ETPs – Estudo Técnico Preliminar Simplificado
Contratação Direta

• IDENTIFICAÇÃO

Demanda (ID / Título):	21863963 - Aquisição de Certificado SSL WildCard OV Validade 3 anos		
Resp. pelo atendimento (matrícula/nome):	T0074567 / Clenilson Castilho Leite		
Líder Técnico: (matrícula/nome):	T0009779 / Carlos Henrique Lopes Dias		
Unidade organizacional:	DIRFOR	**Gerência:**	
Id Jira / Título do ETP:	CODAP-3172 / Aquisição de Certificado SSL WildCard OV		
Proc. SEI da contratação:			

• DESCRIÇÃO SUCINTA DO OBJETO

DESCRIÇÃO	UND.	QUANTIDADE
Aquisição de Certificado SSL WildCard OV Validade 3 anos	**UN**	**1**

• FUNDAMENTAÇÃO DA CONTRATAÇÃO

• Contextualização, necessidade e motivação da contratação

A instalação e uso de certificado SSL (Secure Sockets Layer) nos servidores web da Instituição se justificam principalmente por:

1. Propiciar maior segurança dos dados trafegados pois o protocolo SSL criptografa as informações trocadas entre o navegador do usuário e o servidor, protegendo dados sensíveis (senhas, informações bancárias, etc.) de serem interceptados por terceiros;

2. Garantir aos usuários dos serviços e informações web disponibilizados pelo TJMG que o servidores com os quais está se comunicando são legítimos e autênticos, impedindo que sites fraudulentos ou mal-intencionados se passem por sites confiáveis;

3. Proporcionar integridade dos dados trafegados, pois além de criptografar os dados, o SSL também assegura que as informações não sejam alteradas ou corrompidas durante a transmissão, garantindo que os dados cheguem ao destino sem modificações.

4. Manter a conformidade com a Resolução nº 181/2017 de 06 de dezembro de 2017 do Conselho Nacional de Justiça e com a Lei Geral de Proteção de Dados Pessoas (LGPD).

- **Consequências da não contratação**

  Não usar um certificado SSL (Secure Sockets Layer) em um servidor web pode trazer diversas consequências negativas, tanto para os usuários quanto para o próprio site. Algumas das principais são:

1. Falta de Segurança na Transmissão de Dados. Sem SSL, as informações enviadas entre o usuário e o servidor (como senhas e informações pessoais) ficam vulneráveis a ataques de interceptação, como *Man-in-the-Middle (MITM)/*

2. Perda de Credibilidade e Confiança dos Usuários. Navegadores como Chrome, Firefox e Edge exibem alertas de "Não seguro" para sites sem HTTPS. Isso afasta visitantes e reduz a credibilidade. Por se tratar de uma entidade governamental jurisdicional, os serviços e informações prestadas pelo TJMG precisam transmitir o maior nível de credibilidade possível;

3. Impacto no SEO (Search Engine Optimization). O Google prioriza sites com HTTPS nos resultados de busca. Sem SSL, o site pode perder posicionamento e visibilidade nos motores de busca.

4. Risco de Ataques de Phishing e Spoofing. Hackers podem criar páginas falsas se passando pelo seu site legítimo. Sem SSL, fica mais fácil enganar usuários e roubar suas credenciais.

5. Possível Bloqueio por Navegadores e Firewalls. Alguns navegadores e redes corporativas podem bloquear o acesso a sites sem SSL, tornando o conteúdo inacessível para muitos usuários.

- **ALINHAMENTO DA DEMANDA COM DIRETRIZES E METAS INSTITUCIONAIS (PEI) DO TJMG OU O PLANEJAMENTO ESTRATÉGICO DE TIC (PETIC) E O PLANO ANUAL DE CONTRATAÇÕES**

- Planejamento Estratégico Institucional – PEI

  - MACRODESAFIO: XII Fortalecimento da Estratégia de Tecnologias da Informação e Comunicação - TIC e de Proteção de Dados

  - Iniciativa: 24. Governança, Gestão e Infraestrutura de Tecnologia da Informação e Comunicação.

- **DEFINIÇÃO DOS REQUISITOS**

- **ESPECIFICAÇÃO TÉCNICA**

- Tipo de Certificado: SSL WildCard
- Criptografia: 256 bits
- Chave Pública: 2048 bits (RSA) / Suporte para ECC
- Algoritmo de Assinatura: SHA-2 (SHA-256)
- Protocolos Compatíveis: TLS 1.2, TLS 1.3, HTTPS
- Validação OV (Organizational Validation)
- Segurança através do protocolo SSL (Secure Sockets Layer) em ilimitados sites e servidores.

• REQUISITOS DE IMPLANTAÇÃO

A implantação será efetuada por servidores e/ou colaboradores lotados na Coordenação de Administração de Aplicações - CODAP

• REQUISITOS DE GARANTIA, MANUTENÇÃO E SUPORTE TÉCNICO

- Suporte técnico qualificado em Português por email, helpdesk, chat e telefone durante toda a validade do certificado (36 meses).
- Reemissão gratuita durante toda a validade do certificado (36 meses).
- Licença de uso do mesmo certificado em ilimitados servidores sem custo adicional.

• ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS

Atualmente, os servidores web da Instituição possuem certificado SSL instalado na modalidade wildcard e EV (*.tjmg.jus.br e pje.tjmg.jus.br).

Será adquirido 01 (um) Certificado SSL WildCard OV com validade 3 anos. a ser instalado em todos os servidores web do TJMG, inclusive os servidores do Pje.

O certificado WildCard SSL, também conhecido como certificado coringa, possibilita que você adicione a segurança SSL em ilimitados sites e em ilimitados servidores. Esse tipo de certificado além de proporcionar economia de custos para a Instituição, também oferece maior flexibilidade na configuração e gerenciamento dos sites e servidores.

Foi definido um prazo de validade do 36 meses por ser mais adequado à Instituição, tendo em

vista que essa tecnologia não pode deixar de ser implantada nos servidores institucionais pelos motivos citados no item 3.2 acima.

Importante ressaltar que apesar de ter validade de 36 meses, a validação organizacional deve ocorrer anualmente. Após essa validação organizacional a entidade certificadora emite novo certificado gratuitamente que deverá ser instalado nos servidores. Após o término do período total de validade de 36 meses, novo certificado deverá ser adquirido.

Os certificados SSL/TLS têm validade máxima de 1 ano (ou, mais precisamente, 398 dias) por questões de segurança e controle, como por exemplo:

Redução de Riscos de Segurança. Certificados mais antigos são mais vulneráveis a ataques, especialmente se as chaves privadas forem comprometidas. A renovação frequente reduz a chance de um certificado comprometido permanecer ativo por muito tempo.

Adaptação a Novos Padrões de Segurança. O setor de segurança digital evolui rapidamente, e certificados mais curtos ajudam a implementar melhorias mais rapidamente. Novos algoritmos e práticas seguras podem ser adotados com mais frequência.

Prevenção de Abusos. Certificados de longa validade podem ser explorados por agentes mal-intencionados para phishing e outros golpes.

- **SOLUÇÃO**

  - **6.1. CUSTOS DA SOLUÇÃO**

    - **EMPRESAS CONSULTADAS**

	Empresa	Data da Consulta	Link da Consulta
1	Certisign Certificadora Digital S.A.	05/02/2025	https://certisign.com.br/certificados/ssl/ssl-ov-wildcard
2	Comodo Brasil Tecnologia Ltda. (Sectigo)	05/02/2025	https://www.sectigo.com.br/certificados-wildcard.php
3	soluti.com.br	05/02/2025	https://www.soluti.com.br/certificado_digital/certificado-ssl/?_gl=1*bgw4s1*_gcl_au*NTc1Mjc5MDUwLjE3NDAwNzU5

	(Globalsign)		MDA.
4	ActiveWeb Segurança Digital	05/02/2025	https://rapidssl.com.br/certificado-ssl/wildcard/

- ## 6.2. CUSTO TOTAL E VALOR DE REFERÊNCIA

Certificado SSL WildCard OV Validade 3 anos									
Solução única		Certisign Certificadora Digital S.A.		Comodo Brasil Tecnologia Ltda. (Sectigo)		soluti.com.br (Globalsign)		ActiveWeb Segurança Digital	
		Data: 05/02/2025		Data: 05/02/2025		Data: 05/02/2025		Data: 05/02/2025	
Item	**Quant.**	**Meses**	**Total**	**Meses**	**Total**	**Meses**	**Total**	Meses	**Total**
SSL Wildcard OV	1	12	R$2.418,90	12	R$1.890,00	12	R$2.688,22	12	R$1.790,00

Item	**Menor Valor**	**Valor Médio**	**Valor Mediano**	**Valor de Referência ***	**Quant.**	**Valor Total**
SL Wildcard OV	R$1.790,00	R$2.196,78		R$1.790,00	36 **	R$5.370,00
					Valor Total	R$5.370,00

*O Valor de Referência foi escolhido levando-se em conta o menor preço

** Foi feita cotação de preços do valor de certificado de validade anual para efeitos de compração, porém a aquisição será para um certificado de 36 meses com reemissão gratuita a cada ano conforme explicitado no item 5.

- ## DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

A Solução é composta pela aquisição e de um Certificado SSL WildCard OV com prazo de validade 3 anos com reemisão anual gratuita durante os 36 meses.

Tendo em vista que a empresa ActiveWeb Segurança Digital apresentou o menor preço pelo mesmo produto, foi feita solicitação à esta de envio de proposta comercial que se encontra anexada no Processo SEI 0043563-36.2025.8.13.0000, em que especifica desconto de 10% (dez por cento) para o certificado trienal

O custo máximo previsto para a solução é de R$4.833,00

- **APROVAÇÃO E ASSINATURA**

Integrante Técnico	**Integrante Demandante**
Carlos Henrique Lopes Dias / T0009779 GETEC	Clenilson Castilho Leite CODAP
A ATEND realizou a análise de conformidade do documento de acordo com Resolução nº 468/2022 do Conselho Nacional de Justiça.	
Nome e matrícula do revisor da AV Nome da Assessoria	Nome e matrícula do Assessor Nome da Assessoria