

TERMO DE REFERÊNCIA

1. CONTEXTUALIZAÇÃO

O efetivo cumprimento da Secretaria de Estado da Fazenda de Sergipe - SEFAZ/SE na captação e gestão dos recursos financeiros para o desenvolvimento sustentável do Estado e a promoção da cidadania fiscal, dada sua complexidade e relevância, requer constante aprimoramento tecnológico no compartilhamento de informações institucionais e no desenvolvimento de novas técnicas de trabalho. Para isso, faz-se necessária a constante modernização da sua estrutura tecnológica.

Esta Secretaria aprimora a postura de segurança e expansão do seu portfólio de soluções tecnológicas de forma segura. A integração de funcionalidades, reduções de riscos e custos são premissas para a promoção dos meios instrumentais e tecnológicos.

Muitos procedimentos são realizados por meio da Internet, é portanto, pressuposto da Superintendência de Tecnologia da Informação, garantir o elevado nível de segurança, sigilo e integridade de informações no ambiente tecnológico desta Secretaria.

2. OBJETO

É de expresse interesse da SEFAZ/SE a aquisição de Certificado digital E-CNPJ Tipo A1, Certificado SSL tipo A1, Certificado SSL Wildcard e OV.

A pretendida adesão visa proporcionar maior visibilidade e informações sobre a segurança de todo ambiente tecnológico da SEFAZ/SE, mediante eficientes práticas de segurança que minimizem riscos cibernéticos.

3. DESCRIÇÃO DOS PRODUTOS/SERVIÇOS

Para alcance do objeto acima proposto, mediante nível de conveniência e necessidade da SEFAZ/SE e, atendendo aos padrões de qualidade, especificação e funcionalidade técnicas exigidas no Instrumento Licitatório, segue o detalhamento de produtos/serviços a serem adquiridos:

Nº ITEM	DESCRIÇÃO	DEMANDA SOLICITADA
1	Certificados Digitais SSL - SECTIGO - RAIZ INTERNACIONAL - 12 meses	12
2	Certificado e-CNPJ - 12 meses A1	4
3	Certificados Digitais SSL - ICP-BRASIL - SERPRO	12

4. ESPECIFICAÇÕES TÉCNICAS - CERTIFICADOS DIGITAIS SSL

- Certificado digital SSL do tipo WILDCARD para servidores WEB;
- Certificado tipo WILDCARD, que permite certificar um único domínio e infinitos subdomínios (um nível);
- Certificado de validação completa;
- Instalação em servidor adicional sem custo e ilimitado;
- Licença de uso do mesmo certificado em ilimitados servidores e/ou equipamentos;
- Reemissão gratuita e ilimitada durante o período de validade do certificado; □ Utilizar algoritmo de criptografia SHA-256;
- Suportar chaves RSA com 2048 bits;
- Ser compatível com o protocolo SSL- Secure Sockets Layer, versões SSLv2, SSLv3, TLS – Transport Layer Security na versão TLSv1 (SSLv3. 1) e HTTPS;
- Compatível com 100% dos servidores WEB que suportem os protocolos SSL e TLS, dentre eles podemos explicitar Apache, Microsoft Internet Information Services, Nginx e A10;
- Ser reconhecido por todos os navegadores web que suportem certificados SSL/TLS, sem a necessidade de nenhuma intervenção manual do usuário ou instalação de cadeias adicionais;
- Compatível com dispositivos móveis, celulares, smartphones e tablets;
- Possuir selo de segurança Site Seguro;
- Verificação do status do Certificado em tempo real (OCSP);
- Possuir conformidade WebTrust;
- Incluir prestação de suporte técnico remoto, via telefone, e-mail, chat e/ou website, por equipe de técnicos especializados, para esclarecimento de dúvidas técnicas e cadastrais, tais como: geração do CSR, validação da solicitação de compra, instalação do certificado e selo do site seguro e outras necessárias à

perfeita execução do objeto contratado;

- Garantia de reposição do Certificado ou a correção da solicitação pendente, em caso de constatação de erro técnico no CSR, no prazo máximo de 02 (dois) dias após a emissão do mesmo;
- Validade mínima de 12 (doze) meses, contada a partir da data de sua emissão;
- Não serão aceitos certificados de autoridades certificadoras descredenciadas pela Apple, Microsoft, Mozilla e Google.

5. FUNCIONALIDADES CERTIFICADOS DIGITAIS SSL

5.1. Criptografia

- Criptografia de Dados: Protege a comunicação entre o navegador e o servidor web, garantindo que os dados transmitidos sejam ilegíveis para terceiros. Isso impede que informações sensíveis, como senhas e números de cartão de crédito, sejam interceptadas e lidas por pessoas não autorizadas.
- Criptografia de Sessão: Estabelece uma conexão segura usando criptografia simétrica durante a sessão de navegação. A criptografia simétrica usa a mesma chave para codificar e decodificar os dados.

5.2. Autenticação

- Verificação de Identidade: Garante que o servidor web ao qual o usuário está se conectando é realmente quem diz ser. Isso ajuda a prevenir ataques de phishing e outras fraudes online.
- Confiança na Identidade: Fornece informações sobre a organização que possui o site, quando aplicável (em certificados de validação de organização e validação estendida).

5.3. Integridade dos Dados

- Proteção Contra Alteração: Assegura que os dados transmitidos entre o cliente e o servidor não sejam alterados durante o trânsito. Qualquer alteração nos dados é detectada e a comunicação é interrompida.
- Assinatura Digital: Utiliza assinaturas digitais para garantir que os dados não tenham sido modificados desde que foram enviados.

5.4 Estabelecimento de Conexão Segura

- Handshake SSL/TLS: Durante o processo de handshake (aperto de mão) SSL/TLS, o

navegador e o servidor negociam os parâmetros de criptografia a serem usados, garantindo que ambos estejam de acordo sobre o nível de segurança da conexão.

- **Certificação de Cifras e Protocolos:** Define e estabelece os algoritmos de criptografia e protocolos de segurança que serão utilizados durante a conexão.

5.5. Indicação Visual de Segurança

- **Ícones de Segurança no Navegador:** Navegadores modernos exibem ícones visuais, como um cadeado na barra de endereços, para indicar que a conexão é segura. Em certificados de validação estendida (EV), o nome da empresa pode aparecer na barra de endereços.
- **HTTPS:** URLs seguras começam com "https://" em vez de "http://", sinalizando que a comunicação é criptografada.

5.6. Proteção Contra Ataques

- **Ataques Man-in-the-Middle (MitM):** Os certificados SSL/TLS ajudam a proteger contra ataques em que um invasor intercepta e possivelmente modifica a comunicação entre o cliente e o servidor.
- **Ataques de Interceptação:** Impede que dados sensíveis sejam capturados por interceptadores maliciosos.

5.7. Conformidade e Regulação

- **Regulamentações de Segurança:** Auxilia as organizações a atenderem aos requisitos de segurança e privacidade estabelecidos por regulamentos e padrões, como PCI-DSS (para pagamentos com cartão de crédito) e GDPR (Regulamento Geral sobre a Proteção de Dados).

5.8. Gerenciamento e Recomendação

- **Revogação de Certificados:** Permite a revogação de certificados comprometidos ou inválidos através de listas de certificados revogados (CRLs) e o protocolo OCSP (Online Certificate Status Protocol).
- **Renovação e Atualização:** Facilita a renovação de certificados expirados para garantir a continuidade da segurança.

5.9 Integração com Outras Tecnologias

- **Integração com Servidores Web:** Trabalha em conjunto com servidores web, como Apache, Nginx e Microsoft IIS, para garantir que as comunicações sejam seguras.
- **Suporte a Protocolos de Segurança Adicionais:** Pode ser usado em conjunto com outros protocolos de segurança para oferecer uma proteção mais abrangente.
- **Em resumo,** os certificados SSL/TLS desempenham um papel essencial na proteção das informações transmitidas pela internet, garantindo a segurança, autenticidade e integridade das comunicações entre usuários e serviços online.

6. ESPECIFICAÇÕES TÉCNICAS - CERTIFICADO E-CNPJ A1

- O certificado Digital deverá permitir a criação de cópias em outras máquinas / servidores;
- Possibilitar realização de backup do arquivo;
- Poderá ser hospedado no servidor do órgão;
- Incluir prestação de suporte técnico remoto via telefone, e-mail, chat e/ou website, por equipe de técnicos especializados, para esclarecimento de dúvidas técnicas e cadastrais.
- Validade mínima de 12 (doze) meses, contada a partir da data de sua emissão.

7. FUNCIONALIDADES DO CERTIFICADO E-CNPJ A1

7.1. Autenticação Digital

- Identificação da Empresa: O e-CNPJ A1 permite que a empresa se identifique de forma segura em transações eletrônicas, como envio de documentos para a Receita Federal, declarações fiscais e outras interações com órgãos públicos.
- Acesso a Sistemas Governamentais: Facilita o acesso a sistemas online, como a Receita Federal, o Portal do e-Social, e outras plataformas que requerem a autenticação de identidade corporativa.

7.2. Assinatura Digital

- Assinatura de Documentos: Permite a assinatura digital de documentos, garantindo a autenticidade e integridade dos mesmos. Assinaturas digitais com o e-CNPJ A1 têm o mesmo valor jurídico que assinaturas manuscritas.
- Validade Jurídica: Assinaturas feitas com o e-CNPJ A1 têm validade legal, conforme a legislação brasileira, e são aceitas como prova em processos judiciais.

7.3. Segurança e Integridade

- Criptografia: Utiliza criptografia avançada para proteger dados e comunicações. O certificado garante que as informações enviadas ou recebidas não sejam interceptadas ou modificadas.
- Proteção Contra Fraudes: Ajuda a prevenir fraudes e acessos não autorizados, garantindo que apenas usuários autorizados possam realizar ações em nome da empresa.

7.4. Certificação e Autorização

- **Certificado Digital:** O e-CNPJ A1 é um certificado digital tipo A1, que é armazenado diretamente no computador ou dispositivo do usuário (diferente do A3, que é armazenado em um token ou smartcard). Isso permite acesso direto e fácil ao certificado.
- **Certificado da Receita Federal:** O e-CNPJ A1 é emitido pela Receita Federal e tem validade de um ano. É uma forma de garantir que as interações com a Receita Federal e outras entidades estejam autenticadas.

7.5. Compliance e Regulamentação

- **Conformidade Legal:** Atende aos requisitos legais e regulamentares para a realização de transações eletrônicas e envio de documentos fiscais e contábeis, como SPED (Sistema Público de Escrituração Digital), NF-e (Nota Fiscal Eletrônica), e outros.
- **Atendimento a Normas Técnicas:** Segue os padrões técnicos estabelecidos pela ICP-Brasil (Infraestrutura de Chaves Públicas Brasileira) para certificação digital.

7.6. Acesso e Gestão

- **Gerenciamento de Certificados:** Permite a administração e renovação do certificado digital, incluindo a revogação em caso de comprometimento ou necessidade de atualização.
- **Facilidade de Uso:** O e-CNPJ A1 é geralmente mais fácil de usar e gerenciar em comparação com certificados que requerem hardware específico, como o A3.

7.7. Integração com Sistemas Empresariais

- **Integração com ERP e Sistemas Contábeis:** Facilita a integração com sistemas de ERP e softwares contábeis, permitindo o envio automatizado de documentos fiscais e relatórios.
- **Automação de Processos:** Permite a automação de processos empresariais que envolvem a assinatura e envio de documentos digitais, melhorando a eficiência e reduzindo erros.

7.8. Suporte e Atualizações

- **Suporte Técnico:** Disponibiliza suporte técnico para instalação, configuração e resolução de problemas relacionados ao certificado.
- **Atualizações Regulares:** Assegura que o certificado esteja atualizado com as últimas práticas de segurança e conformidade, através de renovação anual.

7.9. Conclusão

- O Certificado e-CNPJ A1 é uma ferramenta crucial para a segurança e conformidade das operações digitais de uma empresa no Brasil. Ele fornece autenticação segura, permite assinaturas digitais legalmente válidas, e facilita a interação com sistemas

governamentais e regulatórios. Ao utilizar o e-CNPJ A1, empresas garantem a integridade e a proteção das suas transações eletrônicas, mantendo conformidade com as exigências legais.

8. ESPECIFICAÇÕES TÉCNICAS CERTIFICADOS DIGITAIS SSL - ICP-BRASIL

8.1.Emissão de Certificados Digitais do tipo A1 ICP-Brasil para servidor Web, conforme características abaixo:

8.2.Emitido por autoridade certificadora credenciada pela Infraestrutura de Chaves Públicas Brasileiras (ICP-Brasil);

8.3.Validade mínima de 12 (doze) meses, contados da data de emissão do certificado;

8.4.Ser baseado em SSL/TSL (Secure Sockets Layer/Transport Layer Security);

8.5.Ter ativo o protocolo OCSP (Online Certificate Status Protocol);

8.6.Permitir a comunicação segura por SSL com criptografia forte de 256 bits;

8.7.Tamanho de chave RSA de 2048 bits;

8.8.Algoritmo do certificado SHA 2 (256bits).

9. FUNCIONALIDADES DO CERTIFICADOS DIGITAIS SSL - ICP-BRASIL

9.1.Criptografia: Protegem os dados transmitidos entre o servidor e o cliente, tornando-os iConfiabilidade: Sites que utilizam SSL com certificação da ICP-Brasil transmitem uma imagem de segurança e profissionalismo, aumentando a confiança dos usuários.

9.2.Compatibilidade com Navegadores: Certificados SSL da ICP-Brasil são reconhecidos por todos os principais navegadores, garantindo que a conexão segura seja validada corretamente.Criptografia: Protegem os dados transmitidos entre o servidor e o cliente, tornando-os legíveis para terceiros.

9.3.Autenticação: Garantem que o site é realmente quem diz ser, ajudando a evitar fraudes e phishing.

9.4.Integridade dos Dados: Asseguram que os dados não foram alterados durante a transmissão.

9.5.Confiabilidade: Sites que utilizam SSL com certificação da ICP-Brasil transmitem uma imagem de segurança e profissionalismo, aumentando a confiança dos usuários.

9.6.Compatibilidade com Navegadores: Certificados SSL da ICP-Brasil são reconhecidos por todos os principais navegadores, garantindo que a conexão segura seja validada corretamente.

Esses certificados são essenciais, especialmente para sites que lidam com informações sensíveis, como dados pessoais e financeiros.

10. OBRIGAÇÕES DO FORNECEDOR

Manter atualizados seus dados cadastrais junto a Secretaria do Estado da Fazenda/SE;

Cumprir com os prazos de entrega, sob pena de aplicação de sanções administrativas;

Assumir total responsabilidade pela entrega dos serviços e equipamentos registrados, obedecendo ao que dispõe a proposta apresentada e observando as constantes da Ata de Registro de Preços e seus anexos, inclusive reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, vícios ou incorreções que forem detectados;

Cumprir fielmente as obrigações assumidas, observando as especificações técnicas deste Termo de Referência;

Comunicar a SEFAZ/SE, por escrito, quaisquer anormalidades que ponham em risco o êxito e o cumprimento dos prazos da entrega dos serviços e / ou equipamentos, propondo as ações necessárias para a execução dos mesmos;

Assumir todos os encargos de possível demanda trabalhista, cível ou penal, relacionadas à execução dos serviços e entrega dos equipamentos objeto deste Termo de Referência, bem como custos relativos ao deslocamento e estada de seus profissionais, caso existam;

Responder civil e penalmente por quaisquer danos ocasionados à Administração e seu patrimônio e/ou a terceiros, dolosa ou culposamente, em razão de sua ação ou de omissão ou de quem em seu nome agir;

Não embaraçar ou frustrar a fiscalização e o acompanhamento da execução do objeto deste Termo de Referência por servidor designado pelo Órgão Gerenciador;

Responsabilizar-se técnica e administrativamente pelo objeto registrado, não sendo aceito, sob qualquer pretexto, a transferência de responsabilidade a outras entidades, sejam fabricantes, técnicos ou quaisquer outros.

11. OBRIGAÇÕES DA CONTRATANTE

Prestar as informações necessárias para que a contratada possa cumprir com suas obrigações, dentro das normas e condições firmadas no contrato;

Designar formalmente, na forma do art. 117, da Lei n. 14.133/2021, representantes para gerenciar o Contrato e para exercer a fiscalização da execução do mesmo, independente do acompanhamento e controle exercido pela contratada.

Prestar, por meio do fiscal, as informações e os esclarecimentos pertinentes à execução dos serviços, que porventura venham a ser solicitados pela Contratada.

Informar à contratada sobre atos que possam interferir direta ou indiretamente na entrega do serviço.

Notificar a CONTRATADA quanto a irregularidades ou defeitos verificados na execução das atividades objeto deste Termo de Referência, bem como quanto a qualquer ocorrência relativa ao comportamento de seus técnicos, quando em atendimento, que venha a ser considerado prejudicial ou inconveniente para o CONTRATANTE.

Promover a fiscalização do contrato, sob os aspectos qualitativos, por intermédio de profissional especialmente designado, o qual anotará em registro próprio as falhas detectadas e as medidas corretivas necessárias. O mesmo deverá acompanhar o desenvolvimento do contrato, conferir os serviços executados e atestar os documentos fiscais pertinentes quando comprovada a execução fiel e correta dos serviços, podendo, ainda, sustar, recusar, mandar fazer ou desfazer qualquer procedimento que não esteja de acordo com os termos contratuais.

Exigir o cumprimento de todos os compromissos assumidos pela Contratada, de acordo com os termos do contrato assinado.

Proporcionar todas as condições e prestar as informações necessárias para que a Contratada possa cumprir com suas obrigações, dentro das normas e condições contratuais.

Comunicar oficialmente à contratada quaisquer falhas verificadas no cumprimento do contrato, determinando, de imediato, as providências necessárias à sua regularização.

Registrar e oficializar a Contratada sobre as ocorrências de desempenho ou comportamento insatisfatório, irregularidades, falhas, insuficiências, erros e omissões constatados, durante a execução do contrato, para as devidas providências pela Contratada.

Rejeitar, no todo ou em parte, os serviços executados, com especificações inferiores às definidas neste Termo de Referência.

Aprovar ou rejeitar, no todo ou em parte, os serviços que não estiverem em conformidade com as especificações constantes da proposta apresentada pela CONTRATADA.

Efetuar o pagamento devido pela configuração e manutenção do software, desde que cumpridas todas as formalidades e exigências contratuais.

12. A CONTRATANTE OBRIGA-SE A:

12.1 Efetuar o pagamento na forma convencionada, dentro do prazo previsto, desde que atendidas às formalidades pactuadas;

12.2 O responsável pelo recebimento da Nota Fiscal procederá, no prazo de 05 (cinco) dias úteis, à conferência se a descrição contida no documento corresponde às especificações solicitadas, junto com a unidade solicitante para aceitá-la ou rejeitá-la.

12.3 Serão recusadas as Notas Fiscais que relacione especificações diferentes daquelas solicitadas e/ou constantes da proposta e do termo de homologação.

12.4 Na hipótese do subitem anterior, a contagem do prazo para pagamento somente começará a fluir após a correção do documento fiscal.

12.5 Nenhum pagamento será efetuado à contratada enquanto pendente de liquidação qualquer obrigação financeira que lhe for imposta em virtude de penalidade ou inadimplência, a qual poderá ser compensada com o(s) pagamento(s) pendente(s), sem que isso gere direito a acréscimos de qualquer natureza.

12.6 A contratada deverá emitir Nota Fiscal em atenção às normas pertinentes, indicando a instituição bancária, número da conta corrente e agência com a qual opera e discriminando em seu bojo as especificações do produto entregue para Secretaria de Estado da Fazenda de Sergipe.

13.ORIGEM DOS RECURSOS

As despesas com o pagamento do referido objeto correrão por conta da Dotação Orçamentária a ser especificada pela Superintendência de Planejamento Financeiro/SEFAZSE.

14. LOCAL DA ENTREGA

Todos os produtos e serviços acima mencionados serão entregues e/ou implantados na Sede Aracaju Boulevard, com prazo de até 10 (dez) dias úteis após a assinatura do contrato, para iniciar planejamento para elaboração do Cronograma de instalação dos equipamentos e soluções, em conjunto com a CONTRATANTE.

Aracaju, 16 de outubro de 2024



ASSINADO ELETRONICAMENTE
Verificar autenticidade conforme mensagem
apresentada no rodapé do documento

ANTONIONI ASSIS ANDRADE DO MONTE
Gerente de TI

Protocolo de Assinatura(s)

O documento acima foi proposto para assinatura digital. Para verificar as assinaturas acesse o endereço <http://edocsergipe.se.gov.br/consultacodigo> e utilize o código abaixo para verificar se este documento é válido.

Código de verificação: VAHJ-6G3P-RNPJ-ZSLK



O(s) nome(s) indicado(s) para assinatura, bem como seu(s) status em 05/11/2024 é(são) :

Legenda: ● Aprovada ● Indeterminada ● Pendente

- ANTONIONI ASSIS ANDRADE DO MONTE - 16/10/2024 12:08:08 (Docflow)