TERMO DE REFERÊNCIA

CONTRATAÇÃO DE EMPRESA ESPECIALIZADA NO FORNECIMENTO DE RECURSOS, SERVIÇOS E GARANTIA DO FIREWALL WHATCHGUARD DO COREN-BA.

1. DO OBJETO

1.1. Contratação de empresa especializada no fornecimento de recursos, serviços e garantia do firewall WhatchGuard do Coren-BA, conforme condições e especificações constantes neste Termo.

CONTRATAÇÃO DE SERVIÇOS E PRODUTOS

LOTE I		
ITEM	**DESCRIÇÃO**	**QUANTIDADE**
01	Renovação da Licença de Software WatchGuard Total Security M370 – por 12 meses – Ativo/Ativo, para equipamentos modelo M370 (Seriais: 8013065E212F9 e 8013066824228)	02

LOTE II		
ITEM	**DESCRIÇÃO**	**QUANTIDADE**
01	Serviço de Suporte Técnico Especializado para os equipamentos Firewall WatchGuard (Modelo M370)(Seriais: 8013065E212F9 e 8013066824228)	01

2. DA JUSTIFICATIVA

2.1. O Conselho Regional de Enfermagem da Bahia mantém, nas suas instalações, um parque computacional com diversos sistemas aplicativos em produção, para subsidiar a execução de suas atribuições legais e atividades administrativas, bem como para

processamento dos serviços de atendimento à categoria de Enfermagem em todo estado da Bahia.

2.2. Para proteger os servidores que hospedam aplicações deste conselho, tais como Servidor de Arquivos, Servidor do Sistema Incorp, Servidor de Impressão, Servidores do Sistema de atendimento (Proxximo) entre outros, e manter operacional a sede e subseções deste conselho, contamos com 1 (um) cluster de equipamentos (appliance) Firewall do fabricante Watchguard modelo M370. Esses equipamentos foram adquiridos em 2020, por meio do processo PAD Nº 294/2019.

2.3. Os equipamentos tecnológicos do tipo Firewalls são responsáveis por todo o controle de acesso, (entrada e saída) aos dados do COREN-BA. Estes equipamentos são agrupados em dois, formando uma solução com alta disponibilidade — cluster.
O cluster faz a proteção dos equipamentos servidores que hospedam serviços que são disponibilizados na Internet, como o sistema IncorpNet. Eles controlam o que pode ser acessado de acordo com o perfil do usuário, além de possibilitar o aviso de possíveis ataques a esses ambientes — módulo IPS (Intrusion Prevention System), protegem os equipamentos servidores internos do Coren-BA que disponibilizam os dados aos usuários, como por exemplo o serviço de banco de dados. Esses equipamentos controlam os acessos de acordo com a permissão/perfil dos usuários, além de permitir uma auditoria em possíveis ataques ou vazamento de dados.

2.4. Com a contratação de recursos, serviços e garantia do firewall Watchguard iremos manter atualizadas as seguintes funcionalidades:

Access Portal: que oferece suporte para implementações de single-on (SSO) para acesso centralizado a aplicativos hospedados em nuvem e à recursos internos via RDP e SSH. O Access Portal permite a criação de túneis VPN seguros e acesso remoto sem a necessidade de hardware ou software adicional, usando um proxy de camada de aplicativo que atua como um buffer seguro entre as solicitações do usuário recebidas de servidores de internet

pública e de aplicativos back-end para proteger a infraestrutura da rede.

Proteção contra ameaças ocultas: O Coren-BA possui nos seus desktops, notebooks e servidores o antivírus BitDefender que é baseado em assinaturas de antivirus como primeira linha de defesa eliminando ameaças conhecidas. Entretanto ainda há necessidade de uma proteção contra ataques desconhecidos que passam por ela. O Watchguard APT Blocker disponibiliza a análise comportamental para determinar se um arquivo é mal- intencionado, identificando e enviando arquivos suspeitos para uma sandbox na nuvem, onde o código é emulado, executado e analisado para determinar seu potencial de ameaça. Caso se constate que o arquivo suspeito é mal-intencionado, o APT Blocker toma medidas para garantir segurança dos ativos digitais e de rede. Os malwares modernos incluindo ameaças persistentes, ransomware e ataques day-zero são projetados para reconhecer as defesas tradicionais e passar por elas. A emulação de um sistema completo pelo APT Blocker que simula um ambiente físico, fornece maior proteção contra malware avançado.

Intelligent AV: possui mecanismo de aprendizado de máquina para defender melhor contra ataques de dia zero em desenvolvimento continuo. Ele consegue prever ameaças meses antes de serem liberadas proporcionando uma proteção preditiva. O malware moderno muda a uma taxa incrível e pode sofrer alterações a cada hora, tornando obsoleta a detecção de assinatura dos antivírus. O inteligente AV detecta os malwares que tentam entrar na rede usando modelos matemáticos que não exigem conectividade na nuvem, assinaturas ou análises comportamentais, mantendo o ambiente seguro mesmo quando os bancos de assinaturas não estiverem atualizados.

Threat Detection and Response (TDR): por meio de pacotes sofisticados, criptografia e poliformismo os criminosos cibernéticos conseguem disfarçar seus ataques. O TDR correlaciona indicadores de ameaças dos appliances do Firebox e sensores de host para ameaças conhecidas, desconhecidas e evasivas. O Host Ransonware Prevention (HRP) é um módulo específico de ransomware dentro do TDR que utiliza análise comportamental e honeypots para procurar sinais de ransomware. Se for detectado o HRP automaticamente intervém para parar o ransomware antes dos arquivos se perderem.

Phishing: bloquear conexões mal-intencionadas ao DNS e proteger contra ataques de phishing, por meio do Watchguard DNSWatch que é um serviço baseado em nuvem que

acrescenta a filtragem de nível de DNS para detectar e bloquear conexões potencialmente perigosas e proteger a rede do Coren-BA contra ataques prejudiciais.

Application Control: serviço de assinatura que permite monitorar e controlar o uso de aplicativos na rede. O controle de aplicativos usa mais de 1.800 assinaturas que podem identificar e bloquear mais de 1.000 aplicativos. Permite bloquear o uso de aplicativos específicos e permite a geração de relatórios do uso de aplicativos e tentativas de uso. Para alguns aplicativos, pode bloquear comportamentos específicos do aplicativo, como transferência de arquivos.

Reputation Enabled Defense (RED): O WatchGuard RED usa um servidor de reputação WatchGuard baseado em nuvem que atribui uma pontuação de reputação entre 1 e 100 a cada URL. Quando um usuário acessa um site, a RED envia o endereço da Web solicitado (ou URL) para o servidor de reputação da WatchGuard. O servidor WatchGuard responde com uma pontuação de reputação para esse URL. Com base na pontuação de reputação e nos limites configurados localmente, o RED determina se o Firebox deve eliminar o tráfego, permitir o tráfego e verificá-lo localmente com o Gateway AntiVirus ou permitir o tráfego sem uma verificação local do Gateway AntiVirus. Isso aumenta o desempenho, porque o Gateway AntiVirus não precisa verificar URLs com boa ou má reputação.

WebBlocker: Ao fornecer aos usuários acesso ilimitado aos sites, a instituição poderá sofrer perda de produtividade e ocupação da largura de banda do link de internet. A navegação descontrolada na Internet também pode aumentar os riscos de segurança e a responsabilidade legal. A assinatura de segurança do WebBlocker permite o controle dos sites que estão disponíveis para os usuários. O WebBlocker usa um banco de dados que agrupa endereços de sites em categorias de conteúdo. Quando um usuário na rede tenta se conectar a um site, o Firebox procura o endereço no banco de dados do WebBlocker e executa a ação específica para a categoria do conteúdo.

Intrusion Prevention Service (IPS): fornece proteção em tempo real contra ameaças, incluindo spyware, injeções de SQL, script entre sites e estouros de buffer. Quando um novo ataque é identificado, são registradas as características que tornam o ataque de intrusão único. Esses recursos gravados são conhecidos como assinatura. O IPS usa essas assinaturas para identificar ataques de intrusão.

Gateway AntiVirus: Os hackers usam muitos métodos para atacar computadores na Internet. Os vírus, incluindo worms e trojans, são programas de computador maliciosos que se autoreplicam e colocam cópias de si mesmos em outros códigos executáveis ou documentos em seu computador. Quando um computador é infectado, o vírus pode destruir arquivos ou gravar teclas digitadas. Para ajudar na proteção da rede contra vírus, o Coren-BA utiliza o serviço de assinatura do Gateway AntiVirus. O Gateway AntiVirus opera com os proxies SMTP, IMAP, POP3, HTTP, FTP, Explícito e TCP-UDP. Quando um novo ataque é identificado, são registradas as características que tornam o vírus único. Esses recursos gravados são conhecidos como assinatura. O Gateway AntiVirus usa assinaturas para encontrar vírus quando o conteúdo é verificado pelo proxy.

2.5. Considerando parte da arquitetura atual, onde são realizados acessos externos através dos notebooks, bem como das subseções via VPN no âmbito do Coren-BA, faz-se necessária maior segurança para garantir que os computadores pessoais se conectem na rede do Coren-BA, mantendo a segurança e integridade da mesma.

2.6. Importante destacar que na solução atual, alguns usuários dos notebooks corporativos possuem perfis de administrador, podendo instalar novos programas, por isso, mais do que nunca se faz necessário o controle destas instalações. Por isso, é imperativo controlar também o acesso desses equipamentos. Tais computadores podem estar infectados gerando risco de propagarem vírus desconhecidos e vazamento de informações ao se conectarem na rede do Coren-Ba.

2.7. O Firewall do Coren-BA ainda é necessário para prover segurança aos acessos VPN (Virtual Private Network) aos sistemas internos e dados armazenados no servidor de arquivos desta Autarquia, realizando inclusive filtro de sites que sejam considerados indesejados pelo Coren-BA.

2.8. O Plano Diretor de Tecnologia da Informação e Comunicação (PDTI) do Coren-BA é um instrumento de diagnóstico, planejamento e gestão dos recursos e processos de

Tecnologia da Informação que visa atender às necessidades tecnológicas e de informação do Coren-BA. A necessidade desta contratação está prevista no PDTIC, no item 8 (Diagnósticos e recomendações) — Atualização de infraestrutura de segurança da informação do COREN.

2.9. Em relação a referida disponibilidade e segurança, a garantia de 12 (doze) meses, podendo ser renovada de acordo com a lei 8.666/9, é necessária de modo a permitir que os dados que trafegam na rede de dados do Coren-BA e que estão armazenados no Storage estejam disponíveis de forma permanente e continua. Essa garantia visa assegurar que uma interrupção firewall não comprometa a prestação dos serviços do Coren-BA, bem como o cumprimento da sua missão institucional.

2.10. Face ao acima exposto, considerando que a solução em pauta irá proteger os dados e equipamentos do Coren-BA contra software malicioso e ataques e invasões perpetradas por hackers, os quais poderiam:

- comprometer a confidencialidade de dados, promovendo vazamentos que afetariam a imagem do Coren-BA;
- afetar a integridade dos dados - algumas modalidades como o Ransomware sequestram dados exigindo resgates e outras técnicas podem inclusive apagar / destruir dados de uma organização; e
- atingir a disponibilidade dos dados e sistemas.

2.11. Conclui-se que se trata de um serviço essencial cuja necessidade pública ocorre de modo permanente e continuo, por mais de um exercício financeiro, assegurando a integridade do patrimônio público e o funcionamento das atividades finalísticas do Coren-BA, de maneira que sua interrupção poderia comprometer a prestação de serviços como o Genf, ou o cumprimento da missão institucional do Coren-BA.

3. DA CLASSIFICACAO DE SERVICO COMUM

3.1. O objeto desta licitação se enquadra nos termos do parágrafo único, do Art. 1º, da Lei

Federal nº 10.520/2002, que regulamenta a modalidade de licitação denominada pregão, por se tratar de bem comum, com características e especificações usuais de mercado.

3.2. Embora a Lei do Pregão nos forneça um conceito do tipo aberto sobre o que seja comum, verificou-se que as especificações são usuais no mercado após analisar os três aspectos listados abaixo:

3.3. A possibilidade de padronizar o objeto por meio de critérios objetivos e desempenho e qualidade comuns no mercado correspondente;

3.4. Disponibilidade no mercado destes bens; e

3.5. Verificado se as especificações adotadas eram usuais neste mesmo mercado.

3.6. A presente aquisição foi considerada comum e verificou-se que as especificações são usuais pelo mercado.

4. DA FUNDAMENTAÇÃO LEGAL

4.1. A aquisição obedecerá ao disposto na Lei Federal nº 10.520, de 17 de julho de 2002, Decreto Federal nº 10.024, de 20 de setembro de 2019, e aplicando-se subsidiariamente a Lei Federal nº 8.666, de 21 de Julho de 1993 e alterações posteriores, bem como demais normativos constantes no Instrumento Convocatório.

5. DO CRITÉRIO DE JULGAMENTO

5.1. O critério de julgamento adotado será o de menor preço por item, em atenção ao Art. 7º, caput, do Decreto Federal nº 10.024/2019.

5.2. Serão desclassificadas as propostas que não atenderem às especificações e exigências contidas neste Termo de Referência e/ou edital, bem como aquelas que apresentarem preços excessivos ou manifestamente inexequíveis, comparados aos preços de mercado, em consonância com o disposto no Art. 48, Inciso II, 55 1º e 2º, da Lei nº 8.666/1993.

6. DA ESPECIFICAÇÃO DO OBJETO E DO VALOR ESTIMADO

6.1. Contratação de recursos, serviços e garantia do firewall Watchguard por 12 meses.

6.2. O valor estimado da renovação de serviços e recursos do firewall Watchguard é de R$ 94.195,96 (Noventa e quatro mil, cento e noventa e cinco reais e noventa e seis centavos).

6.3. LOTE I — Renovação da Licença de Software WatchGuard Total Security M370 – por 12 meses – Ativo/Ativo, para equipamentos modelo M370 (Seriais: 8013065E212F9 e 8013066824228).

6.4. Características das licenças:

6.4.1. Access Portal: que oferece suporte para implementações de single-on (SSO) para acesso centralizado a aplicativos hospedados em nuvem e a recursos internos via RDP e SSH. O Access Portal permite a criação de túneis VPN seguros e acesso remoto sem a necessidade de hardware ou software adicional, usando um proxy de camada de aplicativo que atua como um buffer seguro entre as solicitações do usuário recebidas de servidores de internet pública e de aplicativos back-end para proteger a infraestrutura da rede;

6.4.2. Proteção contra ameaças ocultas: O Coren-BA possui nos seus desktops, notebooks e servidores o antivírus Bitdefender que é baseado em assinaturas de antivírus como primeira linha de defesa eliminando ameaças conhecidas. Entretanto ainda há necessidade de uma proteção contra ataques desconhecidos que passam por ela. O Watchguard APT Blocker disponibiliza a análise comportamental para determinar se um arquivo é mal-intencionado, identificando e enviando arquivos suspeitos para uma sandbox na nuvem, onde o código é emulado, executado e analisado para determinar seu potencial de ameaça. Caso se constate que o arquivo suspeito é mal-intencionado, o APT Blocker toma medidas para garantir 02(duas) camadas de segurança dos ativos digitais e de rede. Os malwares modernos incluindo ameaças persistentes, ransomware e ataques day-zero são projetados para reconhecer as defesas tradicionais e passar por elas. A emulação de um sistema completo pelo APT Blocker que simula um ambiente físico, fornece maior proteção contra malware avançado;

6.4.3. Intelligent AV: possui mecanismo de aprendizado de máquina para defender melhor contra ataques de dia zero em desenvolvimento continuo. Ele consegue prever ameaças

meses antes de serem liberadas proporcionando uma proteção preditiva. O malware moderno muda a uma taxa incrível e pode sofrer alterações a cada hora, tornando obsoleta a detecção de assinatura dos antivírus. O inteligente AV detecta os malwares que tentam entrar na rede usando modelos matemáticos que não exigem conectividade na nuvem, assinaturas ou análises comportamentais, mantendo o ambiente seguro mesmo quando os bancos de assinaturas não estiverem atualizados;

6.4.4. Threat Detection and Response (TDR): por meio de pacotes sofisticados, criptografia e poliformismo os criminosos cibernéticos conseguem disfarçar seus ataques. O TDR correlaciona indicadores de ameaças dos appliances do Firebox e sensores de host para ameaças conhecidas, desconhecidas e evasivas. O Host Ransonware Prevention (HRP) é um módulo específico de ransomware dentro do TDR que utiliza análise comportamental e honeypots para procurar sinais de ransomware. Se for detectado o HRP automaticamente intervém para parar o ramsomware antes dos arquivos se perderem;

6.4.5. Phishing: bloquear conexões mal-intencionadas ao DNS e proteger contra ataques de phishing, por meio do Watchguard DNSWatch que é um serviço baseado em nuvem que acrescenta a filtragem de nível de DNS para detectar e bloquear conexões potencialmente perigosas e proteger a rede do Coren-BA contra ataques prejudiciais;

6.4.6. Application Control: serviço de assinatura que permite monitorar e controlar o uso de aplicativos na rede. O controle de aplicativos usa mais de 1.800 assinaturas que podem identificar e bloquear mais de 1.000 aplicativos. Permite bloquear o uso de aplicativos específicos e permite a geração de relatórios do uso de aplicativos e tentativas de uso. Para alguns aplicativos, pode bloquear comportamentos específicos do aplicativo, como transferência de arquivos.

6.4.7. Reputation Enabled Defense (RED): O WatchGuard RED usa um servidor de reputação WatchGuard baseado em nuvem que atribui uma pontuação de reputação entre 1 e 100 a cada URL. Quando um usuário acessa um site, a RED envia o endereço da Web solicitado (ou URL) para o servidor de reputação da WatchGuard. O servidor WatchGuard responde com uma pontuação de reputação para esse URL. Com base na pontuação de reputação e nos limites configurados localmente, o RED determina se o Firebox deve eliminar o tráfego, permitir o tráfego e verificá-lo localmente com o Gateway AntiVirus ou permitir o tráfego

sem uma verificação local do Gateway AntiVirus. Isso aumenta o desempenho, porque o Gateway AntiVirus não precisa verificar URLs com boa ou má reputação.

6.4.8. WebBlocker: Ao fornecer aos usuários acesso ilimitado aos sites, a instituição poderá sofrer perda de produtividade e ocupação da largura de banda do link de internet. A navegação descontrolada na Internet também pode aumentar os riscos de segurança e a responsabilidade legal. A assinatura de segurança do WebBlocker permite o controle dos sites que estão disponíveis para os usuários. O WebBlocker usa um banco de dados que agrupa endereços de sites em categorias de conteúdo. Quando um usuário na rede tenta se conectar a um site, o Firebox procura o endereço no banco de dados do WebBlocker e executa a ação específica para a categoria do conteúdo.

6.4.9. Intrusion Prevention Service (IPS): fornece proteção em tempo real contra ameaças, incluindo spyware, injeções de SQL, script entre sites e estouros de buffer. Quando um novo ataque é identificado, são registradas as características que tornam o ataque de intrusão único. Esses recursos gravados são conhecidos como assinatura. O IPS usa essas assinaturas para identificar ataques de intrusão.

6.4.10. Gateway AntiVirus: Os hackers usam muitos métodos para atacar computadores na Internet. Os vírus, incluindo worms e trojans, são programas de computador maliciosos que se autoreplicam e colocam cópias de si mesmos em outros códigos executáveis ou documentos em seu computador. Quando um computador é infectado, o vírus pode destruir arquivos ou gravar teclas digitadas. Para ajudar na proteção da rede contra vírus, o Coren-BA utiliza o serviço de assinatura do Gateway AntiVirus. O Gateway AntiVirus opera com os proxies SMTP, IMAP, POP3, HTTP, FTP, Explícito e TCP-UDP. Quando um novo ataque é identificado, são registradas as características que tornam o vírus único. Esses recursos gravados são conhecidos como assinatura. O Gateway AntiVirus usa assinaturas para encontrar vírus quando o conteúdo é verificado pelo proxy.

6.4.11. As licenças deverão ser associadas aos appliances com Seriais: 8013065E212F9 e 8013066824228 do Coren-BA;

6.4.12. Atualizações de todas as licenças que integram o pacote Total Security Suite durante a vigência do contrato;

6.4.13. Vigência de 12 (doze) meses, podendo ser renovado de acordo com a lei 8.666/93.

6.5. LOTE II - Serviço de Suporte Técnico Especializado para os equipamentos Firewall WatchGuard modelo M370. (Seriais: 8013065E212F9 e 8013066824228).

6.5.1. Prover suporte técnico, manutenção/garantia com substituição de peças e atualização de firmware por 12 meses;

6.5.2. Substituir o equipamento por outro equivalente/superior quando ficar inoperante por mais de 72 horas;

6.5.3. Durante a vigência do contrato deverá ser fornecido suporte técnico pela licitante seguindo as especificações abaixo:

6.5.3.1. A Licitante deverá realizar atendimento na modalidade on-site / online, modalidade a ser definida pela CONTRATANTE, no endereço fornecido pela CONTRATANTE durante a vigência do Contrato de (12 meses);

6.5.3.2. Número de chamados ilimitados;

6.5.3.3. Atendimento deverá ser realizado via contato telefônico e e-mail;

6.5.3.4. Suporte técnico 24 x 7 (24 horas por dia durante 7 dias por semana), prestado unicamente à equipe de segurança da área de informática da contratante, referente a problemas de funcionamento do produtos fornecidos.

6.5.4. A Licitante deverá ser parceira da WatchGuard a partir do nível Silver. Comprovado na fase de habilitação da empresa.

7. FORMALIZAÇÃO E VIGÊNCIA DO CONTRATO

7.1. Para a contratação de recursos, serviços e garantia do firewall Watchguard, será formalizado um Contrato Administrativo estabelecendo em suas cláusulas todas as condições, garantias, obrigações e responsabilidades entre as partes, em conformidade com este Termo de Referência e com a proposta de preços da licitante vencedora.

7.2. O prazo de vigência do contrato deverá ser de 12 (doze) meses, contados a partir da data de assinatura do contrato, podendo ser renovado de acordo com a legislação vigente.

7.3. Quando da assinatura do contrato a licitante deverá apresentar carta do fabricante informando que é um parceiro autorizado no Brasil para venda de produtos, licenças e

prestação de serviços de suporte técnico

8. PRAZO DE ENTREGA E DO RECEBIMENTO

8.1. Em até 5 (cinco) dias úteis após a assinatura do contrato,o Coren-BA irá solicitar formalmente à CONTRATADA, por meio de Ordem de Serviço, a instalação e configuração das Licenças do Firewall, na sede do Coren-BA, localizado na Rua General Labatut 273 – Barris – Salvador/BA – CEP:40.070-100.

8.2. Após essa solicitação formal, a CONTRATADA deverá executar o serviço de instalação e configuração da solução, conforme regras e padrões definidos neste Termo de Referência, no prazo máximo de 10 (dez) dias (corridos).

8.3. Provisoriamente, será procedida a verificação do produto de acordo com as características descritas no edital, sendo posteriormente aferida a conformidade e atestado por escrito o seu perfeito funcionamento.

8.4. Definitivamente, no prazo máximo de 15 (quinze) dias (úteis), contados a partir do recebimento provisório, depois de constatado que todos os requisitos solicitados foram atendidos e/ou corrigidos por solicitação no atesto provisório e sua consequente aceitação mediante emissão de Termo de Recebimento Definitivo, assinado pelas partes.

9. DO LOCAL DA PRESTAÇÃO DE SERVIÇO

9.1. A prestação da contratação de recursos, serviços e garantia do firewall Watchguard seré realizadana sede do Coren-BA, localizado na Rua General Labatut 273 – Barris – Salvador/BA – CEP:40.070-100.

9.1.1. A prestação dos serviços será realizada 24 x 7 (24 horas por dia durante 7 dias por semana).

9.2. O atendimento deverá ser preferencialmente online.

10. DOS NÍVEIS DE SERVIÇO

10.1. Dos níveis de serviços:

10.1.1. As solicitações de serviço devem seguir os níveis de serviço abaixo, de acordo com o seu nível de severidade (que deverá ser informado no momento da abertura do chamado):

Severidade	Descrição	Prazo para atendimento	Prazo de solução definitiva

Crítico	Indisponibilidade no ambiente de produção	Em até 2 horas	Em até 24 horas, após a abertura do chamado
Grave	Incidentes ou erros que impactam em ambiente de produção, mas não gera a interrupção do sistema ou serviço	Em até 8 horas	Em até 48 horas, após a abertura do chamado
Relevante	Incidentes com serviços secundários ou quenão sejam essenciais ou que posssam ser contornados	Em até 12 horas	Em até 72 horas, após a abertura do chamado

10.1.2. Será considerado o início do atendimento a hora da abertura do chamado técnico.

10.1.3. Será considerado término do chamado o momento em que as funcionalidades da solução estejam disponíveis para uso, com ateste do Gestor do Contrato.

10.1.4. Todo atendimento técnico presencial deverá ser registrado por meio de relatórios técnicos detalhados.

10.2. Abertura de Chamados:

10.3. A abertura do chamado deverá ser realizada por meio de uma das seguintes opções:

10.4. Via telefone com DDD nacional, 24 x 7 (24 horas por dia durante 7 dias por semana);

10.5. E-mail informado pela CONTRATADA;

10.6. Site da CONTRATADA.

11. DA QUALIFICAÇÃO TÉCNICA

11.1. Para fins de comprovação da capacidade técnica, a empresa deverá apresentar no mínimo um Atestado de Capacidade Técnica fornecido por pessoa jurídica de direito público ou privado, declarando ter a empresa realizado ou estar realizando a execução dos serviços, compatível em características com o objeto deste Termo de Referência.

11.2. A empresa vencedora do lote II, além do item anterior, deverá comprovar também ser parceira da WatchGuard a partir do nível Silver.

12. DAS OBRIGAÇÕES DA CONTRATADA

12.1. Designar o preposto para, durante o período de vigência, representa-lo na execução

do contrato.

12.2. O preposto deverá acompanhar todos os trabalhos realizados para atuar como interface entre a equipe técnica do Coren-BA e a equipe da CONTRATADA;

12.3. Fornecer, em qualquer época, as informações e os esclarecimentos técnicos solicitados pelo Coren-BA sobre a execução dos trabalhos;

12.5. Os profissionais e prepostos da CONTRATADA não terão qualquer vínculo empregaticio com a CONTRATANTE, correndo por conta exclusiva da primeira, todas as obrigações decorrentes da legislação trabalhista, previdenciária, infortunistica do trabalho, fiscal, comercial e outras correlatas, as quais se obrigam a saldar na época.

12.6. Responsabilizar-se perante a Administração pelos eventuais danos ou desvios causados aos bens que lhe forem confiados ou aos seus prepostos, devendo efetuar o ressarcimento correspondente, imediatamente após o recebimento da notificação da Administração, sob pena de glosa de qualquer importância que tenha direito a receber;

12.7. Executar os serviços de acordo com as especificações e com os requisitos de qualidade e segurança, recomendados pela Associação Brasileira de Normas Técnicas — ABNT e legislação pertinentes;

12.8. Substituir as licenças/produtos, objeto deste termo, que apresentarem qualquer tipo de defeito ou que estiverem fora das especificações contidas na proposta de preços, no prazo de até 10 (dez) dias úteis, após a comunicação formal do Coren-BA;

12.9. Sanar em tempo hábil todas as irregularidades apontadas pelo Coren-BA;

12.10. Assumir total responsabilidade pelos atos administrativos e encargos previstos na legislação trabalhista, tais como: controle de frequências, ausências permitidas, licenças autorizadas, promoções, férias, punições, admissões, demissões, transferências, como também pelo cumprimento de todas as obrigações trabalhistas, fiscais, previdenciárias e comerciais, inclusive a responsabilidade decorrente de acidentes, indenizações e seguros e outros correlatos;

12.11. Manter sigilo absoluto sobre todas as informações provenientes dos serviços realizados;

12.12. Não transferir a terceiros, no todo ou em parte, por qualquer forma, as obrigações assumidas oriundas do contrato, nem subcontratar;

12.13. A CONTRATADA deverá manter vínculo empregaticio com todos os profissionais alocados aos serviços descritos neste Termo de Referência;

12.14. Executar os serviços conforme especificações do Termo de Referência e do Instrumento Convocatério, com os recursos necessários para o perfeito cumprimento das cláusulas contratuais.

12.15. Arcar com a responsabilidade civil por todos e quaisquer danos materiais e morais causados pela ação ou omissão de seus empregados, trabalhadores, prepostos ou representantes, dolosa ou culposamente, ao Coren-BA ou a terceiros;

12.16. Utilizar empregados habilitados e com conhecimentos básicos dos serviços a serem executados, de conformidade com as normas é determinações em vigor;

12.17. Relatar à Administração toda e qualquer irregularidade verificada no decorrer da prestação dos serviços;

12.18. Não permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos; nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre;

12.19. Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

12.20. Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, devendo complementá-los, caso o previsto inicialmente em suz proposta não seja satisfatório para o atendimento ao objeto da licitação, exceto quando ocorrer algum dos eventos arrolados nos incisos do 5 1º do art. 57 da Lei nº 8.666, de 21 de junho de 1993;

12.21. Todos os custos com pessoal são de responsabilidade da empresa contratada na forma deste documento, sem quaisquer ônus posteriores ao contrato. Todos os impostos, transportes e outros aspectos financeiros deverão estar contidos nos preços da proposta comercial;

12.22. A CONTRATADA deverá declarar que respeita os termos estipulados na Lei nº 5.061, de 08 de março de 2013, que proíbe o uso de mão de obra infantil;

13. DAS OBRIGAÇÕES DA CONTRATANTE

13.1. Nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato, com o objetivo de acompanhar e fiscalizar a execução do contrato, conforme o disposto no Art. 30 da IN 4, de setembro de 2014;

13.2. Prestar as informações e os esclarecimentos solicitados pela Contratada;

13.3. Permitir e acompanhar o acesso dos funcionários da contratada às suas dependências, para execução dos serviços referentes a garantia do objeto, sempre que necessário;

13.4. Emitir relatórios sobre os atos relativos à execução do contrato que vier a ser firmado, em especial, quanto ao acompanhamento e fiscalização da execução dos serviços, à exigência de condições estabelecidas e propostas de aplicação de sanções;

13.5. Impor sanções contratuais caso suas demandas de correção de irregularidades, notificadas à contratada, não sejam corrigidas dentro do prazo estabelecido;

13.6. Recusar no todo ou em parte, com a devida justificativa, qualquer produto entregue ou serviço prestado em desconformidade com o especificado neste Termo de Referência, no Edital, no Contrato e/ou na Proposta da Contratada;

13.7. Efetuar o pagamento devido à Contratada, após o recebimento definitivo dos produtos e apresentação da nota fiscal do objeto, dentro dos prazos estabelecidos;

13.8. Comunicar à Contratada todas e quaisquer ocorrências relacionadas com o objeto da contratação e, se for o caso, com a utilização da garantia dos equipamentos;

13.9. Notificar, por escrito, a Contratada acerca da aplicação de eventuais penalidades, garantindo-lhe o direito ao contraditório e a ampla defesa;

13.10. Aplicar à Contratada as sanções administrativas regulamentares e contratuais cabíveis, quando necessário;

13.11. Outras aplicáveis que a Lei estabelecer.

14. DOS DOCUMENTOS DE COBRANÇA

14.1 A empresa contratada deverá apresentar juntamente com o documento de cobrança a comprovação de que cumpriu as seguintes exigências, cumulativamente:

- Certidão de regularidade com a Fazenda Federal;
- Certidão Negativa de Débitos Trabalhistas;
- Certidão de regularidade com o FGTS;
- Certidão de regularidade com a Fazenda Estadual;
- Certidão de regularidade com a Fazenda Municipal;

Os documentos de cobrança deverão ser entregues pela empresa contratada, eletronicamente, em e-mail informado posteriormente.

15. DO PAGAMENTO

15.1. O pagamento será efetuado em até 30 (trinta) dias úteis, contados a partir da data de apresentação da Nota Fiscal, desde que o documento de cobrança esteja em condições de liquidação de pagamento.

15.2. Passados 30 (trinta) dias úteis sem o devido pagamento por parte da Administração, a parcela devida será atualizada monetariamente, desde o vencimento da obrigação até a data do efetivo pagamento de acordo com a variação pro rata tempore do IPCA.

15.3. O pagamento será efetuado em parcela única.

16. DA GARANTIA CONTRATUAL

16.1. A CONTRATADA, no prazo de até 15 (quinze) dias corridos após a assinatura do Termo de Contrato, prestará garantia no valor correspondente a 2% (dois por cento) do valor do Contrato, podendo optar por qualquer das modalidades previstas no art. 56 da Lei nº 8.666, de 1993.

17. DO REAJUSTE

17.1. Será admitido o REAJUSTE do valor do contrato, com base no Índice Nacional de Preços ao Consumidor Amplo — IPCA apurado durante o período, observada a periodicidade mínima de 12 (doze) meses, a contar da apresentação da proposta, conforme o Decreto nº 37.121/2016

18. DO ACOMPANHAMENTO E FISCALIZAÇÃO

18.1. O acompanhamento e a fiscalização da execução do contrato consistem na verificação da conformidade da prestação dos serviços e da alocação dos recursos necessários, de forma a assegurar o perfeito cumprimento do contrato, devendo ser exercido por comissão designada, na forma dos Arts 67 e 73 da Lei nº 8.666/93 ;

18.2. Não obstante a contratada seja a única e exclusiva responsável pela execução de todo o objeto deste Termo de Referência, a Contratante reservar-se o direito de, sem que de qualquer forma restrinja a plenitude desta responsabilidade, exercer a mais ampla e completa fiscalização sobre a prestação de serviços;

18.3. Caberá ao Gestor do Contrato:

- Acompanhar a prestação de serviços de instalação, configuração, de manutenção e de execução da garantia técnica;
- Gerir o contrato;
- Certificar-se do cumprimento dos acordos de serviços;
- Acompanhar a execução do contrato;
- Anotar em registro próprio todas as ocorrências relacionadas com a execução do Contrato determinando o que for necessário à regularização das faltas, falhas ou defeitos observados.

18.4. A existência de fiscalização do Coren-BA de nenhum modo diminui ou altera a responsabilidade da CONTRATADA na prestação dos serviços a serem executados;

18.5. O Coren-BA poderá exigir o afastamento de qualquer profissional ou preposto da CONTRATADA que venha causar embaraço à fiscalização ou que adote procedimentos incompativeis com o exercício das funções que lhe forem atribuídas;

18.6. Para facilitar a gestão do Contrato e o relacionamento entre as partes, a CONTRATADA deverá indicar apenas 01 (um) Gerente de Relacionamento (preposto), que terá como competência:

18.6.1. Gerenciar e supervisionar a execução dos serviços, franqueando ao Gestor do Contrato, a qualquer tempo, o acesso a seus registros, para efeito de acompanhamento e fiscalização de serviços técnicos efetivamente utilizados;

18.6.2. Tratar com o Gestor do Contrato questões relevantes a sua execução e providenciar a

regularização de falhas ou defeitos observados;

18.6.3. Elaborar e encaminhar relatório mensal dos atendimentos realizados no mês ao Gestor do Contrato;

18.6.4. Tal profissional deverá ter experiência comprovada em gerência de contratos de serviços especializados em tecnologia da informação, envolvendo a gestão de projetos e a gestão de recursos humanos, em níveis compativeis com os serviços contratados pelo Coren-BA;

18.7. Independente dos sistemas de acompanhamento e supervisão que serão exercidos pela CONTRATADA, o Coren-BA exercerá o seu processo de supervisão e acompanhamento do Contrato por meio de um ou mais técnicos designados para este fim, sob a supervisão do Gestor do Contrato.

19. DAS SANÇÕES ADMINISTRATIVAS

19.1. A disciplina das infrações e sanções administrativas aplicáveis no curso da licitação e da execução é aquela prevista no Instrumento Convocatório.

20. SUSTENTABILIDADE

20.1. A CONTRATADA deverá declarar que atende aos requisitos de sustentabilidade previstos no art. 2º da Lei nº 4.770/2012, em conformidade com o Decreto nº 7.746/2012, que regulamenta o art. 3º da Lei nº 8.666/93.

21. DO CONSÓRCIO E DA SUBCONTRATAÇÃO

21.1. A participação de consórcios não será admitida, uma vez que o objeto a ser adquirido é amplamente comercializado por diversas empresas no mercado. Tal permissibilidade poderia causar dano à administração por frustrar o próprio caráter competitivo da disputa pelo menor preço;

21.2. Pelo mesmo fato não há motivos para se admitir a subcontratação, de forma a gerar outros instrumentos contratuais e consequentemente outras atribuições à administração pública. Deste modo, é vedada a subcontratação co objeto.

Salvador, 10 de março de 2023

_____
Marcos Félix
Gerente do DETI

_____
Diego Wesley Miranda de Andrade
Coordenador de Planejamento e Orçamento

_____
Saymon de Jesus Oliveira
Gerente do DEADM - Interino

Rua General Labatut, 273, Barris
CEP: 40070-100
Tel: (71) 3277-3100
www.coren-ba.gov.br