidade de que um desastre no local destrua todas as cópias das informações;
1.1.6. Auditoria de remoção: A solução deve registrar as informações sobre os documentos apagados após o período de retenção, assegurando rastreabilidade dos repositórios;
1.1.7. Escalabilidade: A solução deve ser escalável para acomodar grandes volumes de documentos até pentabytes.

2. DA JUSTIFICATIVA

2.1. O Tribunal de Justiça do Estado do Amazonas – TJAM, tem desenvolvido nas últimas décadas políticas e estratégias relacionadas à Tecnologia de Informação e Comunicação, mantendo-se alinhado com as políticas nacionais de informatização do Poder Judiciário. As políticas aplicadas no segmento de Tecnologia da Informação resultaram na modernização na gestão dos processos judiciais, por meio de solução informatizada para virtualização dos processos judiciais de forma segura e confiável, instrumentalizando a prestação jurisdicional para que a resolução dos conflitos e a pacificação social venham a ocorrer com maior celeridade e produtividade, tudo no interesse maior do Tribunal de Justiça do Estado do Amazonas. Tendo em vista o supracitado, torna-se imprescindível a adoção de medidas capazes de assegurar a integridade/confiabilidade das informações armazenadas nos bancos de dados utilizados pelo sistema de automação do judiciário - SAJ. Não obstante, a despeito destas importantes conquistas e benefícios, a propagação destas iniciativas demanda ações visando melhorias na gestão e no armazenamento dos documentos eletrônicos, uma vez que o volume de peças digitalizadas ou nativamente digitais no banco de dados do TJAM cresce em ritmo acelerado, demandando novas soluções para a gestão do crescimento deste acervo no curto e médio prazo. Projeta-se que dentro em breve haverá sérios problemas de ordem prática, a saber:
2.1.1. Degradação de performance: com o crescimento do volume de documentos, o hardware e o software serão cada vez mais penalizados, com reflexos negativos na performance da aplicação;
2.1.2. Risco de indisponibilidade operacional: com o uso do Processo Digital a Instituição torna-se dependente do documento neste meio. Assim, uma eventual falha no ambiente operacional (ex: hardware) poderá paralisar a distribuição e a tramitação processual, causando sérios prejuízos à prestação jurisdicional e à reputação da Instituição;
2.1.3. Integridade da informação: atualmente os documentos são armazenados em tabelas do banco de dados.

Embora estas tabelas estejam protegidas sob algumas políticas e controles de segurança, sabe-se que o acesso a elas pode ser realizado por determinados usuários com privilégios elevados. Assim, estes documentos estão, em certa medida, vulneráveis, podendo causar prejuízos enormes de ordem econômica, ética e legal;
2.1.4. Inviabilização do backup: Se mantido as mesmas mídias atuais de armazenamento, o backup rotineiro das informações do sistema SAJ, que já encontra-se em níveis críticos, a médio prazo será impraticável, em razão do volume de documentos existentes no repositório. A "janela de backup" disponível será insuficiente para ler e salvar as informações na mídia de contingência, em função do grande volume de documentos. Da mesma forma, o procedimento de restore de informações, caso necessário, tende a comprometer a disponibilidade dos sistemas aplicativos por um longo período de tempo.
2.1.4.1. Nesse viés, com o escopo de trazer um reporte quantitativo da situação atual do TJAM associada a uma projeção para os próximos anos, a DVTIC, através de levantamentos obtidos, realizou análises internas e projeções para destacar a economia que será alcançada com a implantação da solução de armazenamento seguro, de forma totalmente sustentável, ante o crescimento das bases de dados, vejamos:
2.1.4.2. Através dos dados coletados observa-se que, tomando por base a capacidade de armazenamento atual do conjunto de bases do SAJ (PG, SG e NET), já se tem o total parcial em 2016 de 19 terabytes consumidos, conforme imagem abaixo:

Crescimento da base de dados (Tb)					
Bases	2016	2017	2018	2019	2020
PG, SG e NET	19,067	24,454	31,363	40,223	51,588

2.1.4.3. Com isso, através de projeção realizada, em 2020, utilizando-se as mesmas mídias atuais de armazenamento e considerando a atual taxa de crescimento de 28,25% (ano), o TJAM chegará a um total de mais de 51 terabytes, que corresponderão a um aumento de 270,5%; tal crescimento irá impactar diretamente na capacidade e disponibilidade do storage do TJAM, inclusive para execução plena das aplicações SAJ.
2.1.4.4. Com a implantação da solução de armazenamento seguro no TJAM, projeta-se uma economia de armazenamento de 85,3%, de acordo com os dados inframencionados, nota-se a vultosa economia e redução de armazenamento em storage que a solução poderá gerar, vejamos:

Armazenamento com solução de armazenamento seguro (Tb)					
Bases	2016	2017	2018	2019	2020
PG, SG e NET	2,805	3,597	4,613	5,917	7,589

2.1.4.5. Os dados coletados nos apresentam um cenário de armazenamento em storage já no primeiro ano com economia de quase 21 terabytes em 2017, e em 2020, dentro da projeção realizada, um armazenamento que reduzirá de 51,5 para 7,5 terabytes (Redução de 44 Tb), totalizando dessa forma ao TJAM uma economia de armazenamento em torno de 85,3%.
2.1.4.6. Ainda no que concerne à economicidade, é de bom alvitre trazer ao contexto o tempo de backup realizado pelo TJAM atualmente, bem como a projeção para os próximos anos.
2.1.4.7. De acordo com o levantamento realizado e disposto acima, o TJAM precisa hoje de 51h55min para concluir o processo de backup de dados do conjunto de bases de Produção, ou o equivalente a mais de 2 dias.
2.1.4.8. Ainda, levando-se em consideração a projeção realizada através do estudo e levantamento executados, bem como a elevada taxa de crescimento das bases (28,25% ao ano), o TJAM, em 2020, precisará de 140h27min, isto é, mais de 5 dias, para execução e conclusão do backup em comento, se utilizado o mesmo procedimento de backup e armazenamento atual.
2.1.4.9. Com isso, a solução de armazenamento seguro vem propondo a reversão desse cenário, para dar guarida e sustentabilidade ao TJAM na redução drástica desses números. Ante o levantamento e estudo realizados, o tempo de backup reduzirá já de imediato (2017) de 66h35min para 06h12min, o que corresponde a uma minoração de 91% no tempo de execução, totalizando, dentro do contexto apresentado na projeção acima (até 2020), um ganho/economia de tempo de 90,68%.

Tempo de backup (Horas)					
Bases	2016	2017	2018	2019	2020
BKP atual	51:55	66:35	85:23	109:31	140:27
Backup com solução de armazenamento seguro	4:50	6:12	7:57	10:12	13:05

2.1.4.10. Novamente reforçamos, se mantido o mesmo método atual, o backup rotineiro destas informações será impraticável, em razão do volume de documentos existentes no repositório. A "janela de backup" disponível será insuficiente para ler e salvar as informações na mídia de contingência, em função do grande

volume de documentos. Da mesma forma, o procedimento de restore de informações, caso necessário, tende a comprometer a disponibilidade dos sistemas aplicativos por um longo período de tempo.
2.1.4.11. Ante ao exposto, importa mais uma vez destacar quanto à necessária adoção de um novo método/solução para gerir o aumento deste acervo, desde que atendendo aos requisitos de alta disponibilidade, segurança, retenção de dados e performance.
2.2. Igualmente preocupante são as dificuldades observadas para atender aos requisitos de conformidade e regulamentações específicas aplicáveis ao Processo Digital. A Lei 11.419/06, por exemplo, em seu art. 12 § 1o estabelece fortes exigências de segurança e preservação do acervo digital, ao determinar que “Os autos dos processos eletrônicos deverão ser protegidos por meio de sistemas de segurança de acesso e armazenados em meio que garanta a preservação e integridade dos dados, sendo dispensada a formação de autos suplementares.” (grifo nosso).
2.3. Em termos práticos, isso significa que as peças digitais precisam ser protegidas quanto à sua integridade e armazenadas em dispositivos que garantam a sua preservação, evitando que os autos sejam alvo de adulteração ou eliminação indevida. Estes são requisitos de difícil atendimento com as plataformas atualmente em uso, que não foram projetadas para operar com este tipo de aplicação. É fato que os servidores de arquivos não são preparados para armazenar milhões de objetos, nos moldes demandados pelo Processo Digital. Já os sistemas de banco de dados relacionais (SGBDs), por sua vez, perdem desempenho gradativamente e não conseguem escalar adequadamente para grandes volumes de objetos (BLOBs).
2.4. Cabe lembrar que os sistemas de arquivos tradicionais, assim como os sistemas de bancos de dados, proporcionam apenas níveis básicos de controle de integridade. Os objetos neles armazenados podem ser acessados por usuários privilegiados, colocando em risco a integridade e confiabilidade do acervo. Acrescente-se, ainda, que os documentos deverão ser mantidos por períodos que podem chegar a mais de vinte anos. Este requisito adiciona significativa complexidade ao cenário de gestão do acervo digital, e requer um planejamento adequado, com visão de médio e longo prazos.
2.5. Ante o exposto, entendemos que é preciso repensar a estratégia atualmente em uso, implementando ações práticas, focadas em conceber e adotar um modelo sólido e planejado de gestão dos acervos digitais, sob pena de um colapso na capacidade operacional do ambiente de TI da Instituição, dentre outros riscos vislumbrados. Isto ocasionaria sérios prejuízos institucionais, motivo pelo qual passamos a detalhar uma proposta de solução para mitigar estes riscos, preservando o investimento e os benefícios auferidos com as inovações introduzidas com o uso do Processo Digital.
2.6. O projeto proposto visa à ampliação e consolidação da virtualização da justiça estadual amazonense, objetivando aumentar o nível de segurança dos procedimentos de gestão e armazenamento de documentos dos processos digitais da Justiça Estadual por meio de solução especifica, de modo a aumentar os ganhos e benefícios oriundos das tecnologias relacionadas ao processo digital, e também atender aos requisitos de segurança e a preservação de informações, apresentando conformidade ao padrão de gestão documental regulamentado pelo Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Poder Judiciário.

3. DA 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:
3.2 Resolução n° 25/2019 TJ-AM de 15 de janeiro de 2020.

4. DO REGISTRO DE PREÇO

4.1. O objeto deste Termo de Referência **não** será contratado mediante Sistema de Registro de Preços, na medida em que a contratação não se enquadra nas condições estabelecidas no art. 3º do Decreto nº. 7892/2013.

5. DAS ESPECIFICAÇÕES DO OBJETO

5.1. Armazenamento e capacidade de processamento
5.1.1. A Solução de Armazenamento Seguro deverá ser composta por 2 (dois) subsistemas de armazenamento independentes denominados subsistemas, a serem instalados em dois sites distintos;
5.1.2. Os subsistemas deverão ser interligados para fins de replicação e deverão replicar seu conteúdo de forma automática e assíncrona.
5.1.3. Cada conjunto da Solução de Armazenamento Seguro deverá possuir capacidade líquida de, no mínimo, 150 TB (Terabytes) em disco. Para o cálculo da capacidade líquida de armazenamento:
5.1.3.1. Subtrair as áreas utilizadas para algoritmos de proteção;
5.1.3.2. Subtrair as áreas utilizadas para dynamic-spare;
5.1.3.3. Subtrair as áreas utilizadas para nodes-spare;
5.1.3.4. Subtrair as áreas utilizadas para uso interno da Solução;
5.1.3.5. Subtrair as áreas utilizadas para o armazenamento dos índices para localização dos objetos

arquivados;
5.1.3.6. Desconsiderar qualquer tipo de compactação ou compressão de dados;
5.1.3.7. Adotar para 01 TB (um terabyte) o valor de 2^40 (dois elevado à potência quarenta) bytes.
5.1.4. A Solução deverá utilizar arquitetura RAIN (Redundant Array of Independent Nodes) ou utilizar arquitetura RAID (Redundant Array of Independent Disks).
5.1.5. A capacidade de armazenamento deverá ser configurada para utilização em uma das arquiteturas de proteção abaixo:
5.1.5.1. RAID-4, na combinação 7D + 1P;
5.1.5.2. RAID-5, nas combinações 6D+1P, 5D+1P ou 4D+1P;
5.1.5.3. RAID-6, com 2 (dois) discos de paridade, na combinação 5D+2P ou 6D+2P;
5.1.5.4. RAIN em Mirroring na combinação 1N+1N;
5.1.5.5. Para todas as arquiteturas descritas neste item, cada conjunto da Solução de Armazenamento Seguro deverá garantir que os objetos armazenados continuem acessíveis em caso de falha/perda de qualquer um dos nodes que compõem a Solução, independentemente da funcionalidade de replicação;
5.1.5.6. Para todas as arquiteturas descritas neste item, cada conjunto da Solução de Armazenamento Seguro deverá garantir que os objetos armazenados continuem acessíveis em caso de falha/perda de qualquer um dos HDs que compõem a Solução, independentemente da funcionalidade de replicação.
5.1.6. A solução deverá contar com proteção por espelhamento de dados e não de discos, ou seja, todo objeto gravado deverá ter uma cópia idêntica disponível;
5.1.7. Em nenhuma circunstância a falha de um dos componentes do equipamento poderá comprometer mais do que 25% da disponibilidade e performance do mesmo.
5.1.8. Cada conjunto da Solução de Armazenamento Seguro deverá suportar escalabilidade até, no mínimo, 200 TB (duzentos terabytes) de capacidade líquida em disco de acordo com o item 4.1.5, sem a necessidade de interrupção no acesso aos dados pelas aplicações e em um único cluster.
5.1.9. Cada conjunto da Solução de Armazenamento Seguro deverá suportar escalabilidade para endereçar, no mínimo, 5.000.000.000 (cinco bilhões) de objetos líquidos em um único cluster.
5.1.10. Cada subsistema deverá ser compatível com os sistemas operacionais WINDOWS 2003 SP4, Windows 2008 Server – Standard e Enterprise (32 bits e 64 bits), Linux, AIX, HP-UX e Solaris.
5.1.11. Todo e qualquer recurso necessário para a comunicação entre os nodes deverá fazer parte da Solução de Armazenamento Seguro e estar contemplado na proposta.
5.1.12. Todos os HDs (Hard Disks) da Solução de Armazenamento Seguro deverão possuir as mesmas características de tamanho, capacidade de armazenamento, taxa de transferência na interface e velocidade de rotação, conforme segue:
5.1.12.1. Interface SATA com taxa de transferência 3 (três) Gbps (Gigabits por segundo) ou superior;
5.1.12.2. Capacidade máxima de armazenamento de 1 (hum) TB (Terabyte), sem considerar qualquer tipo de compressão ou compactação dos dados;
5.1.12.3. Velocidade mínima de rotação de 7.200 (sete mil e duzentos) RPM (Rotações Por Minuto).
5.1.13. O diâmetro máximo de cada HD dos subsistemas de discos propostos é de 3,5 (três e meia) polegadas.
5.1.14. A solução deverá permitir expansão futura com discos rígidos de maior capacidade operando simultaneamente no mesmo subsistema.
5.1.15. Cada conjunto da Solução de Armazenamento Seguro deverá ser novo, de primeiro uso, com garantia do fornecedor de que nunca foi usado e de que sua descontinuação ainda não foi anunciada pelo fabricante. Caso a Solução seja descontinuada até a data de licitação, o fornecedor deverá entregar outra, em substituição, com qualidade superior e sem ônus adicional para o Tribunal de Justiça.
5.1.16. Deverá permitir a coexistência de nodes de diferentes capacidades de processamento e de HDs de diferentes capacidades de armazenamento.
5.1.17. Cada conjunto da Solução deverá possuir redundância de todos os seus componentes, de maneira que não haja interrupção no seu funcionamento devido a um ponto único de falha.
5.1.18. Cada conjunto da Solução deverá possuir suporte remoto pró-ativo e auto-call, com monitoração 24 (vinte e quatro) horas, 7 (sete) dias por semana. Os dispositivos necessários para a implementação da funcionalidade serão de responsabilidade do fornecedor, à exceção da linha telefônica comum.
5.1.19. As manutenções ou substituições de componentes defeituosos da Solução de Armazenamento Seguro deverão ocorrer de forma totalmente transparente, ou seja, sem causar qualquer tipo de indisponibilidade no acesso aos dados pela aplicação ou ingestão de novos objetos.
5.1.20. A Solução de Armazenamento Seguro deverá possuir caminhos de conexão redundantes, que permitam aos servidores a ela conectados a utilização de caminho alternativos para o caso de falha em qualquer das conexões.

5.1.21. Os componentes da Solução de Armazenamento Seguro deverão ser montados em RACKS, que deverão ser fornecidos junto com a Solução. Os RACKS deverão possuir circuito elétrico redundante para permitir a utilização de fontes de energia independentes. Os circuitos elétricos dos RACKS deverão possuir também conjuntos de tomadas (PDUs – Power Distribution Units) suficientes para suportar a capacidade máxima de dispositivos por RACK, independentemente da configuração proposta. A altura máxima permitida para os RACKS será de 42 U (quarenta e dois Rack Unit).
5.1.22. Todos os componentes da Solução de Armazenamento Seguro deverão ser de um único fabricante.
5.2. Conectividade
5.2.1. Cada conjunto da Solução de Armazenamento Seguro deverá possuir, no mínimo, 08 (oito) interfaces Ethernet/Fast Ethernet 10/100/1000Base-TX, autosense.
5.2.2. Cada conjunto da Solução de Armazenamento Seguro deverá implementar os seguintes protocolos de acesso: CIFS, NFS, HTTP, HTTPS, WebDAV, e NDMP ou por meio do emprego de API compatível com a especificação XAM da SNIA.
5.2.3. O subsistema deverá permitir o uso de diferentes segmentos de rede visando segregar o tráfego dos dados de gerenciamento e armazenamento.
5.3. Gerenciamento de Conteúdo
5.3.1. A Solução de Armazenamento Seguro deverá prover acesso rápido aos objetos, por intermédio do suporte à indexação, garantindo autenticidade, imutabilidade, unicidade e disponibilidade, durante o período de retenção configurado, além de ser transparente quanto ao local de armazenamento para aplicações e usuários.
5.3.2. A Solução de Armazenamento Seguro deverá possuir capacidade para armazenar dados não estruturados e seus metadados, denominados objetos, conforme descrito abaixo:
5.3.2.1. Dados não estruturados: Objetos em geral que podem ser do tipo documento (XML, PDF, TXT, Microsoft Office, OpenOffice), imagem, vídeo;
5.3.2.2. Metadados: Objetos internos à Solução de Armazenamento Seguro que descrevem os objetos armazenados na Solução. Os metadados devem conter informações relativas aos objetos e com essas informações deve ser possível identificar informações pertinentes aos objetos como data e hora da criação do objeto, período de retenção e tamanho, entre outras.
5.3.3. A Solução de Armazenamento Seguro deverá possuir de forma nativa, no mínimo, um algoritmo de autenticação de 128 (cento e vinte e oito) bits que não possua nenhum tipo de falha conhecida e provada. Usando um algoritmo de autenticação, a Solução deverá ser capaz de:
5.3.3.1. Garantir que quando um objeto for inserido na Solução seja gerado um “finger print” (identificador) único, usando o próprio conteúdo do objeto como base;
5.3.3.2. Disponibilizar o “finger print” para as aplicações externas;
5.3.3.3. Garantir que dois objetos diferentes não tenham o mesmo “finger print”.
5.3.4. A Solução de Armazenamento Seguro deverá possuir de forma nativa as seguintes capacidades de proteção:
5.3.4.1. Permitir automaticamente que um objeto original possua múltiplas cópias, de forma que cada cópia seja armazenada em locais diferentes do objeto original;
5.3.4.2. Recuperar de forma automática um objeto arquivado;
5.3.4.3. Fazer replicação e recuperação de forma automática de objetos entre soluções geograficamente distantes, sem envolvimento de aplicações e sem limite de distância.
5.3.5. A Solução de Armazenamento Seguro deverá possuir de forma nativa as seguintes capacidades de segurança:
5.3.5.1. Garantir de forma automática que um objeto original não seja alterado ou corrompido durante o período de retenção configurado, através de sua própria “finger print”. No caso de alteração do objeto original, a Solução deverá recalcular a assinatura digital e tratá-lo como um novo objeto no sistema, não alterando nenhuma referência ou política do objeto original. No caso de corrupção do objeto original, a Solução deverá descartá-lo e fazer uma nova cópia a partir de uma cópia autêntica do objeto original, gerada pela política de proteção;
5.3.5.2. Garantir que um objeto não seja acessado por usuário ou aplicação não autorizados.
5.3.6. A Solução de Armazenamento Seguro deverá possuir de forma nativa os seguintes controles de retenção:
5.3.6.1. Após a configuração do período de retenção de um objeto, a solução não deverá permitir que este seja diminuído ou apagado, até que o tempo de retenção configurado tenha expirado;
5.3.6.2. Quando um período de retenção for especificado, o sistema deverá garantir que as tais informações não poderão ser excluídas antes do vencimento do prazo estabelecido e ainda garantir que os prazos estabelecidos não sejam reduzidos ou eliminados;

5.3.6.3. O sistema/relógio que controla o tempo de retenção dos objetos tem que ser interno à solução e de maneira nenhuma deverá permitir que este sistema/relógio possa ser alterado ou sincronizado com servidor, sistema ou relógio externo, nem permitir a sua reconfiguração por administradores ou usuário/aplicação da solução;
5.3.6.4. O prazo de retenção deverá ser atribuído a cada objeto armazenado, volumes, pastas ou qualquer outro mecanismo de agrupamento de objetos de acordo com o especificado no subitem 4.3.6.a;
5.3.6.5. Possuir opção de configurar período de retenção “a definir”, onde o objeto terá retenção infinita até que um período específico seja estabelecido;
5.3.6.6. Possuir funcionalidade que permita que os objetos sejam mantidos mesmo após a expiração do seu prazo de retenção.
5.3.7. A solução deverá prover de forma nativa a seguinte funcionalidade no momento de deleção de um objeto:
5.3.7.1. Permitir que um objeto seja apagado somente após o tempo de retenção ter expirado.
5.3.8. A solução deverá oferecer uma utilização eficiente no armazenamento, ou seja, utilizar mecanismos de endereçamento exclusivo derivado do conteúdo, garantindo que somente uma cópia protegida do conteúdo será armazenada, não importando quantas vezes venha a ser gravada no subsistema.
5.3.9. A solução deverá permitir a criação de regras para a definição de senhas de acesso administrativo, visando adequação às políticas corporativas da Instituição.
5.3.10. A solução deverá permitir a criação de filtros para o envio dos alertas de acordo com o tipo ou importância.
5.3.11. A solução deverá permitir a configuração de mensagens de notificação específicas relacionadas ao equipamento, a serem exibidas a todos os usuários administrativos quando efetuarem a conexão ao sistema de gerenciamento do equipamento.
5.3.12. A Solução de Armazenamento Seguro deverá possuir características de armazenamento equivalente aos dispositivos WORM (Write Once Read Many), onde é impossível mudar conteúdo dos objetos armazenados. A característica WORM do storage deve ser inerente ao equipamento, não sendo disponibilizada por meio de softwares externos ao equipamento.
5.3.13. Deverá permitir a criação de lista de servidores que poderão interagir com a solução de armazenamento.
5.3.14. Possuir as funcionalidades de autoconfiguração, autorrecuperação e autogerenciamento.
5.3.15. Cada gabinete deve possuir funcionalidade de detecção e utilização automática dos incrementos de capacidade (expansão) sem a necessidade de modificação ou interrupção no(s) servidor(es) de aplicação (hot-swap).
5.3.16. A Solução de Armazenamento Seguro deverá possuir uma taxa de ingestão de, no mínimo, 100 (cem) objetos por segundo, considerando um tamanho médio de 25 (vinte e cinco) KB (Kilobytes) e sem concorrência com o processo de recuperação de objetos.
5.3.17. A Solução de Armazenamento Seguro deverá possuir uma capacidade de recuperação de objetos de, no mínimo, 500 (quinhentos) objetos por segundo, considerando um tamanho médio de 25 (vinte e cinco) KB (Kilobytes) e sem concorrência com o processo de ingestão de objetos.
5.3.18. A Solução de Armazenamento Seguro deverá garantir que a replicação dos objetos entre os dois conjuntos fornecidos seja feita de forma automática e assíncrona.
5.3.19. Permitir aplicações com as seguintes finalidades: leitura, gravação, deleção, configuração de retenção, busca e recuperação de objetos.
5.3.20. O sistema deverá ser capaz de armazenar e proteger simultaneamente diferentes tipos de informação sem restrições relacionadas ao formato.
5.3.21. Possuir capacidade de reconstrução automática dos dados a partir de cópia criada e mantida pelo próprio sistema em caso de erros.
5.3.22. Possuir a funcionalidade de configuração que permita manter a informação por períodos de retenção pré-estabelecidos e ainda permitir a reutilização dos espaços liberados ao final dos prazos de retenção de cada informação gravada.
5.3.23. Quando um período de retenção for especificado, o sistema deverá garantir que as informações não poderão ser excluídas antes do vencimento do prazo estabelecido. Adicionalmente, deve garantir que os prazos estabelecidos não sejam reduzidos ou eliminados.
5.4. Gerenciamento da Solução de Armazenamento Seguro
5.4.1. A Solução de Armazenamento Seguro deverá possuir software de gerenciamento de configuração que permita, no mínimo, executar as seguintes funções sem causar indisponibilidade do acesso aos dados pelas aplicações:
5.4.1.1. Definição de servidores de aplicação e/ou de usuários para acesso à Solução;

5.4.1.2. Provisionamento e liberação de área de armazenamento.
5.4.2. A Solução de Armazenamento Seguro deverá possuir software para análise e gerenciamento de desempenho, com tratamento de dados históricos, que permita, no mínimo:
5.4.2.1. Monitoração automática de todos os seus componentes, inclusive através de traps SNMP v2 e/ou v3;
5.4.2.2. Definição de limites (thresholds) para geração de alertas;
5.4.2.3. Gerenciamento dos objetos armazenados (número de objetos, espaço alocado, prazo de retenção);
5.4.2.4. Geração de relatórios e estatísticas de utilização dos recursos.
5.4.3. O gerenciamento da Solução, compreendendo configuração, monitoramento, gerenciamento de desempenho, ativação/desativação e controle de funcionalidades da mesma, deverá ser redundante, sem ponto único de falha;
5.4.4. Caso seja necessário o fornecimento de servidores, estes deverão possuir configuração igual ou superior ao mínimo recomendado pelo fabricante do(s) software(s) de gerenciamento.
5.4.5. A Solução de Armazenamento Seguro deverá possuir funcionalidades de monitoração automática e periódica de seus componentes.
5.4.6. Prover software de gerenciamento para total administração e configuração do sistema de forma local ou remota.
5.4.7. Possuir reconfiguração automática e replicação de objetos em caso de falha de hardware, com notificação automática ao fabricante por meio de sistema de correio eletrônico e/ou modem.
5.5. Integração com o sistema SAJ
5.5.1. A solução deverá nativamente integrar com os sistemas SAJ com as seguintes funcionalidades:
5.5.1.1. Enviar conteúdo binário de documento para a SOLUÇÃO DE ARMAZENAMENTO SEGURO, retornando um identificador único para o documento, que é devolvido para a aplicação que fez a requisição, para que seja vinculado aos metadados do documento no banco de dados, permitindo posterior recuperação do conteúdo do documento;
5.5.1.2. Recuperar arquivos da solução de armazenamento seguro: recebimento como parâmetro de entrada do identificador único (ID) do documento cujo conteúdo deseja-se recuperar da SOLUÇÃO DE ARMAZENAMENTO SEGURO e devolver o conteúdo binário do documento recuperado;
5.5.1.3. Percorrer a base de dados buscando nas tabelas de documentos digitalizados e emitidos documentos cujo conteúdo ainda não tenha sido enviado para a SOLUÇÃO DE ARMAZENAMENTO SEGURO e que já tenham sido finalizados e liberados na pasta digital; identificados os documentos nessa situação, a solução deverá realizar cópia do conteúdo destes documentos para a SOLUÇÃO DE ARMAZENAMENTO SEGURO, recebendo como retorno um identificador único (ID) para o documento enviado. Que deverá ser gravado no banco de dados o ID no metadados do documento correspondente;
5.5.1.4. Registrar a quantidade de documentos enviados diariamente para a SOLUÇÃO DE ARMAZENAMENTO SEGURO em tabelas de log na base de dados, permitindo que haja monitoramento automatizado para verificar se a quantidade de documentos enviados por dia é diferente de zero, emitindo alerta para solução de armazenamento seguro seja igual a zero;
5.5.1.5. Identificação, na base de dados, de documentos emitidos e digitalizados que já foram copiados para a SOLUÇÃO DE ARMAZENAMENTO SEGURO, mas cujos conteúdos ainda permanecem na base de dados; uma vez localizados documentos pendentes de remoção da base de dados, uma rotina deverá realizar procedimento para recuperar do SOLUÇÃO DE ARMAZENAMENTO SEGURO o conteúdo destes documentos; deverá haver verificação se há idêntico conteúdo do documento na SOLUÇÃO DE ARMAZENAMENTO SEGURO e do documento na base de dados, e, em caso positivo, deverá ser apagado efetivamente da base de dados o conteúdo do documento;
5.5.1.6. Registrar a quantidade de documentos removidos da base de dados em tabelas de log na base de dados, permitindo que haja monitoramento automatizado para verificar se a quantidade de documentos enviados por dia é diferente de zero, emitindo alerta caso seja igual a zero;
5.5.1.7. Remover os documentos de petições eletrônicas armazenados nas bases NET, mediante regras pré–estabelecidas no arquivo de configuração, certificando-se que os documentos já se encontram na respectiva base PG ou SG ou já foram movidos para o SOLUÇÃO DE ARMAZENAMENTO SEGURO; independente de estarem na base PG ou SG ou no SOLUÇÃO DE ARMAZENAMENTO SEGURO, deverá possibilitar a recuperação do conteúdo de cada documento candidato à remoção e compará-lo com o conteúdo do mesmo documento na base NET; caso o conteúdo seja idêntico, deverá ser realizada a exclusão do conteúdo do documento na base NET;
5.5.1.8. Registrar a quantidade de documentos removidos diariamente em tabelas de log na base de dados, permitindo que soluções de monitoramento automatizadas possam periodicamente verificar nestas tabelas se a quantidade de documentos removidos por dia é diferente de zero; caso seja igual a zero, um alerta para investigação deve ser emitido.

6. DA CARACTERIZAÇÃO DO OBJETO

6.1. O objeto do presente Termo de Referência é considerado comum, nos termos do parágrafo único do art. 1º da Lei n. 10.520/02.

ITEM	CÓDIGO SIASG	DESCRIÇÃO	UND	QUANT
1	27472 - Licenciamento de direitos permanentes de uso de outros softwares ,programas de computador.	Contratação de empresa especializada para a prestação de serviços de gestão e armazenamento de documentos eletrônicos dos processos judiciais. Os serviços de gestão deverão promover o armazenamento e o rápido acesso aos documentos eletrônicos, por meio de atributos WORM (uma gravação e várias leituras) de proteção contra regravação e contra exclusão.	UN	1

7. VALOR ESTIMADO DA CONTRATAÇÃO

A partir de pesquisa realizada no mercado, estima-se a aquisição em:

ITEM	DESCRIÇÃO	UND	VALOR MENSAL	VALOR ANUAL
1	**CAS**	**REAL**		

8. DO CRITÉRIO DE JULGAMENTO

8.1. Tendo em vista que no julgamento das propostas, será considerado o de menor preço.

9. DA NECESSIDADE DE CONTRATO

9.1. Deverá ser formalizado contrato para os serviços previstos neste termo de referência, tendo em vista as características do objeto a ser contratado, com a existência de obrigações futuras, incluindo a garantia, continuidade e confiabilidade do mesmo nos termos do art. 62 da Lei 8.666/93.

10. FORMAS DE FORNECIMENTO

10.1. Para o fornecimento da solução de armazenamento seguro, a CONTRATADA deverá realizar os serviços a seguir especificados:

10.1.1. Planejamento do projeto e estudo técnico

10.1.1.1. A CONTRATADA deve elaborar um estudo técnico com o dimensionamento de aplicações necessárias para utilização da solução de armazenamento seguro, bem como realizar o planejamento das atividades e o detalhamento do cronograma do projeto, com a definição de papéis e responsabilidades.

10.1.2. Instalação e configuração da solução de armazenamento seguro

10.1.2.1. Consiste na instalação, configuração e homologação da solução de armazenamento seguro nas dependências do TJAM.

10.1.3. Homologação do SAJ com a solução de armazenamento seguro

10.1.3.1. Consiste na homologação do SAJ com a solução de armazenamento seguro garantido que novos documentos assinados e liberados na pasta digital sejam gravados e recuperados na solução de armazenamento seguro, bem como, documentos já migrados para solução de armazenamento seguro sejam visualizados na integra no SAJ.

10.1.4. Carga Inicial de Documentos Eletrônicos

10.1.4.1. A CONTRATADA deve realizar a cópia dos documentos da base de dados para a solução de armazenamento seguro realizando essa atividade de forma controlada, monitorando e validando a execução da operação, por meio da comparação de dados dos documentos contidos no banco de dados e dos documentos armazenados na solução de armazenamento seguro.

10.1.4.2. Essas atividades deverão ser realizadas para os documentos das bases PG5 e SG5 e dos protocolos das bases NET.

10.1.5. Exclusão de Documentos das Bases PG/SG e Exclusão de Protocolos das Bases NET

10.1.5.1. A CONTRATADA, após a carga inicial dos documentos, deve realizar a exclusão dos documentos das bases PG5 e SG5 e dos protocolos das bases NET.

11. DA SOLICITAÇÃO DE SERVIÇOS

11.1. A solicitação para prestação do serviço será realizada pela Secretaria de Tecnologia da Informação e Comunicação - SETIC, por meio do seu Secretario. Proporcionar todas as facilidades para que a CONTRATADA possa desempenhar seus serviços;

12. VALOR ESTIMADO DA CONTRATAÇÃO

12.1. O valor estimado do objeto a ser adquirido será levantado pela Divisão de Compras e Operação – DVCOP, por meio de consulta de mercado (Apêndice I).

13. DA NECESSIDADE DE CONTRATO

13.1. Para a entrega do objeto ou execução do serviço faz-se necessária a formalização de contrato administrativo, nos termos do art.62 da Lei 8.666/93.

14. DO PERÍODO DE VIGÊNCIA E REPACTUAÇÃO

14.1. A vigência do contrato a ser firmado será de 12 (Doze) meses, a contar da data da assinatura do respectivo termo, podendo ser prorrogado por iguais e sucessivos períodos, até o limite de 60 (sessenta) meses, na forma do art. 57 da Lei nº 8.666/93, com vistas à obtenção de preços e condições mais vantajosas para a Administração;

14.2. Os preços inicialmente contratados serão reajustados após o interregno no mínimo de 1 (um) ano da data de apresentação da proposta, com base na variação do IGPM/FGV, considerando o mês anterior ao da proposta e o mês anterior ao da data de reajuste, inclusive.

14.2.1. Para efeito de reajustamento, os índices iniciais a serem considerados serão os da data de apresentação da proposta.

15. DAS OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATANTE

15.1. Respeitar a titularidade do direito autoral, patrimonial e comercial da CONTRATADA sobre a solução, seus componentes de software, suas adaptações, derivações e customizações resultantes da execução dos serviços objeto deste Termo de Referência, comprometendo-se a não doar, ceder, disponibilizar e permitir o manuseio e utilização dos códigos-fonte e componentes de software por terceiros ou praticar qualquer outra forma de transferência dos aplicativos sem anuência da CONTRATADA, conforme legislação especifica.

15.2. Acompanhar e fiscalizar os serviços, quanto aos aspectos qualitativos e quantitativos, anotando em registro próprio as falhas e solicitando as medidas corretivas.

15.3. Fornecer a infraestrutura de hardware e software necessária para a instalação e operação da solução, incluindo servidores, rede computacional, tokens de assinatura digital, scanners e outros recursos necessários, caso demandar a instalação em ambiente computacional específico do TJAM.

15.4. Comunicar à CONTRATADA, sempre por escrito, as solicitações e quaisquer alterações ocorridas.

15.5. Prestar os esclarecimentos solicitados pela CONTRATADA, atinentes ao objeto desta Licitação.

15.6. Notificar à CONTRATADA, 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.

15.7. Tomar providências necessárias para que sejam seguidas as recomendações da CONTRATADA, concernentes às condições de uso correto da solução.

15.8. Atestar as faturas correspondentes, por intermédio da fiscalização.

15.9. Realizar os pagamentos em até 30 (trinta) dias após a apresentação da nota fiscal de prestação de serviços pela CONTRATADA. Em caso de atraso dos pagamentos por culpa exclusiva da Administração, será aplicado como índice de atualização monetária o IGP-M da Fundação Getúlio Vargas (FGV). Caso exista inadimplência por mais de 60 (sessenta) dias consecutivos, a CONTRATADA poderá interromper a prestação dos serviços, sem ônus ou sanções por parte do TJAM, desde que com aviso prévio de no mínimo 30 (trinta) dias.

16. DAS OBRIGAÇÕES RESPONSABILIDADES DA CONTRATADA

16.1. Adicionalmente às responsabilidades estabelecidas nos demais tópicos constantes deste documento, incumbe à CONTRATADA observar os seguintes requisitos:

16.1.1. Política de segurança da informação

16.1.1.1. A CONTRATADA deverá submeter-se à Política de Segurança de Informação definida pelo TJAM em seus regulamentos.

16.1.1.2. O TJAM comunicará à CONTRATADA as alterações posteriores introduzidas na Política de Segurança da Informação, bem como a edição dos regulamentos complementares, e definirá, de comum acordo com a CONTRATADA, o prazo necessário para a implementação dessas alterações.

16.1.1.3. A CONTRATADA deverá executar as atividades previstas neste Termo de Referência através de comunicação remota, por intermédio de conexão segura entre a sua rede e a do TJAM.

16.1.1.4. A CONTRATADA será responsável pelos custos de comunicação remota entre sua sede e as instalações (datacenter) do TJAM.

16.1.1.5. O acesso remoto ao ambiente de produção do TJAM pela CONTRATADA se dará apenas por meio

de funcionários autorizados com respectivo usuário e senha individual.
16.1.2. Dos equipamentos
16.1.2.1. Os equipamentos Serão disponibilizados pela CONTRATADA e instalados nas dependências do TJAM.
16.1.2.2. A partir da instalação do equipamento, a CONTRATANTE verificará as condições de uso e funcionamento e emitirá relatório.
16.1.2.3. O fornecimento e as condições de rede e infraestrutura, para o funcionamento dos equipamentos, serão de responsabilidade do TJAM.
16.1.3. Horário padrão para atendimento de chamados
16.1.3.1. O atendimento a chamados serão prestados em dias úteis, de segunda a sexta feira, no horário padrão compreendido das 8h00min às 18h00min, horário local, excetuando-se os casos expressamente previstos neste Termo de Referência.
16.1.4. Abertura dos chamados
16.1.4.1. A CONTRATADA disponibilizará meio para abertura e acompanhamento dos chamados dos serviços deste Termo de Referência.
16.1.4.1.1. Os chamados pelo Portal do Cliente poderão ser abertos pelos usuários do TJAM, habilitados para este fim.
16.1.5. Cômputo dos prazos para atendimento dos chamados
16.1.5.1. Os prazos serão computados da seguinte forma:
16.1.5.1.1. Nos prazos estabelecidos em dias úteis, o início da fluência do prazo ocorrerá no horário padrão do primeiro dia útil subsequente à data da abertura do chamado, e encerrará no último minuto do prazo.
16.1.5.1.1.1. Para efeito do cômputo dos prazos, 1 (um) dia útil equivale a 10 (dez) horas úteis.
16.1.5.1.2. Nos prazos estabelecidos em dias corridos, o início da fluência do prazo ocorrerá no primeiro minuto do dia subsequente à data da abertura do chamado, e encerrará no último minuto do prazo.
16.1.5.1.2.1. Para efeito do cômputo dos prazos, 1 (um) dia corrido equivale a 24 (vinte e quatro) horas corridas
16.1.5.1.3. Nos prazos estabelecidos em horas, o cômputo se dará da seguinte forma:
16.1.5.1.3.1. Quando a abertura do chamado ocorrer em dia útil, no horário padrão, a fluência do prazo iniciará no minuto imediatamente subsequente ao horário em que foi registrada a abertura do chamado, e encerrará no último minuto do prazo.
16.1.5.1.3.2. Quando a abertura do chamado ocorrer em horário excepcional, a fluência do prazo iniciará no primeiro minuto do horário padrão, do primeiro dia útil imediatamente subsequente à data de abertura do chamado, e encerrará no último minuto do prazo.
16.1.6. Pedidos de prorrogação de prazos
16.1.6.1. Para os prazos relacionados aos serviços e documentos comprobatórios, caso a entrega demande tempo superior ao estabelecido, a CONTRATADA deverá comunicar formalmente ao TJAM, justificando a solicitação e estabelecendo o novo prazo.
16.1.6.2. Os pedidos de prorrogação do prazo deverão ser formulados antes do respectivo término previsto.
16.1.6.3. Caso haja necessidade de novo pedido de prorrogação de prazo, a CONTRATADA deverá solicitar formalmente ao TJAM, antes do término do prazo concedido, justificando o problema e estabelecendo o novo prazo.
16.1.6.4. O decurso do prazo estipulado será suspenso a partir da data em que a CONTRATADA formalizar o pedido de prorrogação, e voltará a fluir a partir da data em que o TJAM formalizar sua decisão.
16.1.6.5. O TJAM, de forma fundamentada, poderá indeferir os pedidos de prorrogação.
16.1.6.6. Caso a CONTRATADA não concorde com a justificativa apresentada pelo TJAM, poderá solicitar que a divergência possa ser apreciada pelos gestores do contrato de ambos.
16.1.6.7. Caso o gestor do contrato do TJAM não aceite o pedido de prorrogação, deverão ser mantidos os prazos definidos neste Termo de Referência.
16.1.6.8. Caso o gestor do contrato do TJAM aceite o pedido de prorrogação, o novo prazo será o constante do pedido.
16.1.7. Níveis mínimos de serviços
16.1.7.1. Serão aferidos os níveis mínimos de serviços necessários à mensuração da qualidade dos serviços continuados visando adequar os pagamentos relativos aos serviços prestados, prevendo-se, para tais serviços, redutores a serem aplicados sobre os respectivos valores.
16.1.7.2. A qualquer tempo, de comum acordo entre as partes, em função da alteração ou inclusão de funcionalidades no SAJ ou por interesse das partes, os níveis mínimos de serviços poderão ser revistos e modificados, por meio de termo aditivo.
16.1.7.3. O período de até 60 (sessenta) dias corridos após o início da execução será considerado como

período de estabilização e ajustes das regras estabelecidas, em que as eventuais não conformidades estarão isentas da aplicação de redutores previstos neste documento, mediante justificativa da CONTRATADA.
16.1.8. Propriedade, sigilo, restrições
16.1.8.1. Todas as informações obtidas ou extraídas pela CONTRATADA quando da execução dos serviços deverão ser tratadas como confidenciais, sendo vedada qualquer divulgação a terceiros.
16.1.8.2. A obrigação assumida de Confidencialidade permanecerá válida durante o período de vigência do contrato principal e o seu descumprimento implicará em sanções administrativas e judiciais contra a CONTRATADA, previstas no CONTRATO e na legislação pertinente;
16.1.8.3. À CONTRATADA será garantido o direito de propriedade intelectual da solução de armazenamento seguro , consubstanciado no direito autoral, patrimonial e comercial, seus componentes de software, suas adaptações, derivações e customizações resultantes da execução dos serviços previstos no Termo de Referência, consoante Leis 9.609/98.
16.1.9. Encerramento do contrato
16.1.9.1. Em caso de encerramento do contrato, deverão ser observados os seguintes procedimentos:
16.1.9.2. A CONTRATADA deverá disponibilizar aplicativo de software para recuperar todos os arquivos armazenados nos equipamentos, cujas chaves de acesso, estejam disponíveis nas bases de dados do contratante. Durante a recuperação destes arquivos, o aplicativo permitirá materializar os arquivos recuperados em um sistema de arquivos ou reincluir os arquivos na base de dados.
16.1.9.3. É responsabilidade do TJAM realizar a execução da migração (de para).

17. DO PRAZO E LOCAL DE ENTREGA
17.1. O objeto deste termo deverá ser entregue na Secretaria de Tecnologia da Informação e Comunicação (SETIC) do Tribunal de Justiça do Amazonas, sito a Avenida Andre Araujo s/n, Prédio Desembargador Arnoldo Peres - Bairro Aleixo – CEP 69.060-000.

19. DO PAGAMENTO:
19.1. *O pagamento será realizado em moeda corrente nacional, quando da solicitação de disponibilização dos itens, mediante Ordem Bancária Eletrônica, e ocorrerá em 30 (trinta) dias, a contar da apresentação da nota fiscal/fatura pelo contratado, que devera ser submetida ao atesto pelo setor competente pela fiscalização do contrato.*
19.2. *O TJAM pagará à CONTRATADA pela execução dos serviços previstos neste Termo de Referência, diante das seguintes condições:*
19.2.1 O TJAM emitirá autorização para pagamento obedecendo aos prazos descritos neste Termo de Referência. Depois de autorizada, A CONTRATADA entregará a nota fiscal junto ao TJAM acompanhada da seguinte documentação (artigo 71, combinado com o artigo 55, inciso XIII, da Lei n. 8.666, de 21 de junho de 1993):
19.2.1.1 Comprovante da regularidade perante a Fazenda Federal;
19.2.1.2 Comprovante da regularidade perante a Fazenda Estadual;
19.2.1.3 Comprovante da regularidade perante a Fazenda Municipal;
19.2.1.4 Comprovante da regularidade perante a União – Dívida Ativa;
19.2.1.5 Comprovante da regularidade perante a Seguridade Social (INSS);
19.2.1.6 Comprovante da regularidade perante o FGTS;
19.2.1.7 Comprovante de regularidade perante a Justiça do Trabalho.
19.2.2 As certidões previstas no item anterior só serão aceitas com prazo de validade determinado no documento ou com data de emissão não superior a 180 (cento e oitenta) dias corridos e deverão ser apresentadas em cópias autenticadas ou exibidas com os originais.
19.2.3 Sobre o valor de cada parcela incidirão as retenções previstas em lei; para tanto, a CONTRATADA deverá fazer apenas destaque na nota fiscal.
19.2.4 Os pagamentos mensais relativos aos serviços poderão ser calculados proporcionalmente, caso a assinatura e início da vigência do instrumento contratual não coincida com o primeiro dia do mês, situação que será repetida ao final da respectiva vigência.

19.3. O A solicitação de emissão das notas fiscais pela CONTRATADA deverá estar acompanhada da documentação comprobatória dos serviços executados, necessária para análise e emissão de Parecer Técnico de prestação dos serviços.
19.3.1 O Parecer Técnico necessário para autorizar a emissão das notas fiscais para os valores incontroversos limitar-se-á ao atesto da disponibilização dos serviços solicitados e a entrega da

documentação comprobatória. Não haverá apuração dos níveis mínimos de serviço para autorizar a emissão das notas fiscais referentes aos valores incontroversos.
19.3.2 O Parecer Técnico necessário para autorizar a emissão das notas fiscais para os valores controversos deverá conter a aferição dos serviços objetivando quantificar eventual incidência de redutores a serem aplicados sobre o valor controverso, obtidos através da apuração dos níveis mínimos de serviço.

19.4.O TJAM compromete-se a efetuar o pagamento até o 10º. (décimo) dia útil a contar da data de recebimento da respectiva nota fiscal, desde que cumpridas as condições de pagamento supracitadas, devendo o aceite correspondente ocorrer dentro deste prazo de pagamento.
19.4.1 No caso do não-pagamento da nota fiscal até o 10º. (décimo) dia útil, ou em caso de atraso na emissão da nota fiscal provocado por procedimentos, de responsabilidade do TJAM, adotados fora dos prazos determinados no presente Termo de Referência, desde que a CONTRATADA não tenha concorrido com o atraso, será efetuada a compensação financeira do 11° (décimo primeiro) dia até a data da efetiva quitação, ou do período de atraso mencionado, reajustando-se o valor com base na variação do IGPM/FGV ocorrida no período, em observância ao que dispõe o artigo 40, inciso XIV, alínea "c", da Lei n. 8.666, de 21 de junho de 1993.

20. DA FISCALIZAÇÃO E ACOMPANHAMENTO
20.1. Todos os serviços executados pela empresa CONTRATADA serão acompanhados e fiscalizados pela Secretaria de Tecnologia da informação e comunicação do Tribunal de Justiça/AM, com autoridade para exercer em nome do TJAM, toda e qualquer ação de orientação geral, controle e fiscalização dos serviços;

Manaus/AM, 30 de Junho de 2022.

Breno Figueiredo Corado
Secretario de Tecnologia da Informação e Comunicação – SETIC

Mauro Sérgio Sales da Silva
Assessor de Aquisições e Contratos

Documento assinado eletronicamente por **BRENO FIGUEIREDO CORADO**, **Secretário(a)**, em 01/07/2022, às 08:34, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Mauro Sérgio Sales da Silva**, **Servidor**, em 01/07/2022, às 08:34, 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 **0613374** e o código CRC **65CE1D58**.