ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO

ATENÇÃO: A cópia impressa a partir da *intranet* é cópia não controlada.

1- DESCRIÇÃO DA SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO

Contratação de empresa especializada na prestação de serviço de emissão e validação de certificados digitais com fornecimento de mídia criptográfica, em local próprio da Contratada, contendo os seguintes itens:

1. Certificados digitais para pessoa física padrão ICP-Brasil do tipo A3 a ser prestado por uma AC-JUS, com validade de 03 (três) anos, armazenados em dispositivos de mídias criptografadas, ou em HSM (Hardware Security Module).
2. Certificados digitais para equipamentos servidores do tipo SSL Site Seguro, com validade mínima de 01 (um) ano;
3. Certificados digitais para equipamentos servidores do tipo SSL Múltiplos Domínios, com validade mínima de 01 (um) ano.
4. Certificados digitais para pessoa jurídica do tipo A1, com validade mínima de 01 (um) ano;
5. Serviços especializados de AR (Autoridade de Registro) para emissão e validação de certificados em local próprio da Contratada, com capacidade de atendimento dentro de cada uma das cidades sedes que compõem os NURs, distribuídos pela capital e interior do Rio de Janeiro;
6. Dispositivo de mídia criptografada para armazenamento dos certificados tipo A3.
7. Certificados digitais para equipamentos servidores do tipo SSL Site Seguro, com validade mínima de 01 (um) ano no padrão internacional OV (Organization Validation), cuja AC emita estes certificados contendo o campo de Transparência de Certificado - CT (Certificate Transparent) obrigatoriamente preenchidos;
8. Certificados digitais para equipamentos servidores do tipo SSL Múltiplos Domínios, com validade mínima de 01 (um) ano no padrão internacional OV (Organization Validation), cuja AC emita estes certificados contendo o campo de Transparência de Certificado - CT (Certificate Transparent) obrigatoriamente preenchidos;

2- REQUISITOS DE NEGÓCIOS UNIDADE DEMANDANTE

2.1 – NECESSIDADE DE NEGÓCIO

Necessidade 1: Certificado Tipo A3:

9. Prestação de serviço de emissão e validação de certificados digitais para pessoa física padrão ICP-Brasil do tipo A3 a ser prestado por uma AC-JUS, com validade de 03 (três) anos, armazenados em dispositivos de mídias criptografadas, ou em HSM (Hardware Security Module).

A presente contratação é essencial para assegurar o atendimento aos objetivos do PETI do TJERJ, com foco especial em:

- CP1 - Contribuir com soluções de TI eficazes para agilizar os procedimentos administrativos e jurisdicionais;
- CP3 - Disponibilizar informações para tomada de decisão gerencial e administrativa;
- P1 - Garantir a integridade e disponibilidade de todos os serviços de TI do Poder Judiciário;
- P5 - Aprimorar a comunicação com públicos externos e internos;
- P6 - Promover iniciativas de segurança da informação.

Funcionalidade	Ator Envolvido
1 - Emitido por autoridade certificadora credenciada pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), dentro da hierarquia AC-JUS;	Contratada TJERJ (Magistrados e Servidores)
2 - Deverá permitir assinatura de e-mails e documentos eletrônicos, autenticação de cliente, acesso legítimo aos sistemas e realizar *logon* na rede com garantia da integridade das informações;	
3 - Deverá ser compatível com os principais clientes de e-mail (Microsoft Outlook 2010 e Office365 ou versões superiores);	
4 - Ser aderente às normas ICP-Brasil;	
5 - Possuir validade de 03 (três) anos;	
6 - Deverá ser armazenado em dispositivo de mídia criptografada, ou em HSM (Hardware Security Module).	
7 - Deverá fornecer software destinado ao Windows 10 Professional (release 1809 e versões superiores)	

capaz de realizar o processo de emissão de certificado ICP-Brasil diretamente no HSM (modelo Dínamo XP homologado para uso pela ICP-Brasil) realizando as comunicações necessárias junto a Autoridade Certificadora por meio da Internet. Tal software deve ser compatível com o proxy de rede do TJERJ, sem restrições de distribuição e uso pelo TJERJ, e ser mantido funcional durante toda execução do contrato. Tal emissão será executada pelo usuário detentor do certificado digital através da operação do software mencionado e pode prescindir de fornecimento de documento pela certificadora durante a sua validação presencial;	
8 - Deverá fornecer meio de comunicação pela Internet para que o TJERJ possa futuramente providenciar a construção de software customizado que realize a mesma função executada pelo Software fornecido no item 7 acima.	
Necessidade 2: Certificados digitais para equipamentos servidores do tipo SSL Site Seguro: Prestação de serviço de emissão e validação de certificados digitais para equipamentos servidores do tipo SSL Site Seguro, com validade mínima de 01 (um) ano. A presente contratação irá contribuir com o plano de infraestrutura do TJERJ. A presente contratação é essencial para assegurar o atendimento aos objetivos do PETI do TJERJ, com foco especial em: • R1 – Manter a infraestrutura de TI segura, apropriada e otimizada.	
Funcionalidade	**Ator Envolvido**
1 - Emitido por autoridade certificadora credenciada pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil);	Contratada DGTEC-DISER
2 - Possuir validade mínima de 01 (um) ano;	
3 - Deve permitir sua utilização em servidores Windows Server 2008 e superiores e Linux RedHat 5 ou superiores;	
4- Ser totalmente compatível com Exchange 2010, 2013 e Office 365 ou versões superiores;	
5 - Ser aderente às normas do Comitê Gestor da ICP-Brasil;	
6- Deve garantir a autenticidade do site e oferecer um canal seguro de comunicação com criptografia de dados do protocolo SSL;	
7- Ser do tipo A1, ou seja, armazenado no equipamento servidor;	
8- Compatibilidade com os principais navegadores de internet.	
Necessidade 3: Certificados digitais para equipamentos servidores do tipo SSL Múltiplos Domínios: Prestação de serviço de emissão e validação de certificados digitais para equipamentos servidores do tipo SSL Múltiplos Domínios, com validade mínima de 01 (um) ano. A presente contratação irá contribui com o plano de infraestrutura do TJERJ. A presente contratação é essencial para assegurar o atendimento aos objetivos do PETI do TJERJ, com foco especial em: • R1 – Manter a infraestrutura de TI segura, apropriada e otimizada.	
Funcionalidade	**Ator Envolvido**
1 – Emitido por autoridade certificadora credenciada pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil);	Contratada DGTEC-DISER
2 – Possuir validade mínima de 01 (um) ano;	

3 – Deve permitir sua utilização em servidores Windows Server 2008 e superiores e Linux RedHat 5 ou superiores;	
4 – Ser aderente às normas do Comitê Gestor da ICP-Brasil;	
5- Deve garantir a autenticidade do site e oferecer um canal seguro de comunicação com criptografia de dados do protocolo SSL;	
6- Ser do tipo A1, ou seja, armazenado no equipamento servidor;	
7- Ser totalmente compatível com Exchange 2010, 2013 e Office365 ou versões superiores;	
8- Proteger, no mínimo, 5 endereços/domínios em um único certificado;	
9- Compatibilidade com os principais navegadores de internet;	
10- Compatibilidade com servidores web que suportam o protocolo SSL/TSL.	

Necessidade 4: Certificados digitais para pessoa jurídica do tipo A1:
Prestação de serviços de emissão e renovação de certificados digitais para pessoa jurídica do tipo A1, com validade mínima de 01 (um) ano.
A presente contratação é essencial para assegurar o atendimento aos objetivos do PETI do TJERJ, com foco especial em:

- P1 - Garantir a integridade e disponibilidade de todos os serviços de TI do Poder Judiciário.

Funcionalidade	Ator Envolvido
1 - Emitido por autoridade certificadora credenciada pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil);	Contratada TJERJ
2 - Possuir validade mínima de 01 (um) ano;	
3 - Ser aderente às normas do Comitê Gestor da ICP-Brasil;	
4 - O Tribunal indicará seu(s) representante(s) legal(is) para vinculação do(s) certificado(s) digital(is).	

Necessidade 5:
Prestação de serviço especializado de AR (Autoridade de Registro) para emissão e validação de certificados em local próprio da Contratada, com capacidade de atendimento dentro de cada uma das cidades sedes que compõem os NURs, distribuídos pela capital e interior do Rio de Janeiro.
A presente contratação é essencial para assegurar o atendimento aos objetivos do PETI do TJERJ, com foco especial em:

- CP1 - Contribuir com soluções de TI eficazes para agilizar os procedimentos administrativos e jurisdicionais;
- P1 - Garantir a integridade e disponibilidade de todos os serviços de TI do Poder Judiciário;
- P5 - Aprimorar a comunicação com públicos externos e internos;
- P6 - Promover iniciativas de segurança da informação.

Funcionalidade	Ator Envolvido
1 - A Contratada deverá possuir capacidade de atendimento para emissão de certificados com entrega de dispositivo de armazenamento nas cidades sedes dos NURs (Rio de Janeiro, Niterói, Petrópolis, Duque de Caxias, Volta Redonda, Campos dos Goytacazes, Vassouras, Itaguaí, Nova Friburgo, Itaperuna, Cabo Frio), em até 30 (trinta)	Contratada TJERJ (Magistrados, Servidores e Equipamentos)

dias, após assinatura do contrato, conforme quadro de endereço constante no Anexo II, com no máximo 10 km de distância entre a Autoridade Registro (AR) e a sede do Fórum da respectiva cidade;	
2 - Os recursos necessários (instalações, materiais, equipamentos, humanos, entre outros) para emissão de certificados deverão ser providos pela Contratada, sem ônus para o Contratante;	
3 - A empresa contratada deverá atender às solicitações de agendamentos com base nas publicações do TJERJ relativas à utilização dos certificados digitais;	
4 - Para a emissão inicial dos certificados, a Autoridade de Registro (AR) da Contratada deverá operar com Agentes de Registro que tenham capacidade de realizar todo o ciclo de emissão do certificado, com a entrega imediata ao usuário dispositivo de mídia criptografada, em local próprio da Contratada;	
5 - A Contratada deverá ser capaz de iniciar os serviços de emissão de certificados com entrega dos dispositivos em até 30 (trinta) dias corridos após assinatura do contrato, emissão do memorando de início pelo fiscal do contrato e solicitação formal do TJERJ, que poderá ser feita por e-mail ou qualquer outro meio de comunicação formal ao representante da Contratada;	
6 - A Contratada deverá ser capaz de fornecer alternativa de emissão e validação de certificados A3, no formato “on-line”, não presencial, feita a distância, através de serviço WEB, principalmente para casos emergenciais;	
7 - A Contratada deverá disponibilizar um canal de atendimento gratuito de serviço WEB para agendamento, o qual deverá estar disponível de segunda a sexta-feira no horário compreendido entre as 09 às 17 horas, no mínimo, sem custos adicionais para o Contratante;	
8 - Qualquer despesa decorrente do suporte técnico realizado durante o período de garantia do produto será de responsabilidade da contratada, não podendo haver qualquer limitação para o número de solicitações de suporte técnico;	
9 - O suporte técnico deverá ser prestado no regime 8x5 (oito horas por dia, de segunda a sexta feira) para resolução dos problemas registrados. O atendimento será efetuado em no máximo 48 horas após a solicitação;	
10- A conclusão do atendimento técnico gerado por essa ordem de serviço deverá ser reportada ao Fiscal Técnico do Contrato, que deverá comunicar à Contratada a autorização de substituição do certificado digital;	
Necessidade 6: Dispositivo de mídia criptografada para armazenamento do certificado tipo A3. A presente contratação é essencial para assegurar o atendimento aos objetivos do PETI do TJERJ, com foco especial em:	

- CP1 - Contribuir com soluções de TI eficazes para agilizar os procedimentos administrativos e jurisdicionais;
- CP3 - Disponibilizar informações para tomada de decisão gerencial, administrativa e gerencial;
- P1 - Garantir a integridade e disponibilidade de todos os serviços de TI do Poder Judiciário;
- P6 - Promover iniciativas de segurança da informação.

Funcionalidade	Ator Envolvido
1 - Deverá ser capaz de armazenar certificados, chaves e cadeias de certificados aderentes às normas do Comitê Gestor da ICP-Brasil;	Contratada TJERJ
2 - Deverá estar homologado pelo Instituto Nacional de Tecnologia da Informação – ITI;	
3 - Totalmente compatível com as especificações do certificado digital do tipo A3;	
4 - Possuir conector USB (Universal Serial Bus) tipo A versão 2.0 (ou superior compatível com 2.0);	
5 - Permitir conexão direta na porta USB, sem necessidade de interface intermediária (equipamento externo) para leitura;	
6 - Seguir as regras estabelecidas para o nível 3 (ou superior) de segurança do padrão FIPS 140-2 e também ser aderente às demais normas do Comitê Gestor da ICP Brasil;	
7 - Possuir capacidade de armazenamento de certificados e chaves privadas de, no mínimo, 72 Kbytes;	
8 - Ter suporte à tecnologia de chaves pública/privada (PKI), com geração onboard do par de chaves RSA de, no mínimo, 2048 bits;	
9 - Possuir carcaça resistente à água e à violação;	
10 - Fornecer driver e programa de gerenciamento para o sistema operacional Linux (kernel 2.6 ou versões superiores);	
11 - Fornecer driver e programa de gerenciamento para o sistema operacional Microsoft Windows 7 Professional x64 ou versões superiores;	
12 - Deve permitir sua utilização sem a necessidade de instalação de software cliente em equipamentos com o sistema operacional Windows 7 Professional x64 ou versões superiores;	
13 - Fornecer driver e programa de gerenciamento para o sistema operacional Mac OS X ou versões superiores;	
14 - Permitir a exportação automática de certificados armazenados no dispositivo para o Certificate Store do ambiente Microsoft Windows 7 Professional x64 ou versões superiores;	
15 - Ter compatibilidade com sistemas operacionais Windows (7 Professional x64 ou superiores) e Linux (kernel 2.6 ou superiores);	
16 - Possuir middleware para Windows (7 Professional x64 e superiores) e Linux (kernel 2.6 ou superiores);	
17 - Possuir CSP - Cryptographic Services Provider para Windows (Windows XX e versões superiores) e em conformidade com o padrão da CryptoAPI 2.0, da	

Microsoft (Windows 7 Professional x64 ou versões superiores);	
18 - Possuir biblioteca de objetos compartilhados em ambiente linux (.so) e dynamic-link library (.dll) em ambiente Windows que implemente, em sua completude, o padrão PKCS#11 v2.0 ou mais recente;	
19 - Disponibilizar driver para os ambientes Windows e Linux de forma que os frameworks Java JCA e Java JCE se comuniquem em perfeita harmonia com a biblioteca PKCS#11 nativa do token, de tal forma que aplicações em Java possam utilizar qualquer das funcionalidades existentes no padrão PKCS#11 por meio dos frameworks Java JCA e Java JCE;	
20 - Permitir criação de senha de acesso ao dispositivo de, no mínimo, 8 (oito) caracteres;	
21 - Permitir criação de senhas com caracteres alfanuméricos;	
22 - Permitir geração de chaves, protegidas por PINs (Personal Identification Number), compostos por caracteres alfanuméricos;	
23 - Permitir gravação de chaves privadas e certificados digitais que utilizam a versão 3 do padrão ITU-T X.509 de acordo com o perfil estabelecido na RFC 2459;	
24 - Utilizar algoritmo simétrico 3-DES ou AES com chaves de, no mínimo, 128 bits, para cifrar as chaves privadas armazenadas;	
25 - Utilizar algoritmo simétrico 3-DES com três chaves distintas (k1, k2 e k3);	
26 - Possuir o algoritmo simétrico AES, sua chave gerada por derivação, a partir de um código de acesso escolhido pelo titular do repositório;	
27 - Permitir personalização eletrônica através de parâmetro identificador interno (label);	
28 - Implementar mecanismo de autenticação tipo challenge-response;	
29 - Armazenar chaves privadas em repositório de dados próprio, controlado pela solução;	
30 - Possuir ativação de funções que utilizem as chaves privadas, que somente possam ser realizadas após autenticação da identidade do titular do dispositivo;	
31 - Suportar, pelo menos, os seguintes navegadores: Microsoft Internet Explorer (versão 9 e superiores), Firefox (versão 31.7 ESR ou superiores) e Chrome (versão 4.0 e superiores);	
32 - Permitir inicialização e reinicialização do dispositivo mediante a utilização de PUK (Pin Unlock Key);	
33 - Implementar troca obrigatória da senha padrão no primeiro acesso;	
34 - Forçar a troca da senha padrão no primeiro acesso;	
35 - Bloquear o dispositivo, depois de excedida a quantidade de tentativas de autenticação com códigos inválidos, conforme parâmetro quantitativo	

definido no momento da formação do dispositivo, que deverá vir preenchido, por padrão, com o valor de 15 (quinze) tentativas, podendo ser alterado;	
36 - Avisar o titular do dispositivo, a cada vez que uma função for ativada, utilizando a sua chave privada. Nesse caso, deverá haver autenticação para liberar a utilização pretendida;	
37 - Bloquear a exportação da chave privada, realizando as transações apenas dentro do dispositivo;	
38 - Permitir a exportação de certificados armazenados no dispositivo;	
39 - Permitir a importação de certificados em formato PKCS#12 para área de armazenamento do dispositivo;	
40 - Permitir a importação de certificados em formato PKCS#7 para área de armazenamento do dispositivo, de acordo com a RFC 2315;	
41 - Possuir indicador luminoso de estado de uso do dispositivo, chassi em plástico resistente E capa protetora para o conector USB;	
42 - Permitir a visualização de certificados armazenados no dispositivo;	
43 - Permitir a remoção de chaves e outros dados contidos no dispositivo após autenticação do titular;	
44 - Apagamento de chaves e outros dados contidos no dispositivo, sendo exigida, para esse fim, a autenticação do titular do dispositivo;	
45 - Reutilização de dispositivos bloqueados, por meio de remoção total dos dados armazenados e geração de nova senha de acesso;	
46 - O software de gerenciamento do dispositivo deverá estar no idioma Português do Brasil;	
47 - Caso o dispositivo apresente erro que comprometa o funcionamento do certificado ali armazenado, o titular do dispositivo deverá abrir uma ordem de serviço na Central de Atendimento da DGTEC;	
48 - A conclusão do atendimento técnico gerado pela ordem de serviço acima deverá ser reportada ao Fiscal Técnico do Contrato, que deverá comunicar à Contratada a autorização de substituição do token;	
49 - Comprovado o erro ou defeito e havendo necessidade de substituição do token a empresa terá um prazo de até 2 (dois) dias úteis para substituição, contados da data da comunicação feita pela DGTEC ao representante da Contratada, que poderá ser através de e-mail ou outra forma de comunicação, sem ônus para o Contratante;	
50 - Será de responsabilidade da empresa qualquer atualização do dispositivo definidas pelo Instituto Nacional de Tecnologia da Informação (ITI), Comitê-Gestor da ICP-Brasil ou outros órgãos/entidades que venham a ser criados ou a atuar em sua regulamentação.	
51 - Garantia técnica mínima de 3 (três) anos, contado a partir da entrega definitiva de cada token;	
Necessidade 7: Certificados digitais para equipamentos servidores do tipo SSL Site Seguro:	

Prestação de serviço de emissão e validação de certificados digitais para equipamentos servidores do tipo SSL Site Seguro, com validade mínima de 01 (um) ano, no padrão internacional OV (Organization Validation).
A presente contratação irá contribuir com o plano de infraestrutura do TJERJ.
A presente contratação é essencial para assegurar o atendimento aos objetivos do PETI do TJERJ, com foco especial em:

- R1 – Manter a infraestrutura de TI segura, apropriada e otimizada.

Funcionalidade	Ator Envolvido
1 - Emitido por autoridade certificadora credenciada pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil);	Contratada DGTEC-DISER
2 - Possuir validade mínima de 01 (um) ano;	
3 - Deve permitir sua utilização em servidores Windows Server 2008 e superiores e Linux RedHat 5 ou superiores;	
4- Ser totalmente compatível com Exchange 2010, 2013 e Office365 ou versões superiores;	
5 - Conter o campo de Transparência de Certificado - CT (Certificate Transparent) obrigatoriamente preenchido;	
6- Deve garantir a autenticidade do site e oferecer um canal seguro de comunicação com criptografia de dados do protocolo SSL;	
7- Ser do tipo A1, ou seja, armazenado no equipamento servidor;	
8- Compatibilidade com os principais navegadores de internet.	

Necessidade 8: Certificados digitais para equipamentos servidores do tipo SSL Múltiplos Domínios:
Prestação de serviço de emissão e validação de certificados digitais para equipamentos servidores do tipo SSL Múltiplos Domínios, com validade mínima de 01 (um) ano, no padrão internacional OV (Organization Validation).
A presente contratação irá contribui com o plano de infraestrutura do TJERJ.
A presente contratação é essencial para assegurar o atendimento aos objetivos do PETI do TJERJ, com foco especial em:

- R1 – Manter a infraestrutura de TI segura, apropriada e otimizada.

Funcionalidade	Ator Envolvido
1 – Emitido por autoridade certificadora credenciada pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil);	Contratada DGTEC-DISER
2 – Possuir validade mínima de 01 (um) ano;	
3 – Deve permitir sua utilização em servidores Windows Server 2008 e superiores e Linux RedHat 5 ou superiores;	
4 – Conter o campo de Transparência de Certificado - CT (Certificate Transparent) obrigatoriamente preenchido;	
5- Deve garantir a autenticidade do site e oferecer um canal seguro de comunicação com criptografia de dados do protocolo SSL;	
6- Ser do tipo A1, ou seja, armazenado no equipamento servidor;	
7- Ser totalmente compatível com Exchange 2010, 2013 e Office365 ou versões superiores;	
8- Proteger, no mínimo, 5 endereços/domínios em um único certificado;	

9- Compatibilidade com os principais navegadores de internet;	
10- Compatibilidade com servidores web que suportam o protocolo SSL/TSL.	
2.2– Demais Requisitos	
Tipo 1: Capacitação	**Requisito:** • Será de responsabilidade da Contratada manter pessoal capacitado para o serviço de emissão de certificados e entrega dos dispositivos em suas instalações durante todo o período contratual; • Ficará a cargo da Contratada qualquer treinamento necessário à execução da presente contratação.
Tipo 2: Legais	**Requisito:** • Respeitar, durante todo o período contratual, a legislação vinculada as normas e regras definidas pelo Instituto Nacional de Tecnologia da Informação (ITI), Comitê-Gestor da ICP-Brasil ou outros órgãos/entidades que venham a ser criados ou a atuar em sua regulamentação; • Cumprir e fazer cumprir por seus profissionais as normas e os regulamentos internos do Contratante, sem quaisquer ônus para o Contratante; • Atender, em suas atividades, à legislação federal, estadual, municipal, normas e regulamentos em vigor.
Tipo 3: Certificados e Dispositivos	**Requisito:** • Caso o certificado e/ou dispositivo apresente erro ou defeito ou sejam detectados problemas na realização dos serviços de emissão dos certificados ou fornecimento dos dispositivos, a empresa contratada deverá realizar a emissão do certificado ou a troca do dispositivo defeituoso por outro novo, de primeiro uso, com no mínimo, as mesmas características do objeto contratado, num prazo de até 2 (dois) dia úteis, contados da data da comunicação feita pela DGTEC ao representante da Contratada, através de e-mail, podendo ser aceita também outra forma de comunicação, sem ônus para o Contratante; • O suporte técnico deverá ser prestado no regime 8x5 (oito horas por dia, de segunda a sexta-feira) para resolução dos problemas registrados. O atendimento deverá ser efetuado com a resolução do problema em no máximo 2 (dois) dia úteis após a solicitação;
Tipo 4: Temporais	**Requisito:** • A execução dos serviços terá início a partir da assinatura do contrato e emissão do memorando de início, pelo fiscal do contrato;

	• A Contratada deverá ser capaz de iniciar os serviços em até 30 (trinta) dias corridos após a assinatura do contrato, emissão do memorando de início e solicitação formal do TJERJ, que poderá ser feita por e-mail ou outra forma de comunicação ao representante da Contratada; • Em até 48 horas após o recebimento do empenho, a empresa deverá apresentar-se ao órgão fiscalizador do contrato – Diretoria Geral de Tecnologia da Informação localizada à Praça XV de Novembro, nº 2 – Mezanino – Sala M05, Rio de Janeiro, para reunião de planejamento; • A emissão dos certificados com entrega de dispositivos deverá ser efetuada de segunda a sexta-feira, no período compreendido entre 09 às 17 horas, nas cidades sedes dos NURs, mediante agendamento, durante a vigência do contrato; • Solicitado o agendamento para emissão do certificado digital a empresa deverá agendar o serviço em até 2 (dois) dias úteis a partir da data da solicitação; • O prazo acima estabelecido poderá ser estendido a critério e conveniência do solicitante; • A Contratada deverá dispor de 3 (três) opções de data para agendamento do serviço de certificação digital, quando for solicitado; • Em casos de pedidos de urgências para emissão dos certificados, o período para emissão não poderá ultrapassar o prazo de 24 (vinte e quatro) horas a partir da solicitação.
Tipo 5 : Segurança	**Requisito:** • Respeitar os critérios de sigilo, aplicáveis aos dados, informações e às regras de negócios relacionados com a prestação do serviço contratado; • Todas as informações transmitidas pelo Contratante para a Contratada e aos seus funcionários são de caráter confidencial e não poderão ser transmitidas ou facilitadas a quem quer que seja, sem expressa autorização do Contratante.
Tipo 6 : Sociais, ambientais e culturais	**Requisito:** • Obedecer aos critérios de gestão ambiental estabelecido nas legislações, normas e regulamentos específicos ao serviço, visando a melhoria e o desempenho dos processos de trabalho quanto aos aspectos ambientais, sociais e econômicos; • Atender, em suas atividades, à legislação federal, estadual, municipal, normas e regulamentos em vigor;

	• As atividades desempenhadas pela Contratada devem ser conduzidas considerando a preservação, conservação e a recuperação do ecossistema, desenvolvendo suas ações de forma a valorizar o bem estar dos trabalhadores, promovendo a qualidade de vida.

3- LEVANTAMENTO DAS SOLUÇÕES EXISTENTES

Solução	Entidade	Valor
1 – XXXXXXX XXXXX XXXXX	XXXXX	R$ XXX.XXX,XX
Descrição: XXXXX.		
Fornecedor: XXXXXX.		
Solução	**Entidade**	**Valor**
2 – XXXXXX.	XXXXX	R$ X.XXX,XX
Descrição: XXXX.		
Fornecedor: XXXXXXXX .		

4- ANÁLISE DAS SOLUÇÕES E ALTERNATIVAS EXISTENTES

Requisito	Identificação da Solução existente	Sim	Não	Não se aplica
A solução encontra-se implantada em outro órgão ou entidade da Administração pública federal?	Certificados digitais e-CPF A3 para pessoa física padrão ICP-Brasil, certificados digitais e-CNPJ A3 padrão ICP-Brasil e voucher para certificado digital A1 SSL para servidor web.	x		
A solução está disponível no Portal do Software Público Brasileiro			x	
A solução é um software livre ou software público			x	
A solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões e-PING, e-MAG?		x		
A solução é aderente às regulamentações da ICP-Brasil?		x		
A solução é aderente às orientações, premissas e especificações técnicas e funcionais do – Moreq-Jus Brasil?		x		

5-JUSTIFICATIVA DA SOLUÇÃO ESCOLHIDA

5-1- Solução Escolhida

Descrição:

Contratação de empresa especializada na prestação de serviço de emissão e validação de certificados digitais com fornecimento de mídia criptográfica tipo token, em local próprio da Contratada, contendo os seguintes itens:

1. Certificados digitais para pessoa física padrão ICP-Brasil do tipo A3 a ser prestado por uma AC-JUS, com validade de 03 (três) anos, armazenados em dispositivos de mídias criptografadas, ou em HSM (Hardware Security Module).
2. Certificados digitais para equipamentos servidores do tipo SSL Site Seguro, com validade mínima de 01 (um) ano;
3. Certificados digitais para equipamentos servidores do tipo SSL Múltiplos Domínios, com validade mínima de 01 (um) ano.
4. Certificados digitais para pessoa jurídica do tipo A1, com validade mínima de 01 (um) ano;
5. Serviços especializados de AR (Autoridade de Registro) para emissão e validação de certificados em local próprio da Contratada, com capacidade de atendimento dentro de cada uma das cidades sedes que compõem os NURs, distribuídos pela capital e interior do Rio de Janeiro, e;
6. Dispositivo de mídia criptografada tipo token para armazenamento dos certificados tipo A3.

Bens e Serviços	Valor Proposto (Valor Média da Pesquisa – Pesquisa de Preços -2021)
7.150 (sete mil, cento e cinquenta) certificados digitais para pessoa física padrão ICP-Brasil do tipo A3 a ser prestado por uma AC-JUS, com validade de 03 (três) anos armazenados em mídias criptografadas tipo token, ou em HSM(Hardware Security Module);	R$ 1.669.548,83
16 (dezesseis) certificados digitais para equipamentos servidores do tipo SSL Site Seguro, com validade mínima de 01 (um) ano;	R$ 16.376,00
16 (dezesseis) certificados digitais para equipamentos servidores do tipo SSL Múltiplos Domínios, com validade mínima de 01 (um) ano;	R$ 28.721,41
8 (oito) certificados digitais para pessoa jurídica do tipo A1, com validade mínima de 01 (um) ano;	R$ 1.529,87
7.222 (sete mil, duzentos e vinte e dois) serviços especializados de AR (Autoridade de Registro) para emissão e validação de certificados em local próprio da Contratada;	R$ 914.786,67
6.000 (seis mil) dispositivos de mídia criptografada tipo token para certificado tipo A3.	R$ 429.990,00
16 (dezesseis) certificados digitais para equipamentos servidores do tipo SSL Site Seguro, com validade mínima de 01 (um) ano, no padrão internacional OV (Organization Validation).	R$ 14.394,67
16 (dezesseis) certificados digitais para equipamentos servidores do tipo SSL Múltiplos Domínios, com validade mínima de 01 (um) ano, no padrão internacional OV (Organization Validation);	R$ 27.141,33
TOTAL	R$ 3.102.488,78

Justificativa:

O certificado digital é um documento eletrônico que identifica pessoas, equipamentos e empresas no mundo digital, provando sua identidade e permitindo acessar serviços online com a garantia de autenticidade, integridade e não repúdio.
A autenticidade garante a autoria de um documento, o acesso legítimo a um sistema, entre outros. A integridade garante que as informações não foram alteradas sem a devida autorização. O não repúdio impede que o autor do documento ou da autenticação do sistema conteste a sua validade negando sua autoria.
Neste sentido justifica-se a presente prorrogação para que a Diretoria Geral de Tecnologia da Informação possa dar continuidade aos serviços de Certificação Digital para prover este Tribunal de Justiça com mecanismos que garantam a autenticidade, confidencialidade e integridade das informações eletrônicas.
A implantação do processo eletrônico no TJERJ segue as diretrizes determinadas pelo CNJ, oferecendo maior celeridade à prestação jurisdicional, com mais transparência, acessibilidade, publicidade e economicidade ao erário, encampando novas tecnologias e procedimentos.
Essa virtualização suprime o meio físico e necessita de um nível maior de segurança, tanto de infraestrutura e sistemas informatizados, bem como da garantia da autenticidade dos arquivos eletrônicos que compõe o processo.
A autenticidade dos documentos gerados pelos sistemas que fazem parte da modernização do judiciário é comprovada através dos certificados digitais que mostram através de dados como nome e número público exclusivo denominado de chave pública, quem somos para pessoas e sistemas de informação.
Frise-se ainda que os certificados devem possuir obrigatoriamente prazo de validade e precisam ser renovados periodicamente, sendo classificados como do tipo A3 para pessoa física, utilizados por

Magistrados e Servidores, tipo A1 para pessoa jurídica, tipo SSL Site Seguro e tipo SSL Múltiplos Domínios para equipamentos servidores.
Os certificados são gerados e armazenados em dispositivo tipo tokens de forma segura em atendimento às normas ICP-Brasil (Infraestrutura de Chaves Públicas Brasileiras), criada pela Medida Provisória número 2.200-2.
Os tokens devem atender padrões rigorosos de fabricação e qualidade FIPS 140-2, pois são responsáveis por guardar informações de caráter sigiloso.
Atualmente os certificados digitais são fornecidos através do Contrato n° 003/0135/2016, tendo sido aditivado pelo termo nº 003/428/2018, que será finalizado em 20/03/2020.

6-BENEFÍCIOS ESPERADOS

Benefício
1 – Eficiência operacional do sistema processual eletrônico garantindo maior agilidade e facilidade de acesso no trâmite de processos;
2 – Ampliação do processamento virtual;
3 – Melhor comunicação do TJERJ com demais atores do processo e com outros órgãos do poder público;
4 – Permanente integração dos sistemas corporativos;
5 – Ampliação dos meios nos quais o judiciário poderá ser provocado;
6 – Alinhamento e integração com os sistemas entre os órgãos do Poder Judiciário.

7-AVALIAÇÃO DAS NECESSIDADES DE ADEQUAÇÃO PARA EXECUÇÃO CONTRATUAL

Tipo de Necessidade	Descrição
1 – Não se aplica	Não se aplica

EQUIPE DE FISCALIZAÇÃO DA CONTRATAÇÃO

Fiscal Demandante	Fiscal Técnico	Fiscal Administrativo
Humberto Vieira da Cruz Matrícula 04101004-2	Braulio Bezerra de Menezes Souza Matrícula 17/11841335	Sérgio Mattos Magalhães da Cunha Matrícula 01/27.426

Rio de Janeiro, _____de _____ de 20_____