CONTRATO DE PRESTAÇÃO DE SERVIÇOS Nº 036/2023
Processo n° 033/2023

EMENTA: Contratação de empresa especializada para a locação de Appliance de Firewall, com redundância, incluindo serviço de armazenamento e gestão de logs em nuvem e monitoramento dos acessos e suporte ao produto 24x7, para o Complexo de Saúde São Bernardo do Campo.
LOCADORA: Infoready Tecnologia Ltda.

Por este instrumento contratual, as partes, de um lado a **FUNDAÇÃO DO ABC – COMPLEXO DE SAÚDE SÃO BERNARDO DO CAMPO,** inscrita no CNPJ/MF sob nº 57.571.275/0025-70, estabelecida à Estrada dos Alvarengas, 1001 – Bairro Alvarenga – São Bernardo do Campo/SP, neste ato representada por sua Diretora Geral, Dra. Agnes Mello Farias Ferrari, brasileira, casada, médica, portadora do RG/UF nº 11.801.246-0 e inscrita no CPF/MF sob o nº 083.923.878-99, doravante denominada apenas **LOCATÁRIA** e, de outro, a empresa **INFOREADY TECNOLOGIA LTDA**, com sede a Avenida Poços de Caldas, 148 – Galpão 2 – Sala D, Bairro Distrito Industrial CEP: 37.504-110 – Município de Itajubá/MG, inscrita no CNPJ/MF sob o nº 13.727.635/0001-37, representada por Leandro André Rodrigues Barasniewski, portador do RG/UF nº 28.334.672-3 e do CPF/MF nº 267.787.948-44, doravante denominada **LOCADORA**, tendo em vista o constante e decidido no Processo nº 033/2023, têm como justo e acordado o que segue:

1. DO OBJETO

1.1. Contratação de empresa especializada para especializada para a locação de Appliance de Firewall, com redundância, incluindo serviço de armazenamento e gestão de logs em nuvem e monitoramento dos acessos e suporte ao produto 24x7, para o Hospital de Clínicas Municipal José Alencar, Hospital de Urgência , Hospital Anchieta e Hospital da Mulher, unidades que integram o Complexo de Saúde São Bernardo do Campo, conforme especificações técnicas exigidas no Anexo II, pelo período de 36 (trinta e seis) meses.

1.1.1. A Proposta Comercial da LOCADORA, no que não for contrária ao estabelecido no presente instrumento, é parte integrante deste Contrato.

2. DA EXECUÇÃO DOS SERVIÇOS

2.1. A LOCADORA prestará os serviços nas seguintes unidades e endereços:

Unidade	Endereço
HC	Rua Paulo Coppini, nº 35, Alvarenga - São Bernardo do Campo/SP.
HA	Rua Silva Jardim, nº 470, Centro - São Bernardo do Campo/SP.
HU	Rua Joaquim Nabuco, n° 380, Centro - São Bernardo do Campo/SP.
HMU	Av. Bispo Cesar D´Acorso Filho, nº 161, Rudge Ramos - São Bernardo do Campo/SP.

2.2. Implantação e configuração das soluções.

2.2.1. Características Específicas.

2.2.1.1. A LOCADORA deve entregar cada equipamento no seu local indicado pela LOCATÁRIA.

2.2.1.2. Toda a instalação dos equipamentos seja física ou lógica é de responsabilidade da LOCADORA, desde a instalação em rack ou outro lugar indicado e disponibilizado pela LOCATÁRIA, até a ativação das interfaces de rede, conectorização dos cabos, organização dos cabeamentos ligados aos equipamentos fornecidos, configuração e qualquer outro serviço ou equipamento que seja necessário para o bom funcionamento deles, como transceivers multimodo de 10GB para curtas distâncias indicado pela fabricante do firewall, cordões de fibra e transceivers de 10GB nos switches da LOCADORA onde a rede lógica funciona nesta velocidade.

JURÍDICO CSSBC

2.2.1.3. A LOCADORA deve entender a necessidade da LOCATÁRIA em cada local e configurar o equipamento conforme a necessidade, bem como providenciar os transcrever ou licenças para atender o projeto.

2.2.1.4. A instalação deverá ser realizada sem custo adicional a LOCATÁRIA.

2.2.1.5. Os equipamentos devem ser entregues em no máximo 45 (quarenta e cinco) dias corridos a partir da solicitação inicial.

2.2.1.6. Os equipamentos devem ser configurados e instalado em no máximo 60 (sessenta) dias corridos a partir da data de entrega.

2.2.1.7. Antes de cada entrega ou instalação, a LOCADORA deverá validar as localidades para entrega e instalação de cada equipamento junto à equipe gestora do contrato.

2.2.1.8. O Plano de Implantação deverá dispor também sobre o cronograma de execução das atividades, previsão de recursos, pessoas envolvidas e atividades a serem desenvolvidas pela LOCADORA e indicar os principais riscos e forma de mitigação.

2.2.1.9. A LOCADORA deverá entregar a documentação de "Projeto Executivo" e documentação de "As-Built" na fase de conclusão do projeto.

2.2.1.10. A LOCADORA na execução das atividades elencadas nos itens anteriores se deparando com problema em equipamento ou software deverá manter contato com a fabricante criando chamado e abertura de garantia quando necessário.

2.2.1.11. Todas as configurações serão realizadas pela LOCADORA deverão estar em conformidade com a recomendação do fabricante dos equipamentos e softwareswares da solução, boas prácas de implementação recomendada pelo fabricante e os requisitos fornecidos pelo LOCATÁRIA para o ambiente em questão.

2.3. Suporte técnico, manutenção e monitoramento 24X7.

2.3.1. Tipos de Atendimento:

2.3.1.1. A LOCATÁRIA poderá abrir chamados de manutenção através de chamada gratuita a número 0800, por correio eletrônico e aplicativo de troca de mensagens instantâneas sem necessidade de prévia consulta e/ou qualquer liberação por parte da LOCADORA. Não deve haver limite para aberturas de chamados, sejam de dúvidas/configurações e/ou resolução de problemas de hardware ou software. O atendimento deverá ocorrer com SLA 24x7.

2.3.1.2. O atendimento deverá ocorrer com SLA 24x7 em todos os canais, telefônico, correio eletrônico e aplicativo de troca de mensagens instantâneas. A interação por todos estes canais, deverão ser registradas em chamado, nos casos de atendimento telefônico, a ligação deverá ser gravada e adicionada ao chamado como registro do atendimento.

2.3.1.3. O aplicativo de troca de mensagens instantâneas deverá ser disponibilizado como App para os sistemas Android e iOS por meio dos principais repositórios de aplicativos mobile, tais como, Google Play e Apple Store.

2.3.2. Atendimento nível 1, 2 e 3:

2.3.2.1. O Atendimento atuará para incidentes e requisições de serviço, em especial aqueles relacionados à infraestrutura descrita neste documento.

2.3.2.2. A equipe que cuidará deste serviço buscará, tem como responsabilidade prevenir a ocorrência de problemas e seus incidentes resultantes, eliminar incidentes recorrentes correlacionando-os e identificando a causa-raiz e sua solução, além de minimizar o impacto dos incidentes que não podem ser prevenidos (Gerenciamento de Problemas).

2.3.3. São atribuições dos Técnicos de Atendimento:

2.3.3.1. Realizar atendimento remoto e local de segundo nível aos usuários do CHSBC, a partir das solicitações recebidas dos técnicos ou gestores de contrato CHSBC, via sistema de Service Desk, respeitando os níveis de serviço acordados.

2.3.3.2. Contatar, se necessário, outras equipes ou prestadores de serviço do CHSBC que porventura possuam correlação com o incidente, problema ou requisição a ser tratada.

2.3.3.3. Elaborar procedimentos, roteiros ou scripts a serem seguidos pelo Atendimento Nível 1 no cumprimento de requisições de serviço, resolução de incidentes ou outras solicitações de usuários.

2.3.3.4. Monitorar as tecnologias descritas no Anexo II, a fim de trabalhar com visibilidade e assertividade na identificação de problemas e a sua causa-raiz, solucioná-la e prevenir novas ocorrências.

2.3.3.5. Elaborar relatórios e pareceres técnicos.

2.3.3.6. Executar ações correlatas, que demandem maior esforço ou complexidade (ex: atualizações de software em grande quantidade de equipamentos, elaboração de roteiro específico, etc.), solicitadas

JURÍDICO CSSBC

diretamente pelo Gestor do Contrato por parte da LOCATÁRIA e devidamente registradas no Sistema de Service Desk.

2.3.3.7. Realização de otimizações nas configurações para melhora do desempenho, quando observadas quedas de desempenho ou indisponibilidades pela LOCATÁRIA.

2.3.3.8. Emissão de relatório do tipo "healthcheck" com análise dos resultados e proposição de ajustes via definição e manutenção dentro do plano de melhorias.

2.3.4. Ferramenta de Service Desk.

2.3.4.1. A LOCADORA deverá realizar a abertura e resolução de todos os chamados e requisições através de ferramenta de Service Desk aderente ao ITIL:

2.3.4.1.1. AVM = Gerenciamento de Disponibilidade.

2.3.4.1.2. PM = Gerenciamento de Problemas.

2.3.4.1.3. CHG = Gerenciamento de Mudanças.

2.3.4.1.4. RF = Cumprimento de Requisição.

2.3.4.1.5. EV = Gerenciamento de Eventos.

2.3.4.1.6. IM = Gerenciamento de Incidente.

2.3.4.1.7. SLM = Gerenciamento de Nível de Serviço.

2.3.4.1.8. KM = Gerenciamento de Conhecimento.

2.3.4.2. Deve fornecer o cálculo dos acordos de níveis de serviço (SLA) tanto para o tempo de atendimento quanto para o tempo de solução.

2.3.4.3. A solução deve ter acesso por meio de sistemas moveis com suporte a Android e iOS, com App disponível para download na Google Play Store ou Apple Store.

2.3.4.4. A LOCADORA deverá emitir relatórios mensais abrangendo, no mínimo, requisições, incidentes, problemas, mudanças, configurações, base de conhecimento e gerenciamento do nível de serviço.

2.3.4.5. Níveis de serviço para suporte técnico.

2.3.5. A LOCADORA deverá obedecer a critérios de nível de serviço contidos nas tabelas abaixo:

Prioridade	Descrição	Multa por evento PA/PSC/PCR	Valor de referência
1 (Emergencial)	O serviço está fora de operação ou há um impacto crítico nas operações dos negócios.	0,3%	Valor do contrato
2 (Alta)	O serviço está degradado, ou aspectos significativos das operações de negócio sofreram impactos negativos pelo desempenho inadequado.	0,2%	Valor do contrato
3 (Média)	Serviço funcionando com pequenos problemas sem impacto direto na operação.	0,1%	Valor do contrato
4 (Baixa)	O desempenho operacional do serviço está prejudicado, causando quebra de funcionalidade ou de operação. Dúvidas, auditorias, configurações pontuais no cliente e outros.	0,05%	Valor do contrato

2.3.6. Todos os serviços relacionados aos equipamentos descritos neste documento devem ser enquadrados nas tabelas acima e são de responsabilidade da LOCADORA. Para todos a LOCADORA deverá diagnosticar e solucionar problemas. Para melhor ilustar as descrições da tabela acima, segue uma lista, não finalística, de exemplos de serviços associados a prioridades.

2.3.6.1. (Emergencial) - O serviço está fora de operação ou há um impacto crítico nas operações dos negócios

2.3.6.2. - (Alta) - O serviço está degradado, ou aspectos significativos das operações de negócio sofreram impactos negativos pelo desempenho inadequado.

2.3.6.3. (Média) - Serviço funcionando com pequenos problemas sem impacto direto na operação.

2.3.6.4. 4 (Baixa) - O desempenho operacional do serviço está prejudicado, causando quebra de funcionalidade ou de operação. Dúvidas, auditorias, configurações pontuais no cliente ou controladora e outros.

JURÍDICO CSSBC

2.3.7. Quando houver dúvidas quanto a classificação do incidente o Gestor do Contrato definirá a urgência devida, dado a LOCADORA direito de explicitar sua argumentação diante de discordância.

Serviço	Prioridade do Chamado	Nível de Serviço (Tempo)
Primeiro Atendimento (PA) (Retorno do Especialista)	1 (Emergencial)	30 minutos
	2 (Alta)	1h
	3 (Média)	2h
	4 (Baixa)	4h
Prazo de Solução de Contorno(PSC)	1 (Emergencial)	2h
	2 (Alta)	4h
	3 (Média)	7h
	4 (Baixa)	14h
Prazo de Resolução do Chamado (PRC)	1 (Emergencial)	7h
	2 (Alta)	14h
	3 (Média)	21h
	4 (Baixa)	35h
Troca de Reposição de Pontos de Acesso em Comodato		31h

2.3.8. O não atendimento do Prazo para Resolução do Chamado (PRC) ou Prazo de Solução de Contorno (PSC) que trata a presente Tabela de Severidade de Chamado constitui prática de irregularidade contratual.

2.3.9. O Prazo para Resolução do Chamado (PRC) ou Prazo de Solução de Contorno (PSC) poderá ser prorrogado em caso de defeitos que exijam a intervenção da engenharia do fabricante da solução, desde que aprovado pela LOCATÁRIA, Através do Fiscal Técnico ou Gestor do Contrato, solicitado pela LOCADORA antes do término do prazo definido na Tabela de Níves de Serviço, e que a solução não esteja com problemas graves de operação e que se tenha esgotada quaisquer ação de mitigatória possível.

2.3.10. Todos os prazos para atendimento (Primeiro atendimento, PSC e PCR) começarão a ser contados a partir da solicitação para abertura do chamado através do meios disponíveis ou do alerta de monitoramento.

2.3.11. Dentro do prazo máximo de solução está compreendido o prazo de atendimento.

2.3.12. Dentro do prazo máximo de atendimento, cabe a LOCADORA dar início às providências que serão adotadas para a solução do chamado junto ao Fabricante, quando necessário.

2.3.13. Quando para a resolução de chamado é necessário acionamento de Manutenção com Troca de Reposição (RMA) os prazos serão interrompidos a partir da solicitação ao fabricante e retomados no ato da devolução do equipamento.

2.3.14. A cada evento, PA, PSC ou PCR infringidos em qualquer chamado haverá a multa descrinada na "Tabela de Prioridades de Serviço e Multas" de acordo com a referido Nível de Serviço.

2.3.15. Para efeitos de multa nos chamados vencidos o prazo de PRC serão calculadas multas a cada período relativo ao tempo do prazo em questão.

2.3.16. Constitui prática de irregularidade contratual:

2.3.16.1. Não cumprimento do prazo de 10% do total de chamados por mês inicidindo em multa de 0,1% do contrato.

2.3.17. A contagem do prazo se dará durante os dias úteis e em horário de expediente.

2.3.17.1. Os chamados terão seus prazos pausados, quando sua execução estiver dentro do prazo e encerrar o horário de expediente da LOCATÁRIA, devendo prosseguir, a contagem do prazo, a partir do início do horário de expediente, no próximo dia útil.

2.3.18. Não se aplicam aos chamados com prioridade emergencial o disposto no item anterior.

2.3.19. Se o problema for originado pela LOCADORA, ela deverá resolve-lo em no máximo 1 (uma) hora. Não o fazendo incidirá em prática de irregularidade contratual.

2.4. Serviços de manutenção.

JURÍDICO CSSBC

2.4.1. Intervenção em caso de perda de acesso por parte dos usuários, ou problema em determinado equipamento.

2.4.2. Manutenção preventiva com periodicidade semestral.

2.4.3. Manter a documentação do ambiente descrito no item 1 atualizada com periodicidade trimestral.

2.4.4. Manter repasse de conhecimento e formação do Nível 1 (Helpdesk) e pessoal de atendimento presencial. Realizando treinamento remoto sempre quando necessário.

2.5. Manutenção corretiva.

2.5.1. Sempre que necessário, a LOCADORA deverá estabelecer contato com o fabricante/fornecedor para troca/substituição dos equipamentos e/ou peças relacionados para os elementos descritos no item 1 deste termo de referência durante a vigência do contrato.

2.5.2. A LOCADORA deverá, ao final de cada execução de serviço de assistência técnica, registrar e a ocorrência através de fermenta de Service Desk com número do chamado (trouble chamado) contendo o número do chamado, data e hora do início e término do atendimento, número de série (ou etiqueta de serviço) e providências adotadas.

2.5.3. Os serviços a serem prestados deverão estar de acordo com os procedimentos e padrões estabelecidos pela do CHSBC.

2.6. Serviços de monitoramento de ativos.

2.6.1. Deverá ser monitorado em regime 24x7 todas os elementos contemplados no item 1 deste termo de referência, incluindo os softwares de controle e gestão da solução.

2.6.2. A ferramenta deverá ter disponibilidade de 99,99% e deverá estar hospedada em data Center Tier3 e/ou cloud pública, afim de garantir o serviço de forma ininterrupta.

2.6.3. A indisponibilidade da ferramenta acarretara multa de 0,01% por incidente no valor mensal do contrato.

2.6.4. A indisponibilidade da ferramenta por um período superior a 4h mensais incidirá em multa de 0,3% valor mensal do contrato e constitui prática de irregularidade contratual.

2.7. Arquitetura do software de monitoramento.

2.7.1. A mesma solução de monitoração pode ser oferecida tanto no modelo SaaS quanto On premisses.

2.7.2. Prover suporte para a instalação da solução em ambientes Windows, Unix e Linux.

2.7.3. Utilizar protocolo TCP como meio de comunicação entre os diversos componentes da solução.

2.7.4. A solução deve permitir ser instalada em ambientes de alta disponibilidade.

2.7.5. Os agentes caso utilizados devem utilizar menos de 20MB de instalação.

2.7.6. Os agentes caso utilizados devem utilizar menos de 1% de CPU dos servidores.

2.7.7. Os agentes caso utilizados devem utilizar menos de 10MB de Memória RAM.

2.7.8. A instalação de agente não deve necessitar de reboot do sistema.

2.7.9. Mudanças de configuração no agente não devem precisar de reboot do sistema.

2.7.10. Quando o agente gerar um evento, ele deve ser responsável por entregar este evento no console, com garantia de entrega.

2.7.11. A solução deve permitir instalar os agentes de forma manual.

2.7.12. A solução deve ter mecanismo de distribuição do agente.

2.7.13. A solução deve permitir a distribuição de configuração aos agentes de forma automatizada.

2.7.14. A solução deve ser escalável.

2.7.15. A solução deve suportar usuários concorrentes.

2.7.16. A comunicação entre manager e agente deve suportar links com pouca capacidade.

2.7.17. Os agentes devem ser configurados via interface gráfica a partir do manager.

2.7.18. Os agentes devem suportar configuração manual via edição de arquivos e via API.

2.7.19. A solução deve permitir reutilizar configuração criada para a monitoração em vários agentes.

2.7.20. A atualização de versão de agente não deve alterar a configuração de thresholds.

2.7.21. No caso de problema de conexão com o manager o agente deve armazenar as informações por período definido. Uma vez reestabelecida a conexão ele deve enviar as informações coletadas.

2.8. Alertas-Escalação.

JURÍDICO CSSBC

2.8.1. A solução deve ter eventos com severidades previamente configurados para diversos tipos de monitoração.

2.8.2. solução deve permitir criar novos eventos definindo o texto e severidade.

2.8.3. A solução deve permitir que eventos e/ou alarmes seja escalado, reiniciados, e/ou suprimidos baseado em critérios múltiplos como fonte, conteúdo, horário ou outros itens que sejam obtidos pela monitoração.

2.8.4. O agente deve permitir executar ações em um sistema.

2.8.5. O agente deve permitir executar ações de remediação no caso de uma situação identificada na monitoração. Por exemplo iniciar um processo ou serviço no caso de queda do mesmo.

2.8.6. A console de gerenciamento deve permitir notificação por e-mail e SMS.

2.8.7. A console de gerenciamento deve permitir executar ações por gatilhos de um alarme.

2.8.8. A solução deve permitir que sobre os alarmes gerados os usuários possam aceitá-los, assinalar, assumir responsabilidade e tomar ação apropriada.

2.8.9. A solução deve permitir consultar o histórico dos alarmes.

2.8.10. A solução deve permitir o uso de variáveis no texto do alarme.

2.8.11. A solução deve permitir ao usuário/operador filtrar e/ou ordenar os alarmes por meio de campos do alarme.

2.8.12. A solução deve permitir que se defina que usuário/operador possa ver quais tipos de alarmes.

2.8.13. A solução deve permitir ao usuário/operador adicionar comentários aos alarmes.

2.8.14. A solução deve permitir criar regrar de correlação de eventos para a geração de alarmes.

2.8.15. A solução deve ter portal web com informações gráficas contendo o status, alarmes e métricas dos sistemas monitorados.

2.8.16. O portal da solução deve apresentar informações atualizadas e históricas.

2.8.17. O portal da solução deve ter visões pré configuradas.

2.8.18. A portal da solução deve ser acessado via web browsers de mercado tais como Safari, Microsoft Edge, Google Chrome e Mozilla Firefox.

2.8.19. A solução deve suportar múltiplos métodos de notificação, incluindo e-mail, SMS, SNMP Traps ou abertura em sistema de Trouble Chamado.

2.8.20. A solução deve ter sistema de agendamento para a tomada de ação de escalonamento/notificação de alertas.

2.9. Painéis e Relatórios.

2.9.1. A solução deve ter sistema de geração de relatórios baseado nos dados contidos no banco de dados relacional da solução.

2.9.2. O sistema de relatórios deve conter relatórios prontos para uso com temas sobre utilização, capacidade ou disponibilidade.

2.9.3. Os relatórios devem conter gráficos, tabelas ou objetos gráficos contendo dados de desempenho.

2.9.4. Os relatórios devem conter gráficos, tabelas ou objetos gráficos (como imagens, URL links) contendo dados de desempenho.

2.9.5. Os usuários devem ter acesso apenas aos relatórios que são destinados a eles.

2.9.6. Os relatórios devem ser acessíveis via HTML.

2.9.7. Os relatórios devem permitir versão em formato PDF.

2.9.8. Os relatórios podem ser enviados via e-mail (com formato PDF).

2.9.9. O sistema deve permitir o agendamento de relatórios.

2.9.10. A solução deve ter portal web com informações gráficas contendo o status, alarmes e métricas dos sistemas monitorados e a ferramenta de relatórios.

2.9.11. O portal da solução deve ser acessado via web browsers de mercado tais como Microsoft Edge, Safari, Google Chrome e Mozilla Firefox.

2.9.12. A solução deve possuir relatórios pré-definidos.

2.9.13. Possibilitar a duplicação de relatórios existentes e edita-los logo após.

2.9.14. Possuir a capacidade de personalização de capas para os relatórios.

2.9.15. Permitir de forma centralizada visualizar os logs recebidos por um ou vários.

2.9.16. dispositivos externos incluindo a capacidade de uso de filtros nas pesquisas deste log.

2.9.17. Logs de auditoria para configurações de regras e objetos devem ser visualizados em uma lista diferente da que exibe os logs relacionados a tráfego de dados.

2.9.18. Possuir a capacidade de personalização de gráficos como barra, linha e tabela para inserção aos relatórios.

2.9.19. Dever ser possível fazer download dos arquivos de logs recebidos.

2.9.20. Deve possuir agendamento para gerar e enviar automaticamente relatórios.

2.9.21. Permitir customização de quaisquer relatórios fornecidos pela solução, exclusivamente pelo administrador, adaptando-o às suas necessidades..

2.9.22. Permitir o envio de maneira automática de relatórios por email.

2.9.23. Deve permitir a escolha do email a ser enviado para cada relatório escolhido.

2.9.24. Permitir programar a geração de relatórios, conforme calendário definido pelo administrador.

2.10. Gerenciamento de níveis de serviço.

2.10.1. A solução deve ter capacidade de medir níveis de serviço da infraestrutura monitorada que seja relacionada as aplicações de negócios.

2.10.2. O sistema de Service Level Manager (SLM) deve permitir a criação e modificação dos Service Level Aggreements (SLAs).

2.10.3. O sistema de SLM deve permitir visualizar e imprimir gráficos e relatórios relacionados aos SLAs.

2.10.4. Os SLAs devem conter campos como: Nome, descrição, período de análise e percentual de atendimento.

2.10.5. Os SLAs devem ter associados a eles Service Level Objectves (SLOs). Logo para que um SLA seja atendido o SLO deve ser atendido.

2.10.6. Os SLOs são compostos por métricas coletadas e armazenadas na solução de monitoração bem como o período operacional de cálculo e formula de cálculo.

2.10.7. A solução deve ter relatórios que mostrem detalhes dos SLAs.

2.10.8. Os relatórios de SLA devem ser acessados via portal da solução, em formato HTML e respeitando perfil de usuário.

2.10.8.1. Os relatórios de SLA podem ser gerados por períodos (diário, mensal, semanal ou anual).

2.10.8.2. Os relatórios de SLA podem incluir períodos futuros, como por exemplo, quartil mostrando potencial quebra de SLA com a projeção baseada em dado já coletado.

2.10.9. A solução deve permitir a adequação dinâmica dos relatórios de SLA's conforme a inclusão de novos sistemas monitorados na solução de monitoração.

2.10.10. Deve ser monitorado no mínimo os parâmetros abaixo:

2.10.10.1. Deve permitir o gerenciamento com ou sem uso de agente.

2.11. Base de conhecimento.

2.11.1. A LOCADORA deverá manter mensalmente as informações de topologia lógica e física documentadas e disponíveis para acesso pelo navegador e App.

2.11.2. A LOCADORA deverá ser notificada automaticamente por correio eletrônico e App sobre qualquer alteração nas documentações da base de conhecimento.

2.11.3. Acesso a ferramenta por web browser para desktops e notebooks e por App para tablet e celulares.

2.11.4. A ferramenta deve notificar sempre que novas informações forem adicionadas.

2.11.5. Os usuários com permissão de acesso a página, poderão manifestar opinião sobre o conteúdo, na própria página em que estão as informações.

2.11.6. A ferramenta deverá permitir a criação de grupos de acesso.

3. DAS OBRIGAÇÕES DA LOCADORA

3.1. A LOCADORA arcará com todos os custos e despesas, tais como: custos diretos e indiretos, tributos, encargos sociais, trabalhistas e previdenciários, seguros, taxas, lucro e outros necessários ao cumprimento integral do objeto, sendo quaisquer tributos, custos e despesas diretas ou indiretas omitidos da proposta ou incorretamente cotadas, serão considerados inclusos nos preços, não podendo ser cogitado pleito de acréscimo, a esse ou qualquer título, devendo o objeto ser fornecido sem ônus adicional.

3.2. A LOCADORA deverá garantir o mais rigoroso sigilo sobre quaisquer dados, informações, documentos e especificações que a ela venham a ser confiados ou que venham a ter acesso em razão dos serviços prestados,

JURÍDICO CSSBC

não podendo, sob qualquer pretexto, revelá-los, divulgá-los, reproduzi-los ou deles dar conhecimento a quaisquer terceiros.

3.3. A LOCADORA deverá substituir ou sanar às suas expensas, no total ou em parte, os serviços em que se verificarem vícios, defeitos, ou incorreções resultantes da fabricação, manutenção ou de materiais empregados, no prazo de 24 (vinte e quatro) horas, a contar da informação a ser realizada preferencialmente por escrito.

3.4. A LOCADORA deverá informar imediatamente ao gestor do contrato eventual suspensão da prestação do serviço, alteração de horário de atendimento, supressão de agenda, remarcações ou qualquer anormalidade verificada na execução do contrato, devendo do mesmo modo, prestar todos os esclarecimentos que lhe forem solicitados pela LOCATÁRIA.

3.5. A LOCADORA deverá garantir todo o apoio técnico por profissional especializado nos serviços, referente a treinamento de pessoal junto às unidades usuárias, caso seja solicitado pela LOCATÁRIA.

3.6. A LOCADORA deverá atribuir no momento da assinatura do Contrato, o responsável para o atendimento a LOCATÁRIA, fornecendo o contato telefônico e e-mail do mesmo.

3.6.1. Eventual alteração do responsável técnico deverá ser imediatamente informada a LOCATÁRIA, encaminhando imediatamente o novo contato.

3.7. A LOCADORA é responsável por garantir a execução plena do objeto deste Contrato, sem qualquer interrupção, independentemente de suas eventuais necessidades de adaptação, desde a assinatura do presente Contrato, salvo caso fortuito ou força maior.

3.8. Durante a execução do contrato a LOCADORA obriga-se a adotar todas as preocupações e cuidados tendentes a evitar danos materiais e pessoais a seus funcionários, seus prepostos e a terceiros, pelos quais será integralmente responsável.

3.9. A LOCADORA deverá indicar um profissional, na condição de preposto contratual, responsável pelo atendimento à LOCATÁRIA em todos os assuntos pertinentes à execução do Contrato.

3.10. A LOCADORA deverá exigir que seus profissionais, quando no ambiente da LOCATÁRIA, apresentem-se de forma adequada, identificados com crachá da empresa com foto recente, que obedeçam aos regulamentos internos do local de trabalho, normas técnicas e protocolos recomendados para os procedimentos realizados.

3.10.1. A LOCADORA deverá manter disciplina nos locais dos serviços substituindo, após notificação, qualquer mão-de-obra cujo comportamento seja considerado inconveniente pela LOCATÁRIA.

3.10.2. A LOCADORA deverá informar previamente, com no mínimo 48 (quarenta e oito) horas de antecedência ao procedimento, o nome completo e o número do documento do profissional que prestará os serviços esporadicamente nas instalações ou então encaminhar mensalmente relatório dos funcionários que prestarão os serviços nas unidades.

3.11. A LOCADORA deverá comunicar previamente a LOCATÁRIA nos casos de modificação ou indisponibilidade da marca dos materiais utilizados, dando as justificativas da alteração e apresentando as outras marcas do material para análise e aprovação da LOCATÁRIA, se obrigando a manter os preços estabelecidos no presente Contrato, caso esses sejam de maior valor.

3.11.1. A solicitação de alteração de marca deverá ser realizada dentro de um prazo mínimo de 10 (dez) dias antecedentes a próxima entrega, informando junto a solicitação a data em que o fornecimento será regularizado.

3.11.2. Caso a marca proposta não seja aprovada, a LOCADORA deverá apresentar outra opção que seja compatível com os padrões já utilizados.

3.11.3. Se, após as análises, nenhuma marca apresentada for aprovada, a LOCATÁRIA se faculta o direito de buscar empresas que forneçam o item em questão no mercado, cabendo a LOCADORA arcar com as custas no tocante a diferença do valor contratado com o valor adquirido, até a regularização do fornecimento da marca inicialmente LOCADORA.

3.12. A LOCADORA deve cumprir, além das normas vigentes de âmbito Federal, Estadual ou Municipal, as Normas de Segurança e Medicina do Trabalho.

JURÍDICO CSSBC

3.13. A LOCADORA não reproduzirá, divulgará ou utilizará em benefício próprio, ou de terceiros, quaisquer informações de que tenha tomado ciência em razão da execução dos serviços discriminados, sem o consentimento prévio e por escrito da LOCATÁRIA.

3.14. A LOCADORA não utilizará o nome da LOCATÁRIA, ou sua qualidade de LOCADORA, em quaisquer atividades de divulgação empresarial, como, por exemplo, em cartões de visita, anúncios e impressos, sem o consentimento prévio e por escrito da LOCATÁRIA.

3.15. A LOCADORA instruirá sua mão-de-obra, quanto à prevenção de acidente no trabalho de acordo com as normas vigentes instituídas pela Engenharia de Segurança do Trabalho da LOCATÁRIA, provendo-os dos equipamentos de proteção individual (EPI), com exceção aos itens constantes no item 5.6 do anexo II, bem como fiscalizando o seu uso.

3.16. A LOCADORA prestará os serviços dentro dos parâmetros de rotinas estabelecidas, fornecendo todos os materiais e equipamentos em quantidade, qualidade e tecnologia adequadas, com a observância das normas técnicas e legislações vigentes.

3.17. A LOCADORA garantirá livre acesso a informações, dos procedimentos e à documentação referente aos serviços prestados, aos gestores indicados pela LOCATÁRIA, para o acompanhamento da gestão contratual.

3.18. A LOCADORA responsabiliza-se pelos danos causados diretamente à LOCATÁRIA ou a terceiros, em decorrência de suas ações, tendo direito a LOCATÁRIA ao ressarcimento da LOCADORA, por força contratual, em eventual responsabilidade da LOCATÁRIA em decorrência de defeitos nos serviços da LOCADORA, podendo inclusive denunciá-la à lide para evitar o ajuizamento de ação de regresso.

3.19. Ao final da vigência deste Contrato, toda a documentação, históricos, processos estabelecidos e arquivos gerados, deverão ser entregues pela LOCADORA à LOCATÁRIA.

3.20. A LOCADORA se responsabilizará por todas as despesas com encargos e obrigações sociais, trabalhistas, fiscais e comerciais decorrentes da execução contratual, sendo que os empregados da LOCADORA não terão, em hipótese alguma, qualquer relação de emprego com a LOCATÁRIA.

3.20.1. Caberá a LOCADORA requerer a exclusão da LOCATÁRIA do polo passivo de eventuais ações demandadas por seus funcionários em face LOCATÁRIA, visando minimizar prejuízos judiciais e econômicos para esta Instituição.

3.21. A LOCADORA terá seu desempenho submetido a acompanhamentos sistemáticos de acordo com os critérios de avaliação e controle da LOCATÁRIA, através de formulários próprios.

3.22. A fiscalização ou acompanhamento da execução deste Contrato, por parte dos órgãos competentes da LOCATÁRIA, não exclui nem reduz a responsabilidade da LOCADORA.

3.23. A LOCADORA cumprirá o Regimento Interno e as demais Normas Internas do LOCATÁRIA, assim como outras normas relativas à engenharia de segurança do trabalho com base na lei 6.514, de 22/09/1977, portaria 3.214, (NR) e demais disposições legais e às regulamentações da Agência Nacional de Vigilância Sanitária (ANVISA) e do Ministério da Saúde.

3.24. A LOCADORA manterá completo e absoluto sigilo sobre quaisquer dados, materiais, pormenores, informações, documentos, especificações técnicas ou comerciais, inovações que venha a ter conhecimento ou acesso, ou que venha a ser confiado em razão deste contrato, inclusive os dados protegidos pela Lei Geral de Proteção de Dados Pessoais nº 13.709/2018, não podendo, sob qualquer pretexto, divulgar, revelar, reproduzir, utilizar, tratar, ou deles dar conhecimentos a terceiros a esta contratação, sob pena da lei.

3.25. A LOCADORA será responsável por todos os ônus e tributos, emolumentos, honorários ou despesas incidentais sobre os serviços contratados, bem como cumprir rigorosamente, todas as obrigações trabalhistas, previdenciárias e acidentárias relativas ao pessoal que empregar para a execução dos serviços, inclusive as

decorrentes de convenções, acordos ou dissídios coletivos, mantendo a disposição do LOCATÁRIA toda e qualquer documentação pertinente (ficha de registro, guias de recolhimento dos encargos trabalhistas e previdenciários, exames admissionais e periódicos).

3.26. A LOCADORA assume a defesa contra quaisquer reclamações ou demandas ambientais, administrativas e judiciais, arcando com os respectivos ônus, decorrentes de quaisquer falhas na prestação dos serviços ora contratados ou danos que venham a ser causados durante o período de execução dos serviços, seja na atuação direta, seja por seus empregados ou prepostos.

3.27. A LOCADORA não terá como sócios, gerentes, diretores ou administradores, os cônjuges, companheiros (as) ou parentes em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de funcionários, ocupantes dos cargos de direção, chefia, assessoramento da LOCATÁRIA, sob pena de rescisão contratual.

3.28. A LOCADORA não utilizará na execução do objeto do presente contrato, quaisquer funcionários, administradores ou ocupantes de cargos de direção da Fundação do ABC e de suas mantidas.

3.29. Fica vetado à LOCADORA utilizar na prestação dos serviços, profissionais que sejam funcionários da LOCATÁRIA, bem como ex colaboradores que tenham trabalhado para a LOCATÁRIA nos últimos 18 (dezoito) meses que anteceder a prestação de serviços objeto do presente contrato, conforme artigo 5º-D da Lei 6.019/74.

4. DAS OBRIGAÇÕES DA LOCATÁRIA

4.1. A LOCATÁRIA gerenciará o Contrato, por intermédio de sua Gerência de Tecnologia da Informação.

4.2. A LOCATÁRIA exercerá a fiscalização, examinando quanto ao cumprimento deste Contrato.

4.3. A LOCATÁRIA efetuará os pagamentos, referentes aos serviços prestados, deduzindo-se das faturas as eventuais glosas determinadas pelo Gestor do Contrato, sendo assegurado à LOCADORA o direito à ampla defesa.

4.4. Não obstante a LOCADORA seja a única responsável pela prestação do serviço, a LOCATÁRIA reserva-se o direito de, sem que de qualquer forma restrinja a plenitude desta responsabilidade, exercer a fiscalização mais ampla e completa sobre os serviços prestados e aceitos pela LOCATÁRIA.

4.5. A LOCATÁRIA assegurar-se-á que o número de empregados alocados ao serviço por parte da LOCADORA seja o suficiente para o adequado desempenho dos serviços.

4.6. A LOCATÁRIA solicitará à LOCADORA e seus prepostos, tempestivamente, todas as providências necessárias ao adequado desempenho dos serviços.

4.7. A LOCATÁRIA emitirá pareceres em todos os atos relativos à execução deste Contrato, em especial, a aplicação de sanções, alterações e repactuações contratuais.

4.8. A LOCATÁRIA permitirá o livre acesso dos empregados da LOCADORA para execução dos serviços, quando autorizados.

4.9. A LOCATÁRIA exigirá, após ter advertido a LOCADORA por escrito, o imediato afastamento de qualquer empregado ou preposto da mesma, que não mereça a sua confiança ou embarace a fiscalização ou, ainda, que se conduza de modo inconveniente ou incompatível com o exercício das funções que lhe forem atribuídas.

4.10. É vedada à LOCATÁRIA, e seus representantes, exercer poder de mando sobre os empregados da LOCADORA, reportando-se somente aos prepostos e responsáveis por ela indicados.

JURÍDICO CSSBC

4.11. A LOCATÁRIA assegurará as condições mínimas para a realização dos procedimentos com segurança, garantindo a guarda e conservação dos serviços, após sua conferência e entrada em seu estabelecimento.

4.12. A LOCATÁRIA fiscalizará por intermédio do gestor/fiscal do contrato os serviços objeto do Contrato.

4.13. A LOCATÁRIA prestará informações e esclarecimentos que eventualmente venham a ser solicitadas pela LOCADORA e que digam respeito à natureza dos serviços que tenham de executar.

5. DAS SANÇÕES ADMINISTRATIVAS E DEMAIS PENALIDADES

5.1. A LOCATÁRIA poderá aplicar advertência quando ocorrer prestação insatisfatória dos serviços ou pequenos transtornos ao desenvolvimento dos serviços, desde que sua gravidade não recomende as sanções posteriormente descritas.

5.2. Em caso de infrações, o CSSBC poderá aplicar à LOCADORA a seguinte sanção de multa:

5.2.1. Multa de 10% (dez por cento), por inexecução parcial do contrato, calculada sobre o valor mensal do Contrato. Na hipótese de reincidência por parte da LOCADORA, a LOCATÁRIA poderá rescindir o contrato, nos termos da cláusula 8.2 da Minuta de Contrato.

5.2.2. Multa de 20% (vinte por cento), por inexecução total do contrato, calculada sobre o valor total do Contrato

5.2.3. Faculta-se ao CSSBC, no caso da LOCADORA não cumprir o serviço contratado, adquirir o serviço de outra empresa, devendo a LOCADORA arcar com os custos que eventualmente forem acrescidos para a aquisição.

5.3. A LOCATÁRIA poderá, em decorrência da gravidade dos atos praticados pela LOCADORA, suspender temporariamente sua participação em coleta de preços a ser realizada pelo Complexo de Saúde São Bernardo do Campo, pelo prazo de até 02 (dois) anos.

5.3.1. A LOCADORA possui plena ciência que a LOCATÁRIA encaminhará relato do ocorrido a municipalidade e a Fundação do ABC, mantenedora da LOCATÁRIA, para que caso assim desejem, também suspendam o direito de participar em processos de compras/contratação por eles iniciados.

5.4. A sanção de multa poderá ser aplicada cumulativamente com as demais sanções, não terá caráter compensatório e a sua cobrança não isentará a LOCADORA de indenizar a LOCATÁRIA por eventuais perdas e danos.

5.5. Constatado o descumprimento de quaisquer obrigações decorrentes do ajuste, a LOCATÁRIA notificará a LOCADORA acerca de sua intenção de aplicar-lhe eventuais penas, sendo-lhe facultada apresentação de defesa escrita, se assim entender, no prazo de 05 (cinco) dias úteis, contados do recebimento da referida notificação.

5.6. Uma vez apresentada a defesa, a LOCATÁRIA poderá, após análise, deferir a pretensão, restando afastada, então, a possibilidade da penalização, ou indeferir a pretensão, dando prosseguimento aos trâmites administrativos visando à efetiva aplicação da pena.

5.6.1. Na hipótese de indeferimento, será a LOCADORA notificada da referida decisão, podendo a LOCATÁRIA realizar o abatimento da multa calculada na nota fiscal emitida para o pagamento dos serviços contratados.

6. DAS CONDIÇÕES DE PAGAMENTO E CRITÉRIOS DE FATURAMENTO

6.1. A LOCATÁRIA deverá pagar à LOCADORA o valor dos produtos fornecidos, exclusivamente através de depósito em conta corrente.

6.1.1. A LOCADORA deverá indicar na documentação fiscal original o número de sua conta corrente, agência e banco no qual deverá ser efetuado o pagamento.

6.1.2. Em nenhuma hipótese serão aceitos títulos via cobrança bancária.

6.2. O pagamento dos serviços/ será realizado no dia 28 (vinte e oito) do mês, subsequente ao mês da prestação dos serviços, desde que a nota fiscal seja entregue à LOCATÁRIA com, no mínimo, 10 (dez) dias de antecedência à data do vencimento, com a apresentação junto a Nota Fiscal / Fatura das certidões de

JURÍDICO CSSBC

regularidade fornecidas pela Secretaria da Receita Federal do Brasil e pela Procuradoria Geral da Fazenda Nacional referente a débitos relativos aos tributos federais e à dívida ativa da União (CND), FGTS (CRF) e Justiça do Trabalho (CNDT), por parte da LOCADORA.

6.2.1. Caso se faça necessária a reapresentação de qualquer fatura por culpa da LOCADORA, o prazo previsto na presente Cláusula será reiniciado.

6.2.2. Dos pagamentos, será retido na fonte, quando for o caso, o valor correspondente ao Imposto Sobre Serviços de Qualquer Natureza (ISSqn), nos termos da legislação específica e demais tributos que recaiam sobre o valor faturado.

6.2.3. A liberação para pagamento da nota fiscal/fatura ficará condicionada ao ateste do Gestor do Contrato e à entrega dos documentos mencionados no item 6.2.

6.2.4. Todas as notas fiscais em seu conteúdo original devem ser emitidas com os seguintes dizeres: **"Despesa realizada com base no C.Gestão SS nº 001/2022 com a PMSBC.**

6.3. A LOCADORA deverá encaminhar a nota fiscal desmembrada para cada unidade, e estas deverão ser emitidas para a Fundação do ABC – Complexo de Saúde São Bernardo do Campo, CNPJ n° 57.571.275/0025-70.

Endereço de Fatura e Cobrança: Estrada dos Alvarengas, 1001 – Bairro Alvarenga – São Bernardo do Campo/SP.

6.3.1. Fica facultado a LOCADORA o envio da nota fiscal eletronicamente.

6.4. A LOCADORA, neste ato, declara estar ciente de que os recursos utilizados para o pagamento dos serviços ora contratados serão aqueles repassados pela Prefeitura Municipal de São Bernardo do Campo, em razão do Contrato de Gestão SS n° 001/2022, firmado entre a LOCATÁRIA e a Prefeitura Municipal de São Bernardo do Campo, para a gestão do Complexo de Saúde São Bernardo do Campo.

6.5. A LOCATÁRIA informa que, a única fonte de receita a ser utilizado para pagamento dos serviços ora contratados é aquela prevista no contrato de gestão 001/2022, sendo vedada a utilização de qualquer outra fonte de recurso para pagamento, nos termos do §7° do artigo 51 do regulamento de compras.

6.6. A LOCATÁRIA compromete-se em pagar o preço irreajustável constante da proposta da LOCADORA, desde que não ocorram atrasos e/ou paralisação dos repasses pela Prefeitura Municipal de São Bernardo do Campo para a LOCATÁRIA, relativo ao custeio do objeto do Contrato de Gestão SS n° 001/2022.

6.7. No caso de eventuais atrasos, os valores serão atualizados de acordo com a legislação vigente, salvo quando não decorram de atrasos e/ou paralisação dos repasses pela Prefeitura Municipal de São Bernardo do Campo para a LOCATÁRIA, em consonância com o disposto nas cláusulas 6.4, 6.5 e 6.6 deste CONTRATO.

7. DAS ALTERAÇÕES DO CONTRATO

7.1. O presente contrato poderá ser alterado, desde que, de forma fundamentada e em consenso, sempre através de termo aditivo.

7.2. As partes poderão realizar acréscimos ou supressões ao objeto do presente contrato desde que previamente acordadas e formalizadas por meio de termo aditivo.

7.2.1. Os acréscimos e supressões poderão ser solicitados pela LOCATÁRIA, cabendo à LOCADORA, em caso de discordância, notificar o interesse no distrato observando o prazo mínimo estipulado neste instrumento.

8. DA RESCISÃO/RESILIÇÃO

8.1. As partes poderão resilir, imotivadamente, o presente Contrato, desde que comunicado por escrito à outra com antecedência mínima de 30 (trinta) dias, ou celebrar, amigavelmente, o seu distrato na forma da lei, em qualquer caso, nenhuma indenização será devida.

8.2. A rescisão, por inadimplemento das obrigações prevista no presente Contrato poderá ser declarada unilateralmente pela LOCATÁRIA, mediante decisão motivada.

8.3. Dar-se-á automaticamente a rescisão dos contratos decorrentes de obrigações contraídas por meio de Convênios Administrativos ou Contratos de Gestão, no caso de rescisão das respectivas avenças administrativas, sendo que nesta hipótese nenhuma indenização será devida, facultando-se a resilição unilateral sem aviso prévio.

8.4. Na hipótese de rescisão por inadimplemento, além das sanções cabíveis, ficará a LOCADORA sujeita à multa de 10% (dez por cento) calculada sobre o saldo do serviço não executado, sem prejuízo da retenção de créditos, reposição de importâncias indevidamente recebidas e das perdas e danos que forem apurados.

9. DA CESSÃO E TRANSFERÊNCIA

9.1. O presente contrato não poderá ser objeto de cessão, transferência ou subcontratação no todo ou em parte, a não ser com prévio e expresso consentimento da LOCATÁRIA e sempre mediante instrumento próprio.

9.1.1. O cessionário fica sub-rogado em todos os direitos e obrigações do cedente e deverá atender a todos os requisitos de habilitação previamente estabelecidos.

10. DO RECURSO AO JUDICIÁRIO

10.1. Caso as partes tenham que ingressar em juízo para haver o que lhe for devido, ficarão sujeitas ao pagamento do principal, despesas processuais e honorários, conforme determinação judicial arbitrada em sentença.

11. DA VIGÊNCIA

11.1. O prazo de vigência deste Contrato será de 36 (trinta e seis) meses, contados a partir da data de sua assinatura.

11.1.1. O prazo contratual poderá ser prorrogado por iguais ou menores períodos e sucessivos, até o limite de 48 (quarenta e oito) meses.

11.1.2. O valor permanecerá inalterado durante a vigência do presente Contrato podendo ser reajustado com base no índice IGP-M a cada período de 12 (doze) meses, desde que seja previamente discutido e acordado entre as partes.

12. DO VALOR

12.1. Dá-se ao presente Contrato o valor total anual estimado de R$ 989.568,00 (novecentos e oitenta e nove mil e quinhentos e sessenta e oito reais), sendo:

Item	Descrição	Qtde.	Valor Unitário	Valor Mensal	Valor Total
1	Firewall Avançado - NGFW	2	RS 7.144,00	RS 14.288,00	RS 514.368,00
2	Firewall Intermediário - NGFW	1	RS 2.050,00	RS 2.050,00	RS 73.800,00
3	Firewall Básico – NGFW	1	RS 700,00	RS 700,00	RS 25.200,00
4	Solução de Gerenciamento de Eventos e Relatórios	1	RS 2.150,00	RS 2.150,00	RS 77.400,00
5	Serviço de implantação e configuração das soluções	1	RS 800,00	RS 800,00	RS 28.800,00
6	Serviço de suporte, monitoramento e gestão das ferramentas	1	RS 7.500,00	RS 7.500,00	RS 270.000,00
Valor Total			-	**R$ 27.488,00**	**RS 989.568,00**

12.1.1. O valor acima descrito se trata de mera estimativa, não se obrigando a LOCATÁRIA, de forma alguma, a atingi-lo.

JURÍDICO CSSBC

13. DA EXCEÇÃO DO CONTRATO NÃO CUMPRIDO

13.1. A LOCADORA não poderá opor a LOCATÁRIA a exceção do Contrato não cumprido como fundamento para a interrupção unilateral do serviço, nos termos de art. 476 do Código Civil.

14. DO FORO DE ELEIÇÃO

14.1. Fica eleito o Foro do município de São Bernardo do Campo, para dirimir qualquer dúvida ou litígio decorrente do presente contrato, com expressa renúncia a outro por mais privilegiado que seja.

15. DAS DISPOSIÇÕES GERAIS

15.1. Fica a LOCADORA obrigada a manter durante a execução deste Contrato todas as condições de qualificação e habilitação exigidas no respectivo procedimento de Coleta de Preços.

15.2. Considerando a possibilidade de as partes negociarem os termos deste contrato, fica desde já afastada, na presente contratação, a aplicabilidade do artigo 423 do Código Civil vigente.

15.3. Os termos deste Contrato são confidenciais e, salvo disposição legal em contrário, a LOCATÁRIA não poderá divulgar esses termos a nenhum terceiro sem o consentimento por escrito da LOCADORA.

15.4. A tolerância por qualquer das Partes quanto ao cumprimento das cláusulas e condições contratuais ora firmadas não implicará renúncia, novação, transação ou precedente, devendo ser havida como mera liberalidade.

15.5. Se uma disposição contratual for considerada inválida, ilegal ou inexequível a qualquer título, tal disposição será considerada em separado e não invalidará as disposições restantes, as quais não serão afetadas por esse fato.

E, por estarem as partes de comum acordo sobre as Cláusulas, termos e condições deste instrumento, firmam-no em 02 (duas) vias de igual teor e conteúdo, na presença de 02 (duas) testemunhas.

São Bernardo do Campo, 02 de junho de 2023.

AGNES MELLO FARIAS FERRARI
Representante

JOSÉ RAMDE UCHÔA JARDIM
Representante

FUNDAÇÃO DO ABC – COMPLEXO DE SAÚDE SÃO BERNARDO DO CAMPO

LEANDRO ANDRÉ RODRIGUES BARASNIEWSKI
Representante
INFOREADY TECNOLOGIA LTDA

Testemunhas:
1- Nome: Joana Coimbra da Silva **CPF.:** 453610[illegible]-13 **Ass.:**
2- Nome: Luis H. C. Galvão **CPF.:** 160.763.150-41 **Ass.:**

JURÍDICO CSSBC

ANEXO I

ESPECIFICAÇÕES TÉCNICAS

ESCOPO DE CONTRATAÇÃO

Item	Descrição	Quantidade
1	Firewall Avançado - NGFW	2
2	Firewall Intermediário - NGFW	1
3	Firewall Básico – NGFW	1
4	Solução de Gerenciamento de Eventos e Relatórios	1
5	Serviço de implantação e configuração das soluções	1
6	Serviço de suporte, monitoramento e gestão das ferramentas	1

1. Características Específicas

- Throughput de, no mínimo, 20 Gbps com a funcionalidade de firewall habilitada para tráfego IPv4 e IPv6, independentemente do tamanho do pacote.
- Suportar no mínimo 7,5 milhões conexões simultâneas.
- Suportar no mínimo 250 mil novas conexões por segundo.
- Throughput de no mínimo 18 Gbps de VPN IPSec.
- Throughput de no mínimo 4 Gbps de VPN SSL.
- Throughput de, no mínimo, 4,5 Gbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito.
- Todas as funcionalidades descritas no item acima deverão estar devidamente licenciadas para utilização durante todo o período contratual.
- Deve possuir, pelo menos, 8 interfaces 1000Base-T com conectores RJ-45.
- Deve possuir, pelo menos, 8 interfaces 1000Base-X com conectores SFP.
- Deve possuir, pelo menos, 2 interfaces 10GBase-X com conectores SFP+.
- Deve possui armazenamento interno, no mínimo, de 240GB em SSD.
- Deve suportar fonte redundante "Hot Swappable".
- Estar licenciado, sem custo adicional, 10 sistemas virtuais lógicos (Contextos) por appliance.

2. Firewall Intermediário – NGFW

- Características Específicas:
  - Throughput de, no mínimo, 4 Gbps com a funcionalidade de firewall habilitada para tráfego IPv4, independentemente do tamanho do pacote.
  - Suportar no mínimo 2 milhões conexões simultâneas.
  - Suportar no mínimo 25 mil novas conexões por segundo.
  - Throughput de no mínimo 3,8 Gbps de VPN IPSec.
  - Throughput de no mínimo 230 Mbps de VPN SSL.
  - Throughput de, no mínimo, 250 Mbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito.
  - Todas as funcionalidades descritas no item acima deverão estar devidamente licenciadas para utilização durante todo o período contratual.

- Deve possuir, pelo menos, 12 interfaces 1000Base-T com conectores RJ-45.

3. Firewall Básico – NGFW

- Características Específicas:
  - Throughput de, no mínimo, 2,5 Gbps com a funcionalidade de firewall habilitada para tráfego IPv4.
  - Suportar no mínimo 1,6 milhões conexões simultâneas.
  - Suportar no mínimo 20 mil novas conexões por segundo.
  - Throughput de no mínimo 90 Mbps de VPN IPSec.
  - Throughput de no mínimo 100 Mbps de VPN SSL.
  - Deve possuir, pelo menos, 5 interfaces 1000Base-T com conectores RJ-45.

4. Características Gerais dos Firewalls Avançado, Intermediário e Básico

- Características Gerais:
  - A solução deve consistir em plataforma de proteção de rede baseada em appliance com funcionalidades de Next Generation Firewall (NGFW), e console de gerência e monitoração.
  - Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões.
  - As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação.
  - A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7.
  - O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta.
  - O gerenciamento da solução deve suportar a interface de administração via web no próprio dispositivo de proteção de rede.
  - Os dispositivos de proteção de rede devem possuir suporte a 4094 VLAN Tags 802.1q.
  - Os dispositivos de proteção de rede devem possuir suporte a agregação de links 8023ad e LACP.
  - Os dispositivos de proteção de rede devem possuir suporte a Policy based routing ou policy-based forwarding.
  - Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM).
  - Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay.
  - Os dispositivos de proteção de rede devem possuir suporte a DHCP Server.
  - Os dispositivos de proteção de rede devem suportar sFlow.
  - Os dispositivos de proteção de rede devem possuir suporte a Jumbo Frames.
  - Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas.
  - Deve suportar NAT dinâmico (Many-to-1).
  - Deve suportar NAT dinâmico (Many-to-Many).
  - Deve suportar NAT estático (1-to-1).
  - Deve suportar NAT estático (Many-to-Many).
  - Deve suportar NAT estático bidirecional 1-to-1.
  - Deve suportar Tradução de porta (PAT).
  - Deve suportar NAT de Origem.
  - Deve suportar NAT de Destino.
  - Deve suportar NAT de Origem e NAT de Destino simultaneamente.
  - Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico.
  - Deve suportar NAT64 e NAT46.
  - Deve implementar o protocolo ECMP.
  - Deve implementar balanceamento de link por hash do IP de origem.
  - Deve implementar balanceamento de link por hash do IP de origem e destino.

- Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, três links.
- Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais.
- Deve permitir monitorar via SNMP falhas de hardware, uso de recursos por número elevado de sessões, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede.
- Enviar log para sistemas de monitoração externos, simultaneamente.
- Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL.
- Proteção anti-spoofing.
- Implementar otimização do tráfego entre dois equipamentos.
- Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2).
- Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3).
- Suportar OSPF graceful restart.
- Os dispositivos de proteção devem ter a capacidade de operar de forma simultânea em uma única instância de firewall, mediante o uso de suas interfaces físicas nos seguintes modos: Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3).
- Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede.
- Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego.
- Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha visibilidade do tráfego.
- Deve suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas.
- Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em modo transparente.
- Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3.
- Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3 e com no mínimo 3 equipamentos no cluster.
- A configuração em alta disponibilidade deve sincronizar: Sessões.
- A configuração em alta disponibilidade deve sincronizar: Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede.
- A configuração em alta disponibilidade deve sincronizar: Associações de Segurança das VPNs
- A configuração em alta disponibilidade deve sincronizar: Tabelas FIB.
- O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link.
- Deve possuir suporte a criação de sistemas virtuais no mesmo appliance.
- Em alta disponibilidade, deve ser possível o uso de clusters virtuais, seja ativo-ativo ou ativo-passivo, permitindo a distribuição de carga entre diferentes contextos.
- Deve permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados por equipes distintas.
- O gerenciamento da solução deve suportar acesso via SSH e interface WEB (HTTPS), incluindo, mas não limitado à exportar configuração dos sistemas virtuais (contextos) por ambas interfaces.
- Controle, inspeção e descriptografia de SSL para tráfego de entrada (Inbound) e Saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos).

- Controle por Política de Firewall:
  - Deverá suportar controles por zona de segurança.
  - Controles de políticas por porta e protocolo.
  - Controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações.

- Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança
- Controle de políticas por código de País (Por exemplo: BR, USA, UK, RUS).
- Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound).
- Deve suportar offload de certificado em inspeção de conexões SSL de entrada (Inbound).
- Deve descriptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2.
- Controle de inspeção e descriptografia de SSH por política.
- Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada.
- Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo).
- QoS baseado em políticas para marcação de pacotes (diffserv marking), inclusive por aplicações.
- Suporte a objetos e regras IPV6.
- Suporte a objetos e regras multicast.
- Deve suportar no mínimo três tipos de resposta nas políticas de firewall: Drop sem notificação do bloqueio ao usuário, drop com notificação do bloqueio ao usuário, Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego, TCP-Reset para o client, TCP-Reset para o server ou para os dois lados da conexão.
- Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

- Controle de Aplicações:
  - Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo.
  - Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos.
  - Reconhecer pelo menos 2200 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.
  - Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs.
  - Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo.
  - Deve detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a Bittorrent e aplicações VOIP que utilizam criptografia proprietária.
  - Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor.
  - Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante.
  - Identificar o uso de táticas evasivas via comunicações criptografadas.
  - Atualizar a base de assinaturas de aplicações automaticamente.
  - Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos.
  - 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 Domain Controller, nem nas estações dos usuários.
  - Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras.

- Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos.
- Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas.
- Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante.
- A criação de assinaturas personalizadas deve permitir o uso de expressões regulares, contexto (sessões ou transações), usando posição no payload dos pacotes TCP e UDP e usando decoders de pelo menos os seguintes protocolos: HTTP, FTP, NBSS, DCE RPC, SMTP, Telnet, SSH, MS-SQL, IMAP, DNS, LDAP, RTSP e SSL.
- O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações.
- Deve alertar o usuário quando uma aplicação for bloqueada.
- Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos.
- Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos.
- Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts chat e bloquear a chamada de vídeo.
- Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos.
- Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc).
- Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Nível de risco da aplicação.
- Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação.

- Prevenção de Ameaças:
  - Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall.
  - Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware).
  - As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.
  - Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade.
  - Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar tcp-reset.
  - As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração.
  - Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança.
  - Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura.
  - Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes politicas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.
  - Deve permitir o bloqueio de vulnerabilidades.
  - Deve permitir o bloqueio de exploits conhecidos.

- Deve incluir proteção contra ataques de negação de serviços.
- Deverá possuir o seguinte mecanismo de inspeção de IPS: Análise de padrões de estado de conexões.
- Deverá possuir o seguinte mecanismo de inspeção de IPS: Análise de decodificação de protocolo.
- Deverá possuir o seguinte mecanismo de inspeção de IPS: Análise para detecção de anomalias de protocolo.
- Deverá possuir o seguinte mecanismo de inspeção de IPS: Análise heurística.
- Deverá possuir o seguinte mecanismo de inspeção de IPS: IP Defragmentation.
- Deverá possuir o seguinte mecanismos de inspeção de IPS: Remontagem de pacotes de TCP.
- Deverá possuir o seguinte mecanismos de inspeção de IPS: Bloqueio de pacotes mal formados.
- Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc.
- Detectar e bloquear a origem de portscans.
- Bloquear ataques efetuados por worms conhecidos.
- Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS.
- Possuir assinaturas para bloqueio de ataques de buffer overflow.
- Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto.
- Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações.
- Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3.
- Suportar bloqueio de arquivos por tipo.
- Identificar e bloquear comunicação com botnets.
- Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo.
- Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação.
- Deve permitir que na captura de pacotes por assinaturas de IPS seja definido o número de pacotes a serem capturados ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos.
- Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas.
- Os eventos devem identificar o país de onde partiu a ameaça.
- Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms.
- Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos.
- Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.

- Filtro de URL:
  - Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora).
  - Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança.
  - Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local.
  - Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local, em modo de proxy transparente e explícito.

- Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL.
- Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs.
- Possuir pelo menos 60 categorias de URLs.
- Deve possuir a função de exclusão de URLs do bloqueio, por categoria.
- Permitir a customização de página de bloqueio.
- Permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão Continuar para permitir o usuário continuar acessando o site).

- Identificação de Usuários:
  - Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local.
  - Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários.
  - Deve possuir integração e suporte a Microsoft Active Directory para os seguintes sistemas operacionais: Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 e Windows Server 2012 R2.
  - Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários ou qualquer tipo de restrição de uso como, mas não limitado à, utilização de sistemas virtuais, segmentos de rede, etc.
  - Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários.
  - Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em Usuários e Grupos de usuários.
  - Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal).
  - Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços.
  - Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD.
  - Permitir integração com tokens para autenticação dos usuários, incluindo, mas não limitado a acesso a internet e gerenciamento da solução.
  - Prover no mínimo um token nativamente, possibilitando autenticação de duplo fator.

- QoS e Traffic Shaping:
  - Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming.
  - Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem.
  - Suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino.
  - Suportar a criação de políticas de QoS e Traffic Shaping por usuário e grupo.
  - Suportar a criação de políticas de QoS e Traffic Shaping por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus.
  - Suportar a criação de políticas de QoS e Traffic Shaping por porta.
  - O QoS deve possibilitar a definição de tráfego com banda garantida.

- O QoS deve possibilitar a definição de tráfego com banda máxima.
- O QoS deve possibilitar a definição de fila de prioridade.
- Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype.
- Suportar marcação de pacotes Diffserv, inclusive por aplicação.
- Suportar modificação de valores DSCP para o Diffserv.
- Suportar priorização de tráfego usando informação de Type of Service.
- Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping.
- Deve suportar QOS (traffic-shapping), em interface agregadas ou redundantes.

- Filtro de Dados:
  - Permitir a criação de filtros para arquivos e dados pré-definidos.
  - Os arquivos devem ser identificados por extensão e tipo.
  - Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc).
  - Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos.
  - Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos.
  - Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.

- Geo Localização:
  - Suportar a criação de políticas por geo-localização, permitindo o trafego de determinado Pais/Países sejam bloqueados.
  - Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.
  - Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas.

- VPN:
  - Suportar VPN Site-to-Site e Cliente-To-Site.
  - Suportar IPSec VPN.
  - Suportar SSL VPN.
  - A VPN IPSEc deve suportar 3DES.
  - A VPN IPSEc deve suportar Autenticação MD5 e SHA-1.
  - A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14.
  - A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2).
  - A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard).
  - A VPN IPSEc deve suportar Autenticação via certificado IKE PKI
  - Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall.
  - Suportar VPN em em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6.
  - Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de troubleshooting.
  - A VPN SSL deve suportar o usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB.
  - A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente.
  - Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies.
  - Atribuição de DNS nos clientes remotos de VPN.

- Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL.
- Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local.
- Suportar leitura e verificação de CRL (certificate revocation list).
- Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL.
- Deve permitir que a conexão com a VPN seja estabelecida das seguintes forma: Antes do usuário autenticar na estação.
- Deve permitir que a conexão com a VPN seja estabelecida das seguintes forma: Após autenticação do usuário na estação.
- Deve permitir que a conexão com a VPN seja estabelecida das seguintes forma: Sob demanda do usuário.
- Deverá manter uma conexão segura com o portal durante a sessão.
- O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bit), Windows 8 (32 e 64 bit), Windows 10 (32 e 64 bit) e Mac OS X (v10.10 ou superior).

- Características de SD-WAN
  - Deve ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico.
  - Deve ser fornecido com a capacidade de implementar ao menos 2 domínios virtuais (Gerência e Operação).
  - O appliance SD-WAN deverá ser fornecido com bandeja ou suporte para montagem em rack.
  - Deve possuir capacidade de agregar e balancear, no mínimo, 4 circuitos de dados utilizando uma interface dedicada para cada circuito.
  - A solução Sd-wan deve ser viabilizada com recursos de segurança integrados de: Firewall, VPN, Antivírus, IPS e Filtro de Segurança Web.
  - A solução Sd-wan deve suportar micro-segmentação de tráfego onde seja possível aplicar políticas de IPS e Antivírus entre segmentos de LAN.
  - A solução Sd-wan deve suportar NAT em contexto de saída (Nat Outbound) para um pool de IPs públicos.
  - A solução deve prover gerência centralizada, e deve ser capaz de oferecer uma gerência Multi-Tenancy.
  - Solução deve ser capaz de prover Zero Touch provisioning.
  - A solução de Zero Touch provisioning deve ser capaz de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN
  - A solução de Zero Touch deve ser escalável, suportando um mínimo, todos os dispositivos da solução em uma mesma comunidade VPN neste context.
  - Solução deve ser capaz de prover uma arquitetura onde em uma comunicação Sede x Subseções, em que a comunicação de uma Subseção A para a Sede esteja comprometida, possa ser utilizada a comunicação entre Subseção B e a Sede, em que através deste circuito, a Subseção A alcance a Sede.
  - Solução deve suportar RFC7018 - ADVPN entre Sede e Subseções com autenticação baseada em padrão x.509 - Certificados Digitais e também PSK.
  - A solução deve ser capaz de criar VPN "Full-Mesh" em interface Gráfica, de forma automática, e sem que o administrador precise configurar site por site.
  - A configuração VPN IPSEC deverá oferecer suporte para versão IKE v2.0.
  - A configuração VPN IPSEC deverá oferecer suporte para DH Group: 14 e 15.
  - Solução deve ser capaz de prover uma arquitetura onde em uma comunicação Sede x Subseção, em que a Subseção também esteja utilizando seu acesso de Internet local para se comunicar com outro elemento de SD-WAN em nuvem pública e caso este circuito venha a falhar, que seja utilizado o túnel VPN com a Sede, para possibilitar a comunicação da Subseção com esta máquina na Nuvem Pública.
  - A solução deve suportar aos seguintes requisitos:
    - IPv6.

- VRRP ou Equivalente.
- VRF.
- BGP.
- OSPF.
- RIPv1.
- Dynamic Multipath.
- Policy Based Routing.

- Reconhecimento em camada 7 totalmente segregado da camada 4.
- Deve de forma alternativa, contar com um banco de Dados interno, onde seja possível atrelar uma aplicação à um determinado IP/ range de IPs de destino.
- O reconhecimento de aplicações, deve ser atualizado de forma dinâmica e totalmente transparente para o no dispositivo
- O reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados.
- Ainda sobre o reconhecimento de Aplicações, a solução deve fornecer o reconhecimento default em camada 7, de pelo menos 2000 aplicações largamente utilizadas em contextos de SaaS, Aplicações na Nuvem, Aplicações Multimídia (Vimeo, YouTube, Facebook, etc).
- A solução, em sua modalidade física e/ou virtual, deve considerar os seguintes intens:
  - 802.1Q.
  - BFD ou BGP.
- A solução de SD-WAN deve suportar Roteamento dinâmico BGP.
- A solução de SD-WAN deve suportar Roteamento dinâmico BGP com suporte a IPv4 e quando requisitado possuir suporte a IPv6 mesmo que seja necessário substituição do equipamento, com o ônus da LOCADORA.
- A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de SD-WAN em condições onde a largura de banda é modificada.
- A solução deve ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss, onde seja possível configurar um valor de Theshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN.
- A solução deve ser capaz de medir o Status de Saúde com Suporte a múltiplos servidores.
- A solução deve permitir modificar configuração de tempo de checagem em segundos para cada um dos links.
- A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorrerá quando o link principal recuperado seja X% (com X variando de 10 à 50) do seu valor de Saúde melhor que o link atual.
- A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorra dentro de um espaço de tempo de X segundos, configurável pelo administrador do sistema.
- A solução deve permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface SD-WAN.
- A solução deve permitir a configuração de políticas de QoS em valores onde o máximo corresponda à totalidade de largura de banda disponível no equipamento
- A solução deve permitir a consulta via SNMPv2/v3 referente aos seguintes dados:
  - Estado atual dos links SD-WAN.
  - Latência.
  - Jitter.
  - Packet Loss.
  - Pacotes enviados / Pacotes Recebidos.
  - Link Bandwitdh.
- A solução deve possibilitar a distribuição de Peso em cada um dos links que compõe o SD-WAN, a critério do administrador, de forma em que o algoritmo de balanceamento utilizado possa ser baseado em:

JURÍDICO CSSBC

- Número de Sessões.
- Volume de Tráfego.
- IP de Origem e Destino.
- Transbordo de Link (Spillover).

- A Solução deve apresentar compatibilidade com modens USB (3G/4G), onde estes sejam capazes de funcionar como circuito Ativo Ativo em relação à saída principal de internet, e também alternativamente funcionar em uma arquitetura Ativo x Standby, onde apenas seja acionado na eventualidade de falha no link principal.
- Solução deve ser capaz de suportar uma arquitetura de transporte Multicast IPv4 e IPv6 através de tuneis VPN IPSEC construídos em ADVPN.
- Solução deve possuir capacidade de autenticar usuários para administração do Equipamento, através de base de dados:
  - Local.
  - Integrada a servidor TACACS+ ou RADIUS.
  - Integrada a servidor Ldap ou RADIUS.
- Alternativamente a solução deve suportar base de dados centralizada própria, onde toda a arquitetura SD-Wan converja a ela.
- A Gerência centralizada da solução SD-WAN deverá ser suportar:
  - Administração Multi-tenancy.
  - Pre-visualização das mudanças em Políticas e Configurações antes que estes entrem em produção.
  - Workflow de Aprovação para Implantação de Mudanças.
  - Telemetria.
- Disparar ações automáticas de: Envio de traps SNMPv2/v3, Alertas por Email e Envio de Log ao Servidor Syslog quando em situações de:
  - HA Failover.
  - Túnel IPSec Up/Down.
  - Interface UP/Down.
  - Appliance em estado inoperante.
- Provisionamento de Templates SD-WAN que considere critérios relacionados à:
- A Alta Disponibilidade provide pela solução de SD-WAN, indepedente em suas modalidades físicas ou virtual, deverá obedecer os seguintes critérios:
- Suportar Balanceamento Ativo – Ativo, Ativo – Passivo, Distribuído Geograficamente.
- A solução SD-Wan deve oferecer Troubleshooting em console de linha de comando ou gráfica, onde seja possível:
  - Executar Packet sniffer do tráfego interessante, filtrando por: IP e Porta.
  - Realizar debug detalhado das fases de negociação VPN.
- A Solução SD-Wan deve oferecer visualização gráfica de:
  - Aplicações mais utilizadas com respectiva largura de banda
  - Shapping de Tráfego SD-WAN.
- IPs de Destino mais utilizados com respectivo número de Sessões e Largura de Banda associados.
- A solução SDWAN deve suportar marcação de pacotes DSCP nas definições e regras para tráfego SDWAN.
- Os appliances devem ser capazes de inspecionar (Descriptografar) tráfego SSL e permitir aplicar regras dentro dos túneis das aplicações.

5. Solução de Gerenciamento de Eventos e Relatórios

- Características Gerais:
- Deverá ser entregue em appliance virtual, compatível com ambiente VMware ESXi 5.5 e 6.0, Microsoft Hyper-V 2008 R2 / 2012 / 2012 R2 e Citrix XenServer 6.0+.
- Deverá possuir licenciamento com capacidade de receber ao menos 15 GBytes de logs diários.

- Deve suportar acesso via SSH, WEB (HTTPS) e Telnet para o gerenciamento da solução.
- Possuir comunicação cifrada e autenticada com usuário e senha para solução de relatórios, tanto como para a interface gráfica de usuário e console de administração por linha de comandos (SSH).
- Permitir acesso simultâneo de administradores permitindo a criação de ao menos 2 (dois) perfis para administração e monitoração.
- Suportar SNMP versão 2 e versão 3 na solução de relatórios.
- Permitir virtualizar a solução de relatórios, onde cada administrador gerencie, visualize e edite apenas os dispositivos autorizados e cadastrados no seu ambiente virtualizado.
- Deve permitir a criação de administradores que acessem à todas as instâncias de virtualização da solução de relatórios.
- Deve permitir habilitar e desabilitar, para cada interface de rede da solução de relatórios, permissões de acesso HTTP, HTTPS, SSH, SNMP e Telnet.
- Autenticação integrada a servidor Radius.
- Geração de relatórios em tempo real, para a visualização de tráfego observado, nos formatos: mapas geográficos e tabela.
- Geração de relatórios em tempo real, para a visualização de tráfego observado, no formato bolhas.
- Autenticação integrada ao Microsoft Active Directory.
- Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações.
- Deve possuir um assistente para adicionar dispositivos via interface gráfica usando o IP, login e senha dos mesmos.
- Deve ser possível visualizar a quantidade de logs enviado de cada dispositivo monitorado.
- Possuir mecanismo para que logs antigos sejam removidos automaticamente.
- Permitir a importação e exportação de relatórios.
- Deve possuir a capacidade de criar relatórios nos formatos HTML.
- Deve possuir a capacidade de criar relatórios nos formatos PDF.
- Deve possuir a capacidade de criar relatórios nos formatos XML.
- Deve possuir a capacidade de criar relatórios nos formatos CSV.
- Deve ser possível exportar os logs em CSV.
- Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração.
- Os logs gerados pelos appliances devem ser centralizados nos servidores de gerência, mas a solução deve oferecer também a possibilidade de utilização de um syslog externo ou similar.
- A solução deve possuir relatórios pré definidos.
- Possuir envio automático de logs para um servidor FTP externo a solução.
- Possibilitar a duplicação de relatórios existentes e edita-los logo após.
- Possuir a capacidade de personalização de capas para os relatórios.
- Permitir de forma centralizada visualizar os logs recebidos por um ou vários dispositivos externos incluindo a capacidade de uso de filtros nas pesquisas deste log.
- Logs de auditoria para configurações de regras e objetos devem ser visualizados em uma lista diferente da que exibe os logs relacionados a tráfego de dados.
- Possuir a capacidade de personalização de gráficos como barra, linha e tabela para inserção aos relatórios.
- Deve possuir mecanismo "Drill-Down" para navegação nos relatórios em realtime.
- Dever ser possível fazer download dos arquivos de logs recebidos.
- Deve possuir agendamento para gerar e enviar automaticamente relatórios.
- Permitir customização de quaisquer relatórios fornecidos pela solução, exclusivamente pelo administrador, adaptando-o às suas necessidades..
- Permitir o envio de maneira automática de relatórios por email.
- Deve permitir a escolha do email a ser enviado para cada relatório escolhido.
- Permitir programar a geração de relatórios, conforme calendário definido pelo administrador.

JURÍDICO CSSBC

- Deve ser possível visualizar através de gráficos em tempo real o consumo de disco e taxa de geração de logs dos dispositivos gerenciados.
- Deve ser possível definir filtros nos relatórios.
- Deve ser capaz de definir o layout do relatório, incluir gráficos, inserir textos e imagens, alinhamento, quebras de páginas, definir fontes, cores, entre outros.
- Permitir que relatórios criados sejam no idioma Português.
- Gerar alertas automáticos via Email, SNMP e Syslog baseados em eventos como ocorrência como log, severidade de log, entre outros.
- Deve permitir o envio automático de relatórios criado a um servidor de SFTP ou FTP externo a solução.
- Deve ser capaz de criar consultas SQL ou semelhante para uso nos gráficos e tabelas de relatórios.
- Ter a capacidade de visualizar na GUI da solução de relatórios informações do sistema como licenças, memória, disco, uso de CPU, taxa de logs por segundo recebidos, total de logs diários recebidos, alertas gerados entre outros.
- Deve possuir uma ferramenta para análise de desempenho para cada relatório gerado, com o objetivo de detectar problemas de performance de sistema de acordo com o relatório criado.
- Permitir que a solução importe arquivos de log, de dispositivos compatíveis conhecidos e não conhecidos pelo sistema, para posterior geração de relatórios.
- Deve ser possível definir o espaço que cada instâncias de virtualização poderá utilizar para armazenamento de logs.
- A solução deve servir como um servidor de syslog e aceitar logs de diferentes fabricantes.
- Deve possuir a informação da quantidade de logs armazenado e estatística de tempo de retenção restante.
- Deve suportar duplo fator de autenticação (token) para os administradores do sistema de relatórios.
- Deve permitir aplicar políticas de senhas para os administradores do sistema como tamanho mínimo e caracteres a usar.
- Deve permitir ver em tempo real os log recebidos.
- Deve permitir a criação de Dashboards customizados para visibilidades do tráfego de aplicativos, categorias de URL, ameaças, serviços, países, origem e destino.
- Deve possuir um Indicador de Comprometimento (IoC), que mostre usuários finais com utilização web suspeita, devendo informar no mínimo: endereço ip do usuário, hostname, sistema operacional, veredito (classificação geral de ameaça), número de ameaças detectadas.
- Deve possuir relatório de PCI DSS Compliance.
- Deve possuir relatório de utilização de aplicações SAAS.
- Deve possuir relatório detalhado de prevenção de perda de dados (DLP).
- Deve possuir relatório de VPN.
- Deve possuir relatório de Sistemas de prevenção de intrusão (IPS).

/////