CPD Informática
Em Brasília desde 1974

ANEXO V

CARTA DE APRESENTAÇÃO DA PROPOSTA COMERCIAL

CONCORRÊNCIA Nº 13746/2022

CPD - CONSULTORIA, PLANEJAMENTO E DESENVOLVIMENTO DE SISTEMAS LTDA, neste ato representada por seu representante legal Sr.(a). Pedro Carvalho Franco de Abreu, vem pela presente apresentar a Proposta Comercial, exigida por força do disposto no item 7 e respectivos subitens do Edital para o processo de licitação acima mencionado do Serviço Nacional de Aprendizagem:

ITEM	DESCRIÇÃO	UNIDADE	QTD	MESES	VALOR MENSAL	VALOR TOTAL
1	Prestação de serviços de solução de alta disponibilidade e proteção dos ativos de negócio 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 e gerenciamento de robôs (botnets) por meio de computação em nuvem na modalidade software as a service – SasS, incluindo os serviços de configuração, ativação, serviços gerenciados e suporte técnico **AKAMAI AAP+DSA***	Terabytes/ Mês	60 TB/mês	24	R$ 88.475,67	R$ 2.123.416,08
2	Franquia Adicional	Terabytes	300 TB		-	R$ 283.731,00
3	Proteção DNS em nuvem para 1 (uma) zona sp.senac.br **AKAMAI Edge DNS**	Zona DNS/Mês	1 Zona/mês		R$ 1.531,70	R$ 36.760,80
4	Transferência de conhecimento	Unitário	1	-	-	R$ 13.547,84
VALOR TOTAL: R$ 2.457.455,72						
VALOR MENSAL (itens 1 e 3): R$ 90.007,37						
VALOR PARCELA ÚNICA (treinamento): R$ 13.547,84						

**Os valores informados estão com todos os impostos inclusos.*

ESPECIFICAÇÕES TÉCNICAS DETALHADAS (DESCRIÇÃO DETALHADA)

*Estão inclusos na oferta:

App & API Protector

Web Application Firewall and API protection

Application DDoS

API Discovery

BOT Mitigation and Visibility

https://www.akamai.com/pt/resources/product-brief/app-and-api-protector-product-brief

Site Shield - https://techdocs.akamai.com/site-shield/docs

SIEM Integration - https://techdocs.akamai.com/siem-integration/docs

Dynamic Site Accelerator - https://techdocs.akamai.com/start/docs/setup-dynamic-site-accelerator

Data Stream 2 - https://techdocs.akamai.com/datastream2/docs

NetStorage - https://www.akamai.com/pt/resources/product-brief/netstorage-product-brief

Edge DNS - https://www.akamai.com/resources/product-brief/edge-dns-product-brief

Mpulse - https://www.akamai.com/pt/products/mpulse-real-user-monitoring

Requisitos de Qualidade - https://www.akamai.com/pt/legal/compliance

Implementação e Suporte Gerenciado CPD + Akamai

Observações:

1) O item Franquia adicional apenas será tarifado mediante a solicitação pelo Senac (sob demanda), conforme disposto no Termo de Referência, sendo, desta forma, pago com base no consumo mês.

2) Validade da Proposta: 90 (noventa) dias;

Dados da empresa que efetuará o faturamento:

Razão Social: CPD - CONSULTORIA, PLANEJAMENTO E DESENVOLVIMENTO DE SISTEMAS LTDA

Endereço: Setor de Autarquias Sul Quadra 05, Bloco "N", nº 07, Salas 1113 a 1122 – Edifício OAB – Asa Sul – Brasília/DF – CEP: 70.070-913

CNPJ/MF sob o nº 00.395.228/0001-28

Inscrição Estadual: sob o n. 07.322.114/001-33

Contato: Pedro Abreu; Fone: (61) 2104.3200; E-Mail: Pedro.Abreu@CPD.com.br; contato@cpd.com.br

Brasília, 26 de abril de 2022.

PEDRO CARVALHO FRANCO DE ABREU
PROCURADOR/REPRESENTANTE LEGAL
Executivo de Negócios
RG: 2403732 – SSP-DF
CPF: 029.326.551-83

ESPECIFICAÇÕES TÉCNICAS

Plataforma de Rede de Distribuição de Conteúdo e Firewall de Aplicação

A CDN descentralizada e sem ponto único de falha, com servidores distribuídos em, no mínimo, 12 (Doze) unidades federativas do Brasil, para entrega de conteúdo estático ou dinâmico de forma criptografada (TLS/SSL) em todos os pontos da rede.

Cada datacenter possui servidores de distribuição de conteúdo e segurança em número suficiente para manter o SLA de 99,99999% de disponibilidade.

A CDN possui um algoritmo de roteamento dinâmico que caso algum data center fique indisponível o tráfego seja redirecionado sem afetar o desempenho dos serviços.

A CDN possui nativamente 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.

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

área de teste possui todas as funcionalidades do ambiente de produção, especificadas neste Termo de Referência.

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

Possível aplica a mesma configuração do ambiente de teste no ambiente de produção, diretamente na interface de gerência.

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

A solução permite 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.

A CDN faz 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).

A CDN 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.

A CDN disponibiliza no mínimo 5GB (cinco gigabytes) de espaço em storages distribuídos em sua rede para receber arquivos estáticos que poderão ser utilizados em campanhas publicitarias ou outra finalidade a critério do Senac;

Os storages permite conexões pelos protocolos FTP, FTPS, SFTP, SCP, RSYNC e RSYNC sobre SSH;

Os dados em storage na nuvem serão replicados automaticamente para manter a disponibilidade dos dados.

A Contratada proverá aceleração e proteção para até 5 (cinco) URLs pertencentes ao Senac, registradas sob domínio sp.senac.br

A CDN provê 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.

A CDN garante 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.

A CDN propaga as mudanças nas listas de liberação e bloqueio em até 15 minutos, permitindo assim a resposta a incidentes de segurança através da infraestrutura da Contratada.

A CDN realiza a expiração de conteúdo (purge) por URL, com suporte a wildcard, em toda a rede, em um prazo máximo de 5 segundos.

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

A CDN acelera 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.

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

Após a configuração dos certificados, serão 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.

Os Certificados Digitais A1 SSL/TLS para Servidor Web terão as seguintes especificações:

Os certificados emitidos serão 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.

Todos os certificados emitidos possuem 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.

A Contratada manterá o certificado válido durante todo o período do contrato.

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

A fornecedora possui a capacidade de configuração das cifras e da versão de TLS utilizadas pelo Senac.

Possui validação da organização emissora do certificado digital, incluindo os dados do Senac, conforme o caso, no certificado digital.

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

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

A CDN permite 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.

A CDN possui os seguintes recursos para a gestão de cache:

Suporte a não armazenagem (no store)

Possui opção para ignorar cache (Bypass cache), nesse caso o conteúdo do cache não será armazenado pela CDN e as requisições serão enviadas para a origem.

A CDN permite 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.

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

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

A CDN capaz de modificar, adicionar ou remover informações do cabeçalho HTTP durante a comunicação com os Data Centers de origem.

A CDN permite a implementação de redirecionamento HTTP otimizando a comunicação com o Data Center de origem.

A CDN fornece o serviço de Geo Localização a nível de país, que permitirá o gerenciamento de listas de permissão e negação de acessos.

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

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

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

A CDN detecta as características dos dispositivos através das informações de navegador de Internet.

A CDN permite a obtenção de objetos cacheados a partir de outros servidores da rede, evitando assim conexão com o Data Center de origem.

A CDN permite 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 consulta a infraestrutura de origem e usa de meios próprios para validação das informações dos usuários.

A CDN proverá 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.

A CDN subdivide e permite 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 até 30 dias de histórico.

A CDN fornece no painel de monitoramento uma ferramenta para geração de filtros, possibilitando a criação de relatórios customizados por site e data.

A CDN disponibiliza painel de monitoramento, que permita acompanhar, o quantitativo de requisições realizadas para cada site WEB.

A CDN disponibiliza informações como: país, endereço IP, descrição da ameaça/regra que está sendo processada, método HTTP utilizado, data e hora da ocorrência. Contém ainda, informações acerca das atividades maliciosas processadas, apresentando:

Quais sites WEB estão sendo atacados e o que está sendo explorado no ataque.

A CDN apresenta no painel de monitoramento os eventos de ataques, com delay máximo de 15 minutos, as informações e permitir a consulta de até 30 dias de dados processados.

A CDN apresenta 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 apresenta 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.

A CDN apresenta 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.

A CDN disponibiliza 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.

A CDN permite o monitoramento real de navegação dos visitantes, conforme abaixo:

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

Monitora 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).

Permite 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.

Possibilita a customização da coleta para monitoramento utilizando técnicas de Label e Tagging.

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

A CDN disponibiliza os Logs das informações dos servidores para download em intervalo não superior a 1 (uma) hora.

Armazenamento de Logs e Exportação de Logs para fontes externas;

Para a análise das atividades das aplicações como desempenho, erros e eventos, fornece visibilidade em tempo real aos dados em pelo menos 10 segundos, possibilitando monitorar e visualizar a integridade das aplicações disponíveis na CDN e seus impactos nos usuários finais;

O serviço de entrega de log fornece controle sobre os fluxos de entrega de dados de registro ao vivo e em baixa latência em a cada 30 segundos, permitindo:

Criar, editar, visualizar e excluir configurações de fluxo de dados;

Coletar, agrupar e transmitir registros de log brutos para um destino escolhido em janelas de tempo selecionadas;

Parar as entregas de logs conforme necessário;

Armazenamento e retenção de dados por até 12 horas, para análise off-line e histórica;

Possibilita a integração para no mínimo as seguintes ferramentas:

Amazon S3

Armazenamento Azure

Datadog

Google Cloud Storage

Splunk

Sumo Logic

Endpoint HTTPS personalizado

Emite alertas de notificação por e-mail em caso de falhas no envio dos logs ajudando a resolver problemas quando os arquivos não forem carregados para o destino por vários motivos, como configurações de destino inválidas ou tempo limite.

Fornece controles de segurança adequadas, incluindo, mas não limitados a: restrição de acesso administrativo a todos os serviços incluídos na solução por meio de um login seguro ou autenticação de dois fatores, de modo que os serviços não podem ser utilizados por terceiros não autorizados

Fornece gerenciamento da conta, acessos de usuários, perfis de acesso, grupo de ativos (configurações, APIs) e as permissões concedidas a usuários e grupos.

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

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

Requisitos de Qualidade:

A solução está aderente aos aspectos de segurança dispostos nos seguintes instrumentos regulatórios:

Normas ISO 27002, NIST 800-53 e SOC 2 Tipo 2

Serviço de WAF para segurança e mitigação de tráfego malicioso

A CDN disponibiliza 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:

Bloqueio por rede e ip.

Geolocalização.

Secure token.

Cross site scripting (XSS).

Remote file inclusion (RFI).

Directory transversal.

SQL injection.

Gestão de robôs

Para gestão de robôs a CDN:

Possui categorias de Bots já conhecidos e pré-definidas através de uma lista gerenciada

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

Detecta o acesso de robôs nos sites do Senac;

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

Capaz de diferenciar entre as requisições legítimas realizadas por usuários humanos das requisições realizadas por bots e ataques automatizados;

Gerencia 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:

Verifica e mitiga bots que imitam bots conhecidos;

Verifica e mitiga comportamentos baseados em User-Agent, com base nos seguintes critérios:

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

Ausência de cabeçalhos (UserAgent, Accept-Language, Accept- Enconding, Cookie, Referer);

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

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

Categoriza os robôs com base em suas ações e no impacto na infraestrutura de serviços do Senac;

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

Monitora o acesso, para avaliação do tráfego;

Libera o acesso;

Ignora ou Pular para que continue uma avaliação adicional;

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

Bloqueia o acesso e retornar com mensagem customizada.

Toda a solução de segurança incluindo a solução de Gestão de robôs será do mesmo fabricante da CDN, não serão aceitas integrações com soluções de terceiros;

A solução possui proteção contra as vulnerabilidades WEB listadas no OWASP* TOP 10 (https://owasp.org/www-project-topten/), descritos abaixo:

Broken Access Control;

Cryptographic Failures;

Injection;

Insecure Design;

Security Misconfiguration;

Vulnerable and Outdated Components;

Identification and Authentication Failures;

Software and Data Integrity Failures;

Security Logging and Monitoring Failures;

Server-Side Request Forgery (SSRF).

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

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

A CDN fornece o serviço de controle de camada IP para bloqueio ou liberação de endereços IP. Tais listas serão propagadas por toda a infraestrutura da Rede de Distribuição de Conteúdo.

A CDN suporta a criação de listas de bloqueio ou liberação de sub-redes.

A CDN possui 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.

A CDN possui 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;

A CDN realiza inspeção completa de corpo de requisições HTML/s, sem limitação de tamanho.

Para evitar falso positivos, a CDN implementa análise e inspeção de corpo de requisições, não limitando-se apenas a assinaturas.

A CDN possui a capacidade de criar regras de segurança customizadas para lidar com situações não incluídas no conjunto de regras padrão afim de corrigir vulnerabilidades rapidamente.

A CDN possui capacidade de proteção de segurança automática, fornecendo atualização automaticamente afim de detectar e mitigar ameaças mais recentes.

Para reduzir a ocorrência de falsos-positivos, a ferramenta possibilita uma estrutura de categorias e assinaturas de defesa WAF através de pontuações de risco. Cada assinatura será atrelada a uma pontuação

e cada categoria de assinaturas terá um limite mínimo de somatória de pontos. Baseado nessa pontuação, a ferramenta tomará uma ação de mitigação/bloqueio do ataque.

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

A CDN proverá 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.

A CDN mitiga 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.

A CDN fornece o serviço de detecção e mitigação de ameaças para tráfego HTTP e HTTPS. O serviço continua escalável instantaneamente e manter alta performance.

A CDN absorve e tratar as ameaças WEB na origem do ataque, absorvendo o tráfego malicioso e criando proteção de perímetro dentro da Internet.

A CDN possui proteção automática de APIs nas camadas abaixo:

Proteção da camada de rede através de bloqueio geográfico e listas negras de IP

Proteção DDoS através de controles de taxa (Rate Limit) para fins de mitigação de ataques volumétricos;

Proteção contra exploração de vulnerabilidade (exploit) em por meio de inspeções de regras WAF.

Solução de DNS autoritativo em nuvem.

A Contratada proverá solução em nuvem para os serviços de DNS autoritativo do Senac.

A solução terá ao menos um ponto de presença para resolução de DNS no Brasil.

O serviço proverá disponibilidade de DNS 24x7x365, com nível de serviço de 99,99999%.

O serviço será provido por uma rede anycast distribuída nos pontos de presença descritos no Termo de Referência.

A Plataforma provê mecanismos para eventual aceleração de resolução de nomes DNS;

Será possível implementar o serviço como DNS primário ou secundário, substituindo ou aumentando a infraestrutura DNS do Senac.

A plataforma de DNS em nuvem provê:

Aceleração de resolução DNS.

Proteção contra-ataques DNS.

Mecanismos que possibilitem a alta disponibilidade do serviço DNS.

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

A Contratada proverá 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 do Senac.