CENTRAIS DE ABASTECIMENTO DE CAMPINAS S.A.
CENTRAIS DE ABASTECIMENTO DE CAMPINAS S.A
Rodovia Dom Pedro I - Bairro Barão Geral - CEP 13082-902 - Campinas - SP
Km 140,5 Pista Norte

CEASA-PRESIDÊNCIA/CEASA-A/CEASA-A-AL/CEASA-A-AL-ALC/CEASA-A-AL-ALCD

TERMO DE REFERÊNCIA

Campinas, 22 de novembro de 2023.

Contrato Nº 058/2023
Vigência do Contrato: 01/12/2023 à 30/11/2028

OBJETO

Contratação de empresa especializada para prestação de serviços de locação de firewall com gerenciamento unificado de ameaças de última geração para proteção de perímetro de rede, em cluster, contemplando o hardware, software de gerenciamento, licenciamento, instalação, configuração, treinamento e atualizações, nas dependências da CEASA Campinas, conforme condições, quantidades estimadas e exigências estabelecidas neste instrumento.

QUANTIDADES E UNIDADES

Item	Qtd	Un	Descrição
1	2	Serviço	Locação de Firewall UTM NGFW.
2	2	Serviço	Instalação e configuração de Firewall UTM NGFW.
3	1	Capacitação	Treinamento com carga horária mínima de 10 (dez) horas, ministrado por profissional certificado pelo fabricante.

JUSTIFICATIVA

Possibilitar a continuidade e aprimoramento dos processos de Segurança da Informação e proteção dos ativos de informações disponíveis na CEASA Campinas. Esta tecnologia permite que seja estabelecido um controle das entradas e saídas de informações, interligando a rede interna de computadores à internet, melhorando o controle e a segurança da rede e diminuindo as vulnerabilidades de navegação não autorizada, além da disponibilização de novos recursos, como balanceamento de links em um sistema com maior disponibilidade e tolerância a falhas. A implementação dessa solução, em relação a outras tecnologias existentes, mostra-se a mais indicada para nosso ambiente diante das seguintes características: (a) redução de complexidade e custos, pela utilização de uma solução única de segurança; (b) simplicidade operacional, evitando-se a instalação e manutenção de diversos sistemas não integrados - hardware e software; (c) eficiência com centralização do gerenciamento, pela integração dos diversos mecanismos de segurança em um único sistema; (d) agilidade na atualização de versões de software e na aplicação de regras de segurança individuais ou globais; (e) facilidade na capacitação de recursos humanos, com a necessidade de treinamento em apenas um produto; (f) melhor atendimento às normas e compliances tais como LGPD (Lei Geral de Proteção de Dados - Lei nº 13.709, de 14 de agosto de 2018), em vigor desde 2018 e Marco Civil da Internet; (g) redução de riscos de vazamento de informações e dados, assim como invasões.

RESULTADOS E BENEFÍCIOS A SEREM ALCANÇADOS

Contribuir para garantia de um nível adequado de disponibilidade, autenticidade e confiabilidade das informações produzidas e armazenadas em meios tecnológicos.

Aprimorar a segurança de TIC da CEASA Campinas frente a ameaças sofisticadas.

Possibilitar o controle de acesso e complementar o conjunto de procedimentos que contemplam a política de segurança, concebendo qualidade no serviço de proteção.

Possibilitar o acesso remoto de maneira estável aos colaboradores de forma segura.

Prestar os serviços de TIC mantendo a segurança adequada às informações organizacionais, principalmente quanto à garantia de disponibilidade e integridade dos dados necessários ao pleno funcionamento dos processos administrativos.

Assegurar a sustentabilidade e desempenho dos serviços da CEASA Campinas, conforme sua topologia e tráfego de rede.

Aumento da capacidade de resposta a incidentes de segurança.

ESPECIFICAÇÕES TÉCNICAS DO SERVIÇO

Solução integrada de forma duplicada para a realização de cluster, para que em caso de falha de um equipamento, o outro entre em operação. A redundância deverá ser realizada através da interligação dos equipamentos de forma que em caso de indisponibilidade de um deles, o outro assumirá as mesmas propriedades e configurações diminuindo eventuais indisponibilidades. Este recurso deve ser nativo do appliance e sem a necessidade de adições de equipamentos ou recursos adicionais. Portanto, a CONTRATADA deverá fornecer a solução sempre em duplicidade de equipamentos, softwares e serviços.

A solução de firewall UTM NGFW deverá ser entregue em formato de equipamentos físicos, sendo vedado o fornecimento de solução virtualizada.

A solução deve estar licenciada para trabalhar em cluster ativo/passivo e ativo/ativo.

O hardware e software que executem as funcionalidades de proteção de rede devem ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico.

Somente serão aceitos equipamentos novos e sem uso anterior. Não serão aceitos equipamentos do tipo end-of-life ou descontinuados pelo fabricante.

Os equipamentos deverão ser entregues nas caixas lacradas pelo fabricante, não sendo aceitos equipamentos com caixas violadas.

Hardware

O dispositivo de hardware deverá possuir as especificações técnicas mínimas abaixo relacionadas:

- Botão de liga/desliga;
- Led indicador de equipamento ligado no painel frontal do gabinete;
- 2 (duas) portas USB no painel frontal do gabinete;
- 1 (uma) porta de vídeo D-Sub (VGA);
- 1 (uma) interface LAN;
- 1 (uma) interface WAN;
- 6 (seis) interfaces de rede Gigabit;
- 2 (duas) interfaces SFP com tecnologia fibra óptica;
- 2 (duas) interfaces acima *bypass*;
- Throughput de 6 GB/s;
- Licenciamento para até 1.000 dispositivos conectados;
- Suporte a 2.000.000 (dois milhões) de conexões simultâneas;
- Suporte a 30.000 (trinta mil) novas conexões por segundo;
- Armazenamento com capacidade de 240 GB SSD;
- Fonte de alimentação AC 100-240VAC interna ao gabinete.

Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19”, incluindo kit para adaptação se necessário e cabos de alimentação.

Administração

A solução deverá possibilitar a configuração através de interface WEB e via console (linha de comando) e gerenciamento centralizado em uma suíte em nuvem para maior segurança, visualização, facilidade e disponibilidade dos serviços de monitoramento.

A interface WEB deverá suportar o idioma Português (BR).

A solução deverá possibilitar o gerenciamento através de interface WEB das seguintes configurações:

- Configurações básicas através de assistente (Wizard);
- Atualização através do painel de configuração;
- Configuração de interface de rede;
- Configuração de permissão de acesso por usuário, por IP;
- Reinicialização do sistema;
- Visualização de log do firewall;
- Configuração de certificados SSL.

Firewall

A solução deverá possuir as seguintes características mínimas relacionadas ao sistema de firewall:

- Permitir configuração de regras de firewall, como bloqueio e liberação;
- Statefull firewall com leitura dos 7 (sete) níveis da camada;
- Capacidade de limitar conexões simultâneas com base em regras;

- Opção de gravação de log do tráfego correspondente a cada regra;
- Possibilidade de alteração de gateway de acordo com a regra;
- Prover mecanismo contra ataques de falsificação de endereços (IP Spoofing);
- Permitir configuração de regras por protocolos, como TCP, UDP, TCP/UDP, ICMP, ESP, AH, GRE, IGMP, entre outros;
- Permitir configuração do tipo de estado de conexão.

A proteção na camada 7 contra tráfego malicioso deverá garantir o bloqueio de, no mínimo, worms, trojans, malwares, além de protocolos de uso não recomendados como: UltraSurf, UltraVPN, CyberGhost, Express VPN, etc.

A solução deverá ainda permitir configurar um servidor PPPoE Server no equipamento, podendo ter autenticação por base local, RADIUS, ou acessar um servidor PPPoE para ativar algum link.

A solução deverá permitir uso de um cliente OpenVPN do fabricante, com opção de autenticação em base AD (Active Directory) ou LDAP, podendo ser instalado em estações de trabalho Windows, MAC OS X, ou dispositivos móveis como iOS (iPhone/iPad) e Android.

Bloqueio por país/região

A solução deverá permitir a configuração de bloqueio de conexões de acordo com o país e/ou continente através do IP de origem.

A solução deverá exibir no Dashboard do equipamento a quantidade de bloqueios e total do tráfego.

A solução deverá possuir dashboard exclusivo com gráficos de informações dos principais países de origem das tentativas de invasões.

A solução deverá possuir recurso para exibir um resumo das tentativas de invasão, infecções identificadas e nível de risco de cada uma delas.

A solução deverá possuir proteção integrada de IPs com assinaturas mantidas também pelo fabricante. Deverá ter disponível uma ferramenta responsável por identificar e bloquear aplicações ou serviços independentes de uso de um Proxy nos dispositivos, com capacidade de bloquear até mesmo tráfego de dispositivos móveis.

NAT

A solução deverá permitir ao equipamento realizar a comunicação entre os hosts da rede interna e a internet, traduzindo os IPs com as seguintes características:

- NAT 1:1;
- NAT de saída;
- NAT Reflection - possibilitando que os serviços possam ser acessados por IP público a partir de redes internas.

QoS e Gerência de Banda

A solução deverá fornecer recursos de gerência de tráfego de rede.

Deverá ser possível a criação de regras dos seguintes tipos:

- Priorização do tráfego, definindo quais protocolos possuem prioridade;
- Limite do tráfego, definindo qual limite máximo de um protocolo;
- Reserva do tráfego com empréstimo em caso de não estar sendo utilizado em seu limite.

DHCP Relay

Permitir que o DHCP Relay encaminhe requisições para um servidor definido em outro segmento de rede.

DHCP Server

A solução deverá dispor de servidor DHCP.

A solução deverá atribuir endereços IPs e configurações relacionadas aos dispositivos da rede.

A solução deverá permitir DNS Forwarder para auxiliar o servidor DNS a consultar nomes na internet.

DNS Dinâmico

A solução deverá permitir uso de DNS dinâmico para que seja registrado o endereço IP público com um número de prestadores de serviços de DNS dinâmico comumente usados para conectar-se com VPNs, Web Servers e Mail Servers.

Registro de Logs

A solução deverá permitir gravar logs separando pelas seguintes categorias:

- Log do sistema;
- Firewall;
- DHCP;
- Autenticação;
- IPSec;
- PPP;
- VPN;
- Load Balance;
- OpenVPN;
- NTP.

A solução deverá permitir o registro de logs em servidor interno ou externo.

Módulo de diagnósticos

O sistema deverá possuir um módulo de diagnósticos com no mínimo as seguintes opções:

- Atividades do sistema;
- Autenticação;
- Autenticação de dois fatores;
- Backup e Restauração;
- Captura de pacotes;
- Configuração de fábrica;
- Desligar sistema;
- DNS Lookup;
- Estados;
- Informações referentes a limites do sistema;
- Monitor de serviços;
- Ping;
- Reiniciar;
- Rotas;
- Sockets;
- Tabela ARP;
- Tabela de Estados;
- Tabela NDP;
- Traceroute.

Balanceamento de Carga e Failover

A solução deverá permitir a configuração de balanceamento de carga (load balancing) no tráfego de saída para internet e/ou failover.

A solução deverá permitir visualizar estrutura de rede conectada entre unidades por meio do painel em nuvem, permitindo visualizar problemas de rotas de conexão entre unidades, e permitir fazer failover sobre conexões de VPN de maneira automática sem intervenção manual.

Servidor NTPD

A solução deverá permitir a sincronização de horário do equipamento utilizando protocolo NTP.

A solução deverá permitir a configuração do servidor NTP com sincronismo a servidores externos.

Roteamento Dinâmico

A solução deverá possuir suporte aos protocolos RIP, OSPF e BGP.

SNMP

A solução deverá possuir suporte ao protocolo de SNMP.

Servidor PPPoE

A solução deverá possibilitar a configuração de um servidor PPPoE com autenticação RADIUS.

NetFlow

A solução deverá possibilitar a configuração a utilização do protocolo NetFlow para coletar informações referentes a tráfego de rede IP.

VPN

A solução deverá possuir suporte aos protocolos IPSec, OpenVPN, PPPTP e L2TP.

A solução deverá permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional da estação de trabalho.

Cluster

Deverá permitir a configuração de dois ou mais firewalls como um grupo de failover, se uma interface falhar no primário ou ficar off-line completamente, o secundário se torna ativo, sem qualquer prejuízo de parada ou interrupções de atividade de operação (quantidade de usuários, conexões simultâneas, troughput, etc.) especificadas no dimensionamento.

A solução deverá ter capacidades de sincronização de configuração, para que as alterações de configuração no firewall UTM primário sincronizem automaticamente com o firewall UTM secundário.

A solução deverá garantir que a tabela de estado do firewall, assim como todas as configurações pertinentes, seja replicada para os firewalls configurados em failover, permitindo que em caso de falha em um equipamento, o outro assuma de modo automático as mesmas configurações e serviços essenciais, melhorando a disponibilidade e segurança na rede.

A solução deverá permitir que seja configurado quais os módulos serão sincronizados através do protocolo de cluster.

A solução deverá permitir que em caso de queda de um firewall UTM, o outro assuma de modo que conexões não sejam interrompidas.

Sistema de prevenção de ameaças - IDS/IPS

Os dispositivos de proteção devem suportar os módulos de IDS/IPS integrado no próprio equipamento de firewall UTM para eventuais ativações.

Possuir capacidade de detecção de assinaturas de ataques pré-definidos.

Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações.

Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS, SMTP, POP3, IMAP, SMB e FTP.

Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos. A identificação deve ser de forma automática, não sendo necessário que o administrador cadastre os domínios considerados maliciosos.

Possuir a capacidade de prevenção de ameaças não conhecidas.

WebFilter e Proxy

A solução deverá possuir filtro de conteúdo web com capacidade para permitir:

- Controle de políticas por aplicações, grupos de aplicações e categorias de aplicações;
- Controle de políticas por usuários, grupos de usuários, IPs e redes;
- Suportar a atribuição de agendamento às políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

Reconhecer aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, VoIP, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail.

Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários.

A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:

- Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs e redes.
- Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via Active Directory e base de dados local.
- Deve bloquear o acesso a sites com conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, mesmo que a opção “Safe Search” esteja desabilitada no navegador do usuário.
- Suportar base ou cache de URLs local no appliance, sendo o cache populado conforme as requisições de verificação das URLs no banco de dados central forem sendo realizadas, evitando atrasos de comunicação e validação das URLs.
- Permitir a customização de página de bloqueio.

A solução deverá permitir a configuração de servidor proxy transparente ou autenticado.

A solução deverá permitir a autenticação dos usuários através de base LDAP e/ou AD (Active Directory), podendo funcionar em Single Sign on.

As soluções de WebFilter podem ou não funcionar sob proxy, desde que atendam aos requisitos de registros de atividades e filtros.

Backup e Restauração

A solução deverá permitir a configuração para geração automática e/ou manual de backup das configurações do equipamento.

A solução deverá permitir a restauração da configuração do equipamento.

Portal do visitante

A solução deverá permitir o controle e criação de regra para autenticação do grupo de visitantes (Captive Portal). A solução deverá ser homologada previamente pela CONTRATANTE.

Monitoramento e alertas

A solução deverá fornecer tela de Dashboard (painel de gestão) onde o administrador de redes tenha uma visão geral de todas as funcionalidades do equipamento.

O Dashboard (painel de gestão) deverá apresentar no mínimo as seguintes informações:

- Informações do sistema (CPU, memória, disco, capacidade, backup);
- Visualização do tráfego de rede em tempo real;
- Análise de tráfego e qualidade do link;
- Perda de pacotes;
- Latência;
- IP de origem;
- Bloqueio por país.

A solução deverá emitir alertas quanto à indisponibilidade ou mal funcionamento de alguns indicadores do firewall, tais como latência e/ou queda de link de internet, CPU, disco e memória, além da capacidade do firewall.

Os alertas deverão ser enviados por PUSH através de aplicativos para iOS, Android e visualização através de um painel web.

A solução deverá contemplar agentes que permitam serem instalados em dispositivos (sem limite de licenças) com sistema operacional Windows com o objetivo de servirem como coletores de informações SNMP que permitam mostrar informações sobre monitoramento dos dispositivos críticos da CONTRATANTE, tais como roteadores WiFi.

No caso de monitoramento de servidores Windows da CONTRATANTE, o endpoint deverá ser instalado direto no servidor e o sistema mostrar informações sobre a saúde do mesmo com alertas para CPU, disco, memória e conexão de rede.

No caso de servidores Windows, o monitoramento deverá mostrar a chave de licença do mesmo, assim como o status do licenciamento.

No caso de servidores Windows, o monitoramento deverá mostrar informações completas do hardware e software dos mesmos, assim como permitir acesso remoto, caso necessário.

Relatórios

A solução deverá permitir a geração de relatórios contendo pelo menos os seguintes itens:

- Por usuários;
- Por consumo;
- Por páginas;
- Filtros por período (recente, 7 dias, 30 dias e em tempo real).

A solução deverá permitir a exportação de relatórios para o formato PDF.

ATUALIZAÇÕES DE SOFTWARE

Durante a vigência contratual, deverá ser possível realizar a atualização do software dos equipamentos para obter novas funcionalidades e correção de bugs, sem custos adicionais para a CONTRATANTE.

INSTALAÇÃO E CONFIGURAÇÃO

Todos os equipamentos devem estar instalados e configurados nas dependências da CONTRATANTE até o dia 01/12/2023.

A CONTRATADA deverá prestar serviços de instalação e configuração da solução, que compreendem, entre outros, os seguintes procedimentos:

- Reunião de alinhamento para criação do escopo do projeto previamente a instalação.

- Instalação física dos equipamentos e configuração da solução no local determinado pela equipe responsável pelo projeto por parte da CONTRATANTE.

Análise da topologia e arquitetura da rede, considerando todos equipamentos já existentes e instalados.

Análise do acesso à internet, sites remotos, serviços de rede oferecidos aos colaboradores e aos usuários externos.

Configuração do sistema de firewall, VPN, IPS, filtro URL, NAT, de acordo com as exigências levantadas.

Toda configuração do sistema deverá ser realizada de acordo com as melhores práticas recomendadas pelo fabricante da solução ofertada, garantindo que no mínimo sejam mantidas as mesmas regras atuais já configuradas.

Configuração do sistema de gerenciamento centralizado.

Repasse de informação das configurações realizadas no formato hands-on para a equipe responsável pelo projeto por parte da CONTRATANTE após validação da instalação e configuração.

A instalação física dos equipamentos deverá ocorrer no Datacenter da CONTRATANTE, em horário comercial (8h às 16h), acordado previamente com a equipe da Coordenadoria de Informática.

TREINAMENTO

Considerando que se trata de contratação de uma solução para a qual a equipe da CONTRATANTE pode não ter conhecimento técnico suficiente para manter em operação, deverá fazer parte da contratação treinamento específico que deverá ser conduzido pelo próprio fabricante ou por um parceiro nacional, capacitado, certificado e autorizado pelo fabricante a ministrar treinamentos oficiais.

A capacitação será ministrada para uma turma com até 3 (três) participantes.

O treinamento deverá ter carga horária mínima de 10 (dez) horas.

SUPORTE TÉCNICO

O suporte técnico tem por finalidade garantir a sustentação e a plena utilização da tecnologia durante a vigência do contrato. Inclui o atendimento para sanar dúvidas relacionadas com instalação, configuração e uso da tecnologia ou para correção de problemas desse, em especial na configuração de parâmetros, falhas, erros, defeitos, manutenção corretiva em geral ou vícios identificados no funcionamento da tecnologia e deverá ser prestado conforme o "SLA - ACORDO DE NÍVEL DE SERVIÇO" descrito neste Termo de Referência.

Com objetivo de maior assertividade na atuação, os alertas deverão ser separados entre **Crítico** (necessária atuação imediata devido a indisponibilidade ou risco eminente de indisponibilidade), **Atenção** (necessária atuação rápida para evitar indisponibilidade de serviços) e **Informação** (informação e conhecimento).

A CONTRATADA deverá fornecer serviço de monitoramento proativo que consistirá na verificação dos alertas durante horário comercial (8h às 17h). Em caso de alertas críticos e/ou repetidos alertas de atenção, a CONTRATADA deverá contatar a equipe técnica da CONTRATANTE a fim de solicitar aprovação de uma ação com objetivo de evitar indisponibilidade de algum serviço.

NÍVEL DE SEVERIDADE DOS CHAMADOS TÉCNICOS

A CONTRATADA deverá prover portal web, e-mail ou número telefônico no Brasil para registro dos acionamentos, com geração de protocolo para o acompanhamento e aferição do cumprimento dos índices indicados na Meta de Disponibilidade e de Atendimento.

Para a prestação do serviço de manutenção e suporte técnico, a CONTRATADA deverá garantir os níveis mínimos de serviço definidos no "SLA - ACORDO DE NÍVEL DE SERVIÇO".

SLA - ACORDO DE NÍVEL DE SERVIÇO

O objetivo do ACORDO DE NÍVEL DE SERVIÇO é garantir, em termos contratuais, características de qualidade, eficiência e eficácia do serviço em questão, definindo o acordo de níveis de serviço (SLA) para as partes e estabelecendo a forma de atendimento e os prazos máximos a serem cumpridos pela CONTRATADA.

DAS DEFINIÇÕES E TERMINOLOGIAS

Requisitos: Conjunto de especificações necessárias para definir a Solução de Tecnologia da Informação a ser contratada.

Incidente: Qualquer evento não esperado que cause interrupção, instabilidade ou perda de performance no serviço contratado pela CONTRATANTE.

Problema: Causa raiz de um ou mais incidentes.

Bug de projeto: Falha ou erro no código que provoque um mau funcionamento no serviço.

Requisição de Serviço (RS): Uma requisição formal da CONTRATANTE para algo a ser fornecido como, por exemplo, informações sobre serviços ou servidores, logs, dados, printscreen, etc., desde que não gere qualquer indisponibilidade no serviço contratado.

Itens de configuração: Equipamentos e soluções que compõem a infraestrutura para fornecimento do serviço adquirido como, por exemplo, plataforma, servidores, banco de dados, aplicação, firewall, solução de alta disponibilidade e rede de dados.

Produto: Solução contratada pela CONTRATANTE.

Usuário: Pessoa que utiliza a solução contratada pela CONTRATANTE.

NÍVEIS DE SERVIÇO

A CONTRATADA compromete-se a manter os níveis de serviço abaixo especificados para a sua solução.

As falhas de responsabilidade da CONTRATADA deverão ser recuperadas conforme prazos especificados abaixo, de acordo com a severidade do incidente, que podem ser classificados em 5 níveis de prioridade (Crítica, Alta, Média, Baixa e Acordado), de acordo com a tabela - Matriz de Prioridade e de acordo com a "curva" matriz de urgência X impacto a seguir, onde:

- **Urgência:** é a percepção de velocidade necessária para se resolver a falha sob ótica do impacto para o negócio.
- **Impacto:** é a extensão do dano causado pelo incidente no negócio da CONTRATANTE.

A urgência será definida pelo CONTRATANTE no momento da abertura do ticket, enquanto o impacto será definido pela CONTRATADA de acordo com os critérios definidos abaixo.

Após avaliação pela CONTRATADA, responsável pelo atendimento dos tickets, pode ocorrer um reenquadramento da classificação de prioridade, de acordo com o entendimento da urgência definida e do real impacto. Em caso de reenquadramento, a equipe de Help Desk irá justificar através de ocorrência o motivo da reclassificação.

Tabela - Matriz de Prioridade

Matriz de Prioridade	**Urgência**		
	Alta	Média	Baixa

Impacto	Alto	Crítica	Alta	Média
	Médio	Alta	Média	Baixa
	Baixo	Média	Baixa	Acordado
	Muito Baixo	Baixa	Acordado	Acordado

Critérios de impacto para falhas na solução da CONTRATADA:

- **Alto:** o produto ficou inoperante ou ocorreu falha de grande impacto e o sistema está parado. Para este nível de severidade o atendimento deve ser imediato e com tempo de resposta de até 1 (uma) hora para resolução total ou encontro de solução temporária de contorno.
- **Médio:** travamento ou parada de ambiente parcial. Para este nível de severidade o tempo de resposta deve ser de até 2 (duas) horas, em horário comercial, para resolução total ou encontro de solução temporária de contorno.
- **Baixo:** redução de performance do equipamento ou aplicação de solução temporária de contorno bem-sucedida. Para este nível de severidade o tempo de resposta deve ser de até 6 (seis) horas, em horário comercial, para resolução total ou encontro de solução temporária de contorno.
- **Muito Baixo:** dúvidas de configuração ou anomalia de baixo impacto. Para este nível de severidade o tempo de resposta deve ser de até 8 (oito) horas, em horário comercial.

Os prazos para recuperação do incidente, mesmo sendo através de uma solução provisória, se dará dentro do prazo definido na tabela - Tempo de Resposta e Recuperação.

O tempo de recuperação será contado a partir do aceite do ticket, através da ferramenta, até a solução da falha.

Os tempos máximos esperados para tratamento de cada ticket também são mostrados na tabela - Tempo de Resposta e Recuperação.

Tabela - Tempo de Resposta e Recuperação

Nível de Prioridade	**SLA**	
	Tempo Máximo de Primeira Resposta	Tempo Máximo de Recuperação
Crítico	1 hora	4 horas
Alto	1 hora	6 horas
Médio	2 horas	12 horas
Baixo	6 horas	48 horas
Acordado	8 horas	72 horas

EQUIPAMENTO DE BACKUP

A CONTRATADA compromete-se a disponibilizar, em até 8 (oito) horas, um equipamento de backup com as mesmas especificações técnicas em caso de indisponibilidade da solução por causa de falhas de componentes ou outros problemas em que a solução exija tempo superior a 48 (quarenta e oito) horas.

A CONTRATADA deverá restaurar no equipamento a ser disponibilizado, um backup das configurações atuais dos equipamentos instalados nas dependências da CONTRATANTE. O arquivo contendo o backup será fornecido pela CONTRATANTE.

O equipamento de backup deverá ser retirado pela CONTRATANTE em local especificado pela CONTRATADA, desde que não ultrapasse 120 (cento e vinte) quilômetros de distância da CONTRATANTE. Caso a distância seja superior a 120 (cento e vinte) quilômetros, a entrega do equipamento de backup será de responsabilidade da CONTRATADA, sem custos adicionais para a CONTRATANTE, mesmo quando for necessário o transporte ou fretamento dos equipamentos, o translado e a estada de técnicos ou qualquer outro tipo de serviço necessário para garantir o cumprimento do serviço.

Em caso de recorrência da indisponibilidade no mesmo chamado, a CONTRATADA deverá disponibilizar visita técnica in loco dentro do SLA previsto para a solução do problema.

OBRIGAÇÕES DA CONTRATADA

Executar os serviços conforme as especificações do contrato, deste Termo de Referência e de sua proposta.

Garantir o cumprimento, durante toda a vigência contratual, dos requisitos mínimos relacionados a perfis profissionais de sua equipe técnica diretamente envolvida na execução do objeto, de acordo com as obrigações contratuais e em conformidade com as normas e determinações em vigor.

Comunicar ao fiscal do contrato, qualquer fato extraordinário ou anormal que ocorra durante a vigência do contrato.

Arcar com todos os custos administrativos de sua responsabilidade relacionados ao objeto e à execução do contrato, responsabilizando-se por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas em legislação específica, cuja inadimplência não transfere responsabilidade ao CONTRATANTE.

Indicar e manter preposto apto a representá-la junto ao CONTRATANTE, que deverá responder pela fiel execução do contrato, de acordo com os requisitos definidos.

Reparar quaisquer danos diretamente causados ao CONTRATANTE ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pelo CONTRATANTE.

Em nenhuma hipótese veicular publicidade ou qualquer outra informação acerca do objeto deste Termo de Referência, sem prévia autorização do CONTRATANTE.

O atendimento às solicitações deverá ser imediato e para tanto entre os pontos de contato, deverá sempre haver um telefone ou site para registro da solicitação de manutenção.

Garantir o suporte de 1º, 2º e 3º nível, entendendo-se:

- 1º nível - atendimento via ferramenta de gerenciamento de incidentes, a partir da abertura do ticket para verificação da falha;
- 2º nível - atendimento através de equipe técnica especializada;
- 3º nível - atendimento através de equipe gerencial.

OBRIGAÇÕES DA CONTRATANTE

Acompanhar e fiscalizar o cumprimento das obrigações assumidas pela CONTRATADA, inclusive quanto à continuidade da prestação dos serviços que, ressalvados os casos de força maior, justificados e aceitos pela CONTRATANTE, não devem ser interrompidos.

Proporcionar todas as facilidades para que a CONTRATADA possa efetuar os serviços dentro das normas estabelecidas no contrato, prestando informações e esclarecimentos que venham a ser solicitados pela CONTRATADA.

Permitir o acesso de técnicos credenciados da CONTRATADA, nas dependências internas da CONTRATANTE, desde que devidamente identificados e designados para eventual visita técnica.

Comunicar à CONTRATADA, na pessoa do Gestor de contrato designado, quaisquer ocorrências em desacordo com o cumprimento das obrigações pactuadas durante o atendimento, podendo sustar ou recusar o recebimento, caso não esteja de acordo com as especificações e condições estabelecidas.

Permitir que somente pessoas autorizadas pela CONTRATADA prestem o suporte técnico especializado e realizem a operação assistida.

Liquidar o empenho e efetuar o pagamento à CONTRATADA, dentro dos prazos preestabelecidos em contrato.

Disponibilizar todos os meios necessários para a execução dos serviços contratados.

DAS CONDIÇÕES DE PAGAMENTO

A CONTRATADA deverá emitir nota fiscal/fatura correspondente aos serviços prestados à CONTRATANTE até o dia 25 (vinte e cinco) do mês correspondente ao da execução dos serviços e entregá-la no prazo de até 1 (um) dia útil ao gestor do contrato da CONTRATANTE.

A CONTRATANTE providenciará o pagamento da nota fiscal/fatura à CONTRATADA até o 5º (quinto) dia útil do mês subsequente ao da emissão da nota fiscal.

DA SUBCONTRATAÇÃO

Não será admitida a subcontratação do objeto contratual.

DA VIGÊNCIA CONTRATUAL

O prazo de vigência contratual é de 60 (sessenta) meses.

Assinam eletronicamente pela Contratante – CEASA Campinas:

Jefferson de Oliveira Penteado

Nilton Silva Fernandes de Souza

Assina eletronicamente pela Contratada – BluePex:

Eldo Lemos Christianini

Documento assinado eletronicamente por **Nilton Silva Fernandes de Souza**, **Usuário Externo**, em 22/11/2023, às 10:02, conforme art. 10 do Decreto 18.702 de 13 de abril de 2015.

Documento assinado eletronicamente por **JEFFERSON DE OLIVEIRA PENTEADO**, **Usuário Externo**, em 22/11/2023, às 15:17, conforme art. 10 do Decreto 18.702 de 13 de abril de 2015.

Documento assinado eletronicamente por **ELDO LEMOS CHRISTIANINI**, **Chefe de Setor**, em 23/11/2023, às 12:12, conforme art. 10 do Decreto 18.702 de 13 de abril de 2015.

A autenticidade do documento pode ser conferida no site https://sei.campinas.sp.gov.br/verifica informando o código verificador **9611472** e o código CRC **EBBA3827**.