TRIBUNAL REGIONAL DO TRABALHO DA 12ª REGIÃO

ESTUDOS PRELIMINARES DE CONTRATAÇÃO DE SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

MARCUS VINICIUS MATTOS
19/09/2022 13:00

ARTHUR FERNANDO DELLAGUSTINA LAGO
19/09/2022 13:21

ARILDO DISARO FILHO
19/09/2022 13:35

PROAD: 5131/2022

1. Capítulo I - ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO

1.1. Objeto

Contratação de prestação de serviços de proteção de borda de rede e de alta disponibilidade através de rede dinâmica de distribuição e aceleração de conteúdo - CDN, integrada a recursos de segurança de firewall de aplicação web – WAF e mitigação contra ataques distribuídos de negação de serviço – DDoS por meio de computação em nuvem na modalidade software como serviço – SAAS, incluindo serviços de configuração, ativação, repasse de conhecimentos e suporte técnico pelo período de 36 (trinta e seis) meses.

1.2. Justificativa

A consolidação do PJe vem proporcionando grandes avanços para a prestação jurisdicional da Justiça do Trabalho. Com o processo judicial existindo e tramitando exclusivamente no meio eletrônico, a tecnologia da informação passou a ser a principal responsável pela guarda, integridade e disponibilidade de todos os autos dos processos.

O contexto atual de crescente demanda de usuários externos e de serviços de consultas processuais automatizadas, providos por empresas conhecidas como *lawtech's*, somado ao crescimento exponencial dos ataques cibernéticos altamente agressivos, requer o uso de tecnologias aprimoradas capazes de suportar essas demandas. Provendo, assim, segurança e melhorando o acesso aos serviços judiciais disponibilizados aos clientes internos e externos, de modo a assegurar a confidencialidade, disponibilidade e integridade dos dados armazenados na infraestrutura tecnológica do Tribunal, bem como nos dispositivos que acessam os sistemas judiciais.

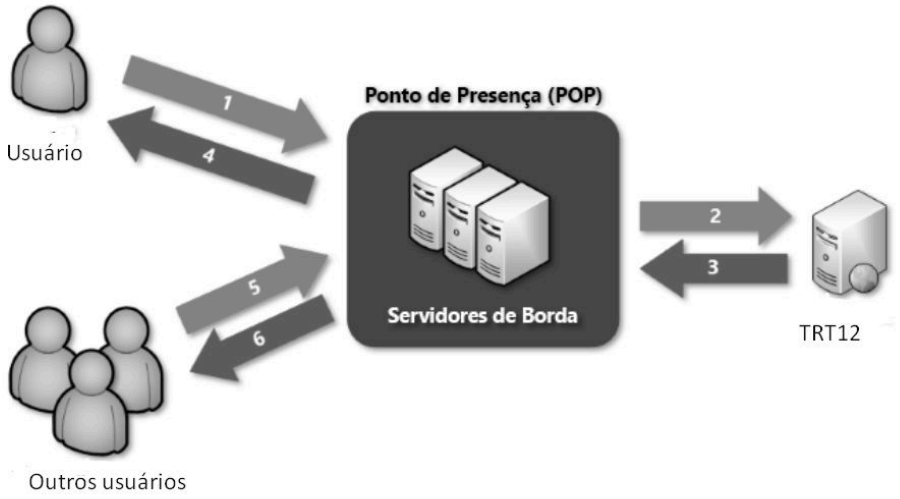
Embora seja uma realidade em grande parte das organizações que sustentam o negócio exclusivamente em meio eletrônico, este Tribunal ainda não utiliza uma solução de proteção de borda de rede que possa monitorar, controlar,

disponibilizar, distribuir e acelerar o acesso aos sistemas judiciários a partir de datacenters localizados em diversas regiões do globo, protegendo seus ativos contra as principais ameaças e mitigando os ataques, como negação de serviço e exploração de vulnerabilidades em sistemas web.

Esse tipo de solução é prestada por empresas especializadas de computação em nuvem, na modalidade de software como serviço (SaaS), por meio da integração de rede dinâmica de distribuição e aceleração de conteúdo (CDN) com firewall de aplicação web (WAF), implementando mitigação contra ataques distribuídos de negação de serviço – DDoS, gerenciamento de robôs (botnets) e proteção de DNS.

A saber:

I) Rede dinâmica de distribuição e aceleração de conteúdo (CDN) - é uma rede distribuída de servidores que fornece o conteúdo da Web para os usuários com maior eficiência. As CDNs armazenam conteúdo em cache em servidores de borda em localizações de ponto de presença (POP) que estão próximas aos usuários finais, para minimizar a latência, melhorando o desempenho dos sites, além de garantir a segurança utilizando WAF.



II) Firewall de aplicação web (WAF) - Um WAF, ou Web Application Firewall, são firewalls de segurança que protegem os sites, através de AIs e machine learning identificam as ameaças, de Hackers, Spammers, DDoS, Injeções SQL e muito outros tipos de Cyber Ataques, e tomam ações garantindo a seguridade do negócio.

O Firewall de aplicação web (WAF) difere dos serviços de Firewall de camada 7, pois o primeiro inspeciona o tráfego que entra no TRT e o segundo o tráfego que sai do TRT, em outras palavras o primeiro visualiza e controla o tráfego do cliente externo ao sítio do TRT, e o segundo visualiza e controla o tráfego que os servidores do TRT acessam na Internet.

Considerando a necessidade de proteger a tecnologia e assegurar o acesso ao PJe no âmbito deste Tribunal, justifica-se a contratação de uma solução

integrada, na modalidade software como serviço, que implemente serviços de CDN, WAF, proteção antirrobôs, mitigação DDoS em nuvem e proteção de DNS.

Desta forma obtemos visibilidade e monitoramento efetivos do tráfego externo destinado às aplicações web do TRT, melhorando o desempenho do acesso externo às aplicações web e mitigando o impacto de tráfego externo espúrio e/ou excedente destinado às aplicações web, mantendo a conformidade com às resoluções e portarias do CNJ, aumentando o nível de segurança do ambiente tecnológico e reduzindo o risco de incidentes cibernéticos.

Estes serviços permitem que o controle de acessos, que hoje é feito nos servidores do TRT, ocorra 24 horas no Servidor de Borda, evitando, por exemplo, ataques distribuídos de negação de serviço – DDoS, mantendo maior disponibilidade e segurança no acesso das aplicações web.

1.3. Quantidade

Item	Descrição	Unidade	QTDE
1	Prestação de serviços de proteção de borda de rede e de alta disponibilidade através de rede dinâmica de distribuição e aceleração de conteúdo – CDN, integrada a recursos de segurança de firewall de aplicação web – WAF, mitigação contra ataques distribuídos de negação de serviço – DDoS, gerenciamento de robôs (botnets) incluindo suporte técnico, por 36 meses, para um tráfego de até **20 TB mensais**	Serviço	1
2	Franquia de tráfego adicional (TB)	TB	10
3	Proteção DNS	Zonas DNS	2

ITEM 1: Prestação de serviços de proteção de borda de rede e de alta disponibilidade

Foi realizado levantamento, pela equipe de infraestrutura, um consumo de tráfego na ordem de 15 TB mensais, acontece que essa medição não é muito precisa pois muitas variantes podem interferir no tráfego em questão, portanto para evitar uso do item dois optou-se por contratar no mínimo 20 TB de tráfego.

ITEM 2: Franquia de tráfego adicional (TB)

Para garantir que, caso haja um aumento repentino de visualizações web, a disponibilização de novos serviços web, o crescimento maior do que o esperado da utilização dos serviços hoje disponíveis, fatores estes que podem prejudicar o

acesso do jurisdicionado ao serviços do TRT, poderá ser contratada franquia adicional na presente solução.

ITEM 3: Proteção DNS

Para garantir, deverá ser provido de serviço DNS autoritativo em nuvem, visando acelerar a resolução de nomes e proteger contra ataques aos serviços de DNS da contratante. Hoje o TRT-SC possui 2 domínios: trt12.jus.br e trt12.gov.br, iremos contratar a princípio somente para o domínio trt12.jus.br, por ser o mais utilizado.

1.4 Definição e Especificação dos Requisitos.

1.4.1. Os serviços devem ser prestados mediante uma plataforma de CDN não intrusiva, ou seja, sem a necessidade de instalação de equipamentos na contratante.

1.4.2. A rede CDN e o WAF devem estar disponíveis mediante alteração do DNS da contratante utilizando CNAMES.

1.4.3. Os serviços contratados deverão prover a infraestrutura de uma CDN e a proteção de WAF, sendo contabilizados por volume de tráfego entregue pela plataforma.

1.4.4. Deverá ser considerado para apuração do tráfego, somente o conteúdo legítimo entregue ao usuário pelos servidores de borda. Não será aceito cobrança por ataque ou por tráfego entre os servidores da rede de distribuição de conteúdo.

1.4.5. Será contratada uma franquia adicional de volume de tráfego excedente, a ser consumido após o esgotamento do tráfego mensal contratado.

1.4.5.1 A menor fração de tráfego adicional será de 1 GB

1.4.6. Deverá prover serviço de bloqueio automático de acessos indevidos, baseado em regra definida pelo contratante, visando evitar que tentativas de ataque sejam contabilizados, para não consumir a franquia contratada.

1.4.7. Deverá ser provido de serviço DNS autoritativo em nuvem, visando acelerar a resolução de nomes e proteger contra ataques aos serviços de DNS da contratante.

1.4.8. O serviço DNS deverá ser compatível com DNSSEC, conforme regras do Registro.br para domínios com o sufixo JUS.BR.

1.4.9. Deverá possuir suporte a zona de pesquisa direta e zona de pesquisa inversa.

1.4.10. Deverá ser provido de serviço de proteção contra ataques (WAF), de forma a proteger os websites e as aplicações da contratante.

1.4.11. Deverá ser provido de serviço de detecção, identificação e gestão de robôs (botnets), de forma a proteger os websites e as aplicações da contratante.

1.4.12. A solução deverá estar aderente aos aspectos de segurança dispostos nos seguintes instrumentos regulatórios: Normas ABNT NBR 27001, ABNT NBR 27002, LGPD, NIST 800-53 e SOC 2 Tipo 2.

1.4.13. Visando assegurar a integração da solução, a licitante deverá comprovar que dispõe de suporte técnico com os mesmos níveis de serviços exigidos no Edital, junto ao respectivo fabricante de cada componente que agregar na solução ofertada.

1.5. Levantamento das alternativas existentes

Conforme estudo técnico, identificou-se quatro possíveis cenários para a contratação de prestação de serviços de proteção de borda de rede e de alta disponibilidade:

Cenário 1 - Não realizar a contratação

Ao deixar de contratar a solução, o Tribunal permanecerá exposto aos riscos crescentes de ameaças cibernéticas de grande potencial de prejuízo aos ativos que sustentam a prestação jurisdicional, especialmente os dados de todos os processos judiciais que existem exclusivamente no ambiente tecnológico.

Trata-se de uma opção de alto risco no cenário atual, especialmente após outros tribunais terem passado por uns recentes ataques. Caso do TRT04 e do TRT 17. Além disso, as oscilações de desempenho e a estabilidade das aplicações causados pelo uso cada vez mais frequentes de robôs externos de pesquisa, prejudicam o uso legítimo dos sistemas, com impacto direto na prestação jurisdicional.

Cenário 2 - Contratação de soluções não integradas e implantadas na infraestrutura interna do Tribunal (on premise)

Embora seja viável a implementação de ferramentas tecnológicas isoladas que possam ser instaladas na infraestrutura interna para tratar de cada demanda da presente contratação, essa prática seria inadequada para o atendimento global das demandas, pois não atingiria um bom resultado na mitigação dos riscos de ataques

cibernéticos.

Além disso, necessitaria de robusta infraestrutura de equipamentos para suportar o funcionamento de cada serviço, o que oneraria os custos de aquisição dos mesmos.

Outro aspecto de grande relevância neste contexto é que, para efetivar esta solução, além dos equipamentos e demais recursos tecnológicos, cada solução internalizada na infraestrutura do Tribunal, requer equipe própria, permanentemente capacitada e disponível para administrar cada elemento desta solução, em prejuízo à sustentação das aplicações do negócio(como o Pje), já que a equipe possui capacidade limitada.

O acréscimo de componentes na infraestrutura também acrescentaria fragilidades e riscos a serem monitoradas e tratadas de forma que não sejam exploradas em um ataque cibernético, onerando ainda mais a equipe técnica e os recursos tecnológicos de proteção a esses ativos.

Por fim, a falta de integração entre os componentes da solução causaria risco de conflitos de responsabilidade no caso de uma solução interferir no funcionamento de outra, bem como iria requerer manter equipe técnica para cada tecnologia de forma isolada, trazendo grande prejuízo ao foco nas aplicações que suportam a prestação jurisdicional.

Cenário 3 - Contratação da solução integrada na modalidade SAAS - software como serviço

A adoção de uma infraestrutura em nuvem diminui a exposição da infraestrutura tecnológica interna do Tribunal aos ataques cibernéticos.

Além disso, dinamiza a instalação, ativação e o funcionamento da solução, reduzindo a curva de aprendizado da equipe técnica para operação da mesma.

Por fim, diminui o investimento inicial, uma vez que a solução é contratada na modalidade de prestação de serviços e não como aquisição de licenças e/ou equipamentos.

A integração entre os diferentes componentes da solução é indispensável para a correta orquestração entre os mesmos, assegurando que as funcionalidades se complementem e ao mesmo tempo não se prejudiquem mutuamente na proteção do ambiente tecnológico e na melhoria do desempenho das aplicações do Tribunal.

	Característica	**Cenário 1**	**Cenário 2**	**Cenário 3**
01	Fabricante/Fornecedor	TRT12	Diversos/ ON Premisses	Diversos/ SAAS

02	Nome solução (modelo)	N/A	Variadas	Variadas
03	Custo efetivo total (CET)	0	Não foram estimados os custos dessa alternativa, uma vez que a mesma se mostra extremamente ineficaz para os propósitos estabelecidos na demanda e de alto custo operacional para o Tribunal	R$ 2.845.589,04
04	Forma de entrega	Construção Própria	Hardware/ Software/ Serviço	Serviço
05	A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública Federal?	N/A	N/A	Sim
06	A Solução está disponível no Portal do Software Público Brasileiro?	N/A	N/A	N/A
07	A Solução é um software livre ou software público?	Não	Sim	Não
08	A Solução é aderente às políticas, premissas e especificações técnicas definidas no MNI do Poder Judiciário? (quando houver intercâmbio de informações de processos judiciais)	N/A	N/A	N/A
09	A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	N/A	N/A	N/A
10	A Solução é aderente a orientações, premissas e especificações técnicas e funcionais do Moreq-Jus? (quando houver documentos digitais produzidos pelo Judiciário)	N/A	N/A	N/A

Contratações Públicas Similares

Foram encontradas as seguintes contratações, no âmbito da administração pública federal, similar, que atendem aos requisitos desta demanda:

TRF 03 PREGÃO ELETRÔNICO No 021/2021

TSE Contrato 86/2020

TJ/RN Pregão 41/2021

1.6. Justificativa da escolha da solução

Desta forma o cenário 1 fica prejudicada embora não apresente custos de contratação, essa opção aumenta a exposição do Tribunal a riscos de oscilações de desempenho e ataques cibernéticos que poderiam causar danos de difícil reparação, devido à especialização e agressividade cada vez maior dos hackers.

O cenário 2, como descrito acima, não contempla todas as necessidades de verificação e proteção para garantir um mínimo de segurança além de demandar uma maior sobrecarga de trabalho das equipes internas. A implantação de soluções isoladas na infraestrutura iria requerer equipamentos e recursos de datacenter, especialmente espaço físico, energia, comunicação de rede e climatização.

O cenário 3, por se tratar de um serviço em nuvem, não requer adaptações na infraestrutura do Tribunal, são necessárias apenas adaptações lógicas para a integração da solução ao ambiente tecnológico e como descrito acima apresenta o melhor custo benefício.

Ressaltamos ainda a recomendação contida na Resolução CNJ nº 370/2021, que instituiu a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD) para o sexênio 2021-2026:

> *Art. 35. Recomenda-se utilizar serviços em nuvem que simplificam a estrutura física, viabilizam a integração, requisitos aceitáveis de segurança da informação, proteção de dados, disponibilidade e padronização do uso dessa tecnologia no Poder Judiciário.*

Pelo exposto, a opção do modelo “Cloud Computing” é justificada pela maior

flexibilidade e eficiência conforme itens 59 e 60 do Acórdão 1739/2015 do TCU, transcritos abaixo:

> "59. Segundo estudo da IDC, as principais vantagens do uso de computação em nuvem são:
>
> 1) Redução de custos de infraestrutura e serviços de TI. O benefício mais significativo vem de hospedar aplicações em infraestrutura em nuvem devido à redução de custos de capital (capital expenditure - Capex) e custos operacionais (operacional expenditure - Opex).
>
> 2) Otimização da produtividade da equipe de TI. A mudança para o uso de IaaS, ao acelerar o desenvolvimento e a implantação de aplicações, bem como automatizar o seu gerenciamento, torna a equipe de TI mais produtiva e capaz de melhorar o suporte de operações de missão crítica.
>
> 3) Melhoria da produtividade do usuário final. Os usuários finais beneficiaram-se de menor indisponibilidade do serviço e recuperação mais rápida, reduzindo o tempo de inatividade em 72% e economizando expressivos recursos de cada aplicativo por ano.
>
> 4) Aumento de benefícios do negócio. Muitas das empresas estão empregando soluções em nuvem para possibilitar novos modelos de negócios e suportar aplicações de geração de receita, atingindo um maior número de usuários/clientes.
>
> 60. Outras vantagens também são apontadas pela Isaca na publicação "Controls and Assurance in the Cloud: Using COBIT 5":
>
> 1) Melhorar a capacidade de resposta. Computação em nuvem fornece serviços flexíveis e escaláveis que podem ser implementados rapidamente para fornecer às organizações a capacidade de responder a mudanças de requisitos e a períodos de picos.
>
> 2) Ciclo mais rápido de inovação. No ambiente de nuvem, a inovação é tratada muito mais rápido do que dentro da empresa. O gerenciamento de patches e atualizações para novas versões tornam-se mais flexíveis.
>
> 3) Redução do tempo para implementação. Computação em nuvem oferece poder de processamento e capacidade de armazenamento de dados conforme a necessidade, quase em tempo real.
>
> 4) Resiliência. Computação em nuvem pode fornecer um ambiente altamente resiliente e reduzir o potencial de falha e o risco de downtime."

Desta forma é possível contratar por licitação própria, ou utilizando a Ata de Registro de Preços. O Tribunal Regional do Trabalho da 4ª Região realizou Pregão Eletrônico para contratação de Solução que auxilie na prevenção e limitação de ataques cibernéticos, através de CDN/WAF, que culminou na Ata de Registro de Preços Nº 05/2022, gerenciada pelo TRT da 4ª Região, da qual este Regional é coparticipante.

Considerando a economia e as vantagens de uma solução para todos os Tribunais, que gera sinergia e favorece a troca de informações, nivelando o conhecimento. Com a utilização desta ata teremos todas as vantagens do Cenário 3, caso os preços da Ata de Registro de Preços do TRT4 estejam dentro dos valores praticados pelo mercado, esta equipe recomenda a sua utilização.

1.7. Especificação completa da solução escolhida

1.7.1 Os serviços devem ser prestados mediante uma plataforma de CDN não intrusiva, ou seja, sem a necessidade de instalação de equipamentos na contratante.
1.7.2 A rede CDN e o WAF devem estar disponíveis mediante alteração do DNS da contratante utilizando CNAMES.
1.7.3 Os serviços contratados deverão prover a infraestrutura de uma CDN e a proteção de WAF, sendo contabilizados por volume de tráfego entregue pela plataforma.
1.7.4 Deverá ser considerado para apuração do tráfego, somente o conteúdo legítimo entregue ao usuário pelos servidores de borda. Não será aceito cobrança por ataque ou por tráfego entre os servidores da rede de distribuição de conteúdo.
1.7.5 Será contratada uma franquia adicional de volume de tráfego excedente, a ser consumido após o esgotamento do tráfego mensal contratado.
1.7.5.1 A menor fração de tráfego adicional será de 1 GB
1.7.6 Deverá prover serviço de bloqueio automático de acessos indevidos, baseado em regra definida pelo contratante, visando evitar que tentativas de ataque sejam contabilizados, para não consumir a franquia contratada.
1.7.7 Deverá ser provido de serviço DNS autoritativo em nuvem, visando acelerar a resolução de nomes e proteger contra ataques aos serviços de DNS da contratante.
1.7.7.1 O serviço DNS deverá ser compatível com DNSSEC, conforme regras do Registro.br para domínios com o sufixo JUS.BR.
1.7.7.2 Deverá possuir suporte a zona de pesquisa direta e zona de pesquisa inversa.
1.7.8 Deverá ser provido de serviço de proteção contra ataques (WAF), de forma a proteger os websites e as aplicações da contratante.
1.7.9 Deverá ser provido de serviço de detecção, identificação e gestão de robôs (botnets), de forma a proteger os websites e as aplicações da contratante.
1.7.10 A solução deverá estar aderente aos aspectos de segurança dispostos nos seguintes instrumentos regulatórios: Normas ABNT NBR 27001, ABNT NBR 27002, LGPD, NIST 800-53 e SOC 2 Tipo 2.

1.7.11 Visando assegurar a integração da solução, a licitante deverá comprovar que dispõe de suporte técnico com os mesmos níveis de serviços exigidos no Edital, junto ao respectivo fabricante de cada componente que agregar na solução ofertada.

Rede dinâmica de distribuição e aceleração de conteúdo – CDN

1.7.12 A CDN deverá ser descentralizada e sem ponto único de falha, distribuída em, no mínimo, 5 pontos de presença física, dos quais pelo menos 2 devem ser em território Brasileiro, devendo o conteúdo estático ou dinâmico de forma criptografada (TLS/SSL) ocorrer em todos os pontos da rede.

1.7.12.1 A solução deverá possuir taxa de disponibilidade mensal de no mínimo 99,999%, considerando o regime integral de operação (24X7), considerando o somatório dos pontos de presença da contratada.

1.7.12.2 A CDN deverá possuir um algoritmo de roteamento dinâmico que caso algum datacenter fique indisponível o tráfego seja redirecionado sem afetar o desempenho dos serviços.

1.7.13 A CDN deverá possuir um ambiente de testes de configurações, onde seja possível aplicar todas as funcionalidades de distribuição de conteúdo e segurança, a fim de validar todas as configurações do website ou aplicação antes de publicar em produção.

1.7.13.1 Este ambiente deverá possuir servidores em nuvem específicos e dedicados para realização dos testes das novas configurações.

1.7.13.2 A área de teste das funcionalidades deverá possuir todas as funcionalidades do ambiente de produção.

1.7.13.3 O ambiente deverá possuir endereços IPs ou hostnames específicos que devem ser usados nos testes, possibilitando que seja testada todas as funcionalidades dos websites ou aplicações protegidas, apenas realizando o direcionamento do navegador do cliente para este ambiente.

1.7.13.4 Deverá ser possível aplicar a mesma configuração do ambiente de teste no ambiente de produção, diretamente na interface de gerência.

1.7.13.5 Com a solução em produção, deverá disponibilizar simultaneamente o ambiente de teste para criação e validação de novas versões de configuração, sem que a versão em produção seja afetada.

1.7.13.6 A solução deverá permitir o versionamento de configurações de distribuição de conteúdo e segurança, com o objetivo de realizar o procedimento de retorno para qualquer versão válida caso seja necessário.

1.7.14 A CDN deverá fazer uso de algoritmos para determinar qual servidor da rede dinâmica possui melhores condições de entrega, utilizando métodos para o redirecionamento do usuário, desde servidores de aplicações, até o redirecionamento no nível de Servidor de Domínio de Nomes (Domain Name Servers, DNS).

1.7.15 A CDN deverá ser configurada para habilitar todos os seus servidores a reconhecer o site de origem, seus conteúdos estáticos (CSS, JS, documentos, imagem, vídeo, áudio, dentre outros) e dinâmicos, tanto no Brasil quanto no exterior.

1.7.16 A contratada deverá prover aceleração e proteção para no mínimo 100 URLs pertencentes à contratante, registradas sob os domínios a serem informados.

1.7.17. A CDN deverá prover disponibilidade dos sites e tempo de carregamento das páginas inferior ao de carregamento sem o uso da CDN, independentemente da quantidade de usuários e dados acessados simultaneamente.

1.7.18. A CDN deverá garantir o desempenho dos acessos através da determinação, em tempo real, de qual servidor de rede dinâmica possui melhores condições de entrega para cada usuário do conteúdo da aplicação acessada.

1.7.19 A CDN deverá propagar as mudanças nas listas de liberação e bloqueio em até 10 minutos, permitindo assim a resposta a incidentes de segurança na infraestrutura da contratante.

1.7.20 A CDN deverá realizar a expiração de conteúdo (purge) por URL, com suporte a wildcard, em toda a rede, em um prazo máximo de 5 minutos.

1.7.21 A CDN deverá possuir caminhos redundantes de acesso e distribuição de conteúdo, a fim de garantir o acesso a seus serviços, bem como ao serviço de origem.

1.7.22 A CDN deverá acelerar e distribuir indistintamente quaisquer aplicações baseadas em Protocolo de Transferência de Hipertexto (Hypertext Transfer Protocol, HTTP e HTTPS), balanceando entre seus POPs, a carga das páginas de modo a garantir melhor performance.

1.7.22.1 Para a aceleração e distribuição de aplicações HTTPS, a contratada deverá realizar, sem custos adicionais para a contratante, a emissão dos certificados digitais necessários para o funcionamento de endereços em SSL.

1.7.22.1.1 Após a configuração dos certificados, deverão ser realizados testes utilizando a ferramenta Qualys SSL Labs (https://www.ssllabs.com/ssltest/), na qual deverá ser obtida a qualificação “A” para todas as URLs.

1.7.22.1.2 Os Certificados Digitais A1 SSL/TLS para Servidor Web deverão ter as seguintes especificações:

1.7.22.1.2.1 Os certificados emitidos deverão ser do tipo A1 SSL/TLS para Servidor Web, podendo ser individualizados para cada URL implantada, do tipo WildCard onde o certificado permite que seja adicionada segurança SSL a ilimitados sites, desde que façam parte de subdomínios de um mesmo domínio ou do tipo SAN onde o certificado permite que seja adicionada segurança SSL a 100 sites.

1.7.22.1.2.2 Todos os certificados emitidos deverão possuir o certificado raiz da autoridade certificadora dentre as que já vêm previamente instaladas e configuradas nos principais navegadores e dispositivos do mercado suportando, no mínimo: Mozilla Firefox, Google Chrome, Internet Explorer, Safari, iPhone, Android e Windows Phone.

1.7.22.1.2.3 A CONTRATADA deverá manter o certificado válido durante todo o período do contrato.

1.7.22.1.2.4 O procedimento para validação dos certificados deverá ser on-line, telefônico ou via validação de DNS.

1.7.22.1.2.5 A fornecedora deverá possuir a capacidade de configuração das cifras e da versão de TLS utilizadas pela contratante.

1.7.22.1.2.6 Possuir validação da organização emissora do certificado digital, incluindo os dados da contratante, conforme o caso, no certificado digital.

1.7.23 A CDN deverá suportar a configuração de uma origem principal e outra backup (standby), que só será utilizada em caso de falha da primeira.

1.7.24 A CDN deverá ser sensível à existência de letras maiúsculas e minúsculas para armazenamento de objetos em cache.

1.7.25 A CDN deverá permitir a seleção de argumentos de query strings e cookies para armazenamento de objetos em cache, fazendo com que o objeto armazenado em cache seja o mesmo para solicitações com características afins.

1.7.26 A CDN deverá possuir os seguintes recursos para a gestão de cache:

1.7.26.1 Suporte a não armazenagem (no store)

1.7.26.2 Deverá possuir opção para ignorar cache (bypass cache), nesse caso o conteúdo do cache não será armazenado pela CDN.

1.7.27 A CDN deverá permitir a criação de políticas de cache que permitam não fazer cache da requisição (bypass) assim como encaminhar os cookies tal como enviados pelos usuários para os servidores de origem.
1.7.28 A CDN deverá responder a diferentes métodos HTTP, considerando, pelo menos: GET, HEAD, POST, PUT, PATCH, DELETE e OPTIONS.
1.7.29 A CDN deverá restringir para determinado site, métodos HTTP específicos, bloqueando outros métodos que não forem habilitados.
1.7.30 A CDN deverá modificar, adicionar ou remover informações do cabeçalho HTTP durante a comunicação com os datacenters de origem.
1.7.31 A CDN deverá permitir a implementação de redirecionamento HTTP otimizando a comunicação com o datacenter de origem.
1.7.32 A CDN deverá fornecer o serviço de geolocalização a nível de país, que permitirá o gerenciamento de listas de permissão e negação de acessos.
1.7.33 A CDN deverá realizar a entrega de qualquer formato e tipo de conteúdo nos protocolos HTTP 1.1 e 2.
1.7.34 A CDN deverá realizar a entrega do conteúdo em cache, mesmo que já expirado, caso a origem do Datacenter esteja inacessível.
1.7.35 A CDN deverá prover aceleração através da compressão de dados (gzip, brotli) desde que suportado pelo navegador ou dispositivo utilizado pelo usuário.
1.7.36 A CDN deverá detectar as características dos dispositivos através das informações de navegador de Internet.
1.7.37 A CDN deverá permitir a obtenção de objetos cacheados a partir de outros servidores da rede, evitando assim conexão com o datacenter de origem.
1.7.38 A CDN deverá permitir a utilização de métodos de validação de usuário através de token de URL, cookie, certificado, definindo se o conteúdo deve ou não ser enviado ao usuário. Durante a validação, não deverá consultar a infraestrutura de origem e deverá usar de meios próprios para validação das informações dos usuários.
1.7.39 A CDN deverá verificar que a requisição está sendo feita por um site autorizado a ter acesso ao conteúdo armazenado.
1.7.40 A CDN deverá prover a infraestrutura necessária para a adequada prestação dos serviços indicados anteriormente, de forma escalável, automaticamente e em tempo real, independentemente da quantidade de acessos simultâneos.
1.7.41 Através do painel de monitoramento deverá subdividir e permitir a consulta de dados referente a tráfego, requisições HTTP e HTTPS, hits, exclusivamente para cada site WEB configurado, permitindo a geração de relatórios específicos para cada site presente na CDN para no mínimo 30 dias de histórico.

1.7.42 O painel de monitoramento deverá possuir opções para geração de filtros, possibilitando a criação de relatórios customizados por site e data.

1.7.43 O painel de monitoramento deverá permitir acompanhar o quantitativo de requisições realizadas para cada site WEB na CDN.

1.7.44 O painel de monitoramento deverá disponibilizar informações como: país, endereço IP, descrição da ameaça/regra que está sendo processada, método HTTP utilizado, data e hora da ocorrência da CDN. Deverá conter, informações acerca das atividades maliciosas processadas, apresentando:

1.7.44.1 Quais sites WEB estão sendo atacados e

1.7.44.2 O que está sendo explorado no ataque.

1.7.45 O painel de monitoramento deverá apresentar as informações e permitir a consulta da CDN, com delay máximo de 15 minutos e de no mínimo 30 dias de dados processados.

1.7.46 O painel de monitoramento deverá apresentar e contabilizar, através de gráficos, todas as requisições de conteúdo realizadas pelo usuário final para todo e qualquer código de status HTTP/HTTPS, gerando relatórios por período, permitindo a identificação dos picos de acesso a CDN.

1.7.47 O painel de monitoramento deverá apresentar e contabilizar, através de gráficos e API, o volume de dados trafegados e requisições entre a CDN e o usuário final para todo e qualquer código de status HTTP/HTTPS da CDN.

1.7.48 O painel de monitoramento deverá apresentar e contabilizar, através de gráficos e API, o volume de dados trafegado, e requisições buscadas a partir da origem ou entregues a partir dos servidores de borda da plataforma da CDN.

1.7.49 Deverá possibilitar a integração com SIEM (Security Information and Event Management), permitindo o gerenciamento de eventos e informações de segurança, incluindo serviço de WAF e gerenciamento de robôs.

1.7.50 Deverá possibilitar o armazenamento de Logs e Exportação de Logs para fontes externas;

1.7.51 O painel de monitoramento deverá disponibilizar os Logs das informações dos servidores para download em intervalo não superior a 1 (uma) hora da CDN.

1.7.52 O painel de monitoramento deverá permitir o monitoramento real de navegação dos visitantes, conforme abaixo:

1.7.52.1 Monitoramento de usuários por meio de injeção de JavaScript no HTML ou do acréscimo de cabeçalhos HTTP para monitorar dados de desempenho e comunicação do cliente;

1.7.52.2 Deverá monitorar o desempenho de navegação dos visitantes dos sites protegidos pela plataforma coletando beacons por meio de injeção automática

de código para as principais plataformas móveis do mercado (Android e iOS) e principais navegadores de internet (Google Chrome, Firefox e MS Edge).

1.7.52.3 Deverá permitir o acompanhamento em tempo real dos dados de desempenho coletados pelos beacons, fornecendo visualização de, no mínimo, as seguintes dimensões: navegador, dispositivo, Sistema Operacional e localidade geográfica.

1.7.52.4 Deverá possibilitar a customização da coleta para monitoramento utilizando técnicas de Label e Tagging.

1.7.53 A CDN deverá disponibilizar via API a consulta e a alteração das configurações de cache e regras de segurança com reflexo em todos os servidores de borda da plataforma.

1.7.54 A CDN deve fornecer controles de segurança adequados, incluindo, mas não limitados a: restrição de acesso administrativo a todos os serviços (administração, entrega) por meio de um login seguro ou autenticação de dois fatores, de modo que os serviços não possam ser utilizados por terceiros não autorizados.

1.7.55 A CDN deve fornecer gerenciamento de conta, acessos de usuários, perfis de acesso, grupo de ativos (configurações, APIs) e as permissões concedidas a usuários e grupos.

1.7.56 Capacidade de dar permissões específicas a diferentes usuários ou grupos de usuários por tipos de serviços (CDN e Segurança) e suas funções.

1.7.57 Capacidade de concessão de perfis de acesso que permitam administração hierárquica dos usuários e seus perfis.

Segurança de firewall de aplicação web – WAF e mitigação de tráfego malicioso

1.7.58 A CDN deverá disponibilizar em todos os Pontos de Presença o serviço de WAF – firewall de aplicação para impedir atividades maliciosas, incluindo pelo menos as seguintes funcionalidades, além de outros tipos de ataques comuns e vulnerabilidades conhecidas a serem bloqueadas:

1.7.58.1 Bloqueio por rede e IP;

1.7.58.2 Geolocalização;

1.7.58.3 Secure token;

1.7.58.4 Cross site scripting (XSS);

1.7.58.5 Remote file inclusion (RFI);

1.7.58.6 Directory transversal;

1.7.58.7 SQL injection.

1.7.59 A solução deverá possuir proteção contra as vulnerabilidades WEB listadas no OWASP TOP 10, descritos em https://owasp.org/Top10/, proteção para a lista de vulnerabilidades para APIs em https://owasp.org/www-project-api-security/, além das novas vulnerabilidades que vierem a ser incluídos no OWASP durante a vigência do contrato.
1.7.60 Deverá possuir proteção contra exploração de vulnerabilidade (exploit) em por meio de inspeções de regras WAF.
1.7.61 A CDN deverá tratar de maneira individualizada as requisições maliciosas direcionadas aos sites WEB da origem e bloqueá-las.
1.7.62 A CDN deverá fornecer o serviço de Geo Localização para permitir o bloqueio por país e redes indesejadas (Exemplo: rede TOR).
1.7.63 A CDN deverá fornecer o serviço de controle de camada IP para bloqueio ou liberação de endereços IP. Tais listas devem ser propagadas por toda a infraestrutura da Rede de Distribuição de Conteúdo.
1.7.64 A CDN deverá suportar a criação de listas de bloqueio ou liberação de sub-redes.
1.7.65 A CDN deverá possuir capacidade de ocultar os websites e aplicações, restringindo o acesso dos usuários diretamente na origem, fornecendo uma camada adicional de proteção, através de uma lista definida de endereços IPs que têm permissão para se comunicar com a origem da aplicação.
1.7.66 A CDN deverá possuir recurso de defesa ativa imediata, cuja solicitação viole um grupo de ataque definido na ação “negar” será colocado em uma caixa de penalidade durante 10 minutos;
1.7.67 A CDN deverá realizar inspeção completa de corpo de requisições HTML/s, sem limitação de tamanho.
1.7.68 Para evitar falsos positivos, a CDN deverá implementar análise e inspeção de corpo de requisições, não limitando-se apenas a assinaturas.
1.7.69 A CDN deverá possuir a capacidade de criar regras de segurança customizadas para lidar com situações não incluídas no conjunto de regras padrão, a fim de corrigir vulnerabilidades rapidamente.
1.7.70 A CDN deverá possuir capacidade de proteção de segurança automática, fornecendo atualizações automaticamente, a fim de detectar e mitigar ameaças mais recentes.
1.7.71 Para reduzir a ocorrência de falsos-positivos, a ferramenta deverá possibilitar uma estrutura de categorias e assinaturas de defesa WAF através de pontuações de risco. Cada assinatura deverá ser atrelada a uma pontuação e cada categoria de assinaturas deverá ter um limite mínimo de somatória de pontos. Baseado nessa pontuação, a ferramenta deverá tomar uma ação de mitigação/bloqueio do ataque.

1.7.72 A solução de segurança deverá contar com uma inteligência de aprendizado para aplicar corretamente as assinaturas de defesa WAF sem causar falsos positivos. Estas ações deverão ser feitas a partir do aprendizado automatizado de tráfego legítimo e sem a interferência manual de configurações.

Mitigação contra ataques distribuídos de negação de serviço – DDoS

1.7.73 A CDN deverá prover serviço de defesa visando mitigar os efeitos de ataques de Distributed Denial-Of-Service (DDoS), sobre o conteúdo distribuído através dos servidores de borda, evitando que estes ataques alcancem a origem dos dados.
1.7.74 A CDN deverá mitigar ataques de forma transparente, absorvendo e bloqueando ataques de TCP/IP SYN flood nos seus endereços IP mantendo a disponibilidade do serviço e entrega das aplicações.
1.7.75 A CDN deverá fornecer o serviço de detecção e mitigação de ameaças para tráfego HTTP e HTTPS. O serviço deve continuar escalável instantaneamente e manter alta performance.
1.7.76 A CDN deverá absorver e tratar as ameaças WEB na origem do ataque, absorvendo o tráfego malicioso e criando proteção de perímetro dentro da Internet.
1.7.77 A CDN deverá possuir proteção automática de APIs nas camadas abaixo:

1.7.77.1 Deverá possuir proteção da camada de rede através de bloqueio geográfico e listas negras de IP.

1.7.77.2 Deverá possuir proteção DDoS através de controles de taxa (*rate limit*).

Gerenciamento de robôs (*botnets*)

1.7.77.3 Possuir categorias de Bots já conhecidos e pré-definidas através de uma lista gerenciada;

1.7.77.4 As categorias de Bots deverão ser atualizadas regularmente e automaticamente com a finalidade de incluir novos bots e/ou remover aqueles que desaparecem;

1.7.77.5 Detectar o acesso de robôs nos sites da contratante;

1.7.77.6 Deve identificar e mitigar botnets automaticamente com base na reputação, heurísticas e métricas de identificação de sua nocividade;

1.7.77.7 Deve ser capaz de diferenciar entre as requisições legítimas realizadas por usuários humanos das requisições realizadas por bots e ataques automatizados;

1.7.77.8 Deve gerenciar de forma ativa as ameaças de bot realizando seu tratamento com base em assinaturas, comportamento, origem e possibilitando a criação de controles e regras padrões, que garantam o tratamento de no mínimo os seguintes comportamentos:

1.7.77.8.1 Verificar e mitigar bots que imitam bots conhecidos;

1.7.77.8.2 Verificar e mitigar comportamentos baseados em User-Agent, com base nos seguintes critérios:

1.7.77.8.2.1 Na assinatura do cabeçalho HTTP como anomalia no nome ou valores do cabeçalho;

1.7.77.8.2.2 Ausência de cabeçalhos (User-Agent, Accept-Language, Accept-Enconding, Cookie, Referer);

1.7.77.8.2.3 Verificação da ordem do cabeçalho e incompatibilidade de versões de navegadores populares (Firefox, Chrome, Safari, Edge);

1.7.77.9 Avaliação e detecção de ferramentas de desenvolvimento conhecidas por construir bots como rubby, java e php.

1.7.77.10 Categorizar os robôs com base em suas ações e no impacto na infraestrutura de serviços da contratante.

1.7.77.11 Aplicar ações de segurança para os robôs, permitindo, no mínimo, as seguintes opções:

1.7.77.11.1 Monitorar o acesso, para avaliação do tráfego;

1.7.77.11.2 Liberar o acesso;

1.7.77.11.3 Ignorar ou Pular para que continue uma avaliação adicional;

1.7.77.11.4 Bloquear o acesso e retornar código de erro HTTP 403 (acesso negado);

1.7.77.11.5 Bloquear o acesso e retornar com mensagem customizada.

Proteção DNS, solução de DNS autoritativo em nuvem (item 5 do objeto)

1.7.78 A contratada deverá prover solução em nuvem para os serviços de DNS autoritativo da contratante.

1.7.79 Os serviços fornecidos deverão ser do tipo DNSSEc (Domain Name System Security Extensions)

1.7.80 A solução deverá ter ao menos um ponto de presença para resolução de DNS no Brasil.
1.7.81 O serviço deverá prover disponibilidade de DNS 24x7x365, com nível de serviço de 99,999%.
1.7.82 O serviço deverá ser provido por uma rede anycast distribuída nos pontos de presença descritos neste Termo de Referência.
1.7.83 A Plataforma deverá prover mecanismos para eventual aceleração de resolução de nomes DNS;
1.7.84 Deverá implementar o serviço como DNS primário ou secundário, substituindo ou aumentando a infraestrutura DNS da contratante.
1.7.85 A plataforma de DNS em nuvem deve prover:

1.7.85.1 Aceleração de resolução DNS;

1.7.85.2 Proteção contra ataques DNS;

1.7.85.3 Mecanismos que possibilitem a alta disponibilidade do serviço DNS;

1.7.85.4 Mecanismos para manutenção da configuração de DNS para os sítios a serem protegidos.

1.7.86 A plataforma deverá ser compatível com DNSSEc (Domain Name System Security Extensions)
1.7.87 A contratada deverá prover interface de gerenciamento dos serviços de DNS por meio de portal em nuvem e por meio de interfaces de programação de aplicação (APIs), permitindo integrações com ferramentas da contratante.

Franquia Adicional (Item 4 do objeto)

1.7.88 A rede deve prover a infraestrutura necessária para a adequada prestação dos serviços especificados, de forma escalável, automaticamente e em tempo real, independentemente da quantidade de acessos simultâneos.
1.7.89 O painel de monitoramento deverá disponibilizar ferramenta que permita a mensuração e controle em tempo real da utilização de tráfego eventualmente transportado. A ferramenta deverá permitir a emissão de relatórios gerenciais com quantitativos e consumos por períodos da CDN.
1.7.90 Será contratada uma franquia adicional de volume de tráfego excedente, pelo período do contrato, a ser consumido após o esgotamento da liberalidade de acessos nativa da infraestrutura implantada.

Implantação da Solução

1.7.91 A implantação da solução deverá ocorrer de acordo com as atividades e cronograma do plano de implantação apresentado pela contratada e aprovado pelo Tribunal contratante.

1.8. Relação entre a demanda prevista e a quantidade adquirida

O quantitativo planejado para esta contratação consta no item 1.3 deste documento, onde são especificados com crescimento na ordem de 25%, que deverá permitir a conclusão do contrato sem nenhuma intercorrência.

1.9. Considerações sobre os preços.

O TRT12 é participante da licitação nacional, da qual resultou a Ata de Registro de Preços Nº 05/2022, Pregão Eletrônico nº 05/2022, gerenciada pelo TRT da 4ª Região, assinada em 16-04-2022.

Fonte 1 - Orçamento CPD - Data: 25/01/2022 (Marcador 11)

Fonte 2 - Orçamento Azion - Data: 24/01/2022 (Marcador 10)

Foram solicitados novos orçamentos contudo a empresa CPD não respondeu a nossa solicitação (marcador 21) e a empresa Azion respondeu que mantém os preços do referido orçamento (marcador 22)

Fonte 3 - Pregão Eletrônico 021/2021 - TRF 3. Data de Homologação: 13/08/2021 (Marcadores 14 e 15)

Fonte 4 - Pregão Eletrônico 041/2021 - TJ/RN. Data de Homologação: 29/12/2021 Homologação (Marcadores 12 e 13)

					Fonte 1	Fonte 2	Fonte 3
Item	Descrição	Unidade	Quant. Compra Inicial	Quantidade Total para Registro	Valor Unitário	Valor Unitário	Valor Unitário

1	Prestação de serviços de proteção de borda de rede e de alta disponibilidade através de rede dinâmica de distribuição e aceleração de conteúdo – CDN, integrada a recursos de segurança de firewall de aplicação web – WAF, mitigação contra ataques distribuídos de negação de serviço – DDoS, gerenciamento de robôs (botnets) incluindo suporte técnico, por 36 meses, para um tráfego de até 20 TB mensais	Serviço	9	20	1.970.263,44	1.710.128,16	-
2	Prestação de serviços de proteção de borda de rede e de alta disponibilidade através de rede dinâmica de distribuição e aceleração de conteúdo – CDN, integrada a recursos de segurança de firewall de aplicação web – WAF, mitigação contra ataques distribuídos de negação de serviço – DDoS, gerenciamento de robôs (botnets) incluindo suporte técnico, por 36 meses, para um tráfego de até 40 TB mensais	Serviço	0	3	2.877.631,200	2.375.969,04	3.380.611,32
3	Prestação de serviços de proteção de borda de rede e de alta disponibilidade através de rede dinâmica de distribuição e aceleração de conteúdo – CDN, integrada a recursos de segurança de firewall de aplicação web – WAF, mitigação contra ataques distribuídos de negação de serviço – DDoS, gerenciamento de robôs (botnets) incluindo suporte técnico, por 36 meses, para um tráfego de até 50 TB mensais	Serviço	3	4	3.500.394,12	2.689.233,12	-
4	Franquia de tráfego adicional (TB)	TB	2346	8795	2.359,80	1.400,00	2.850,00
5	Proteção DNS	Zonas DNS	21	69	117.276,48	43.524,00	250.200,00
VALOR TOTAL COMPRA INICIAL					***R$ 36.232.450,20***	***R$ 27.657.256,80***	***R$ 11.940.300,00***
VALOR TOTAL REGISTRO DE PREÇOS					***R$ 90.886.257,00***	***R$ 67.403.558,80***	***R$ 52.471.383,96***

As fontes 3 e 4 foram utilizadas parcialmente para pesquisa de preço pois não tem a mesma quantidade de franquia do objeto desta contratação, mas servem de parâmetro para validação do preço praticado. Segue análise do Valor do terabyte(TB) da franquia, de acordo com os preços encontrados:

Fonte	Quantidade contratada TB/mês	Valor	Quantidade de meses	Valor do terabyte/ mês R$
1	20	R$ 1.970.263,44	36	R$ 2736,47
2	20	R$ 1.710.128,16	36	R$ 2375,178
3	40	R$ 3.380.611,32	36	R$ 2347,64
4	12	R$ 873.618,90	30	R$ 2426,71
média total TB/mes				R$ 2471,49

Abaixo segue tabela com valores da Ata de Registro de Preço 05/2022 do TRT 04:

LOTE ÚNICO					
Item	Especificação	QTDE	Unid.	VALOR UNITÁRIO R$	VALOR TOTAL
1	Prestação de serviços de proteção de borda de rede e de alta disponibilidade através de rede dinâmica de distribuição e aceleração de conteúdo - CDN, integrada a recursos de segurança de firewall de aplicação web - WAF, mitigação contra ataques distribuídos de negação de serviço - DDoS, gerenciamento de robôs (botnets) incluindo suporte técnico, por 36 meses, para um tráfego de até 20 TB mensais.	1	Serviço	R$ 265.992,32 R$ 369,43 o Terabyte (TB)/mês	R$ 265.992,32
4	Franquia de tráfego adicional (TB) / mês	10 TB / mês	TB	R$ 433,79	R$ 433,79 (conforme uso)
5	Proteção DNS	2	Zonas DNS	R$ 15.475,60	R$ 30.951,20

Podemos verificar que os preços obtidos na Ata de Registro de Preços Nº 5/2022, gerenciada pelo TRT da 4ª Região, estão bem abaixo dos valores de mercado e orçados, para o Item 1 o valor do o Terabyte (TB)/mês é de R$ 369,43, já a média pesquisada foi R$ 2.471,49 Terabyte (TB)/mês. Os outros preços encontram-se dentro do padrão de mercado e como a ata exige a contratação de todos os serviços juntos, razão pela qual esta equipe reafirma a intenção de

utilização da Ata. Os itens 2 e 3 não constam da presente tabela pois o TRT 12º, não se inscreveu nos quantitativos.

1.10 Avaliação das necessidades de adequação do ambiente para viabilizar a execução contratual.

Item	Característica	O que precisa ser feito	Responsável
01	Infraestrutura tecnológica (equipamentos, redes, link, etc..)	Não há necessidade de instalação de equipamentos da solução adquirida no datacenter principal do TRT12.	
02	Infraestrutura elétrica	Não há necessidade de adequação da infraestrutura elétrica	
04	Espaço Físico	Nenhum dos equipamentos previstos na demanda necessitarão de adequação do espaço físico para seu funcionamento.	
05	Mobiliário	Não há necessidade de adequação do mobiliário	
06	Impacto ambiental	Não haverá impacto ambiental.	
07	Liberação de acesso	Permissões de acesso a funcionários da contratada para fazer a instalação nas dependências do tribunal.	Equipe da SEGINFO
08	Outros	Não há conhecimento de outras necessidades de adequação além das já comentadas	

1.11. Disponibilidade Orçamentária

Demanda prevista no item 15903 do PAC. Os recursos previstos para viabilizar a execução contratual serão descentralizados pelo CSJT.

O valor estimado para a contratação no orçamento de 2022 de setembro/22 até dezembro/22 é de R$ 31.274,21, sendo:

Custeio - GND3: R$ 31.274,21

2. Capítulo II - SUSTENTAÇÃO DO CONTRATO

2.1. Recursos Necessários à Continuidade do Negócio Durante e Após a Execução do Contrato

2.1.1. Recursos Materiais.

Os recursos materiais necessários já estão contemplados no item 1.10.

2.1.2 Recursos Humanos

Os recursos humanos para viabilizar o gerenciamento e fiscalização da solução serão os servidores do quadro permanente do TRT12 lotados no Serviço de Infraestrutura de TIC (SEINFRA) e Divisão de Segurança da Informação e Proteção de Dados (SEGINFO). Já a equipe de técnicos especialistas necessários para instalação, suporte e treinamento da solução são de responsabilidade da contratada.

2.2. Estratégia de Continuidade Contratual

Para o caso de interrupção contratual por problemas com fornecedores antes da entrega/atualização dos produtos, o gestor do contrato deve informar à administração do Tribunal para a aplicação das sanções previstas.

2.3. Ações de transição e encerramento contratual

Caso não haja intercorrências, o encerramento do contrato irá restringir o acesso do Tribunal ao objeto da contratação.

Permanecendo a necessidade de uso do produto, o gestor do contrato deverá protocolar nova demanda para aquisição até 90 (noventa) dias antes do encerramento do contrato.

2.3.1. Entrega das versões finais dos produtos

A contratada deve disponibilizar, via site na internet, todas as licenças e manuais dos produtos nas versões mais atuais, do momento do fornecimento até o encerramento da vigência do contrato.

Além disso, a contratada deve fornecer acesso a todas as atualizações que forem produzidas dentro do período do contrato de suporte, independentemente de solicitação do TRT12. Fica a critério do Tribunal, contudo, a instalação dessas atualizações em seu ambiente computacional, em função dos riscos que possam decorrer da alteração de versões de produção.

2.3.2. Transferência final de conhecimentos

Será de inteira responsabilidade da CONTRATADA, sem ônus adicional para a TRT 12, garantir o repasse bem sucedido de todas as informações necessárias para a continuidade dos serviços pelo TRT 12 ou empresa por este designada, sendo realizado na implantação da solução, durante o treinamento ou na vigência do contrato.

2.3.3. Devolução de recursos materiais

Não é aplicável.

2.3.4. Revogação de perfis de acesso

Todos os eventuais acessos criados para os colaboradores da contratada devem ser formalmente solicitados com descrição detalhada das funções que os trabalhadores executarão. Após o término das atividades, o Tribunal revogará todos os acessos utilizados durante o processo de implantação.

2.4. Estratégia de independência

Existem várias soluções no mercado que atendem os requisitos. A solução a ser contratada é proprietária e não customizada. Pode ser fornecida por pelo menos 3 fornecedores diferentes, porém não há integração entre as soluções. Apenas relatórios, guias de implantação, informações do ambiente e dados extraídos das estações e servidores do TRT 12 serão propriedade do Tribunal. Sendo assim, caso

ao fim do contrato o Tribunal opte por mudar de solução, deverá analisar custos, funcionalidades e poderá fazê-lo.

2.4.1. Formas de transferência do conhecimento.

2.4.1.1. A CONTRATADA deverá entregar ao Tribunal toda e qualquer documentação gerada em meio magnético e/ou físico em função da prestação de serviços.

2.4.1.2. As informações geradas pela CONTRATADA estarão disponíveis em ferramentas e em documentos conforme as definições e padrões utilizados pelo Tribunal.

2.4.1.3. Deverá haver transferência de conhecimento da CONTRATADA para o Tribunal em relação às tecnologias utilizadas na prestação de serviços para melhor eficiência, eficácia, efetividade e economicidade com sua adoção.

2.4.1.4. Será de inteira responsabilidade da CONTRATADA, sem ônus adicional para o Tribunal, garantir o repasse bem sucedido de todas as informações necessárias para a continuidade dos serviços pelo órgão ou empresa por este designada.

2.4.1.5. O apoio na fase de implantação, pela transferência técnica, no uso das soluções implantadas pela CONTRATADA, deverá ser viabilizado, sem ônus adicionais para o Tribunal, e baseado em documentos funcionais, técnicos e/ou manuais específicos da solução desenvolvida. O cronograma e horários dos eventos deverão ser previamente aprovados pelo órgão.

2.4.2. Direitos de Propriedade Intelectual (Lei nº 9.610, de 19 de fevereiro de 1998)

Não há previsão de desenvolvimento de qualquer novo conhecimento, código ou outro tipo de conhecimento que se converta em propriedade intelectual.

2.4.3. Outras formas de minimizar dependência

A equipe de fiscalização técnica se manterá atenta à qualidade das entregas para garantia da independência do fornecedor.

3. Capítulo III - ESTRATÉGIA DA CONTRATAÇÃO

3.1. Natureza do objeto

Trata-se de aquisição de serviço comum, cujos padrões de desempenho e qualidade foram objetivamente definidos pelo edital, por meio de especificações usuais no mercado.

3.2. Parcelamento do objeto

Conforme Edital do Pregão Eletrônico nº 05/2022 do TRT da 4ª Região, marcador 17

3.3. Modalidade e tipo de licitação (justificativa)

Verifica-se que o objeto pretendido é oferecido por alguns fornecedores no mercado de TIC, e apresenta características padronizadas e usuais. Assim, pode-se concluir que o objeto é comum e, portanto, a melhor opção de modalidade foi a utilizada pelo TRT da 4ª Região: Pregão eletrônico do tipo menor preço.

Esta equipe sugere adesão à Ata de Registro de Preços Nº 05/2022, resultante do Pregão Eletrônico nº 05/2022, gerenciada pelo TRT da 4ª Região.

3.4. Classificação Orçamentária.

Demanda prevista no item 15903 do PAC. Os recursos previstos para viabilizar a execução contratual serão descentralizados pelo CSJT.

O valor estimado para a contratação no orçamento de 2022 de setembro/22 até dezembro/22 é de R$ 31.274,21, sendo:

Custeio - GND3: R$ 31.274,21

Item 1. Serviço: 33904019 – Computação Em Nuvem - Software Como Serviço-SaaS.

Item 2. Serviço: 33904019 – Computação Em Nuvem - Software Como Serviço-SaaS.

Item 3. Serviço: 33904019 – Computação Em Nuvem - Software Como Serviço-SaaS.

Item 4. Serviço: 33904019 – Computação Em Nuvem - Software Como Serviço-SaaS.

Item 5. Serviço: 33904019 – Computação Em Nuvem - Software Como Serviço-SaaS.

3.6. Equipe de apoio à contratação

Este papel será desempenhado pela equipe de planejamento da contratação.

3.7. Equipe de gestão da contratação

a) Gestor do Contrato e Fiscal Demandante: Serão indicados nominalmente pelo Diretor da Secretaria demandante. A indicação será efetuada no despacho de aprovação dos Estudos Preliminares e Projeto Básico.

b) Fiscal Técnico: Será indicado nominalmente pelo Diretor da SEGINFO, no despacho de aprovação dos Estudos Preliminares e Projeto Básico.

c) Fiscal Administrativo: Será indicado nominalmente pelo Diretor da Secretaria Administrativa e Financeira, por despacho ao determinar a abertura de procedimento administrativo.

4. Capítulo IV - ANÁLISE DE RISCOS

4.1. Riscos da Solução contratada não ter sucesso (riscos do produto/serviço)

RISCO 1	Baixa qualidade da especificação técnica
PROBABILIDADE	BAIXA

DANOS E IMPACTO	Não alcançar o objetivo da aquisição.

AÇÕES A SEREM TOMADAS PARA REDUZIR OU ELIMINAR OS RISCOS	**RESPONSÁVEL**
● Capacitar a equipe que elabora a especificação; ● Estudar soluções disponíveis no mercado; ● Analisar processos semelhantes dos órgãos públicos;	SETIC
DEFINIÇÃO DAS AÇÕES DE CONTINGÊNCIA A SEREM TOMADAS CASO OS RISCOS DE CONCRETIZEM	**RESPONSÁVEL**
● Corrigir erros de especificação técnica no Planejamento da Aquisição; ● Reiniciar o processo de Aquisição. ● Cancelar o processo de Aquisição;	SETIC/SELCO

RISCO 2	Desempenho insuficiente da solução
PROBABILIDADE	MÉDIA
DANOS E IMPACTO	Solução não prover nível adequado de proteção do ambiente tecnológico

AÇÕES A SEREM TOMADAS PARA REDUZIR OU ELIMINAR OS RISCOS	**RESPONSÁVEL**
● Elaborar um plano de implantação da solução robusto, contemplando todas as fases e ações necessárias para a correta configuração e parametrização da solução; ● Correta configuração da solução; Atuação em conjunto entre equipe técnica da contratada e contratante;.	Divisão de Segurança da Informação e Proteção de Dados

DEFINIÇÃO DAS AÇÕES DE CONTINGÊNCIA A SEREM TOMADAS CASO OS RISCOS DE CONCRETIZEM	RESPONSÁVEL
● Revisão das configurações da solução junto ao provedor de serviço gerenciado; ● Realinhamento das ações junto à contratada;	Divisão de Segurança da Informação e Proteção de Dados

5. Capítulo V - ASSINATURAS

Florianópolis, 14 de setembro de 2022

Equipe de Planejamento da Contratação

Integrante Demandante:

Nome: Valdir Luiz da Cunha
Cargo: Diretor da Secretaria da Tecnologia da Informação e Comunicação - SETIC
E-mail: valdir.cunha@trt12.jus.br

Integrante técnico:

Nome: Arthur Fernando Dellagiustina Lago
Cargo: Diretor da Divisão de Segurança da Informação e Proteção de Dados - SEGINFO
E-mail: arthur.lago@trt12.jus.br

Substituto:

Nome: Marcus Vinicius Mattos
Cargo: Técnico Judiciário
Email: marcus.mattos@trt12.jus.br

Integrantes administrativos:

Nome: Sérgio Moritz
Cargo: Analista Judiciário
E-mail: sergio.moritz@trt12.jus.br

Substitutos:

Nome: ARILDO DISARÓ FILHO
Cargo: Técnico Judiciário
Email: arildo.filho@trt12.jus.br