

Secretaria de Tecnologia da Informação e Comunicação - SETIC
Subsecretaria de Contratações de TIC - SUCTI

ESTUDO TÉCNICO PRELIMINAR (TIC) Nº 19/2025

Conformidade com o Guia de Contratações de TIC CNJ Versão 4.0 - Resolução CNJ nº 468/2022

Processo Administrativo Nº 2025-486

Aquisição de Certificado Digital (WildCard) para servidores Web, com validade de 60 meses (cinco vouchers), para atendimento das necessidades do Poder Judiciário do Estado do Acre



Rio Branco/AC, 19 de Setembro de 2025.

PODER JUDICIÁRIO DO ESTADO DO ACRE
Rua Desembargador Jorge Araken, s/n. Via Verde.
69201-311 - Rio Branco-AC - (68) 3212-8277

ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO

1. ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO

1.1. Contextualização

O Poder Judiciário do Estado do Acre (PJAC) disponibiliza uma gama de serviços online cruciais para a sociedade e para o funcionamento do acesso à Justiça, incluindo sistemas como e-Proc, e-SAJ, Malote Digital, SEI, e-mail e ExtraJud. A segurança da informação e a proteção da privacidade dos dados trafegados nestes ambientes são imperativas, em conformidade com as diretrizes do Conselho Nacional de Justiça (CNJ) por meio da Resolução nº 396/2021 e a Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018).

A ausência de um certificado digital robusto e atualizado representa uma fragilidade crítica, que expõe os ativos digitais do PJAC a riscos como interrupção de serviços, vazamento de dados, ataques de negação de serviço e comprometimento da confiança da sociedade na instituição. Um Certificado Digital WildCard, tipo A1, é fundamental para assegurar a autenticidade dos servidores, a integridade da comunicação via HTTPS e a confidencialidade das informações em todos os subdomínios vinculados ao PJAC.

A aquisição deste certificado, com validade de 60 meses (cinco vouchers), visa aprimorar a postura de segurança cibernética do Tribunal, equiparando-o aos mais elevados padrões de segurança adotados por instituições financeiras e governamentais, e minimizando a exposição a ameaças modernas.

1.2. Identificação da demanda no Plano de Contratações de STIC

A demanda está formalmente identificada e contemplada no Plano de Contratações da área de Tecnologia da Informação e Comunicação (PAC SETIC/2025) do Poder Judiciário do Estado do Acre, constante no processo GRP 2025-274, planilha [D16980] item 28. A sequência registrada no PSTIC é a de número 5, sob a descrição "Ferramentas e soluções que visam fomentar a segurança da informação, com vistas a dar cumprimento à Res. 396/2021 e fomentar a maturidade em segurança." No Plano Anual de Contratações 2025, o ID PCA no PNCP é 04034872000121-0-000006/2025, publicado em 29/01/2025, com ID do item no PCA 23 e classificado na Categoria/Grupo 511 - OUTROS SERVIÇOS DE TERCEIROS - PESSOA JURÍDICA.

1.2.1. Alinhamento da Solução

Plano Estratégico Institucional: PEI: Perspectiva do Aprendizado e Crescimento.

Macrodesafio: Fortalecer a Gestão de TIC.

Objetivo: Definir e executar projetos estratégicos de TIC no TJ, conforme resoluções do CNJ.

Meta: Modernizar a estrutura de TI em 70% até 2026.



Plano Diretor institucional (PDTIC): O PDTIC é um instrumento que visa direcionar os investimentos e aquisições de bens e serviços de TIC, objetivando maximizar o cumprimento da estratégia institucional 2021/2026, em consonância às normas nacionais do Poder Judiciário e à visão de longo prazo do Tribunal de Justiça do Acre.

Plano de Contratação de Soluções de Tecnologia da Informação Comunicação - PSTIC: A contratação ora pleiteada está prevista no Plano Anual de Contratação de TIC 2025.

1.3. Caracterização da demanda

1.3.1. Definição e Especificação das Necessidades

A demanda refere-se à aquisição de um Certificado Digital padrão WildCard. Em um contexto cada vez mais digital e interconectado, a proteção das informações demanda uma estrutura operacional robusta que garanta a segurança das comunicações em múltiplos serviços web. O Certificado WildCard é uma solução de criptografia SSL/TLS que protege um domínio principal e todos os seus subdomínios (ex: *.tjac.jus.br) com um único certificado.

Sua indispensabilidade reside na necessidade de:

- **Criptografia:** Proteger a confidencialidade e a integridade dos dados trafegados entre usuários e servidores do PJAC;
- **Autenticidade:** Confirmar a identidade dos sites do TJAC, combatendo a fraude e o phishing;
- **Simplificação da Gestão:** Gerenciar a segurança de múltiplos subdomínios com um único certificado, reduzindo a complexidade administrativa;
- **Redução de Custos:** Evitar a aquisição e gestão de certificados individuais para cada subdomínio.

1.3.2. Definição e Especificação de Requisitos

1.3.2.1. Serviços Gerenciados de Segurança Cibernética

A prestação dos serviços de emissão e suporte do Certificado Digital WildCard deverá contemplar os seguintes componentes integrados:

- **Emissão do Certificado:** Processo de emissão do certificado digital, incluindo validação da titularidade do domínio;
- **Entrega:** Disponibilização do certificado para instalação nos servidores do PJAC por meio de voucher;
- **Suporte Técnico:** Apoio na instalação e configuração, bem como resolução de quaisquer problemas durante a validade do certificado;
- **Propriedade dos Dados:** Todos os dados gerados pelo certificado (chaves, registros) são de propriedade do CONTRATANTE.



1.3.2.2. Requisitos de Suporte e Atendimento Técnico

Prestação de serviços de apoio para a correta implementação e manutenção do certificado digital. A execução deverá observar as boas práticas de segurança da informação. A atuação deverá garantir:

- Apoio na instalação e configuração do certificado nos servidores web do PJAC.
- Atendimento a chamados relacionados a eventuais problemas de funcionamento do certificado.
- Apoio às equipes internas nas tratativas proativas e reativas a incidentes relacionados ao certificado.

1.3.2.3. Requisitos de Gerenciamento do Ciclo de Vida do Certificado

A contratada deverá fornecer o certificado e informações para o gerenciamento de sua validade, que é de 60 meses (cinco vouchers). Caberá à empresa Contratada, se aplicável:

- Garantir a correta emissão e validação do certificado.
- Fornecer as informações necessárias para a gestão da validade do certificado.
- Garantir a integridade, desempenho e eficiência do certificado.

1.3.2.4. Requisitos de Emissão e Validação

Contratação de solução e serviços especializados de emissão de certificado digital, com foco em:

- Emissão de Certificado Digital WildCard, tipo A1.
- Validação de domínio (DV - Domain Validation) ou validação organizacional (OV - Organization Validation), conforme a necessidade do PJAC.
- Garantir a correta vinculação aos domínios do PJAC.

1.3.2.5. Requisitos de Conformidade com Padrões de Segurança

O serviço deve garantir que o certificado digital esteja em conformidade com padrões e boas práticas internacionais e nacionais, tais como:

- Padrões SSL/TLS (Transport Layer Security).
- ICP-Brasil (Infraestrutura de Chaves Públicas Brasileira).
- Normas de criptografia e segurança de dados.



1.3.2.6. Gestão e Controle dos Serviços

A empresa Contratada será responsável por:

- Atuar como ponto único de contato junto à Contratante.
- Assegurar a entrega do certificado conforme prazos e padrões acordados.
- Apresentar relatórios (se aplicável para o tipo de serviço) e indicadores de desempenho (KPIs) para avaliação objetiva, como tempo de emissão.
- Garantir o registro, controle e histórico de todas as solicitações e atendimentos relacionados ao certificado.

1.3.3. Requisitos Funcionais

1.3.3.1. Requisitos de Arquitetura Tecnológica (Configuração):

Os requisitos gerais dos serviços, define os requisitos obrigatórios para todos os serviços que compõem o objeto:

- A CONTRATANTE deverá possuir acesso a todas as chaves e arquivos do certificado com perfil de administração máxima.
- Todos os dados gerados ou coletados pelo certificado (chaves públicas e privadas, informações de registro) são de propriedade do CONTRATANTE.
- Caberá à CONTRATADA adotar as boas práticas para garantir a integridade do processo de emissão.
- Todos os serviços e atendimentos poderão ser prestados remotamente.
- Caberá à empresa CONTRATADA a responsabilidade de prestar suporte remoto à equipe da CONTRATANTE durante o expediente do PJAC, com suporte contínuo à operação local.
- A empresa CONTRATADA deve disponibilizar canais de comunicação, especificamente:
 - Telefone: Para contato direto e imediato em casos de urgência, com atendimento em português.
 - E-mail: Para solicitações formais e documentação de problemas.

1.3.3.1.1. Requisitos Específicos Para A Prestação De Serviços De Certificação Digital

O Centro de Operações (ou a estrutura da Contratada responsável pela emissão) da empresa CONTRATADA deve operar com sistemas seguros, garantindo a integridade e a confidencialidade das informações durante o processo de emissão do certificado. A Contratada deverá indicar o local onde possui sua estrutura de atendimento, que deverá ser estabelecida no Brasil e estará sujeita à diligência por parte da CONTRATANTE, se necessário. Todos os atendimentos devem ser iniciados no Brasil e no idioma português do Brasil.



1.3.3.1.1.1. Requisitos Para A Prestação Do Serviço De Emissão Do Certificado

Para a prestação dos serviços de emissão do certificado digital, a CONTRATADA deverá disponibilizar, por meio de sua estrutura de Autoridade Certificadora, todos os recursos necessários, incluindo infraestrutura, ferramentas tecnológicas e equipe técnica especializada, garantindo o atendimento nas seguintes modalidades:

- **Atendimento Remoto:** Durante e fora do horário regimental de expediente da CONTRATANTE, incluindo períodos noturnos, finais de semana e feriados, o atendimento deverá ocorrer de forma remota, em regime de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano, durante toda a vigência do contrato (considerando a necessidade de suporte).
- **Os Serviços contemplam os seguintes entregáveis:**
 - Receber e efetuar a triagem de chamados relacionados ao certificado digital.
 - Realizar o primeiro atendimento de reportes de problemas de funcionamento.
 - Notificar e registrar apropriadamente eventos de segurança cibernética relacionados ao certificado.
 - Disponibilizar pessoal qualificado para o desempenho das atividades e deve oferecer pessoal suficiente para que não haja interrupção na prestação do serviço de emissão e suporte.

1.3.3.1.1.2. Funcionalidades E Características Do Certificado Digital Wildcard

O Certificado Digital WildCard, tipo A1, deverá possuir as seguintes características:

- **Proteção de Múltiplos Subdomínios:** Capaz de proteger um domínio principal e todos os seus subdomínios (ex: *.tjac.jus.br).
- **Algoritmo de Criptografia:** Utilizar algoritmos criptográficos robustos e atuais (ex: RSA 2048-bit ou ECC), e funções de hash seguras (ex: SHA-256).
- **Validade:** Mínimo de 60 (sessenta) meses.
- **Compatibilidade:** Ser compatível com os principais navegadores web (Mozilla Firefox, Google Chrome, Microsoft Edge, Safari) e sistemas operacionais de servidor.
- **Emissor:** Emitido por uma Autoridade Certificadora (AC) amplamente reconhecida e incluída na lista de confiança dos sistemas operacionais e navegadores.

1.3.3.1.1.3. Documentação E Transferência De Conhecimento

A contratada deverá promover a documentação e, se aplicável, o treinamento básico para a equipe interna do PJAC quanto às boas práticas de instalação, configuração e gestão do certificado digital, contribuindo para a independência tecnológica.



- O material deverá ser compatível com diversos canais de distribuição institucional.
- Os direitos de uso e propriedade intelectual de toda a documentação produzida deverão ser integralmente cedidos ao PJAC.

1.3.3.1.2. Requisitos De Operação E Gestão Do Certificado

A CONTRATADA será responsável pela correta emissão e, se aplicável, pela sustentação do certificado digital, garantindo a sua correta operação e validade contínua, de acordo com as melhores práticas de mercado em segurança da informação.

- Geração de certificados de forma segura e confiável.
- Apoio à investigação e resposta a incidentes relacionados ao certificado.

1.3.3.1.3. Requisitos De Validação E Cadeia De Confiança

Deverá ser fornecido um certificado com cadeia de confiança íntegra e validada, através de uma Solução que atendam os requisitos abaixo:

- **Reconhecimento Global:** O certificado deve ser confiável globalmente pelos navegadores e sistemas operacionais.
- **Conformidade ICP-Brasil:** O certificado deve estar em conformidade com as exigências da ICP-Brasil.
- **Logs de Acesso:** A plataforma de emissão e gestão da contratada deve ter mecanismo de armazenamento de logs de acesso dos usuários por um período mínimo de 1 ano.

1.3.3.1.4. Requisitos De Compatibilidade E Instalação

A CONTRATADA deverá garantir que o certificado digital seja compatível com os servidores web do PJAC e que as instruções de instalação sejam claras e precisas.

- **Compatibilidade com Servidores:** Suporte para instalação em Apache, Nginx, IIS e outros servidores utilizados pelo PJAC.
- **Instruções de Instalação:** Fornecimento de documentação detalhada para a instalação do certificado.

1.3.3.1.5. Requisitos De Gestão De Chaves E Segurança

A solução deve permitir a gestão segura das chaves privadas e públicas associadas ao certificado, garantindo a confidencialidade e a integridade.



- **Segurança das Chaves:** O processo de geração e manuseio das chaves deve seguir as melhores práticas de segurança.
- **Informações Gráficas:** A contratada poderá fornecer (se disponível) informações gráficas sobre a cadeia de confiança e validade do certificado.

1.3.3.1.6. Requisitos de Infraestrutura para Implementação

Para a execução das atividades de instalação do certificado, a CONTRATANTE se compromete a disponibilizar ambiente físico adequado nas suas dependências para a equipe técnica do PJAC, e acesso remoto (se necessário) para a contratada.

- **Acesso à rede local e à internet:** Condicionado às políticas internas de segurança da informação.
- **Credenciais de acesso:** Conforme perfil e função para instalação.

1.3.3.2. Requisitos de Capacitação:

O PJAC deverá promover a conscientização contínua dos usuários internos quanto à importância da comunicação segura via HTTPS, e a equipe de TI deverá ser capacitada na gestão do ciclo de vida do certificado. A CONTRATADA deverá, se aplicável, fornecer material de apoio ou orientações.

1.3.3.3. Requisitos de Manutenção:

A empresa contratada deverá prestar serviços de suporte e, se aplicável, monitoramento da validade do certificado digital, alertando o PJAC sobre a necessidade de renovação.

- **Elaboração de relatórios:** Se houver necessidade de status do certificado (vida útil, etc.).
- **Realização de serviços de suporte técnico:** Em conjunto com o fabricante/AC.

Ambiente computacional a ser analisado (para aplicação do certificado):

Ativos	Quantidade
Servidores Web	[Quantidade de Servidores Web]
Domínios/Subdomínios	1 WildCard para múltiplos subdomínios (ex: >200 aplicações WEB)

1.3.3.3.1. GESTÃO E CONTROLE DE SERVIÇOS



A execução dos serviços deverá ser gerenciada pela Contratada por meio da atuação de uma equipe de Sucesso do Cliente (se aplicável para este tipo de serviço), que será responsável por atuar como canal de comunicação e acompanhar a qualidade dos serviços prestados.

1.3.3.3.2. ACORDO DE NÍVEL DE SERVIÇOS – SLA

A contratada deverá disponibilizar um número único local, para a execução dos serviços de suporte, que demandam contatos telefônicos. O nível de serviço poderá ser definido em função de, no mínimo (SLA), os seguintes tempos para início de atendimento e tratativas para alertas de criticidade detectada no ambiente:

Criticidade	Níveis de Evento	Regime de Atendimento	Início de Atendimento
1 - Crítica	Indisponibilidade do certificado	24 x 7	Em até 30min
2 - Alta	Problemas de compatibilidade/funcionalidade	24 x 7	Em até 1 hora
3 - Média	Dúvidas técnicas	24 x 7	Em até 4 horas
4 - Baixa	Consultas gerais	24 x 7	Em até 8 horas

1.3.3.3.3. FERRAMENTAS PARA A PRESTAÇÃO DO SERVIÇO

As ferramentas utilizadas na emissão e gestão do certificado são de responsabilidade da CONTRATADA (Autoridade Certificadora).

- A ferramenta de emissão deve utilizar base de dados atualizada.
- Deve suportar o armazenamento seguro de chaves, para garantir a integridade do certificado.

1.3.3.3.4. Requisitos de Projeto e de Implementação:

Este subtópico define as metodologias, processos e artefatos esperados para a emissão e implementação do certificado.

- **Fase de Planejamento:** Definição dos objetivos, escopo (domínio e subdomínios), e informações necessárias para a emissão.
- **Fase de Descoberta:** Coleta de informações sobre o domínio a ser certificado e validação da titularidade.
- **Fase de Exploração (Instalação):** Instalação do certificado nos servidores web do PJAC.
- **Fase de Relatório:** Entrega do certificado e de quaisquer relatórios ou instruções de instalação.

1.3.3.3.5. Requisitos de Implantação:



Cada etapa da aquisição e implantação do certificado deverá seguir as seguintes fases:

- **Planejamento:** Definição do tipo de certificado, validade, domínio e subdomínios a serem cobertos.
- **Descoberta:** Validação do domínio (DV) ou da organização (OV) pela Autoridade Certificadora.
- **Exploração (Emissão e Instalação):** Emissão do certificado digital e sua instalação nos servidores do TJAC.
- **Relatório:** Confirmação da emissão e funcionalidade do certificado, com documentação.

1.3.3.6. Requisitos de Experiência e Formação da Equipe:

Os recursos humanos disponibilizados pela Contratada (Autoridade Certificadora ou revendedor) devem possuir experiência comprovada na emissão de certificados digitais e no suporte relacionado.

1.3.3.7. Requisitos de Formação da Equipe

A eficácia da emissão do certificado digital está intrinsecamente ligada à competência da Autoridade Certificadora. Para a comprovação da expertise, são mandatórias as certificações e credenciamentos exigidos para operar como AC no âmbito da ICP-Brasil, se aplicável, ou como revendedor de confiança.

1.3.3.8. Requisitos Temporais:

- **Vigência Contratual:** O prazo inicial do contrato será de 60 (sessenta) meses, alinhado à validade do certificado.
- **Prazo para Início da Operação:** A Contratada deverá entregar o certificado em um prazo máximo de 15 dias úteis a partir da assinatura do contrato.
- **Periodicidade dos Testes (Verificação):** O certificado será verificado após a instalação.

1.3.3.9. Requisitos de Segurança da Informação:

A contratação exige da empresa contratada o compromisso formal com a confidencialidade, a integridade e a proteção dos dados envolvidos na emissão do certificado.

- **Conformidade:** A emissão do certificado deve observar rigorosamente os princípios da confidencialidade, integridade e disponibilidade, conforme a Política de Segurança da Informação (PSI) do PJAC e a LGPD.
- **Termo de Sigilo:** A Prestadora de Serviços deverá assinar um Termo de Sigilo e Confidencialidade.

1.3.3.10. Requisitos Sociais, Ambientais e Culturais:

A presente contratação, em alinhamento com as diretrizes de governança e sustentabilidade do Poder Judiciário, exige da Contratada a demonstração e o compromisso inequívoco com a observância de preceitos sociais, ambientais e culturais.



- **Conformidade com a Política de Sustentabilidade:** A Contratada deverá tomar pleno conhecimento do Plano de Logística Sustentável (PLS) do Poder Judiciário do Estado do Acre, se aplicável.
- **Aspectos Linguísticos e Culturais:** A interação na prestação dos serviços deverá priorizar o idioma Português do Brasil.
- **Alinhamento a Normativos:** A atuação da Contratada, bem como a solução, deverão demonstrar alinhamento com a LGPD e as normas do CNJ.

1.3.3.11. Requisitos Legais:

A solução e os serviços contratados deverão observar integralmente os seguintes instrumentos normativos e legais, nacionais e internacionais:

- Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD).
- Decreto nº 9.637/2018 – Política Nacional de Segurança da Informação.
- Resolução CNJ nº 396/2021 – Política de Segurança da Informação do Judiciário.
- Resolução PJAC nº 334/2025 – Política de Segurança da Informação do PJAC.
- Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).

1.3.3.12. Demais Requisitos Aplicáveis:

Para comprovar a aptidão para execução dos serviços do objeto desta contratação, a empresa CONTRATADA deverá apresentar atestado(s) de capacidade técnica, emitido(s) por pessoa jurídica de direito público ou privado, comprovando a emissão de certificados digitais WildCard ou serviços compatíveis.

1.4. Atendimento da demanda

1.4.1. Portal do Software Público Brasileiro

Conforme análise prévia (*ETP WildCard Antigo*), não há oferta de solução de Certificado Digital WildCard para servidores web disponível no Portal do Software Público Brasileiro que atenda à demanda do PJAC.

Solução	Origem/Órgão Responsável	Atende à demanda do PJAC?	Observações
Certificado Digital WildCard	Portal do Software Público Brasileiro	Não atende	Não há oferta identificada de Certificado Digital WildCard para proteção de múltiplos subdomínios.

1.4.2. Soluções de TIC



Com base na necessidade institucional de implementar segurança de comunicação para múltiplos serviços web e subdomínios, foram consideradas as seguintes abordagens:

- **Solução 1: Aquisição de certificados individuais para cada subdomínio:** tecnicamente viável, mas com alto custo de aquisição e gestão, além de maior complexidade administrativa.
- **Solução 2: Aquisição de um Certificado Digital WildCard (solução proposta):** abordagem mais eficiente e econômica, protegendo todos os subdomínios com um único certificado, simplificando a gestão e reduzindo custos.

Após análise técnica comparativa das alternativas, conclui-se que a aquisição de um Certificado Digital WildCard (Solução 2) representa a abordagem mais eficiente, econômica e segura para atender às necessidades do PJAC.

1.4.3. Contratações Públicas Similares

Contratações de certificados digitais são rotineiras na Administração Pública, validando a viabilidade técnica e jurídica do objeto. Órgãos como o PJSC e outros Tribunais frequentemente adquirem esse tipo de solução para garantir a segurança de suas plataformas digitais, muitas vezes também optando por certificados WildCard pela sua eficiência.

1.4.4. Aderência a padrões e modelos

A contratação de soluções de Tecnologia da Informação e Comunicação (TIC) no âmbito do Poder Judiciário requer a verificação da aderência a padrões e modelos de referência que visam a garantir a interoperabilidade, a segurança, a conformidade legal e a sustentabilidade das plataformas e serviços.

1.4.4.1. Modelo Nacional de Interoperabilidade - MNI

- **Conceituação:** O MNI estabelece princípios e requisitos arquitetônicos para promover a comunicação e o intercâmbio de informações entre diferentes sistemas e órgãos da Administração Pública.
- **Requisito de Verificação:** A solução de Certificado Digital WildCard, por sua natureza, não impacta diretamente a interoperabilidade de sistemas, mas garante a segurança da comunicação subjacente.
- **Justificativa Técnica:** A segurança da comunicação é um pilar para qualquer interoperabilidade, e o certificado contribui indiretamente para a confiança nas interações.

1.4.4.2. Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil

- **Conceituação:** A ICP-Brasil é a infraestrutura pública brasileira que garante a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, em



- **Requisito de Verificação:** A equipe de planejamento da contratação, bem como a futura Contratada, deverão verificar se a demanda requer compatibilidade com a ICP-Brasil, especialmente para garantir a validade e o reconhecimento do certificado no contexto brasileiro.
- **Justificativa Técnica:** A aderência à ICP-Brasil é crucial para garantir a segurança jurídica, o não-repúdio e a confiabilidade das informações e ações executadas, alinhando-se às diretrizes de governo eletrônico e segurança da informação do Estado brasileiro.

1.4.4.3. Modelo de Requisitos MoReq-Jus

- **Conceituação:** MoReq-Jus é uma adaptação brasileira do Modelo de Requisitos para Gestão de Registros Eletrônicos, com foco específico nas necessidades do Poder Judiciário.
- **Requisito de Verificação:** As entregas relacionadas ao Certificado Digital WildCard (como o próprio arquivo do certificado, chaves e documentação) não se enquadram como documentos ou registros eletrônicos oficiais do PJAC no sentido de MoReq-Jus, mas a gestão do ciclo de vida deve garantir a rastreabilidade e a segurança.
- **Justificativa Técnica:** Embora não diretamente aplicável, a preocupação com a gestão documental e a segurança da informação é inerente ao processo.

1.5. Análise dos Custos Totais da Demanda

- **Estimativa de Preço Referencial da Contratação:**
 - A estimativa de valor da contratação é de **R\$ 6.025,40** (seis mil e vinte e cinco reais e quarenta centavos), baseada na pesquisa de mercado por meio de cotação do banco de preços [D25432], em conformidade com o Art. 23 da Lei nº 14.133/2021, para a composição do Mapa de Preços da contratação.
- **Análise Comparativa de Custos (Total Cost of Ownership – TCO):**
 - Para a aquisição de um Certificado Digital WildCard, o TCO é simplificado. Inclui o custo de aquisição e eventuais custos de suporte técnico mínimo.
 - **a) Custos de Aquisição:** Valor do licenciamento do certificado.
 - **b) Custos de Implementação e Implantação:** Despesas com configuração e instalação (normalmente realizadas pela equipe interna, com suporte do fornecedor).
 - **c) Custos Operacionais:** Manutenção da validade e renovação.
 - **f) Custos Indiretos:** Os custos indiretos da *não contratação* (indisponibilidade, vazamento de dados) seriam exponencialmente maiores que o TCO da solução.

ID	Soluções identificadas	Especificação	CATSER	Qtd	Vantagens e Benefícios	Desvantagens e riscos	Custo(s) envolvido(s)
1	Aquisição de Certificados Individuais	Aquisição de certificados SSL/TLS para cada subdomínio separadamente.	27162	>150	Segurança granular por subdomínio.	Alto custo, complexidade de gestão e renovação.	Valor Estimado R\$ 200,00 por certificado A1
2	Aquisição de Certificado Digital WildCard	Aquisição de um único certificado WildCard para o domínio principal e todos os subdomínios.	27170	1	Redução de custos, simplificação da gestão, proteção abrangente.	Dependência de um único certificado para múltiplos pontos.	R\$ 6.025,40 [D25432]

1.6. Escolha e Justificativa da Solução

1.6.1. Descrição da Solução Escolhida

A solução escolhida é a aquisição de 01 (um) Certificado Digital padrão WILDCARD, do tipo A1 para servidores web, com validade de 60 meses (cinco vouchers). Esta solução abrange o domínio principal do TJAC e todos os seus subdomínios (ex: *.tjac.jus.br), garantindo a criptografia e a autenticidade das conexões HTTPS.

1.6.2. Benefícios Esperados

A contratação de um Certificado Digital WildCard trará benefícios significativos ao Poder Judiciário do Estado do Acre (PJAC), tanto do ponto de vista técnico quanto gerencial e institucional.

1.6.2.1. Eficácia

- Redução substancial dos riscos cibernéticos relacionados à interceptação de dados e falsificação de identidade.
- Aumento da resiliência dos ativos de informação, com a visibilidade de comunicação segura em todos os subdomínios.
- Detecção precoce de tentativas de acesso não seguro, viabilizando contenção de ameaças.
- Geração de confiança dos usuários nos serviços online do PJAC.

1.6.2.2. Eficiência

- Automatização da gestão de certificados para múltiplos subdomínios, reduzindo a dependência de força de trabalho manual.
- Simplificação dos processos de instalação e renovação.



- Capacitação e transferência de conhecimento para as equipes internas de TIC sobre a gestão do ciclo de vida do certificado.

1.6.2.3. Economicidade

- Redução de custos operacionais indiretos, ao evitar paralisações e perdas de dados decorrentes de ataques.
- Otimização dos investimentos em segurança, ao cobrir múltiplos subdomínios com um único certificado, sendo mais vantajoso que a aquisição individual.
- Melhor custo-benefício frente à alternativa de múltiplos certificados.

1.6.2.4. Padronização

- Adoção de práticas alinhadas a frameworks de segurança da informação, promovendo a padronização das conexões seguras.
- Atualização contínua da Política de Segurança da Informação.

1.6.2.5. Atendimentos aos aspectos específicos exigidos

- **Economia potencial com a correção de potenciais irregularidades:** A proteção HTTPS previne a exploração de vulnerabilidades de comunicação.
- **Resolução de irregularidades não associadas a pagamentos:** Garante a detecção e correção de falhas de segurança na comunicação.
- **Utilização de menor força de trabalho com automação:** O uso de um WildCard simplifica a gestão em vez de múltiplos certificados.
- **Agilidade e maior segurança na gestão de pessoas:** Garante que as comunicações internas e externas sejam seguras.

1.6.3. Resultados Esperados

- **Monitoramento contínuo** da segurança da comunicação nos servidores web.
- **Proteção contra acessos indevidos** e vazamento de dados.
- **Registro e rastreabilidade** da validade do certificado e de eventos relacionados.
- **Alinhamento às normas e boas práticas** de segurança, como ICP-Brasil e Resoluções CNJ.
- **Fortalecimento da resiliência institucional** e da confiança dos usuários.

1.6.4. Relação entre a Demanda Prevista e a quantidade de bens e/ou serviços Contratados



ID	Descrição	Catser	Und	Qtd	Valor Unitário	Valor total
1	Aquisição de Certificado Digital padrão WILDCARD, tipo A1 para servidores web, com validade de 60 meses (cinco vouchers).	27170	Unidade	1	R\$ 1.205,08	R\$ 6.025,40 [D25432]

O Valor total da Demanda é de: R\$ 6.025,40 (seis mil e vinte e cinco reais e quarenta centavos), conforme cotação do banco de preços [D25432].

1.7. Declaração de viabilidade da contratação

1.7.1. Declaração de Viabilidade:

- (x) Viável;
() Viável com restrições;
() Inviável.

1.7.2. Justificativa:

A deliberação pela Viabilidade da aquisição do Certificado Digital WildCard é o resultado de uma análise pormenorizada que perpassou a contextualização da demanda, o alinhamento estratégico, a caracterização técnica e a prospecção de mercado. Com base nas informações consolidadas neste Estudo Técnico Preliminar (ETP), observam-se os seguintes fundamentos para a viabilidade da contratação:

- **Necessidade e Alinhamento Estratégico:** A contextualização da demanda revelou a imperativa necessidade de segurança para os serviços online do PJAC, alinhando-se diretamente com os macrodesafios e objetivos estratégicos definidos no Plano Estratégico Institucional (PEI) e no Plano Diretor Institucional (PDTIC), bem como com a previsão do Plano Anual de Contratação de TIC (PSTIC) de 2025.
- **Aderência aos Requisitos Técnicos e Operacionais:** A aquisição do Certificado Digital WildCard, tipo A1 e validade de 60 meses (cinco vouchers), foi identificada como a mais apta a atender a esses requisitos de forma integral, promovendo segurança na comunicação, simplificação da gestão e economicidade.
- **Análise de Custos Totais da Demanda e Vantajosidade Econômica (TCO):** A análise dos custos demonstra que a aquisição de um certificado WildCard apresenta o custo total de propriedade mais vantajoso para o PJAC, sendo significativamente mais econômica que a alternativa de múltiplos certificados individuais.

2. SUSTENTAÇÃO DO CONTRATO

2.1. Adequação do Ambiente

PODER JUDICIÁRIO DO ESTADO DO ACRE			
Item	Descrição	SIM	NÃO
1	Necessidade de adequação de infraestrutura tecnológica?		X

2	Necessidade de adequação de infraestrutura elétrica?		X
3	Necessidade de adequação de logística de implantação?		X
4	Necessidade de adequação de espaço físico?		X
5	Necessidade de adequação de mobiliário?		X
6	Haverá impacto ambiental?		X

2.2. Recursos Materiais e Humanos

A execução da contratação principal exige que a equipe interna de TI do PJAC esteja capacitada para a instalação e gestão do certificado. O ETP WildCard Antigo indica a necessidade de conhecimento técnico no suporte e manutenção da licença de certificação digital, bem como para sanar dúvidas dos técnicos da equipe de TI do TJAC.

2.3. Continuidade do Fornecimento

O planejamento para a continuidade do fornecimento dos serviços de certificado digital é um elemento crítico de mitigação de riscos, visando a preservar a operacionalidade segura dos serviços web do PJAC. A natureza do objeto é permanente, pois a segurança das comunicações web é uma necessidade contínua. Estratégias de alerta prévio e renovação proativa serão implementadas.

2.4. Transição Contratual e Encerramento do Contrato

A fase de transição contratual e o encerramento do contrato, neste contexto, referem-se à gestão do certificado digital ao final de sua validade. O plano de transição deverá garantir que o PJAC mantenha a posse das chaves e arquivos do certificado, assegurando a mínima interrupção e a completa recuperação do controle.

2.5. Estratégia de Independência Tecnológica

A elaboração de uma estratégia robusta de independência tecnológica é fundamental. Serão estabelecidos critérios claros e vinculantes para assegurar a independência do PJAC em relação à Contratada, garantindo a posse e o controle das chaves privadas do certificado, e a capacidade de gerenciar ou renovar com outro provedor, se necessário.

2.6. Sanções contratuais

Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, o Contratado que:

- der causa à inexecução parcial ou total do contrato;



- ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado. As sanções aplicáveis incluirão advertência, impedimento de licitar e contratar, declaração de inidoneidade, e multas (moratória e compensatória), conforme detalhado no Termo de Referência e na Lei nº 14.133/2021.

3. ESTRATÉGIA PARA A CONTRATAÇÃO

3.1. Natureza do Objeto

Este subtópico tem como objetivo a precisa classificação da natureza jurídica e econômica do objeto da contratação.

- **Classificação Contábil:** O objeto da presente contratação configura-se predominantemente como **Despesa Corrente**, pois envolve a aquisição de um serviço de certificação e não de um bem de capital que incorpore o patrimônio de forma duradoura.
- **Classificação Quanto à Continuidade:** Os serviços de certificação digital, por sua intrínseca finalidade de proteção e segurança ininterrupta de um ambiente cibernético, são inequivocamente classificados como **Serviços Contínuos**.
- **Direitos de Propriedade Intelectual e Autoria:** Salvo justificativa técnica excepcional, a propriedade intelectual e os direitos autorais sobre o Certificado Digital WildCard, uma vez emitido, deverão ser integralmente do Poder Judiciário do Estado do Acre.

3.2. Parcelamento do Objeto e Adjudicação

A adjudicação será realizada em **lote único**, garantindo a unicidade de gestão e a abrangência da proteção para todos os subdomínios. Não será permitida a subcontratação dos serviços que compõem o objeto contratual, devendo a empresa contratada executar diretamente todas as atividades previstas. A formação de consórcios também não será admitida.

3.3. Modalidade e Tipo de Licitação

A seleção da modalidade e do tipo de licitação é determinada pela natureza do objeto a ser contratado.

- **Modalidade: Dispensa de licitação por valor**, por se tratar de aquisição de bens ou serviços comuns, bem como o baixo valor, por possuírem padrões de desempenho e qualidade objetivamente definíveis.
- **Tipo de Licitação:** O critério de julgamento será o de **Menor Preço**.

3.4. Vigência do contrato



A definição da vigência contratual é um elemento mandatório que estabelece o período de efetiva prestação dos serviços e a duração do vínculo jurídico. A vigência inicial do contrato será de **60 (sessenta) meses** (cinco vouchers), conforme o prazo de validade do Certificado Digital WildCard.

3.5. Equipe de Apoio à Contratação

Nome	Cargo	Matrícula	Setor
Elielcio Canedo da Silva	Subsecretário	7000710	SUCTI
Ângelo Máximo de Melo Silva	Chefe de Divisão	7002075	DICTI

3.6. Equipe de Gestão do Contrato

Nome	Cargo	Matrícula	Setor
Amilar Sales Alves	Gestor Titular	7000980	SUSEG
João de Oliveira Lima Neto	Gestor Substituto	7001707	DITRO

3.7. Equipe de Fiscalização do Contrato

Nome	Cargo	Matrícula	Setor
Luiz Webister Marinho Aguirre	Fiscal Titular	7002074	DIVDB
Ericson Rodrigues da Costa	Fiscal Substituto	7002073	DITRO

4. ANÁLISE DE RISCOS

Em atenção ao artigo 18, inciso X, da Lei Federal nº 14.133/2021, que destaca a importância da gestão de riscos para o sucesso da licitação e execução contratual, bem como ao artigo 10 da Resolução CNJ nº 468/2022, que prevê ações de gerenciamento de riscos e a elaboração do mapa de gerenciamento, e que este deve ser juntado ao processo de contratação após a elaboração dos Estudos Técnicos Preliminares.

É importante mencionar que, conforme disposto no artigo 22 da Lei Federal nº 14.133/2021, o edital poderá contemplar matriz de alocação de riscos entre o contratante e a Contratada, hipótese em que o cálculo do valor estimado da contratação poderá considerar taxa de risco compatível com o objeto da licitação e com os riscos atribuídos à Contratada, de acordo com metodologia predefinida pelo ente federativo.

De acordo com o art. 22, § 3º da Lei Federal nº 14.133/2021, para contratações de grande vulto, é obrigatório que o edital inclua o Mapa de Gerenciamento de Riscos, que aloca os riscos entre o contratante e a Contratada. Para contratações de menor vulto, a exigência desse artefato fica a critério do órgão, que deve definir o valor estimado para a não exigência do mesmo.



Dessa forma, é ressaltada a importância da elaboração do mapa de gerenciamento de risco, sua criação dependerá de critérios e valores mínimo definidos por normativo específico de cada órgão.

O tratamento dos riscos deve ocorrer ao longo de todo o processo de contratação e de gestão do contrato. Entretanto, o Mapa de Gerenciamento de Riscos deve ser atualizado, no mínimo:

- ao final da elaboração dos estudos técnicos preliminares;
- ao final da elaboração do termo de referência; e
- após eventos relevantes.

Neste tópico, são assinalados os principais riscos detectados envolvidos na contratação e na gestão do contrato.

4.1. Riscos Mapeados

R01	Risco:	Pane lógica na Certificação Digital	
	Probab.:	Média	
	Impacto:	Alto	
	Dano 1:	Paralisação dos serviços que dependem da certificação digital, resultando em indisponibilidade segura dos sites e sistemas do TJAC, perda de confiança e possíveis sanções regulatórias	
	Tratament:	Mitigar	
	Id	Ação Preventiva	Responsável
	1	Exigir da contratada competência técnica comprovada na emissão e suporte de certificados digitais. Realizar testes de funcionalidade pós-instalação	Equipe de Planejamento da Contratação / Fiscal do Contrato
	Id	Ação de Contingência	Responsável
	1	Solicitar os ajustes necessários para a prestação dos serviços de acordo com as especificações. Caso não seja cumprido no prazo, aplicar as sanções previstas no edital/contrato	Gestor do Contrato / Fiscal do Contrato

R02	Risco:	Atraso no atendimento de chamados relacionados ao certificado digital	
	Probab.:	Médio	
	Impacto:	Médio	
	Dano 1:	Paralisação parcial de serviços e sistemas devido a problemas com o certificado, impedindo o acesso seguro por parte dos usuários	
	Tratament:	Mitigar	
	Id	Ação Preventiva	Responsável
	1	Estabelecer no edital/contrato prazos máximos rigorosos para o atendimento de chamados e suporte técnico	Equipe de Planejamento da Contratação
	Id	Ação de Contingência	Responsável
	1	Aplicar as sanções previstas no contrato em caso de descumprimento dos SLAs de atendimento	Gestor do Contrato

R03	Risco:		O Tribunal não usufruir da solução conforme o previsto (problemas de configuração ou compatibilidade)
	Probab.:		Baixa
	Impacto:		Alto
	Dano 1:		Indisponibilidade ou funcionamento inadequado dos serviços online, comprometendo a prestação jurisdicional e a imagem do TJAC
	Tratament:		Mitigar
	Id	Ação Preventiva	Responsável
	1	Acompanhar de perto a execução do contrato, desde a emissão até a instalação e testes de funcionamento do certificado, garantindo conformidade com as especificações	Fiscal do Contrato
	Id	Ação de Contingência	Responsável
	1	Aplicar as sanções previstas no contrato e exigir a correção imediata das não conformidades ou substituição do certificado	Gestor do Contrato

5. APROVAÇÃO E ASSINATURA

Equipe de Planejamento da Contratação, instituída pela Portaria nº 3847/2025, de 20 de Agosto de 2025, bem como pela autoridade competente da área de TIC, aprovam o Estudo Técnico Preliminar e atestam sua conformidade às disposições da Resolução CNJ nº 468/2022.

6. CIÊNCIA DA INSTÂNCIA DELIBERATIVA DE TIC

Confirmo o recebimento do Estudo Técnico Preliminar, no qual tomo ciência de forma integral de seu conteúdo. A partir deste momento, segue para prosseguimento às providências cabíveis visando garantir o encaminhamento do ETP para a instância competente do órgão.

Assinatura Eletrônica da Comissão Permanente de Contratações de Tecnologia da Informação e Comunicação:

Amilar Sales Alves

Subsecretário de Segurança da Informação

Integrante Demandante - Portaria nº 3847/2025/TJAC



Eliélcio Canedo da Silva
Subsecretário de Contratações de TIC

PODER JUDICIÁRIO DO ESTADO DO ACRE
Rua Desembargador Jorge Araken, s/n. Via Verde.
69.915-631 - Rio Branco-AC - (68) 3212-8277

Integrante Técnico - Portaria nº 3847/2025/TJAC

Ângelo Máximo de Melo Silva

Chefe da Divisão de Contratações de TIC

Integrante Técnico - Portaria nº 3847/2025/TJAC

Elson Correia de Oliveira Neto

Secretário de Tecnologia da Informação e Comunicação

Autoridade Superior



Documento assinado eletronicamente por **ELIELCIO CANEDO DA SILVA**, **Técnico Judiciário** em 23/09/2025 às 14:05:15.



Documento assinado eletronicamente por **ELSON CORREIA DE OLIVEIRA NETO**, **Secretário(a)** em 24/09/2025 às 09:32:03.



Documento assinado eletronicamente por **AMILAR SALES ALVES**, **Gerente de Segurança da Informação** em 24/09/2025 às 07:43:47.



Documento assinado eletronicamente por **ANGELO MAXIMO DE MELO SILVA**, em 24/09/2025 às 07:16:29.





Para conferir a autenticidade do documento, utilize um leitor de QRCode ou acesse o endereço <http://appgrp.tjac.jus.br/grp/acessoexterno/programaAcessoExterno.faces?codigo=6702704DL6.CJAQ.ONNN.HA3H> e informe a chancela