DEFENSORIA PÚBLICA DO ESTADO DE RORAIMA
"Amazônia: Patrimônio dos brasileiros"
DIVISÃO DE MODERNIZAÇÃO E GOVERNANÇA DE TI

**Estudo Técnico Preliminar - DMGT/DTIC/DG/DPG**

# ESTUDO TÉCNICO PRELIMINAR
# CONTRATAÇÃO DE EMPRESA PARA FORNECIMENTO DE CERTIFICADO DIGITAL SSL

## 1 - DESCRIÇÃO DA NECESSIDADE

Com o aumento das ameaças cibernéticas e a crescente preocupação com a privacidade e integridade dos dados, tornou-se imperativo adotar medidas robustas para proteger as comunicações digitais. O advento de novas ameaças tecnológicas requer a adoção de soluções de segurança para garantir a integridade dos dados armazenados dentro da nossa infraestrutura de tecnologia da informação. A velocidade com que os ataques estão ocorrendo, bem como a quantidade de novas ameaças que se propagam, é preocupante e requer uma atenção especial da área de Tecnologia da Informação e Comunicação (TIC). Nesse sentido, a implementação de certificados digitais SSL (*Secure Socket Layer*) é essencial para assegurar a criptografia das informações e a autenticidade das comunicações.

Neste contexto, este ETP destina-se à contratação de uma empresa para prestar serviços de fornecimento de Certificado *Secure Socket Layer* (SSL) para solucionar a necessidade de autenticação de segurança de domínio na internet, possibilitando uma melhor atuação da DPE-RR no âmbito da *World Wide Web* (WWW) e garantindo a segurança das transações e comunicações realizadas através dos nossos sistemas online.

Justifica-se a presente contratação em virtude da necessidade de melhoramento da segurança da informação no ambiente computacional da Defensoria Pública do Estado de Roraima. O objetivo do Certificado SSL é proteger dados pessoais ou sigilosos que circulam na internet. Tal implantação se deve à necessidade de incrementar a segurança dos dados que trafegam no domínio da rede da DPE-RR, fazendo com que a transmissão dos dados criptografados dificulte consideravelmente a interceptação, roubo ou corrupção de dados.

Com o Certificado SSL o endereço na web da Defensoria (www.defensoria.rr.def.br) passará a ser exibido com **HTTPS**, com a inscrição "**Seguro**" e a imagem de um cadeado verde. Outra justificativa se deve à implementação de obrigatoriedade de implantação de Certificado SSL para as instituições que tiverem o Sistema Eletrônico de Informações - SEI e que forem atualizar para a versão mais recente e segura.

Ressalta-se também que a contratação de empresa para fornecimento de Certificado SSL beneficiará também toda a rede desta Instituição Pública, uma vez que a segurança a ser implementada servirá para todos os sistemas que funcionem em ambiente WEB, ou seja, Sistema SOLAR (Solução Avançada de Atendimento Referenciado), Sistema ATHENAS (Sistema de Gestão de Pessoal, Almoxarifado e Patrimônio, em implantação), além do Site Institucional (www.defensoria.rr.def.br) e todas as informações que tramitarem no ambiente de rede.

Necessidades Específicas:

- **Criptografia de Dados:** Necessidade de criptografar as informações transmitidas entre os servidores da organização e os dispositivos dos usuários para impedir que dados confidenciais sejam interceptados durante a transmissão.
- **Autenticação de Identidade:** Necessidade de garantir que os usuários estejam se comunicando com servidores legítimos da organização, evitando ataques de *phishing* e outros tipos de fraude *online*.
- **Conformidade com Regulamentações:** Necessidade de cumprir com regulamentações e normas de segurança da informação que exigem a proteção dos dados dos usuários, como a Lei Geral de Proteção de Dados (LGPD) e outros padrões internacionais.
- **Confiança do Usuário:** Necessidade de aumentar a confiança dos usuários nos serviços *online* da organização, mostrando que medidas adequadas de segurança estão sendo adotadas para proteger suas informações.
- **Prevenção de Ataques:** Necessidade de prevenir ataques *man-in-the-middle (MitM)* e outras formas de comprometimento das comunicações digitais, garantindo a integridade dos dados transmitidos.

## 2 - PREVISÃO NO PLANO DE CONTRATAÇÕES ANUAL

A Contratação encontra-se prevista no **Plano de Contratações Anual 2025 (2ª ALTERAÇÃO)**, publicado no dia 30 de abril de 2025 no DEDPE/RR nº 1150, contratação de nº **120** (Contratação de Certificado Digital SSL tipo Wildcard para utilização dos domínios e subdomínios da DPE/RR).

**3 - REQUISITOS DA CONTRATAÇÃO**

**3.1 - Requisitos normativos e legais:**

A presente contratação deverá atender ao que determina à Constituição Federal, à Lei Federal nº 14.133 de abril de 2021, à Resolução CSDPE Nº 98, DE 17 de janeiro de 2024, à LEI COMPLEMENTAR Nº 123, DE 14 DE DEZEMBRO DE 2006, à LEI Nº 13.709, DE 14 DE AGOSTO DE 2018, à LEI Nº 8.078, DE 11 DE SETEMBRO DE 1990 e à instrução normativa SEGES /ME nº 65, de 7 de julho de 2021.

**3.2 - Requisitos Técnicos:**

Especificações técnicas mínimas a serem consideradas:

- Certificado Digital SSL **tipo WildCard** para utilização em domínio único e subdomínios ilimitados da DPE-RR;
- Ter certificado com codificação criptografia mínima de 128 bits;
- Possuir compatibilidade com os navegadores web: O certificado SSL deve ser compatível com todos os navegadores modernos e dispositivos móveis.
- Ser compatível com os sistemas operacionais Windows e Linux;
- Ser compatível com servidores web que suportem os protocolos SSL, TLS e HTTPS;
- Vir acompanhado de documentação técnica em língua portuguesa;
- Manter o serviço de certificação disponível em regime de 24 horas e 7 dias por semana;
- A Licença deve permitir seu uso em quantidade ilimitada de servidores web sem custo adicional;
- Validade de 1 (um) ano.

**3.3 - Requisitos de Conformidade:**

Certificação e Padrões: O fornecedor deve estar em conformidade com os padrões do *CA/Browser Forum* e deve ser uma Autoridade Certificadora (CA) confiável e reconhecida.

Política de Privacidade: O fornecedor deve ter políticas de privacidade que garantam a proteção dos dados dos clientes.

Ramo de atividade: O fornecedor deve atuar na área de cibersegurança/segurança de redes.

Regulamentações: O fornecedor deve estar em conformidade com as regulamentações locais e internacionais, incluindo a Lei Geral de Proteção de Dados (LGPD).

**3.4 - Requisitos de Garantia, Suporte e Manutenção:**

O prazo de garantia contratual dos serviços, complementar à garantia legal, será de, no mínimo, 12 (doze) meses, contado a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto.

Suporte Técnico: O fornecedor deve oferecer suporte técnico 24/7 para resolução de problemas relacionados ao certificado SSL.

Documentação: O fornecedor deve fornecer documentação completa e detalhada para a instalação, configuração e renovação dos certificados SSL.

Serviço de Revogação: O fornecedor deve oferecer um serviço de revogação eficiente e rápido em caso de comprometimento do certificado.

**3.5 - Requisitos de Segurança:**

Armazenamento Seguro: O fornecedor deve garantir que os certificados são gerados e armazenados em ambientes seguros e protegidos contra acessos não autorizados.

Proteção Contra Ataques: O fornecedor deve implementar medidas para proteger seus sistemas contra ataques cibernéticos, como DDoS.

**3.6 - Requisitos de Experiência e Reputação:**

Histórico e Reputação: O fornecedor deve ter um histórico comprovado de fornecimento de certificados SSL e uma reputação positiva no mercado.

Referências: O fornecedor deve fornecer referências de clientes anteriores ou atuais que possam atestar a qualidade de seus serviços.

**3.7 - Requisitos de Metodologia de Trabalho:**

A execução dos serviços está condicionada ao recebimento pelo Contratado de **Ordem de Serviço (OS)** emitida pela Contratante.

A OS indicará o serviço, a quantidade e a localidade na qual os deverão ser prestados.

O Contratado deve fornecer meios para contato e registro de ocorrências da seguinte forma: com funcionamento 24 horas por dia e 7 dias por semana de maneira eletrônica e 24 horas por dia e 7 dias por semana por via telefônica.

A execução do serviço deve ser acompanhada pelo Contratado, que dará ciência de eventuais acontecimentos à Contratante.

**3.8 - Requisito conforme Lei 14.133/2021 Art. 63, IV:**

O licitante deverá apresentar declaração de que cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.

**4 - ESTRATÉGIA PARA CONTRATAÇÃO**

**4.1.** O serviço objeto a ser contratado é **Comum**, assim considerado por possuir padrão de desempenho e qualidade que possam ser objetivamente definidos no Termo de Referência, por meio de especificações usuais no mercado, na forma do inciso XIII do art. 6º da Lei Federal nº 14.133 de abril de 2021; uma vez que é facilmente encontrado no mercado de TIC.

**4.2.** Visando atender à demanda, é necessária a contratação, por meio de **dispensa de licitação, na forma eletrônica**, de acordo com o inciso II do artigo 75, da Lei 14.133/2021, atualizado pelo Decreto nº 12.343/2024, devido ser de valor inferior a R$ 62.725,59 (sessenta e dois mil setecentos e vinte e cinco reais e cinquenta e nove centavos), de empresa especializada para fornecimento de Certificado *Secure Soket Layer* (SSL).

**4.3.** A contratação em questão refere-se a prestação de serviços sem dedicação de mão de obra exclusiva.

**4.4.** A contratação não poderá ser prorrogada, devido à validade do Certificado a ser fornecido que não prevê prorrogação de validade, sendo necessária nova contratação de certificação para manutenção da segurança contratada, após seu vencimento.

**4.5.** O serviço não possui especificidades que impliquem na necessidade de transferência de conhecimento, tecnologia e técnicas empregadas.

**4.6.** A contratação em questão não envolve requisitos de práticas de sustentabilidade.

**4.7. Subcontratação:** É vedada a subcontratação de empresa para fornecimento do certificado SSL.

**4.8. Garantia da Contratação:** Não haverá exigência dos artigos 96 e seguintes da Lei nº 14.133, de 2021, devido o baixo vulto e baixa complexidade.

**5 - ESTIMATIVA DAS QUANTIDADES**

A necessidade apresentada é para **01 (um) certificado** apenas, que servirá de proteção ao site principal (www.defensoria.rr.def.br) e todos os outros sites compostos por seus subdomínios (Ex. sei.rr.def.br, solar.rr.def.br, athenas.rr.def.br, etc).

| Item | CATSER | Descrição dos Serviços | Quantidade (Unidades) |
|---|---|---|---|
| 01 | 27170 | Contratação de empresa para fornecimento de Certificado *Secure Soket Layer* (SSL) | 01 |

**6 - LEVANTAMENTO DE MERCADO E ESCOLHA DO TIPO DE SOLUÇÃO A SER CONTRATADA**

Existem atualmente no mercado **três tipos** de Certificados SSL, quanto ao nível de segurança:

1) Certificado para Validação do Domínio (DV)

1.1) Este é um dos tipos de Certificados SSL mais conhecidos. O nível de segurança fornecido é básico, serve para validar o nível de confiança do domínio. O nível fornecido de criptografia é básico e o custo é bem acessível, pode ser emitido rapidamente, inclusive gratuitamente. É recomendado para pequenos sites e blogs pessoais.

2) Certificado para Validação da Organização (OV)

2.1) Comparando com os outros tipos de Certificados SSL, este é considerado intermediário. O nível de confiança é superior ao certificado de validação do domínio. Esta versão faz a validação do domínio e também verifica as informações da organização.

2.2) Além dos elementos tradicionais de segurança ele também apresenta dados sobre a empresa portadora do domínio. É uma forma de validar tanto a segurança na web, quanto a existência física da empresa e sua idoneidade. É bastante indicado para sites de empresas e *e-commerces* de médio porte.

3) Certificado de Validação Estendida (EV)

3.1) De todos os tipos de Certificados SSL, este é o mais completo. Antes de emitir o certificado é feito um exame aprofundado, tanto da empresa, quanto do site. Por isso, esta é considerada a certificação com maior nível de segurança e confiança. Além de exibir os dados básicos que as versões anteriores também apresentam, esta opção também destaca o nome da empresa na URL antes do domínio. Essa opção é recomendada para grandes empresas e lojas virtuais bastante conhecidas (e é o exigido pelas versões mais recentes do SEI).

Quanto à quantidade de domínios que se pode proteger:

1) Certificado SSL de domínio único:

1.1) permite que apenas um domínio utilize o certificado em questão. Se for necessário instalar o SSL em outro endereço ou subdomínio será preciso adquirir uma nova licença.

2) Certificado SSL multidomínios:

2.1) Permite que vários domínios utilizem o mesmo certificado, mas há um limite para a quantidade de domínios que podem ser incluídos no certificado. Este limite pode variar dependendo da empresa que o emite.

3) Certificado SSL coringa (ou WildCard):

3.1) Seu diferencial está na capacidade de ser usado em todos os subdomínios vinculados ao domínio principal. Assim, este é o certificado ideal para sites que possuem muitos subdomínios e que desejam ter todos eles.

**Portanto, a DPE-RR precisará de um Certificado do Tipo Coringa (Wildcard) para domínio Único. O que pretendemos proteger são os subdomínios.**

Não foram identificadas Atas de Registro de Preços de Certificado tipo WildCard que buscamos.

## 7 - ESTIMATIVA DO PREÇO DA CONTRATAÇÃO

O certificado SSL WildCard é emitido para o nome comum *.dominio. Basta trocar o * por qualquer nome e utilizar a segurança SSL automaticamente em todos os subdomínios (um nível).

Em pesquisa de mercado a sites nacionais, que poderão emitir nota fiscal, e faturar em moeda nacional (Real), seguem os valores encontrados:

| Item | Empresa | Link | Tipo | Valor Anual | Pesquisado em | Média Aritmética do Valor nos Fornecedores Pesquisados |
|---|---|---|---|---|---|---|
| 01 | FLEXBOX | https://flexbox.cloud/pt-br/certificado-ssl | Thawte DV Wildcard SSL | 499,00 | 08/08/2025 | R$700,95 |
| 02 | SOLUTI | soluti.com.br | SSL ALPHA GLOBALSIGN | 596,22 | 08/08/2025 | |
| 03 | Rapid SSL | https://rapidssl.com.br/certificado-ssl/wildcard/ | Rapid SSL Pro Wildcard | 690,00 | 08/08/2025 | |
| 04 | MEUSSL | meussl.com.br | Certificado Sectigo PositiveSSL Wildcard | 1.018,58 | 08/08/2025 | |

A estimativa do valor médio da contratação é de **R$ 700,95 (setecentos reais e noventa e cinco centavos).**

## 8 - DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

A solução proposta para a implementação de certificados digitais SSL (*Secure Socket Layer*) na Defensoria Pública do Estado de Roraima (DPE-RR) envolve uma série de etapas e componentes que visam garantir a segurança das comunicações digitais e a integridade dos dados transmitidos através dos sistemas online da instituição. A solução será composta pelos seguintes elementos:

**8.1. Seleção e Contratação do Fornecedor:**
Escolha do Fornecedor: Seleção de uma empresa certificada e reconhecida como Autoridade Certificadora (CA) confiável, com histórico comprovado na emissão de certificados SSL.
Formalização do Contrato: Estabelecimento de um contrato detalhado que abranja todas as especificações técnicas, requisitos de suporte, manutenção e prazo de validade do certificado.
Necessário que o fornecedor emita nota fiscal em moeda corrente nacional (Real) e aceite pagamento após o recebimento definitivo do Certificado, via transferência bancária ou pagamento de boleto/fatura.

**8.2. Implementação Técnica:**
Geração e Configuração do Certificado: Geração dos certificados SSL pela Autoridade Certificadora e configuração nos servidores da DPE-RR.
Configuração dos Servidores: Ajuste das configurações dos servidores web e de aplicação para utilizar os certificados SSL, garantindo que todas as comunicações sejam criptografadas.
Teste e Validação: Realização de testes para assegurar que os certificados SSL estão funcionando corretamente e que a criptografia está ativa em todas as comunicações.

**8.3. Integração com Sistemas Existentes:**
Compatibilidade: Garantia de que os certificados SSL são compatíveis com todos os navegadores modernos e dispositivos móveis utilizados pelos usuários dos sistemas da DPE-RR.
Atualização de Aplicações: Atualização das aplicações e serviços online para suportar a autenticação e a criptografia proporcionadas pelo certificado SSL.

**8.4. Suporte e Manutenção:**
Suporte Técnico 24/7: Disponibilidade de suporte técnico contínuo para resolução de quaisquer problemas relacionados ao funcionamento do certificado SSL.

**8.5. Benefícios Esperados:**
Segurança das Informações: Criptografia das comunicações entre servidores e usuários, protegendo dados sensíveis contra interceptações e acessos não autorizados.
Confiança e Conformidade: Aumento da confiança dos usuários nos serviços online da DPE-RR e conformidade com regulamentações de segurança da informação.
Prevenção de Ataques: Proteção contra ataques cibernéticos, como *man-in-the-middle* (MitM), que poderiam comprometer a integridade dos dados transmitidos.

Essa solução completa e integrada permitirá que a DPE-RR fortaleça significativamente sua segurança digital, proporcionando um ambiente online seguro e confiável para todos os seus usuários e protegendo os dados transmitidos através de seus sistemas online.

## 9 - JUSTIFICATIVA PARA O NÃO PARCELAMENTO DA SOLUÇÃO

Não haverá necessidade de parcelamento da solução, pois se trata de **um único certificado.**

## 10 - DEMONSTRATIVO DOS RESULTADOS PRETENDIDOS

Aumento do nível de segurança e confiabilidade do domínio "rr.def.br" e seus subdomínios, na internet, visando segurança dos dados que trafegarem no domínio da rede da Defensoria Pública do Estado de Roraima - DPE-RR.

## 11 - PROVIDÊNCIAS PRÉVIAS AO CONTRATO

Não haverá necessidade de providências prévias ao contrato.

## 12 - CONTRATAÇÕES CORRELATAS/INTERDEPENDENTES

Não haverão contratações correlatas a serem feitas.

Esta DPE possui um Certificado SSL tipo *wildcard* que tem validade até 05/12/2025, que não poderá ser prorrogado, devendo-se fazer nova contratação para fornecimento de nova certificação.

## 13 - IMPACTOS AMBIENTAIS

Não haverão impactos ambientais a serem relatados.

## 14 - JUSTIFICATIVA DE DISPENSA DE ANÁLISE DE RISCO

Nos termos do art. 260, §1º, da Resolução CSDPE nº 98, de 17 de janeiro de 2024, e da Lei nº 14.133/2021, entende-se que o gerenciamento dos riscos pode ser dispensado considerando-se a baixa complexidade da contratação e o valor inferior ao valor limítrofe previsto no art. 75, II da Lei Federal nº Lei nº 14.133/2021, conforme **Justificativa de Dispensa de Análise de Riscos** (SEI nº 0721552).

## 15 - VIABILIDADE DA CONTRATAÇÃO

Com base nos elementos anteriores do presente documento de estudos preliminares, DECLARAMOS que:

**(X) É VIÁVEL** a presente contratação.

**Elaborado por:**

**Natércio Leite Dutra**

Chefe da Divisão de Modernização e Governança de TI - DMGT

Defensoria Pública do Estado de Roraima

**Revisado por:**

**Rogério Lima Albuquerque**

Chefe da Seção de Governança de TI - SGTI

Defensoria Pública do Estado de Roraima

**Jarliani Feitoza de Brito**

Assessora Especial III

Defensoria Pública do Estado de Roraima

**Aprovado por:**

**Ricardo Nattrodt de Magalhães**

**Diretor do Departamento de Tecnologia da Informação e Comunicação - DTIC**

Defensoria Pública do Estado de Roraima

Em 07 de agosto de 2025.

Documento assinado eletronicamente por **NATÉRCIO LEITE DUTRA**, **Chefe da Divisão de Modernização e Governança de TI**, em 12/08/2025, às 11:05, conforme horário oficial de Boa Vista/RR, com fundamento no art. 6°, § 1° do Decreto n° 8.539, de 8 de outubro de 2015, e Portarias DPG nº 877, de 1° de setembro de 2017 e nº 1251, de 15 de dezembro de 2017.

Documento assinado eletronicamente por **ROGÉRIO LIMA ALBUQUERQUE**, **Chefe da Seção de Governança de TI**, em 12/08/2025, às 11:12, conforme horário oficial de Boa Vista/RR, com fundamento no art. 6°, § 1° do Decreto n° 8.539, de 8 de outubro de 2015, e Portarias DPG nº 877, de 1° de setembro de 2017 e nº 1251, de 15 de dezembro de 2017.

Documento assinado eletronicamente por **JARLIANI FEITOZA DE BRITO**, **Assessora Especial III**, em 12/08/2025, às 11:40, conforme horário oficial de Boa Vista/RR, com fundamento no art. 6°, § 1° do Decreto n° 8.539, de 8 de outubro de 2015, e Portarias DPG nº 877, de 1° de setembro de 2017 e nº 1251, de 15 de dezembro de 2017.

Documento assinado eletronicamente por **RICARDO NATTRODT DE MAGALHÃES**, **Diretor do Departamento de Tecnologia da Informação e Comunicação**, em 12/08/2025, às 11:52, conforme horário oficial de Boa Vista/RR, com fundamento no art. 6°, § 1° do Decreto n° 8.539, de 8 de outubro de 2015, e Portarias DPG nº 877, de 1° de setembro de 2017 e nº 1251, de 15 de dezembro de 2017.

A autenticidade deste documento pode ser conferida no site http://sei.rr.def.br/autenticidade, informando o código verificador **0720435** e o código CRC **52E3FB37**.