TERMO DE REFERÊNCIA

1 OBJETO

1.1 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 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 Detalhamento dos Bens e Serviços que compõem a Solução:

Item	Descrição	Unidade	Quantidade Registro de Preços
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	12
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	2
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	1
4	Franquia de tráfego adicional (TB)	TB	4860
5	Proteção DNS	Zonas DNS	35

1.3 Detalhamento das quantidades por órgão participante:

Item	Descrição	Unidade	TRT 1	TRT 4	TRT 5	TRT 7	TRT 11	TRT 12	TRT 13	TRT 14	TRT 15	TRT 16	TRT 17	TRT 18	TRT 20	TRT 22	TRT 24
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	0	0	1	1	1	1	1	1	0	1	1	1	1	1	1
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	1	0	0	0	0	0	0	1	0	0	0	0	0	0

Item	Descrição	Unidade	TRT 1	TRT 4	TRT 5	TRT 7	TRT 11	TRT 12	TRT 13	TRT 14	TRT 15	TRT 16	TRT 17	TRT 18	TRT 20	TRT 22	TRT 24
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	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	Franquia de tráfego adicional (TB)	TB	1440	180	180	180	180	180	180	180	720	180	180	540	180	180	180
5	Proteção DNS	Zonas DNS	4	5	2	2	2	2	1	2	3	2	2	3	1	2	2

2 FUNDAMENTAÇÃO

2.1 A contratação destina-se a aumentar a segurança da borda de rede do Tribunal, provendo uma maior visibilidade e controle do tráfego com a Internet, e assegurar o desempenho efetivo dos serviços frente às variações de demandas de acessos ocasionados muitas vezes por tentativas de ataques ou uso excessivo de robôs.

2.2 Os demais elementos pertinentes que fundamentam a presente contratação fazem parte dos estudos técnicos preliminares constantes nos seguintes documentos:

2.2.1 Documento de Oficialização da Demanda;

2.2.2 Análise de Viabilidade da Contratação;

2.2.3 Plano de Sustentação;

2.2.4 Estratégia da Contratação;

2.2.5 Análise de Riscos.

3 ESPECIFICAÇÃO TÉCNICA

3.1 Disposições gerais:

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

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

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

3.1.4 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.

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

3.1.5.1 A menor fração de tráfego adicional será de 1 GB

3.1.6 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.

3.1.7 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.

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

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

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

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

3.1.10 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, bem como ao disposto em Payment Card Industry Data Security Standard (PCI DSS).

3.1.11 Para garantir segurança e agilidade na gestão, toda a solução deverá ser do mesmo fabricante e possuir console única de gerenciamento, de forma que todas as configurações e monitorações possam ser feitas de forma centralizada. Não será permitido integração com soluções de terceiros.

3.2 Rede dinâmica de distribuição e aceleração de conteúdo – CDN

3.2.1 A CDN deverá ser descentralizada e sem ponto único de falha, com pontos de presença física distribuídos em, no mínimo, 5 unidades federativas do Brasil, para entrega de conteúdo estático ou dinâmico de forma criptografada (TLS/SSL) em todos os pontos da rede.

3.2.1.1 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.

3.2.1.2 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.

3.2.2 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.

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

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

3.2.2.3 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.

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

3.2.2.5 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.

3.2.2.6 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.

3.2.3 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).

3.2.4 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.

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

3.2.6 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.

3.2.7 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.

3.2.8 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.

3.2.9 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.

3.2.10 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.

3.2.11 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.

3.2.11.1 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.

3.2.11.1.1 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.

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

3.2.11.1.2.1 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.

3.2.11.1.2.2 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.

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

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

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

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

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

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

3.2.14 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.

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

3.2.15.1 Suporte a não armazenagem (no store)

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

3.2.16 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.

3.2.17 A CDN deverá responder a diferentes métodos HTTP, considerando, pelo menos: GET, HEAD, POST, PUT, PATCH, DELETE e OPTIONS.

3.2.18 A CDN deverá restringir para determinado site, métodos HTTP específicos, bloqueando outros métodos que não forem habilitados.

3.2.19 A CDN deverá modificar, adicionar ou remover informações do cabeçalho HTTP durante a comunicação com os datacenters de origem.

3.2.20 A CDN deverá permitir a implementação de redirecionamento HTTP otimizando a comunicação com o datacenter de origem.

3.2.21 A CDN deverá fornecer o serviço de geolocalização a nível de país, que permitirá o gerenciamento de listas de permissão e negação de acessos.

3.2.22 A CDN deverá realizar a entrega de qualquer formato e tipo de conteúdo nos protocolos HTTP 1.1 e 2.

3.2.23 A CDN deverá realizar a entrega do conteúdo em cache, mesmo que já expirado, caso a origem do Datacenter esteja inacessível.

3.2.24 A CDN deverá prover aceleração através da compressão de dados (gzip, brotli) desde que suportado pelo navegador ou dispositivo utilizado pelo usuário.

3.2.25 A CDN deverá detectar as características dos dispositivos através das informações de navegador de Internet.

3.2.26 A CDN deverá permitir a obtenção de objetos cacheados a partir de outros servidores da rede, evitando assim conexão com o datacenter de origem.

3.2.27 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.

3.2.28 A CDN deverá verificar que a requisição está sendo feita por um site autorizado a ter acesso ao conteúdo armazenado.

3.2.29 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.

3.2.30 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.

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

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

3.2.33 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:

3.2.33.1 Quais sites WEB estão sendo atacados e

3.2.33.2 O que está sendo explorado no ataque.

3.2.34 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.

3.2.35 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.

3.2.36 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.

3.2.37 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.

3.2.38 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.

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

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

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

3.2.41.1 Monitoramento de usuários por meio de injeção de JavaScript no HTML para monitorar dados de desempenho e informações do cliente;

3.2.41.2 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).

3.2.41.3 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.

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

3.2.42 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.

3.2.43 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.

3.2.44 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.

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

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

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

3.3.1 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:

3.3.1.1 Bloqueio por rede e IP;

3.3.1.2 Geolocalização;

3.3.1.3 Secure token;

3.3.1.4 Cross site scripting (XSS);

3.3.1.5 Remote file inclusion (RFI);

3.3.1.6 Directory transversal;

3.3.1.7 SQL injection.

3.3.2 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.

3.3.3 Deverá possuir proteção contra exploração de vulnerabilidade (exploit) em por meio de inspeções de regras WAF.

3.3.4 A CDN deverá tratar de maneira individualizada as requisições maliciosas direcionadas aos sites WEB da origem e bloqueá-las.

3.3.5 A CDN deverá fornecer o serviço de Geo Localização para permitir o bloqueio por país e redes indesejadas (Exemplo: rede TOR).

3.3.6 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.

3.3.7 A CDN deverá suportar a criação de listas de bloqueio ou liberação de sub-redes.

3.3.8 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.

3.3.9 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;

3.3.10 A CDN deverá realizar inspeção completa de corpo de requisições HTML/s, sem limitação de tamanho.

3.3.11 Para evitar falsos positivos, a CDN deverá implementar análise e inspeção de corpo de requisições, não limitando-se apenas a assinaturas.

3.3.12 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.

3.3.13 A CDN deverá possuir capacidade de proteção de segurança automática, fornecendo atualizações automaticamente, a fim de detectar e mitigar ameaças mais recentes.

3.3.14 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.

3.3.15 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.

3.4 Mitigação contra ataques distribuídos de negação de serviço – DDoS

3.4.1 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.

3.4.2 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.

3.4.3 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.

3.4.4 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.

3.4.5 A CDN deverá possuir proteção automática de APIs nas camadas abaixo:

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

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

3.5 Gerenciamento de robôs (*botnets*)

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

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

3.5.1.3 Detectar o acesso de robôs nos sites da contratante;

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

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

3.5.1.6 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:

3.5.1.6.1 Verificar e mitigar bots que imitam bots conhecidos;

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

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

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

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

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

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

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

3.5.1.9.1 Monitorar o acesso, para avaliação do tráfego;

3.5.1.9.2 Liberar o acesso;

3.5.1.9.3 Ignorar ou Pular para que continue uma avaliação adicional;

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

3.5.1.9.5 Bloquear o acesso e retornar com mensagem customizada.

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

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

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

3.6.3 A solução deverá ter ao menos um ponto de presença para resolução de DNS no Brasil.

3.6.4 O serviço deverá prover disponibilidade de DNS 24x7x365, com nível de serviço de 99,999%.

3.6.5 O serviço deverá ser provido por uma rede anycast distribuída nos pontos de presença descritos neste Termo de Referência.

3.6.6 A Plataforma deverá prover mecanismos para eventual aceleração de resolução de nomes DNS;

3.6.7 Deverá implementar o serviço como DNS primário ou secundário, substituindo ou aumentando a infraestrutura DNS da contratante.

3.6.8 A plataforma de DNS em nuvem deve prover:

3.6.8.1 Aceleração de resolução DNS;

3.6.8.2 Proteção contra ataques DNS;

3.6.8.3 Mecanismos que possibilitem a alta disponibilidade do serviço DNS;

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

3.6.9 A plataforma deverá ser compatível com DNSSEc (Domain Name System Security Extensions)

3.6.10 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.

3.7 Franquia Adicional (Item 4 do objeto)

3.7.1 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.

3.7.2 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.

3.7.3 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.

3.8 Implantação da Solução

3.8.1 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.

3.9 Repasse de conhecimento

3.9.1 Deve ser realizado repasse de conhecimento sobre a administração da solução para, no mínimo, 8 profissionais da contratante.

3.9.1.1 O repasse deverá ser autorizado pelo fabricante da solução, devendo ser realizado na plataforma online do fabricante ou no centro autorizado de treinamento.

3.9.1.2 Duração mínima de 24 horas, divididas em 6 dias, abordando no mínimo os seguintes aspectos:

3.9.1.2.1 Apresentação do projeto/solução implementado;

3.9.1.2.2 Estratégias de implementação da solução;

3.9.1.2.3 Procedimentos de instalação de toda solução;

3.9.1.2.4 Operação e administração de toda solução;

3.9.1.2.5 Descrição e uso das funcionalidades da solução;

3.9.1.2.6 Resolução de problemas.

3.9.1.3 Deve ser realizado em português do Brasil.

3.9.1.4 Deve ser realizado na modalidade telepresencial síncrona.

3.9.1.5 O repasse de conhecimento deverá ser realizado em até 60 dias após a assinatura do contrato.

3.9.1.6 Deve fornecer, ao término, certificado de realização para cada participante, contendo, no mínimo, nome do curso, carga horária, conteúdo programático, nome do instrutor e período de realização e em português do Brasil.

3.9.1.7 O Tribunal poderá solicitar a repetição do repasse de conhecimento caso entenda que o mesmo não atingiu os objetivos estipulados.

4 MODELO DE PRESTAÇÃO DO OBJETO

4.1 Prazos e Condições:

4.1.1 A vigência do contrato iniciará com a sua assinatura e findará 36 meses após a data de recebimento definitivo da solução, podendo ser prorrogado nos termos do artigo 57, inciso II, da Lei no 8.666/1993.

4.1.1.1 O contrato poderá ser reajustado, a cada período de doze meses, de acordo com o índice oficial aplicável.

4.1.2 No prazo máximo de 15 dias, contados da assinatura do contrato, deverá ser realizada a reunião inicial de gestão do contrato.

4.1.2.1 Deverão estar presentes na reunião o preposto e um integrante da equipe técnica da contratada. A pauta da reunião deverá abordar o planejamento detalhado da implantação da solução contratada, além das condições contratuais.

4.1.2.2 Na ocasião, a contratada deverá submeter à aprovação do Tribunal os planos de implantação da solução e de continuidade de negócio (PCN).

4.1.3 O Plano de Implantação da Solução deverá contemplar, no mínimo, o detalhamento das atividades, do respectivo cronograma detalhando as fases de implementação da solução, o contato do Gerente de Projetos e dos principais técnicos da CONTRATADA envolvidos na implementação da solução.

4.1.4 O Plano de Continuidade de Negócios (PCN), a ser executado na hipótese de encerramento contratual, deverá contemplar, no mínimo, as ferramentas, atividades e o suporte técnico necessários para o rollback das configurações e ajustes realizados para transferir o acesso aos sistemas e serviços por meio da solução, ou para viabilizar a migração para outra solução, provida pelo Tribunal ou terceirizada;

4.1.5 A implantação da solução deverá ocorrer em até 60 dias após a assinatura do contrato.

4.1.6 O repasse de conhecimento deverá ser concluído no prazo máximo de 60 dias a contar da assinatura do contrato.

4.2 Serviços de Garantia

4.2.1 A garantia será de 36 (trinta e seis) meses e terá início a partir da data de emissão do Termo de Recebimento Definitivo.

4.2.2 A CONTRATADA deve realizar, sem quaisquer custos adicionais à CONTRATANTE, a atualização de novas versões da solução implantada, decorrentes da evolução funcional ou correções dos componentes da mesma, de modo a assegurar o pleno funcionamento.

4.3 Serviços de Suporte Técnico

4.3.1 O serviço de suporte técnico compreende ações corretivas, proativas e consultivas, contemplando, no mínimo, as seguintes atividades: auxílio na configuração e administração da solução, instalação e atualização de novas versões, patches, hotfixes, esclarecimento de dúvidas e recomendação de melhores práticas.

4.3.2 Os serviços serão solicitados pela equipe técnica do Tribunal mediante abertura de chamado junto à contratada, via chamada telefônica, e-mail ou internet, devendo o recebimento dos chamados ocorrer em período integral (24x7).

4.3.3 Não haverá limite de quantidade de chamados durante a vigência do contrato.

4.3.4 A contratada deverá informar o número do chamado e disponibilizar um meio de acompanhamento do seu estado.

4.3.5 A contratada deverá emitir relatório técnico mensal contendo as seguintes informações: nº dos chamados, categoria de prioridade, descrição do problema e da solução, procedimentos realizados, data e hora da abertura e do fechamento do chamado, data e hora do início e do término da execução dos serviços, identificação do técnico da empresa.

4.3.6 Os prazos de solução dos chamados deverão atender aos seguinte critérios:

SEVERIDADE	CLASSIFICAÇÃO	PRAZO DE SOLUÇÃO
ALTA	Indisponibilidade total da solução, problema generalizado no ambiente tecnológico causado pela solução	2 horas a contar da abertura do chamado

MÉDIA	Falha, simultânea ou não, de uma ou mais funcionalidades, que não cause indisponibilidade, mas que apresente problemas de funcionamento e/ou desempenho da solução ou no ambiente tecnológico, incluindo configurações necessárias para correção de uma falha ou circunstância crítica de operação	4 horas a contar da abertura do chamado
BAIXA	Instalações, configurações, atualizações de versões, dúvidas dentre outros	5 dias a contar da abertura do chamado

5 ELEMENTOS PARA GESTÃO DO CONTRATO

5.1 Indicação da Equipe de Gestão e Fiscalização do Contrato:

Integrante	Titular	Substituto	Unidade
Gestor:	Lucas Pozatti	Ricardo Krause Kurylenko	Escritório de Segurança da Informação / Escritório de Processos
Fiscal Requisitante/Técnico:	Charles Ferreira Falcão	Carlos Costa Jordão	Escritório de Segurança da Informação
Fiscal Administrativo:	Caroline Rocha Molina	Karen de Souza Del Mauro	Seção de Apoio a Contratações de TIC

5.2 Procedimentos de Gestão e Fiscalização do Contrato:

5.2.1 O gestor do contrato ficará responsável por:

5.2.1.1 Organizar a reunião inicial;

5.2.1.2 Encaminhar alterações contratuais;

5.2.1.3 Controlar prazos e indicadores contratuais;

5.2.1.4 Atestar notas fiscais;

5.2.1.5 Tratar eventuais irregularidades constatadas na execução contratual;

5.2.1.6 Realizar o recebimento definitivo e emitir o respectivo termo;

5.2.1.7 Verificar as obrigações previstas no encerramento do contrato.

5.2.2 O Fiscal Administrativo do contrato ficará responsável por:

5.2.2.1 Participar da reunião inicial;

5.2.2.2 Conferir cumprimento de prazos contratuais;

5.2.2.3 Conferir o atendimento dos níveis de serviços contratados;

5.2.2.4 Conferir documentação exigida no contrato;

5.2.2.5 Verificar a conformidade do faturamento do objeto contratado;

5.2.2.6 Informar ao gestor do contrato qualquer irregularidade na execução do objeto ou descumprimento dos níveis de serviços contratados;

5.2.3 O fiscal requisitante do contrato ficará responsável por:

5.2.3.1 Participar da reunião inicial;

5.2.3.2 Acompanhar a execução do objeto de acordo com o contrato;

5.2.3.3 Monitorar cumprimento de prazos contratuais;

5.2.3.4 Encaminhar demandas para a contratada por meio de ordens de serviço e/ou chamados;

5.2.3.5 Aferir as entregas da execução em relação ao objeto contratado;

5.2.3.6 Atestar se os requisitos de negócio da contratação foram atendidos;

5.2.3.7 Informar ao gestor do contrato qualquer irregularidade na execução do objeto ou descumprimento dos níveis de serviços contratados.

5.2.4 O fiscal técnico do contrato ficará responsável por:

5.2.4.1 Participar da reunião inicial;

5.2.4.2 Acompanhar a execução do objeto de acordo com o contrato;

5.2.4.3 Monitorar cumprimento de prazos contratuais;

5.2.4.4 Encaminhar demandas para a contratada por meio de ordens de serviço e/ou chamados;

5.2.4.5 Aferir as entregas da execução em relação ao objeto contratado;

5.2.4.6 Atestar se os requisitos de técnicos da contratação foram atendidos;

5.2.4.7 Informar ao gestor do contrato qualquer irregularidade na execução do objeto ou descumprimento dos níveis de serviços contratados.

5.3 Deveres e Responsabilidades do Tribunal:

5.3.1 Zelar pela segurança dos softwares, evitando o manuseio por pessoas não habilitadas.

5.3.2 Proporcionar as facilidades indispensáveis à boa execução dos serviços, inclusive permitir o acesso dos técnicos do fornecedor às dependências do Tribunal onde os serviços serão executados.

5.3.3 Acompanhar e fiscalizar, sempre que entender necessário, o(s) técnico(s) da contratada em suas visitas;

5.3.4 Relatar, por escrito, com a devida comprovação, as eventuais irregularidades na prestação de serviços;

5.3.5 Sustar a execução de quaisquer trabalhos por estarem em desacordo com o especificado ou por qualquer outro motivo que caracterize a necessidade de tal medida;

5.3.6 Efetuar os pagamentos devidos.

5.4 Deveres e Responsabilidades da Contratada:

5.4.1 Indicar um preposto para o contrato, sendo este o interlocutor da contratada junto ao Tribunal para os assuntos relativos ao cumprimento das cláusulas contratuais e para participar de reuniões de acompanhamento, sempre que solicitado por este Regional.

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

5.4.3 Responder integralmente por perdas e danos que vier a causar ao Tribunal ou a terceiros em razão de ação ou omissão, dolosa ou culposa, sua ou dos seus prepostos, independentemente de outras combinações contratuais ou legais a que estiver sujeita.

5.4.4 Fornecer a seus técnicos todos os instrumentos necessários à execução dos serviços.

5.4.5 Submeter a relação dos técnicos credenciados a prestarem os serviços.

5.4.6 Responder pelas despesas relativas a encargos trabalhistas, de seguro de acidentes, impostos, contribuições previdenciárias e quaisquer outras

que forem devidas e referentes aos serviços executados por seus empregados, uma vez que os mesmos não tem nenhum vínculo empregatício com o Tribunal.

5.4.7 Responder por valores adicionais ao valor do contrato, tais como custos de deslocamento, alimentação, transporte, alojamento, trabalho em sábados, domingos, feriados ou em horário noturno, bem como qualquer outro valor adicional.

5.4.8 Comprovar sempre que solicitado a aptidão técnica exigida dos técnicos que prestarão os serviços de consultoria e suporte técnico.

5.4.9 Garantir o mais rigoroso sigilo sobre quaisquer dados, informações, documentos e especificações que venham a ter acesso em razão dos serviços prestados, não podendo, sob qualquer pretexto, revelá-los, divulgá-los ou reproduzi-los.

5.4.10 Manter, durante toda a vigência do contrato, as condições de habilitação exigidas na licitação.

5.5 Critérios de Aceitação e Cronograma Físico e Financeiro

CRITÉRIOS DE ACEITAÇÃO E CRONOGRAMA FÍSICO-FINANCEIRO				
Item	**Entrega**	**Forma de recebimento**	**Prazo**	**Percentual de pagamento**
-	Entrega do Plano de Implantação da Solução	Aprovação pela equipe técnica do Tribunal do Plano de Implantação da solução	15 dias da assinatura do contrato	-
-	Elaboração do Plano de Continuidade de Negócios (PCN)	Mediante aceite da Equipe de Gestão e Fiscalização do Contrato	15 dias após assinatura do contrato	-
1 a 3	Prestação de serviços de solução de alta disponibilidade e proteção dos ativos de negócio através de rede dinâmica de distribuição e aceleração de conteúdo	Ateste na nota fiscal	60 dias da assinatura do contrato	Pagamento mensal a contar do recebimento definitivo
4	Franquia de tráfego adicional para os itens 1 a 3	Ateste na nota fiscal	60 dias da assinatura do contrato	Pagamento mensal sob demanda a contar do

				recebimento definitivo
5	Proteção DNS para 5 zonas	Ateste na nota fiscal	60 dias da assinatura do contrato	Pagamento mensal a contar do recebimento definitivo
-	Implantação da solução	Recebimento Definitivo + ateste na nota fiscal	60 dias da assinatura do contrato	-
-	Repasse de conhecimento	Recebimento	60 dias da assinatura do contrato	-

5.6 Descontos aplicáveis por descumprimento dos níveis de serviço

5.6.1 Tendo em vista a criticidade dos ativos de negócio que farão parte da solução, o Índice de Disponibilidade do Serviço Mensal - IDSM da solução, a ser cumprido pela CONTRATADA, deverá ser de 99,999%.

5.6.2 Pelo não cumprimento do IDSM, a CONTRATADA estará sujeita a desconto calculado sobre o valor mensal do item 1, conforme abaixo:

Disponibilidade	Desconto
Entre 99,999% e 99,99%	10% sobre a fatura mensal
Entre 99,98% e 99,95%	20% sobre a fatura mensal
Entre 99,94% e 99,9%	30% sobre a fatura mensal
Abaixo de 99,9%	50% sobre a fatura mensal

5.6.3 A partir do terceiro mês consecutivo em que a disponibilidade da solução fique abaixo de 99%, a CONTRATADA estará sujeita às penalidades previstas, podendo esse fato, a critério da CONTRATANTE, ensejar a rescisão do contrato.

5.7 Propriedade, Sigilo e Restrições:

5.7.1 Na execução dos serviços, a empresa contratada cumprirá todos os padrões de segurança e regras de uso e de controle de acesso às instalações do Tribunal. A empresa contratada se compromete a manter

sigilo acerca das informações obtidas e geradas no decorrer do trabalho, mediante assinatura de Termo de Compromisso com a Segurança da Informação, conforme modelo em anexo, quando do início da prestação dos serviços.

5.7.2 Pertencerão exclusivamente ao Tribunal os direitos relativos aos produtos desenvolvidos e elaborados durante a vigência do Contrato, sendo vedada sua reprodução, transmissão e/ou divulgação sem o seu respectivo consentimento.

5.7.3 Durante a execução dos serviços, a Contratada deverá observar as Políticas de Controle de Acesso definidas pelo Tribunal.

5.8 Transferência de Conhecimento:

5.8.1 A transferência de conhecimento ocorrerá na implantação e repasse de conhecimento da solução.

5.9 Mecanismos Formais de Comunicação

5.9.1 O mecanismo formal de comunicação utilizado no contrato será o e-mail, conforme detalhamento a seguir:

Assunto	E-mail
Envio de notas fiscais e informações sobre faturamento	setic.contratos@trt4.jus.br
Informações técnicas	lucas.pozatti@trt4.jus.br

5.9.2 Será realizada uma reunião inicial do contrato com a participação da contratada, do gestor e fiscais do contrato.

6 ESTIMATIVA DE PREÇO E ADEQUAÇÃO ORÇAMENTÁRIA

6.1 O valor da contratação foi estimado com base no menor preço obtido no mercado.

6.2 O quadro a seguir refere-se a análise comparativa entre os preços de um orçamento obtido no mercado e um contrato similar de outro órgão público.

6.3 Indica-se como fonte de recursos para a contratação o Programa de Apreciação de Causas da Justiça do Trabalho, classificando as despesas conforme discriminado no quadro a seguir.

						Fonte 1	Fonte 2	Fonte 3
Item	Descrição	Unidade	Classificação da Despesa	Qtd Compra Inicial	Qtd 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	33904019	0	12	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	33904019	0	2	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	33904019	0	1	3.500.394,12	2.689.233,12	-
4	Franquia de tráfego adicional (TB)	TB	33904019	0	4860	2.359,80	1.400,00	2.850,00
5	Proteção DNS	Zonas DNS	33904019	0	35	117.276,48	43.524,00	250.200,00
VALOR TOTAL ESTIMADO REGISTRO						***R$ 48.472.122,60***	***R$ 36.290.049,12***	**-**

7 SANÇÕES APLICÁVEIS

7.1 Em caso de descumprimento do objeto, a contratada ficará sujeitas às sanções a seguir, sem prejuízo das demais sanções administrativas previstas no Edital.

7.1.1 Na hipótese de atraso na entrega do Plano de Implantação, fica estabelecido o percentual de 0,05% sobre o total adjudicado, a título de multa, por dia de atraso, até o limite de 5% do valor total da contratação.

7.1.2 Na hipótese de atraso na conclusão da execução do Plano de Implantação da Solução, fica estabelecido o percentual de 0,1% sobre o valor dos itens em atraso, a título de multa, por dia de atraso, até o limite de 5% do valor total da contratação.

7.1.3 Na hipótese de atraso na entrega do Plano de Continuidade de Negócios (PCN), fica estabelecida multa de 0,1% sobre o valor adjudicado, por dia de atraso, até o limite de 5% do valor total da contratação.

7.1.4 Na hipótese de atraso na realização do repasse de conhecimentos, fica estabelecido o percentual de 0,1% sobre o valor do item 4, a título de multa, por dia de atraso, até o limite de 5% do valor total da contratação.

7.1.5 Na hipótese de atraso na solução dos chamados de suporte de severidade alta, fica estabelecido o percentual de 0,5% sobre o valor da mensalidade do item 1, a título de multa, por hora de atraso, até o limite de 5% do valor total da contratação.

7.1.6 Na hipótese de atraso na solução dos chamados de suporte de severidade média, fica estabelecido o percentual de 0,2% sobre o valor mensalidade do item 1, a título de multa, por hora de atraso, até o limite de 5% do valor total da contratação.

7.1.7 Na hipótese de atraso na solução dos chamados de suporte de severidade baixa, fica estabelecido o percentual de 0,1% sobre o valor mensal do item 1, por dia de atraso, até o limite de 5% do valor total da contratação.

8 FORMA DE SELEÇÃO DO FORNECEDOR

8.1 O objeto da contratação pretendida possui requisitos de desempenho e qualidade objetivamente definidos por meio de especificações usuais de

mercado, razão por que se entende adequada a utilização do Pregão eletrônico.

8.2 Considerando o interesse de outros órgãos no certame, a contratação será realizada mediante Ata de Registro de Preços com a participação dos interessados, visando a economia de escala.

Será considerada vencedora a empresa que apresentar, além dos requisitos exigidos no Termo de Referência, a proposta com o menor preço global.

8.3 O licitante de menor lance deverá apresentar, juntamente com a proposta comercial, documento(s) técnicos contendo a(s) especificação(ões) técnica(s) detalhada(s) do(s) serviço(s) incluso(s) na solução ofertada, tais como folders, catálogos ou manuais.

9 CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

9.1 Requisitos de Seleção do Fornecedor:

9.1.1 A empresa a ser contratada deverá possuir qualificação e experiência compatíveis com a complexidade do objeto, mediante apresentação da documentação que segue:

9.1.1.1 Comprovar ter fornecido serviço de rede dinâmica de distribuição e aceleração de conteúdo – CDN integrada a recursos de segurança de firewall de aplicação web – WAF e mitigação de ataques de negação de serviço – DDoS com tráfego de no mínimo 15 TB mensais.

9.1.1.2 Comprovar ter fornecido serviço de rede dinâmica de distribuição e aceleração de conteúdo – CDN integrada a recursos de gerenciamento de robôs (botnets) com tráfego no mínimo de 15 TB mensais.

9.1.1.3 Comprovar ter fornecido serviço de proteção compatível com DNSSEC para no mínimo 2 zonas.

9.1.2 A organização emitente do atestado de capacidade técnica deverá ser usuário da solução fornecida, não sendo aceitos atestados emitidos por quaisquer intermediários.

9.1.3 Será aceito somatório de atestados desde que pertencentes a contratos executados simultaneamente, haja vista que a execução

sucessiva de objetos de pequena dimensão não capacita a empresa para a execução de objetos maiores.

Equipe de Planejamento da Contratação	
Documento assinado digitalmente LUCAS POZATTI Integrante Requisitante	*Documento assinado digitalmente* CHARLES FERREIRA FALCÃO Integrante Técnico
Documento assinado digitalmente WOLMAR AUGUSTO COZUBEK MALLET Integrante Administrativo da Secretaria de Administração	*Documento assinado digitalmente* RICARDO KRAUSE KURYLENKO Integrante Administrativo da Secretaria de Tecnologia da Informação e Comunicações

Anexo I

TERMO DE COMPROMISSO COM A SEGURANÇA DA INFORMAÇÃO

A empresa _____, parte CONTRATADA no contrato___/____, neste ato representado pelo(a) Sr.(a)_____, portador(a) da CI/RG n.º _____ e do CPF nº _____, compromete-se, por intermédio do presente termo, a não divulgar sem prévia autorização informações confidenciais pertencentes ou custodiadas pelo **TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO (TRT)** às quais tiver acesso em decorrência da prestação do objeto do citado contrato, em conformidade com as seguintes cláusulas e condições:

CLÁUSULA PRIMEIRA: Consideram-se informações confidenciais aquelas referentes a dados pessoais e dados pessoais sensíveis existentes no ambiente tecnológico ou físico do TRT ou por ele contratado, bases de dados, topologias, planos, políticas, processos, códigos-fonte, serviços e sistemas tecnológicos vinculados ao TRT.

§ 1º Em relação aos dados pessoais e dados pessoais sensíveis do TRT, a CONTRATADA deverá realizar o tratamento de acordo com o disposto na Lei Geral de Proteção de Dados Pessoais (LGPD) com a Política de Proteção e Privacidade de Dados Pessoais do TRT.

§ 2º – Em caso de dúvida acerca da confidencialidade de determinada informação, a CONTRATADA deverá tratar a mesma sob sigilo até que venha a ser autorizada por escrito pelo TRT a tratá-la diferentemente. De forma alguma se interpretará o silêncio do TRT como a liberação do compromisso de manter o sigilo da informação.

§ 3º Excluem-se das disposições desta Cláusula informações que já estiverem comprovadamente disponíveis ao público em geral de qualquer forma que não em decorrência de sua revelação pela CONTRATADA.

CLÁUSULA SEGUNDA: A CONTRATADA concorda que as informações às quais terá acesso serão utilizadas exclusivamente no desempenho das atividades necessárias para execução do objeto contratado, em conformidade com o presente TERMO.

CLÁUSULA TERCEIRA: A CONTRATADA obriga-se a conhecer e observar a Política de Segurança da Informação disponível no site do TRT.

CLÁUSULA QUARTA: A CONTRATADA compromete-se a aplicar boas práticas de mercado relacionadas à segurança da informação (como, por exemplo, ABNT NBR 27002:2019, CIS *Controls*, OWASP, NIST *Cybersecurity Framework*, dentre outras), pertinentes ao serviço prestado, para garantir a segurança do seu ambiente tecnológico de forma a atender os Acordos de Níveis de Serviços (ANS) e os Acordos de Nível Operacional (ANO) estabelecidos em contrato, bem como garantir a proteção da confidencialidade, integridade e disponibilidade das informações do TRT que vierem a ser tratadas em seu ambiente tecnológico.

CLÁUSULA QUINTA: A CONTRATADA determinará a todos os seus representantes - assim considerados, diretores, administradores, sócios, empregados, prepostos, agentes, colaboradores e prestadores de serviço a qualquer título (incluindo consultores e assessores) que estejam, direta ou indiretamente, envolvidos com a prestação de serviços - a observância do presente Termo, adotando todas as precauções e medidas para que as obrigações oriundas do presente instrumento sejam efetivamente observadas.

CLÁUSULA SEXTA: Caso a CONTRATADA seja obrigada, em decorrência de intimação de autoridade judiciária ou fiscal, a revelar quaisquer informações, notificará por escrito ao TRT imediatamente acerca da referida intimação, de forma a permitir que o TRT possa optar entre interpor a medida cabível contra a ordem judicial ou administrativa ou consentir, por escrito, com a referida revelação.

CLÁUSULA SÉTIMA: A CONTRATADA obriga-se a informar imediatamente ao TRT qualquer violação das regras de sigilo ora estabelecidas que tenha ocorrido por sua ação ou omissão, independentemente da existência de dolo, bem como de seus empregados, prepostos e prestadores de serviço.

CLÁUSULA OITAVA: A CONTRATADA obriga-se a informar imediatamente ao TRT a ocorrência de incidentes, tecnológicos ou não, que possam comprometer (ou possam ter comprometido) a confidencialidade, integridade ou a disponibilidade das informações do TRT que são tratadas em seu ambiente tecnológico ou o cumprimento de ANS e ANO, bem como as medidas adotadas para contenção, tratamento, resposta e erradicação dos incidentes.

CLÁUSULA NONA: O descumprimento de quaisquer das cláusulas do presente Termo acarretará a responsabilidade civil e criminal dos que, comprovadamente, estiverem envolvidos no descumprimento ou violação.

Porto Alegre, ___ de _____ de 20__.

_____

Assinatura do Representante Legal