DELIBERAÇÃO

PREGÃO ELETRÔNICO Nº 90024/2026

Trata-se de questionamentos encaminhados via e-mail, no uso do direito previsto na legislação vigente e nos termos do Edital, por empresa interessada em participar do **Pregão Eletrônico nº 90024/2026**, que tem por objeto a Contratação da prestação dos serviços de mensagens eletrônicas registradas com geração de evidências eletrônicas auditáveis de envio, entrega, não entrega, abertura, autoria e demais eventos associados à comunicação eletrônica.

2. Os questionamentos preenchem os requisitos legais, pois foram apresentados por meio eletrônico e TEMPESTIVAMENTE.

3. Com subsídios da Gestão das Contratações de TI - GCSTI, segue abaixo, o questionamento apresentado com a devida resposta.

Questionamento 01 – Item 6.9 – Retenção de cópia da mensagem enviada. É nosso entendimento que, após a confirmação da entrega da mensagem, a ferramenta a ser utilizada NÃO PODE reter cópia do conteúdo da mensagem ou de seus anexos, em qualquer formato, mídia, sistema, banco de dados, armazenamento temporário, backup ou qualquer outro ambiente sob controle da CONTRATADA ou de seus subcontratados. Está correto nosso entendimento?
Resposta: O conteúdo das mensagens não deve ser mantido em nenhum componente do ambiente da contratada, nos termos previstos no Edital.

Questionamento 02 – Item 6.9 – Retenção em ambientes de backup. É nosso entendimento que a vedação à retenção prevista no item 6.9 também se aplica às cópias de backup, snapshots, réplicas, caches, mecanismos de disaster recovery e demais cópias técnicas, não sendo permitida a manutenção do conteúdo da mensagem nesses ambientes após a confirmação da entrega. Está correto nosso entendimento?
Resposta: O conteúdo das mensagens não deve ser mantido em nenhum componente do ambiente da contratada, nos termos previstos no Edital.

Questionamento 03 – Item 6.9 – Retenção por terceiros. Considerando que o item 8.2 permite a subcontratação de serviços acessórios de infraestrutura tecnológica, hospedagem em nuvem e certificação, é nosso entendimento que a proibição de retenção do conteúdo das mensagens também se aplica integralmente aos ambientes de terceiros, provedores de nuvem, data centers e demais subcontratados, não podendo esses terceiros manter cópias do conteúdo das mensagens após a confirmação da entrega. Está correto nosso entendimento?
Resposta: O conteúdo das mensagens não deve ser mantido em nenhum componente do ambiente da contratada, nos termos previstos no Edital.

Questionamento 04 – Item 6.9 – Diferenciação entre conteúdo e evidências. É nosso entendimento que a obrigação de guarda prevista no item 5.1, referente aos registros e hashes de validação das evidências por cinco anos, não autoriza a guarda do conteúdo das mensagens ou de seus anexos, devendo a retenção limitar-se aos registros, metadados, hashes e demais evidências necessárias à comprovação e validade jurídica da comunicação ocorrida. Está correto nosso entendimento?
Resposta: O conteúdo das mensagens não deve ser mantido em nenhum componente do ambiente da contratada, nos termos previstos no Edital.

Questionamento 05 – Item 6.9 – Ausência de armazenamento para finalidade comercial. É nosso entendimento que o conteúdo das mensagens transmitidas pelo STF não poderá ser utilizado, armazenado ou processado para qualquer finalidade distinta da execução técnica da transmissão e geração das respectivas evidências, incluindo análise comercial, desenvolvimento de produtos, treinamento de modelos, mineração de dados, publicidade ou qualquer outra finalidade secundária. Está correto nosso entendimento?
Resposta: Está correto o entendimento.

Questionamento 06 – Item 6.9 – Acesso ao conteúdo. É nosso entendimento que, em momento algum, mas especialmente após a confirmação da entrega, nenhum administrador, empregado, preposto, subcontratado ou terceiro vinculado à CONTRATADA poderá acessar o conteúdo da mensagem ou seus anexos, uma vez que estes não deverão permanecer armazenados na infraestrutura da solução. Está correto nosso entendimento?
Resposta: O conteúdo das mensagens não deve ser mantido em nenhum componente do ambiente da contratada, nos termos previstos no Edital.

Questionamento 07 – Item 6.9 – Eliminação efetiva do conteúdo. É nosso entendimento que, após a confirmação da entrega, a solução deverá realizar a eliminação efetiva do conteúdo da mensagem e dos anexos de seus ambientes de processamento e armazenamento temporário, inclusive das áreas temporárias utilizadas durante a transmissão, mantendo exclusivamente os registros e evidências previstos no edital. Está correto nosso entendimento?
Resposta: O conteúdo das mensagens não deve ser mantido em nenhum componente do ambiente da contratada, nos termos previstos no Edital.

Questionamento 08 – Item 6.9 – Confirmação da eliminação. É nosso entendimento que a CONTRATADA deverá possuir mecanismos técnicos capazes de comprovar que o conteúdo que tenha sido armazenado temporariamente (conteúdo da mensagem e seus anexos) foram efetivamente eliminados após a confirmação da entrega, inclusive quando houver mecanismos de redundância, replicação ou backup. Está correto nosso entendimento?
Resposta: O conteúdo das mensagens não deve ser mantido em nenhum componente do ambiente da contratada, nos termos previstos no Edital.

Questionamento 09 – Item 6.12.1 – Criptografia em trânsito. Considerando a exigência de TLS 1.2 ou superior, é nosso entendimento que todo o tráfego contendo conteúdo das mensagens e respectivos anexos, desde a origem até o destino, deverá utilizar comunicação criptografada, não sendo admitida transmissão em texto claro em qualquer etapa da comunicação. Está correto nosso entendimento?
Resposta: O conteúdo trafegado deverá possuir criptografia em trânsito e em repouso, conforme termos do Edital.

Questionamento 10 – Item 6.12.1 – Criptografia em repouso. Considerando que o edital exige AES-256 para dados em repouso, é nosso entendimento que qualquer conteúdo de mensagem eventualmente existente durante o processamento temporário da comunicação também deverá estar protegido por criptografia, não sendo permitida a existência de conteúdo armazenado em texto claro. Está correto nosso entendimento?
Resposta: O conteúdo trafegado deverá possuir criptografia em trânsito e em repouso, conforme termos do Edital.

Questionamento 11 – Item 6.12.1 – Chaves criptográficas. É nosso entendimento que a utilização de AES-256 deverá contemplar mecanismos adequados de gerenciamento, proteção, rotação e controle de acesso às chaves criptográficas, impedindo que pessoas não autorizadas tenham acesso às chaves utilizadas para proteção dos dados. Está correto nosso entendimento?
Resposta: O conteúdo trafegado deverá possuir criptografia em trânsito e em repouso, conforme termos do Edital.

Questionamento 12 – Item 6.12.2 – MFA administrativo. Considerando a exigência de autenticação multifator para gestão e controle dos acessos administrativos, é nosso entendimento que 100% das contas com privilégios administrativos sobre a plataforma, infraestrutura, bancos de dados e

componentes que processem dados do STF deverão utilizar MFA. Está correto nosso entendimento?
Resposta: Gestão e controle de acessos administrativos deverão possuir Autenticação Multifator (MFA), conforme termos do Edital.

Questionamento 13 – Item 6.12.2 – Contas privilegiadas. É nosso entendimento que não deverá existir conta administrativa compartilhada ou genérica que permita acesso não individualizado aos ambientes que processam informações do STF, devendo os acessos administrativos ser individualmente identificáveis, rastreáveis e auditáveis. Está correto nosso entendimento?
Resposta: O item citado trata apenas de Autenticação Multifator (MFA) para gestão e controle de acessos administrativos.

Questionamento 14 – Item 6.12.3 – Logs imutáveis. Considerando a exigência de armazenamento e logs de auditoria imutáveis, é nosso entendimento que os registros deverão possuir mecanismos técnicos que impeçam sua alteração ou exclusão por usuários administrativos, preservando sua integridade para fins de auditoria. Está correto nosso entendimento?
Resposta: Os logs de auditoria armazenados devem ser imutáveis, conforme termos do Edital.

Questionamento 15 – Item 6.12.3 – Auditoria dos acessos. É nosso entendimento que os logs deverão registrar, no mínimo, os acessos administrativos à plataforma e aos ambientes que processam informações do STF, incluindo identificação do usuário, data, horário, origem do acesso e operação realizada. Está correto nosso entendimento?
Resposta: Os logs de auditoria armazenados deverão contemplar mecanismos que preservem a integridade dos registros de auditoria e permitam a rastreabilidade dos eventos necessários à comprovação das operações realizadas, conforme termos do Edital.

Questionamento 16 – Item 6.12.4 – Tratamento de dados pessoais. Considerando o item 6.12.4, é nosso entendimento que os dados pessoais tratados pela solução deverão ser utilizados exclusivamente para a execução do objeto contratual, não podendo ser utilizados para finalidades próprias da CONTRATADA ou de terceiros. Está correto nosso entendimento?
Resposta: Sim, conforme termos do Edital.

Questionamento 17 – Item 6.12.4 – Subcontratados. É nosso entendimento que as mesmas obrigações de segurança, confidencialidade, proteção de dados e não retenção aplicáveis à CONTRATADA deverão ser integralmente observadas por seus subcontratados e provedores de infraestrutura, hospedagem, nuvem e certificação. Está correto nosso entendimento?
Resposta: Todas as exigências do Edital se aplicam à solução como um todo.

Questionamento 18 – Item 6.10 – Carimbo de tempo. Considerando a exigência de registro temporal auditável, é nosso entendimento que os timestamps deverão ser gerados de forma tecnicamente confiável, possuir integridade verificável e estar sincronizados com fonte oficial de tempo reconhecida, conforme previsto no edital. Está correto nosso entendimento?
Resposta: Sim, desde que a fonte apresentada assegure sincronização confiável com o UTC e rastreabilidade a padrões oficiais de referência temporal internacional, o que possibilita a comprovação da integridade e auditabilidade dos registros temporais gerados pela solução.

Questionamento 19 – Item 6.13.3 – Eventos da comunicação. É nosso entendimento que o Recibo/Comprovante deverá permitir a identificação individual e auditável, quando aplicável, dos eventos de envio, entrega no servidor de destino e abertura da mensagem, incluindo os respectivos timestamps. Está correto nosso entendimento?
Resposta: O conteúdo do Recibo/Comprovante deve atender aos requisitos do item 6.13 e seus subitens.

Questionamento 20 – Item 6.13.4 – Endereço IP e trilha de auditoria. É nosso entendimento que o Recibo/Comprovante deverá registrar os endereços IP e demais informações necessárias à reconstrução da trilha de auditoria da comunicação, permitindo verificar tecnicamente a origem e os eventos relacionados à transmissão. Está correto nosso entendimento?
Resposta: O conteúdo do Recibo/Comprovante deve atender aos requisitos do item 6.13 e seus subitens.

Questionamento 21 – Item 6.13.5 – Hash do conteúdo. Considerando a exigência de resumo criptográfico do conteúdo e dos anexos, é nosso entendimento que o hash deverá permitir comprovar posteriormente que o conteúdo apresentado como evidência corresponde exatamente ao conteúdo originalmente transmitido, sem necessidade de que a CONTRATADA mantenha qualquer cópia do conteúdo da mensagem. Está correto nosso entendimento?
Resposta: Sim, conforme finalidade de hashs criptográficos e termos do Edital.

Questionamento 22 – Item 6.13.5 – Independência entre hash e conteúdo. É nosso entendimento que a tecnologia proposta deve implementar processos que permitam que a geração e a manutenção do hash seja suficiente para preservar a evidência de integridade da mensagem, sem que isso implique a retenção do conteúdo da mensagem ou de seus anexos pela CONTRATADA. Deve ser garantida também forma automática de verificação e validação dos aspectos de IMUTABILIDADE dos hashs associados ao evento de transmissão, recebimento e abertura da mensagem e seus anexos. Está correto nosso entendimento?
Resposta: Sim, conforme finalidade de hashs criptográficos e termos do Edital.

Questionamento 23 – Item 6.13.6 – Validação independente. Considerando a exigência de mecanismo público ou independente para validação externa da autenticidade da evidência, é nosso entendimento que terceiros deverão conseguir verificar a autenticidade e integridade da evidência apresentada pelo STF sem depender da existência de uma cópia do conteúdo da mensagem armazenada pela CONTRATADA. Está correto nosso entendimento?
Resposta: O mecanismo público/independente deverá permitir validação externa da autenticidade da evidência, conforme termos do Edital.

Questionamento 24 – Item 5.1 – Guarda das evidências por cinco anos. É nosso entendimento que a obrigação de guarda por cinco anos prevista no item 5.1 refere-se exclusivamente aos registros, hashes e evidências digitais gerados pela solução, bem como o CONTEÚDO originalmente transmitido, sendo que o conteúdo das mensagens e respectivos anexos NÃO DEVE ser amazenado em ambiente de terceiros ou acessável por pessoas não autorizadas.. Está correto nosso entendimento?
Resposta: A guarda dos registros e hashes de validação das evidências visa manter e garantir sua integridade, conforme termos do Edital.

Questionamento 25 – Item 5.1 – Conteúdo da mensagem versus evidência. É nosso entendimento que o STF manterá a posse do Recibo Registrado que contém as informações relativas à todo o processo de transmissão e recebimento das mensagens bem como o conteúdo original das mensagens e anexos transmitidos, enquanto a CONTRATADA deverá manter somente as evidências necessárias à comprovação da comunicação, conforme especificado no edital. Está correto nosso entendimento?
Resposta: A contratada obriga-se a manter e garantir a integridade dos registros e hashes de validação das evidências pelo prazo mínimo de 5 (cinco) anos a contar de sua geração, conforme termos do Edital.

Questionamento 26 – Item 5.1 – Exportação do acervo. É nosso entendimento que, ao encerramento do contrato, a exportação integral prevista no item 5.1 deverá contemplar todos os registros, hashes, timestamps, metadados e demais evidências, em formato estruturado e interoperável, sem exigir a transferência de cópias do conteúdo das mensagens os quais não devem – em tempo algum - permanecer armazenados pela CONTRATADA ou terceiros. Está correto nosso entendimento?
Resposta: A contratada deve disponibilizar mecanismo de exportação integral e interoperável de todo o acervo de evidências ao STF ao encerramento do contrato, conforme termos do Edital.

Questionamento 27 – Item 5.1 – Portabilidade das evidências. É nosso entendimento que o formato de exportação das evidências deverá permitir que o STF possa posteriormente verificar sua integridade e autenticidade sem depender exclusivamente da continuidade do serviço ou da infraestrutura da

CONTRATADA. Está correto nosso entendimento?
Resposta: A contratada deve disponibilizar mecanismo de exportação integral e interoperável de todo o acervo de evidências ao STF ao encerramento do contrato, conforme termos do Edital.

Questionamento 28 – Item 2.1 – Guarda de registros e hashes. O item 2.1 estabelece a necessidade de manutenção e guarda dos registros e resumos criptográficos de integridade (hashes) e demais evidências digitais produzidas pelo sistema. É nosso entendimento que essa obrigação não deve ser interpretada como autorização para armazenamento do conteúdo das mensagens ou de seus anexos. Está correto nosso entendimento?
Resposta: Está correto o entendimento, conforme termos do Edital que proíbem o armazenamento de mensagens e seus conteúdos.

Questionamento 29 – Item 2.1 – Cópias técnicas. É nosso entendimento que a expressão "demais evidências digitais produzidas pelo sistema" não inclui cópias integrais ou parciais do conteúdo das mensagens, anexos, arquivos temporários ou qualquer outra forma de armazenamento que permita reconstruir o conteúdo original da comunicação. Está correto nosso entendimento?
Resposta: Está correto o entendimento, conforme termos do Edital que proíbem o armazenamento de mensagens e seus conteúdos.

Questionamento 30 – Item 8.2 – Hospedagem em nuvem. Considerando a possibilidade de subcontratação de hospedagem em nuvem, é nosso entendimento que a utilização de infraestrutura de terceiros não altera ou flexibiliza nenhum dos requisitos de segurança e não retenção estabelecidos no edital, permanecendo a CONTRATADA integralmente responsável pelo seu cumprimento. Está correto nosso entendimento?
Resposta: Está correto o entendimento, pois a responsabilidade integral e irrestrita é da CONTRATADA perante o STF, conforme termos do Edital.

Questionamento 31 – Item 8.2 – Localização dos dados. É nosso entendimento que, caso sejam utilizados serviços de computação em nuvem ou infraestrutura de terceiros, a CONTRATADA deverá informar ao STF onde os dados e evidências são processados e armazenados, incluindo os respectivos ambientes e regiões geográficas, especialmente considerando a natureza das informações tratadas. As práticas e ações relativas ao TRATAMENTO de informações deve ser aderente e em conformidade estrita aos preceitos e regramentos estabelecidos pela LGPD (Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018) quando se tratar de mensagem destinada a entes no Território Nacional ou da GDPR (General Data Protection Regulation ou Regulamento Geral sobre a Proteção de Dados) que é a lei de privacidade e segurança de dados da União Europeia, em vigor desde 25 de maio de 2018, quando a mensagem tiver como destino algum ente da União Européia. Está correto nosso entendimento?
Resposta: A responsabilidade integral e irrestrita é da CONTRATADA perante o STF, conforme termos do Edital.

Questionamento 32 – Item 6.6 e Termo de Confidencialidade – Confidencialidade. Considerando as obrigações de sigilo previstas no edital e no Termo de Confidencialidade, é nosso entendimento que o acesso ao conteúdo das mensagens deverá ser restrito exclusivamente ao estritamente necessário para a execução técnica do serviço, não sendo permitido acesso ou utilização para qualquer outra finalidade. Está correto nosso entendimento?
Resposta: Sim, conforme termos do Edital.

Questionamento 33 – Segurança – Incidentes de segurança. É nosso entendimento que qualquer incidente que possa resultar em acesso não autorizado, cópia, retenção, divulgação ou comprometimento do conteúdo das mensagens ou das evidências deverá ser comunicado imediatamente ao STF, acompanhado das informações necessárias para avaliação do impacto e adoção das medidas cabíveis. Está correto nosso entendimento?
Resposta: A CONTRATADA deverá comunicar imediatamente ao STF qualquer irregularidade que comprometa ou inviabilize a realização dos serviços, conforme termos do Edital.

Questionamento 34 – Segurança – Exclusão ao término do contrato. Ao término da contratação, é nosso entendimento que a CONTRATADA deverá eliminar de seus ambientes e dos ambientes de seus subcontratados todo conteúdo de mensagens e anexos eventualmente existente, mantendo somente as evidências cuja guarda seja expressamente exigida pelo edital ou pela legislação aplicável. Está correto nosso entendimento?
Resposta: O conteúdo das mensagens não deve ser mantido em nenhum componente do ambiente da contratada, nos termos previstos no Edital.

Questionamento 35 – Segurança – Backups após o encerramento. É nosso entendimento que a obrigação de eliminação ao término do contrato deverá abranger também backups, réplicas, snapshots, ambientes de contingência e disaster recovery, não sendo permitida a manutenção indefinida de quaisquer cópias do conteúdo das mensagens ou relativos à transmissão das mesmas nesses ambientes. Está correto nosso entendimento?
Resposta: O conteúdo das mensagens não deve ser mantido em nenhum componente do ambiente da contratada, nos termos previstos no Edital.

Questionamento 36 – Segurança – Comprovação de eliminação. É nosso entendimento que, ao término do contrato, a CONTRATADA deverá ser capaz de apresentar ao STF evidência técnica da eliminação do conteúdo das mensagens e anexos de seus ambientes, incluindo os ambientes eventualmente operados por subcontratados. Está correto nosso entendimento?
Resposta: O conteúdo das mensagens não deve ser mantido em nenhum componente do ambiente da contratada, nos termos previstos no Edital.

Questionamento 37 – Segurança – Princípio da minimização. Considerando o objeto da contratação e os requisitos de segurança estabelecidos, é nosso entendimento que a solução deverá adotar o princípio de minimização de dados, processando e mantendo temporariamente durante o processo de transmissão e coleta de evidências somente as informações estritamente necessárias para transmissão, geração e preservação das evidências eletrônicas exigidas pelo edital. Está correto nosso entendimento?
Resposta: O tratamento de dados pessoais deverá ocorrer estritamente para o cumprimento do objeto contratual, conforme termos do Edital.

Questionamento 38 – Segurança – Separação entre mensagem e evidência. É nosso entendimento que a arquitetura da solução deverá manter separação lógica e de segurança entre o conteúdo da mensagem, que não poderá ser retido após a entrega, e os registros/evidências/hash, que deverão ser preservados pelo prazo estabelecido no item 5.1. Está correto nosso entendimento?
Resposta: A solução deverá atender aos requisitos de preservação das evidências e de não retenção do conteúdo das mensagens, conforme termos do Edital.

Questionamento 39 – Segurança – Recuperação de evidências. Considerando o item 4.2.3, é nosso entendimento que a recuperação das evidências para atendimento às consultas de auditoria deverá ocorrer sem que seja necessário recuperar ou disponibilizar uma cópia armazenada do conteúdo original da mensagem nos ambientes da CONTRATADA ou de terceiros. Está correto nosso entendimento?
Resposta: A recuperação e validação das evidências deverá observar os requisitos previstos no Edital para guarda, integridade e auditoria das evidências eletrônicas.

Questionamento 40 – Requisito geral – Não retenção do conteúdo. Para fins de interpretação uniforme do edital, é nosso entendimento que a solução contratada deverá operar sob o princípio de "no message content retention", ou seja, não poderá manter cópia do conteúdo das mensagens ou de seus anexos após a conclusão da transmissão e confirmação da entrega, independentemente do ambiente tecnológico utilizado, permanecendo armazenadas somente as evidências e informações expressamente previstas no edital. Adicionalmente, e em resumo, entendemos que o conteúdo da mensagem e seus anexos não podem ser persistentemente armazenados pela CONTRATADA ou por seus subcontratados após a confirmação da entrega; somente os elementos de evidência e metadados expressamente exigidos pelo edital podem ser mantidos. Está correto nosso entendimento?
Resposta: O conteúdo das mensagens não deve ser mantido em nenhum componente do ambiente da contratada, nos termos previstos no Edital.

<u>Esclarecimentos de Requisitos Funcionais</u>
Questionamento 01 – sobre o item 1.1 do edital e a forma de utilização da solução pelos usuários do STF. É nosso entendimento que a solução a ser contratada deverá permitir que o usuário realize o envio da mensagem registrada diretamente a partir do Microsoft Outlook, sem necessidade de acessar uma

plataforma externa, copiar e colar o conteúdo da mensagem, realizar novo upload dos anexos ou executar procedimento manual equivalente. Considerando que o objeto contratado consiste na prestação de serviço de mensagens eletrônicas registradas e que o STF utiliza o serviço em seu ambiente corporativo de correio eletrônico, está correto nosso entendimento de que a solução deverá possuir integração com o Microsoft Outlook, permitindo ao usuário acionar o serviço de registro/segurança diretamente no próprio cliente de email?
Resposta: A solução deverá atender aos requisitos funcionais e técnicos previstos no Edital.

Questionamento 02 – sobre os itens 1.1, 2.1 e 6.2 do edital. É nosso entendimento que a integração com o Microsoft Outlook deverá ocorrer de forma nativa ou por meio de componente oficialmente suportado pelo fabricante da solução, disponibilizando ao usuário, no próprio ambiente de composição do Outlook, a funcionalidade para envio da mensagem registrada, preservando o fluxo normal de utilização do correio eletrônico corporativo. Nesse sentido, solicitamos esclarecer se será exigida a disponibilização de botão, add-in ou funcionalidade equivalente diretamente no cliente Microsoft Outlook utilizado pelo STF, permitindo o acionamento da solução sem a necessidade de utilização de portal externo para a operação cotidiana. Está correto nosso entendimento?
Resposta: A solução deverá atender aos requisitos funcionais e técnicos previstos no Edital.

Questionamento 03 – sobre o item 6.12.1 do edital – criptografia em trânsito. O item 6.12.1 estabelece que a solução deverá utilizar protocolos de cifragem em trânsito, com TLS 1.2 ou superior. É nosso entendimento que esse requisito deve ser aplicado a todo o percurso da comunicação, incluindo a transmissão entre o ambiente do STF e a infraestrutura da CONTRATADA, a transmissão entre eventuais componentes intermediários utilizados pela solução e a transmissão entre a infraestrutura da solução e o servidor do destinatário, não sendo suficiente que apenas um dos trechos da comunicação utilize a proteção oferecida pela criptografia TLS. Está correto nosso entendimento?
Resposta: O conteúdo trafegado deverá possuir criptografia em trânsito e em repouso, conforme termos do Edital.

Questionamento 04 – sobre o item 6.12.1 do edital – Criptografia do Conteúdo da Mensagem Considerando que as mensagens poderão conter informações institucionais, pessoais e potencialmente sigilosas, é nosso entendimento que a solução deverá disponibilizar mecanismo de criptografia do próprio conteúdo da mensagem e de seus anexos, de forma que a proteção não dependa exclusivamente da criptografia do canal de transporte. Nesse sentido, solicitamos esclarecer se a solução deverá suportar criptografia em nível de mensagem/conteúdo, além da criptografia do canal de transmissão, permitindo proteger o corpo da mensagem e os respectivos anexos. Está correto nosso entendimento?
Resposta: O conteúdo trafegado deverá possuir criptografia em trânsito e em repouso, conforme termos do Edital.

Questionamento 05 – sobre os itens 6.9 e 6.12.1 do edital – Criptografia associada à Não Retenção Considerando que o item 6.9 determina a disponibilização de mecanismo seguro para transmissão de arquivos de grande porte e estabelece que não deverá ocorrer retenção do conteúdo das mensagens nos servidores da CONTRATADA ou terceiros após a confirmação da entrega, é nosso entendimento que eventual armazenamento temporário necessário ao processamento da comunicação deverá permanecer protegido por criptografia e ser eliminado após o período tecnicamente necessário à entrega, permanecendo somente os registros, hashes e demais evidências cuja guarda seja expressamente exigida pelo edital. Está correto nosso entendimento?
Resposta: O conteúdo trafegado deverá possuir criptografia em trânsito e em repouso, conforme termos do Edital, observados os requisitos de não retenção do conteúdo das mensagens.

Questionamento 06 – sobre o item 6.9 do edital – transferência de Arquivos de Grande Porte. O item 6.9 estabelece que a CONTRATADA deverá fornecer ambiente ou mecanismo seguro com capacidade para transmissão de Arquivos de Grande Porte de até 1 GB. É nosso entendimento que essa funcionalidade deverá permitir ao usuário do STF enviar arquivos com tamanho de até 1 GB como parte integrante da comunicação eletrônica registrada, sem necessidade de utilização de serviço de compartilhamento de arquivos de terceiros não previsto no objeto da contratação. Está correto nosso entendimento?
Resposta: A solução deverá disponibilizar ambiente ou mecanismo seguro para transmissão de arquivos de até 1 GB, conforme termos do Edital.

Questionamento 07 – sobre o item 6.9 do edital – utilização da funcionalidade de Grandes Arquivos. Considerando que a solução será utilizada como serviço de mensagens eletrônicas registradas, solicitamos esclarecer se o mecanismo para envio de arquivos de até 1 GB deverá estar integrado ao fluxo de envio da mensagem, permitindo que o usuário realize o procedimento a partir de seu ambiente corporativo de e-mail, inclusive Microsoft Outlook, sem necessidade de utilizar plataforma externa de compartilhamento de arquivos de forma independente. Está correto nosso entendimento?
Resposta: A solução deverá disponibilizar ambiente ou mecanismo seguro para transmissão de arquivos de até 1 GB, conforme termos do Edital.

Questionamento 08 – sobre os itens 6.9, 6.12.1 e 6.13.5 do edital – Segurança, Evidência e Tratamento dos Arquivos Grandes. É nosso entendimento que os arquivos de grande porte transmitidos deverão estar abrangidos pelos mesmos requisitos de segurança, criptografia, integridade e geração de evidências aplicáveis ao corpo da mensagem, inclusive mediante geração de hash dos anexos, conforme previsto no item 6.13.5. Estes arquivos grandes também estarão sendo tratados como anexos da mensagem transmitida, NÃO SENDO PERMITIDA a guarda de CÓPIA do conteúdo dos mesmos. Está correto nosso entendimento?
Resposta: Os arquivos transmitidos deverão observar os requisitos de segurança, integridade e geração de evidências previstos no Edital, observados os requisitos de não retenção do conteúdo das mensagens.

Questionamento 09 – sobre os itens 6.9 e 6.13.5 do edital – Integridade do Arquivo Transmitido. É nosso entendimento que o comprovante/recibo deverá permitir comprovar não apenas que uma mensagem foi enviada, mas também que os arquivos anexados ou transmitidos correspondem exatamente aos arquivos apresentados pelo remetente no momento do envio, mediante mecanismo criptográfico de integridade. Está correto nosso entendimento?
Resposta: O conteúdo do Recibo/Comprovante deve atender aos requisitos do item 6.13 e seus subitens.

Questionamento 10 – sobre os itens 1.1 e 6.2 do edital – utilização por Caixas Postais Corporativas. Considerando que o serviço será utilizado no ambiente corporativo do STF, solicitamos esclarecer se a solução deverá permitir sua utilização a partir de caixas postais corporativas ou compartilhadas, além de caixas postais individuais de usuários. Está correto nosso entendimento de que uma única caixa postal corporativa poderá ser utilizada por diferentes servidores autorizados, mantendo-se a identificação individual do usuário responsável pelo envio e os respectivos registros de auditoria?
Resposta: A solução deverá atender aos requisitos funcionais e técnicos previstos no Edital.

Questionamento 11 – sobre os itens 6.12.2, 6.12.3 e 6.13 do edital – Rastreabilidade de Usuários em Caixas Postais Corporativas. Caso seja permitida a utilização da solução por caixas postais corporativas ou compartilhadas, é nosso entendimento que o sistema deverá preservar a identificação individual do usuário que realizou o envio, não sendo suficiente registrar apenas o endereço da caixa postal corporativa. Nesse sentido, a evidência deverá permitir identificar, sempre que tecnicamente possível, o usuário autenticado que efetivamente realizou a operação, bem como data, hora, endereço IP e demais informações necessárias à trilha de auditoria. Está correto nosso entendimento?
Resposta: As evidências produzidas pela solução deverão atender aos requisitos de rastreabilidade e auditoria previstos no Edital.

Questionamento 12 – sobre o item 6.13 do edital – Identificação do Remetente. Considerando a possibilidade de utilização de endereços de e-mail institucionais ou caixas postais corporativas, solicitamos esclarecer se o mecanismo de geração de evidências deverá preservar tanto o endereço de e-mail utilizado na comunicação quanto a identificação do usuário autenticado responsável pela operação, quando essa informação estiver disponível no ambiente corporativo do STF. Está correto nosso entendimento?
Resposta: O conteúdo do Recibo/Comprovante deve atender aos requisitos do item 6.13 e seus subitens.

Questionamento 13 – sobre os itens 1.1, 6.2 e 6.8 do edital – comprovação de Autorização do Fabricante. Considerando que o objeto consiste na prestação de serviço especializado baseado em uma solução tecnológica de mensagens eletrônicas registradas e geração de evidências, solicitamos esclarecer se a empresa licitante deverá comprovar que possui relação comercial, técnica ou de parceria oficialmente reconhecida pelo fabricante da solução ofertada, de

modo a assegurar que está autorizada a comercializar, implementar, licenciar, prestar suporte e manter a solução durante toda a vigência contratual. Está correto nosso entendimento?
Resposta: O Entendimento não está correto. O edital não exige que a licitante comprove autorização do fabricante ou outro documento que comprove o vínculo com o fabricante da solução ofertada.

Questionamento 14 – sobre os itens 6.2, 6.8 e 8.1 do edital – Suporte e Responsabilidade do Fabricante. É nosso entendimento que, caso a solução ofertada seja de propriedade de terceiro/fabricante especializado, a CONTRATADA deverá comprovar que possui autorização formal do fabricante para prestação dos serviços objeto desta contratação, incluindo suporte técnico, atualizações, manutenção e acesso aos recursos necessários à execução do contrato. Está correto nosso entendimento?
Resposta: O Entendimento não está correto. O edital não exige que a licitante comprove autorização do fabricante ou outro documento que comprove o vínculo com o fabricante da solução ofertada.

Questionamento 15 – sobre os itens 6.8 e 8.1 do edital – Continuidade da Autorização. Considerando que o serviço será prestado de forma contínua durante toda a vigência contratual, solicitamos esclarecer se a comprovação de parceria, autorização ou credenciamento junto ao fabricante deverá permanecer válida durante todo o período contratual, não sendo suficiente sua existência apenas na data de apresentação da proposta. Está correto nosso entendimento?
Resposta: O Entendimento não está correto. O edital não exige que a licitante comprove autorização do fabricante ou outro documento que comprove o vínculo com o fabricante da solução ofertada.

Questionamento 16 – sobre os itens 6.8 e 8.1 do edital – Comprovação Documental. É nosso entendimento que a comprovação da condição de parceiro, revendedor autorizado, integrador autorizado ou equivalente deverá ser realizada mediante documento emitido ou validável diretamente junto ao fabricante da solução ofertada, permitindo ao STF verificar a autenticidade da relação informada pela licitante. Está correto nosso entendimento?
Resposta: O Entendimento não está correto. O edital não exige que a licitante comprove autorização do fabricante ou outro documento que comprove o vínculo com o fabricante da solução ofertada.

Questionamento 17 – sobre o item 1.1 do edital – Requisitos Funcionais Mínimos da Solução. Considerando que o objeto contempla a prestação de serviço de mensagens eletrônicas registradas e que a solução deverá ser utilizada no ambiente corporativo do STF, solicitamos esclarecer se os requisitos funcionais descritos no Termo de Referência devem ser entendidos como Requisitos Mínimos Obrigatórios de Operação da Solução, incluindo, quando aplicável, integração com o Microsoft Outlook, envio seguro de mensagens e anexos, transmissão de arquivos de grande porte, utilização por caixas postais corporativas, geração de evidências auditáveis e mecanismos de criptografia. Nesse sentido, uma solução que atenda apenas à geração de recibos de envio/entrega, mas que não ofereça as funcionalidades necessárias à integração e utilização no ambiente corporativo do STF, será considerada tecnicamente compatível com o objeto? Está correto nosso entendimento?
Resposta: Os requisitos obrigatórios da contratação são aqueles expressamente previstos no Edital e no Termo de Referência. A compatibilidade da solução será aferida com base no atendimento integral desses requisitos.
4. Considerando a resposta acima, informo que os termos do Edital do Pregão Eletrônico nº 90024/2026, permanecem inalterados, o qual encontra-se disponível no link: https://portal.stf.jus.br/servicos/licitacao/listarEdital.asp
5. Por fim, informo abertura do certame fica mantida para o dia 10/09/2026, às 9 horas, no sítio https://www.gov.br/compras/pt-br.

Atenciosamente,

Documento assinado eletronicamente por **Cezar Augusto Barros Gadelha**, **PRESIDENTE DA CPL**, em 09/09/2026, às 15:52, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sistemas.stf.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **3440724** e o código CRC **E4416195**.