CONTRATO Nº 007/2017

CONTRATO DE FORNECIMENTO QUE ENTRE SI FAZEM, DE UM LADO, COMO CONTRATANTE, A AGÊNCIA GOIANA DE HABITAÇÃO S/A – AGEHAB, E DE OUTRO LADO, COMO CONTRATADA, A EMPRESA CORE SERVIÇOS E INFORMATICA LTDA – ME, EM CONFORMIDADE COM O PROCESSO Nº 775/2016 - 201600031000103.

Por este instrumento particular, as partes abaixo mencionadas e qualificadas, acordam entre si firmar o presente Contrato de fornecimento, conforme as cláusulas e condições a seguir elencadas:

1 – Qualificação das Partes

AGÊNCIA GOIANA DE HABITAÇÃO S/A – AGEHAB**, sociedade de economia mista, portadora do CNPJ nº 01.274.240/0001-47, com sede na Rua 18-A nº 541, Setor Aeroporto, Goiânia – GO, neste ato representada por seu Presidente **Luiz Antonio Stival Milhomens**, brasileiro, casado, contador, portador da Carteira de Identidade nº 3.358.373 2ª Via SSP/GO e CPF nº 839.954.471-04, residente e domiciliado na cidade de Goiânia – Goiás, por seu Diretor Administrativo **Fernando Jorge de Oliveira**, brasileiro, casado, tecnólogo em contabilidade, portador da Carteira de Identidade nº 1792760 SSP-GO e do CPF nº 375.685.581-34, residente e domiciliado nesta Capital e por seu Diretor Financeiro **Hyulley Aquino Machado,** brasileiro, casado, advogado, portador da Carteira de Identidade nº 18481 OAB/GO e do CPF nº 789.352.881-87, residente e domiciliado na cidade de Goiânia – Goiás, doravante designada simplesmente **CONTRATANTE.

CORE SERVIÇOS E INFORMÁTICA LTDA – ME, pessoa jurídica de direito privado, situada na Rua 105-D, nº 104, Setor Sul, Goiânia – Goiás, inscrita no CNPJ sob o nº 11.527.773/0001-47, neste ato representada por Gláucio da Silva Melo, brasileiro, casado, empresário, portador da Cédula de Identidade nº 3.150.294 2ª via e do CPF nº 851.080.301-34, e Lorivaldo Xavier de Oliveira, brasileiro, casado, empresário, portador da Carteira de Identidade nº 1444654 2ª Via SSP/GO e do CPF nº 396.886.071-34, residentes e domiciliados nesta capital, doravante designada simplesmente CONTRATADA.

DO FUNDAMENTO LEGAL

Este contrato decorre da licitação realizada na modalidade Pregão Eletrônico nº 002/2017, de acordo com a Lei Federal nº 10.520/2002, Lei Federal nº 8.666/1993 e suas alterações posteriores, Lei Estadual nº 17.928/2012, Decreto Estadual nº 7.468/2011, Lei Complementar nº 117/2015 e demais normas regulamentares aplicáveis à espécie, conforme termo de Homologação e processo administrativo nº 0775/2016, regendo-o no que for omisso.

2016.01031.000775-29 - ID nº 511181

CLÁUSULA PRIMEIRA – DO OBJETO

1.1. O presente contrato tem por finalidade o fornecimento de APPLIANCE dedicado com subsistemas de FIREWALL STATEFUL, VPN, filtro de URL, FILTRO DE MALWARE, garantia, suporte técnico e serviços de assinatura, conforme descrições contidas no Termo de Referência - ANEXO I e Proposta da Contratada, conforme quadro abaixo:

LOTE 01:

Item	Descrição	Unidade	Quantidade	Preço unitário (R$)	Preço Total (R$)
1	Appliance de Firewall	Un.	01		76.650,00
2	Treinamento Hands-on	UST.	40	283,72	11.348,80
			VALOR TOTAL DA PROPOSTA		87.998,80

DAS CARACTERÍSTICAS DO APPLIANCE FIREWALL

1.2. Suporte a definição de VLAN trunking conforme padrão IEEE 802.1q, a criação de interfaces lógicas associadas às VLANs e o estabelecimento de regras de filtragem (Stateful Firewall) entre elas;

1.3. Deve suportar agregação de portas, com a criação de grupos de pelo menos 08 (oito) portas. Deve ser suportado o padrão LACP (Link Aggregation Control Protocol);

1.4. Construir registro de fluxos de dados relativos a cada sessão iniciada, armazenando para cada uma destas sessões informações tais como endereços de origem e destino dos pacotes, portas TCP (e UDP) de origem e destino, bem como números de sequência dos pacotes TCP, status dos flags "ACK", "SYN" e "FIN";

1.5. Permitir a "randomização" do número de sequência TCP, ou seja, funcionar como um "proxy" de número de sequência TCP de modo a garantir que um host situado em uma interface considerada "externa" (insegura), sob o ponto de vista de política de segurança do firewall, nunca tenha acesso ao número de sequência TCP real do host seguro (interno ao firewall) em uma sessão estabelecida entre os referidos hosts;

1.6. Deve possibilitar o registro de toda a comunicação realizada através do firewall e de todas as tentativas de abertura de sessões e conexões que por ele forem recusadas;

1.7. Suportar a agrupamento lógico de objetos ("object grouping") para criação de regras de filtragem. Possibilidade de criar grupos de pelo menos os seguintes tipos de objetos: hosts, redes IP, serviços. Possibilidade de verificar a utilização ("hit counts") de cada regra de filtragem ("Access Control Entry") individualmente, independentemente do fato de a configuração da política ter utilizado o conceito de agrupamento lógico de objetos;

1.8. Funcionalidade de "proxy" de autenticação ("authentication proxy"), permitindo a

criação de políticas de segurança de forma dinâmica, com autenticação e autorização do acesso aos serviços de rede sendo efetuadas por usuário. Possiblidade de obter as informações de usuário/senha por meio de pelo menos os seguintes protocolos: HTTP, HTTPS e Telnet. Possibilidade do Firewall exigir autenticação inclusive para uso de protocolos que não possuam nativamente recursos de autenticação;

1.9. Suporte a autenticação usando base local de usuários (interna ao equipamento);

1.10. Integração do Firewall com a solução Microsoft Active Directory (MS-AD), permitindo a criação de políticas de filtragem baseados em usuários e grupos de usuários existentes na base MS AD;

1.11. Listas de controle de acesso com no mínimo os seguintes campos: IP de Origem, Nome do Usuário/Grupo do AD, IP de Destino, Serviço de origem, Serviço de destino e Ação (permit/deny). O "nome de usuário" deverá ser identificado de forma automática e transparente para o usuário final através de consultas à base MS-AD;

1.12. Políticas de controle de acesso baseadas em informações de horário;

1.13. Suporte a remontagem virtual de fragmentos ("Virtual Fragment Reassembly") em conjunto com o processo de inspeção stateful, com possibilidade de estabelecer o número máximo de fragmentos por pacotes e timeouts de remontagem;

1.14. Suporte a inspeção "stateful" os seguintes protocolos de aplicação: Oracle SQL*Net Access, Remote Shell, FTP, HTTP, SMTP, ILS (Internet Locator Service), LDAP, ESMTP, TFTP;

1.15. Tradução do endereço IP carregado em uma mensagem DNS Reply (NAT na camada de aplicação) juntamente com a tradução do endereço IP presente no cabeçalho L3;

1.16. Inspeção stateful dos protocolos de sinalização de telefonia H.323(v1, v2, v3, v4), SIP (Session Initiation Protocol), MGCP e SCCP. A partir da inspeção dos protocolos de sinalização o firewall deve criar dinamicamente as permissões pertinentes para o tráfego de mídia (RTP/RTCP) entre os telefones envolvidos;

1.17. Inspeção do protocolo SIP (SIP over TLS) em ambientes com voz criptografada. A partir da inspeção do protocolo de sinalização, devem ser criadas as conexões pertinentes para o tráfego SRTP (Secure RTP);

1.18. Limitar o número de conexões TCP simultâneas para cada IP de origem (sem necessidade de especificar tal endereço IP);

1.19. Limitar o número de conexões TCP incompletas ('half-open') simultâneas para cada IP de origem (sem necessidade de especificar tal endereço IP);

1.20. Limitar o número de conexões TCP simultâneas para um endereço de destino especificado;

1.21. Limitar o número de conexões TCP incompletas ('half-open') simultâneas para um endereço de destino especificado;

1.22. Permitir simultaneamente com a implementação "Network Address Translation" a filtragem "stateful" de pelo menos as seguintes aplicações:

H.323 (v1,v2, v3,v4) , Real Time Streaming Protocol (RTSP), SIP (Session Initiation Protocol), MGCP (Media Gateway Control Protocol)	Microsoft Networking client and server communication (NetBIOS over IP)
Oracle SQL*Net client and server communication, Domain Name System (DNS), SUN Remote Procedure Call (RPC), File Transfer Protocol (FTP) – modos "standard" e "passive"	

1.23. VIRTUALIZAÇÃO

1.23.1. Tecnologia de Firewall Virtual, com instâncias totalmente isoladas entre si. Em cada instância de Firewall deve ser possível definir regras independentes de filtragem, regras de NAT, rotas e VLANs alocadas;

1.23.2. Em cada instância de Firewall deve ser possível alocar no mínimo os seguintes tipos de recursos: número conexões simultâneas, número de endereços IP traduzidos, número de sessões de gerenciamento simultâneas, número de endereços MAC;

1.23.3. Dentro de cada instância de Firewall deve ser possível limitar (promover "rate limiting") os seguintes recursos: taxa de estabelecimento de novas conexões, taxa de inspeção de aplicações, taxa de transmissão de mensagens Syslog;

1.23.4. A exaustão dos recursos alocados para uma dada instância de Firewall não deve ter influência sobre a operação das demais instâncias;

1.23.5. Possibilidade de selecionar o modo de operação de cada instância de Firewall (seleção, por instância, de modo transparente ou roteado);

1.23.6. Suportada qualquer combinação de contextos em modo transparente e roteado, dentro do limite de instâncias solicitado.

1.24. SUBSISTEMA VPN

1.24.1. Suportar a versões do cliente IPSEC VPN fornecido com a appliance para, no mínimo, os seguintes sistemas operacionais: Windows 7 ou superior, Linux (Intel) e MacOS;

1.24.2. Deve suportar a terminação túneis IPSEC do tipo "site-to-site" (LAN-to-LAN), simultânea de conexões IPSEC VPN;

1.24.3. Criação de VPNs IPSEC com criptografia 168-bit 3DES, 128-bit AES e 256-bit AES;

1.24.4. Alta disponibilidade das conexões IPSEC VPN, permitindo a utilização de uma segunda unidade em "standby". Em caso de falha de uma das unidades, não deverá haver perda das conexões ativas (stateful failover) e a transição destas conexões entre as duas unidades deve ser completamente transparente para o usuário final;

1.24.5. Negociação de túneis VPN IPSEC utilizando o protocolo IKE (Internet Key Exchange) nas versões 1 e 2, para garantir a geração segura das chaves de criptografia simétrica;

1.24.6. Integração com servidores RADIUS, LDAP, Microsoft AD e Kerberos, para tarefas de autenticação, autorização e accounting (AAA) dos usuários VPN;

1.24.7. Deve ser capaz de passar pelo menos os seguintes parâmetros para o cliente VPN: endereço IP, WINS Server, IP do DNS Server e Default Domain Name. A configuração do cliente VPN deve ser completamente automatizada, sendo exigida do usuário apenas a instalação do cliente VPN em seu PC;

1.24.8. Deve ser capaz de configurar nos VPN clients uma lista de acesso de "split tunneling", de modo a explicitar quais as redes podem continuar sendo acessíveis de forma direta (sem IPSEC) durante uma conexão VPN à rede corporativa. Deve também ser possível a operação no modo "all tunneling", em que todo o tráfego do VPN client só poderá ser transportado através da conexão protegida;

1.24.9. Criação de "banners" personalizados para indicar se houve sucesso ou falha na requisição de acesso VPN;

1.24.10. Uso de certificados digitais emitidos pela autoridade certificadora ICP Brasil para autenticação das VPNs IPSec;

1.24.11. Criação de base de usuários e grupos de usuários que compartilham a mesma política de segurança de forma interna ao equipamento;

1.24.12. Criação de pools de endereços IP de VPN (endereços privados) internamente ao equipamento e suporte a NAT (Network Address Translation);

1.24.13. Integração com servidores RADIUS para que estes façam a atribuição dos endereços IP de VPN (endereços privados) aos clientes;

1.24.14. Deve permitir que os endereços IP de VPN (endereços privados) sejam obtidos a partir de um servidor DHCP especificado pelo administrador do sistema;

1.24.15. Associação de diferentes pools de endereços IP aos diferentes grupos de usuários que solicitarem conexão ao concentrador VPN;

1.24.16. Definição dos horários do dia e dos dias das semana em que um dado usuário pode requisitar uma conexão VPN;

1.24.17. Suportar operação no modo transparente a NAT ("NAT-transparent mode"), permitindo a utilização dos clientes VPN em ambientes em que já se efetue PAT (Port Address Translation);

1.24.18. Permitir a terminação de conexões no modo IPSEC over TCP e UDP;

1.24.19. Visualizar o número de conexões VPN estabelecidas em um dado instante e os respectivos usuários que estão fazendo uso destas;

1.24.20. Visualizar no cliente VPN o IP privado adquirido durante a negociação da conexão IPSEC;

1.24.21. Possibilidade de definir vários templates de conexão no cliente VPN antes que seja enviado para instalação no computador do usuário final. Templates devem conter o endereço IP ou nome DNS associado ao concentrador e parâmetros definidores das Security Associations (SAs) a serem usadas nas fases 1 (IKE) e 2 (IPSEC) de negociação dos túneis, incluindo algoritmo de criptografia (DES, 3DES,AES), algoritmo de hash (MD5, SHA), grupo Diffie-Hellman (1, 2, 5 e 7) e tempo de duração ("lifetime") da conexão. A configuração destes parâmetros deve ser totalmente transparente para o usuário do VPN cliente;

1.24.22. Suporte a utilização de certificados digitais padrão X.509 para a própria appliance VPN, possuindo integração com pelo menos as seguintes Certificate Authorities (CAs): Baltimore, Entrust, Verisign, Microsoft e RSA. Os clientes VPNs devem ter o mesmo suporte a certificados digitais. Deve suportar o protocolo SCEP para "enrollment" automático na autoridade certificadora (tanto para o concentrador como para os clientes IPSEC);

1.24.23. Deve suportar protocolo Syslog para geração de logs de sistema;

1.24.24. Deve implementar protocolo DTLS (TLS over UDP) de acordo com a RFC 4748;

1.24.25. Mapeamento de atributos LDAP e RADIUS para parâmetros existentes na configuração local de grupos do concentrador. Deve ser possível escolher, para cada grupo, se os parâmetros usados serão os definidos localmente ou os mapeados de um grupo externo LDAP/RADIUS.

1.25. **GERENCIAMENTO E CONECTIVIDADE**

1.25.1. Deve implementar NTP (Network Time Protocol), conforme RFC 1305, contemplando autenticação MD5 entre os peers;

1.25.2. Gerenciável via SNMP, v2c e v3, porta de console, Telnet, SSHv2 e HTTPS;

1.25.3. Uma interface 10/100/1000 dedicada a gerenciamento (out-of-band);

1.25.4. Mecanismo interno de captura de pacotes e guias de configuração ("wizards") quais os pacotes (IP de origem e destino, portas TCP/UDP de origem e destino e interfaces de entrada devem ser capturados);

1.25.5. Armazenar os pacotes capturados em formato TCPDUMP,

1.25.6. Memória flash para armazenamento de imagem do sistema operacional e arquivos de configuração do equipamento;

1.25.7. Deve implementar completamente a porção cliente do protocolo TACACS+ para controle de acesso administrativo ao equipamento. Deve ser possível especificar conjuntos de comandos acessíveis a cada grupo de usuários administrativos e cada comando deve ser autorizado individualmente no servidor TACACS+. Todos os comandos executados bem como todas as tentativas não autorizadas de execução de comandos devem ser enviadas ao servidor TACACS+;

1.25.8. Interface gráfica para gerenciamento das funcionalidades de VPN e Stateful Firewall do dispositivo;

1.25.9. Deve implementar, por interface, as funções de DHCP Server, Client e Relay.

1.26. **ROTEAMENTO**

1.26.1. Deve suportar a criação de rotas estáticas e os seguintes protocolos: RIP, RIPv2, OSPF, OSPFv3 e BGPv4. Suportar a utilização de dois processos de roteamento simultâneos e independentes.

1.26.2. Implementar o protocolo PIM (Protocol Independent Multicast) em Sparse Mode;

1.26.3. Deve suportar a operação como IGMP Proxy Agent.

1.27. **IPv6**

1.27.1. Suporte a inspeção stateful de tráfego IPv6, roteamento estático, simultaneamente a criação de regras IPv4 e IPv6

1.27.2. Implementar randomização do número de sequência TCP para conexões TCP que trafegam sobre IPv6;

1.27.3. Suporte a anti-spoofing (sem uso de ACLs) para endereços IPv6 e stateful failover de conexões IPv6

1.27.4. Suporte a gerenciamento sobre IPv6 nos protocolos de gerência: Telnet, SSH e HTTPS;

1.27.5. Deve suportar agrupamento lógico de objetos IPv6 (redes, hosts, serviços) e criação de regras (ACLs) usando tais objetos.

1.28. ALTA-DISPONIBILIDADE

1.28.1. Suporte a alta disponibilidade em modo ativo-standby com todas as funcionalidades habilitadas;

1.28.2. Suporte a alta disponibilidade em modo cluster, com todas as unidades ativas simultaneamente. O modo cluster deve ser suportado com pelo menos as funcionalidades Stateful Firewall, VPN site-to-site e Next-Generation Firewall/IPS ativas simultaneamente;

1.29. SUBSISTEMA DE FILTRAGEM DE APLICAÇÃO

1.29.1. Suporte a identificação e controle de aplicações através de inspeção profunda de pacotes (Deep Packet Inspection), independentemente das portas usadas pela aplicação;

1.29.2. As aplicações devem ser classificadas de acordo com categoria, tipo e nível de risco;

1.29.3. Suporte a criação de regras para monitoramento e controle das aplicações e serviços, sendo capaz de executar no mínimo as seguintes ações:

1.29.4. Permitir o uso irrestrito de uma ou mais aplicações, para um determinado grupo de usuários, negando totalmente o uso para os demais usuários. Todos os usuários autenticados via servidor LDAP

1.29.5. Restrições de funcionalidades de uma ou mais aplicações para um determinado grupo de usuários, negando totalmente o uso para os demais usuários. Todos os usuários autenticados via servidor LDAP;

1.29.6. Negar totalmente o uso de uma ou mais aplicações independentes do usuário;

1.29.7. Suporte a controle de aplicações Web 2.0, definindo quais são as operações permitidas para cada uma destas aplicações (deve ser possível, no mínimo, restringir operações de "Post", bloquear transferência de arquivos, bloquear uso de "games");

1.29.8. Suporte para controlar as micro-applicações que podem ser utilizadas por cada uma destas aplicações Web 2.0 (esse tipo de controle deve estar disponível, no mínimo, para as aplicações Facebook, Google+, Twitter e Skype);

1.29.9. Suporte a customização de regras de detecção de novas aplicações.

1.30. SUBSISTEMA DE FILTRAGEM DE URL

1.30.1. Criação de regras de controle de acesso com base em informação de reputação dos sites. Essa base deve ser atualizada dinamicamente;

1.30.2. Criação de políticas de acesso baseadas em filtro de categorias de URL, com módulo de filtro de URL integrado na própria ferramenta de Firewall;

1.30.3. Criação de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;

1.30.4. Suporte a criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via LDAP, MS Active Directory;

1.30.5. Integração com RADIUS e LDAP para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e Grupos de usuários;

1.30.6. Suporte a criação de políticas baseadas no controle por URL e categoria de URL;

1.30.7. Controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação;

1.30.8. Deve possibilitar base de URLs local no appliance, evitando delay de comunicação/validação da URLs;

1.30.9. Deverá possuir pelo menos 50 (cinquenta) categorias de URLs;

1.30.10. Suporte a criação categorias de URLs customizadas, exclusão de URLs do bloqueio por categoria, customização de página de bloqueio;

1.30.11. Suporte a 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 possibilitar o usuário continuar acessando o site por um tempo);

1.30.12. Os logs do produto devem incluir informações das atividades dos usuários;

1.30.13. A atualização da base de dados deve ser automática com a opção de ser feita manualmente.

1.31. **SUBSISTEMA IPS**

1.31.1. Suporte a configuração de regras de exceção de inspeção de tráfego por endereço IP origem/destino ou VLAN, por segmento, realizando apenas a comutação do tráfego sem executar inspeção;

1.31.2. Monitoramento de segmentos de rede em modo transparente sem IP associado às interfaces de monitoração;

1.31.3. Suporte a Jumbo Frame, monitorar VLANs padrão 802.1q, protocolo SNTP ou NTP, uso nativo do SNMP versão 3, auditoria das atividades de cada usuário,

1.31.4. Deve ser capaz de visualizar no mínimo as seguintes informações:

1.31.4.1. Incidentes de Intrusão, Políticas aplicadas, Atualizações instaladas, Login e logout na interface web de gerencia, Requisições de aumento de privilégio, Inclusões e remoções de regras, registro de sensores na console de gerenciamento.

1.31.5. Configurações relacionadas ao envio de informações detectada pelos sensores de prevenção contra invasão, para dispositivo de armazenamento externo a solução de gerenciamento;

1.31.6. Envio dos logs de auditoria das atividades de cada usuário, para um servidor de Syslogs, armazenamento dos arquivos de configuração diretamente no appliance;

1.31.7. Deve permitir temporariamente, o armazenamento dos dados coletados e inspecionados em banco de dados local armazenado no sensor de IPS;

1.31.8. Inspeção em IPV6 incluindo tunelamento IPV4 em IPV6, IPV6 em IPV4, IPV6 em IPV6, IPV6 com VLAN e label MPLS e em túneis GRE;

1.31.9. Suporte a identificar/restringir o acesso de hosts externos ao perímetro monitorado baseando-se em informações de reputação de domínios de e ranges de endereço IP;

1.31.10. Suporte a criação de regras independentes para cada segmento monitorado;

1.31.11. Suporte a reconstrução e inspeção no fluxos de dados na camada de aplicação;

1.31.12. Deve possuir capacidade de remontagem de fluxo TCP e IP desfragmentation, resistência às ferramentas de evasão, identificação de protocolos que utilizam portas aleatórias, detectar e bloquear ataques independente do sistema operacional alvo;

1.31.13. Monitoramento de sessões de pacotes na rede, atuando em modo "stateful inspection" (análise pacote a pacote e todo o seu estado), sendo capaz de bloquear ataques e tráfego não autorizado ou suspeito;

1.31.14. Suporte a filtros de "PortScan", protegendo a rede contra ataques do tipo "scan", proteção a equipamentos de rede, protegendo contra ataques a vulnerabilidades de equipamentos de rede (ex.: roteadores, switches, etc.);

1.31.15. Análise e decodificação de fluxos de pacotes nas camadas 2 à 7 nos protocolos de aplicações: IP, DNS, H.323, TCP, RPC, MPLS, SIP, ICMP, HTTP, FTP, P2P, ARP, Telnet, SMTP, IM, UDP, IMAP, SMB;

1.31.16. Suporte a filtros de vulnerabilidades específicos dos protocolos de VoIP que bloqueiem anomalias de protocolos, ataques de negação de serviço, vulnerabilidades específicas conhecidas, ferramentas de ataque e geradores de tráfego que causem degradação ou indisponibilidade de serviços;

1.31.16.1. Proteções contra ataques a aplicações Web: Web Protection, Cross-Site Scripting, SQL Injection, Client-side attacks, Injection Attacks, Malicious Files Execution, Information Disclosure, Path Traversal, Authentication, Buffer Overflow, Brute Force, Directory Indexing.

1.31.17. Criar regras para filtro com base em endereços de origem/destino, protocolo e VLAN ID;

1.31.18. Proteção contra ataques DDoS através dos métodos: Controle (limite de quantidade) de conexões por origem, por destino, requisições "SYN" por origem e destino, Controle (limite de quantidade) de conexões (origem e Destino) e Controle (limite de quantidade) de requisições "SYN"(Origem e Destino), possibilitar que os pacotes sejam capturados para análise;

1.31.19. Identificar e bloquear ataques baseados em análises de anomalias de tráfego, anomalias de protocolo (RFC Compliance, Protocol Decoders, Normalização), assinaturas e vulnerabilidades;

1.31.20. Fornecido com uma configuração de filtros recomendados pré-configurados;

1.31.21. Permitir a inclusão de informações de vulnerabilidades oriundas de ferramentas de varredura externa (ex.: Nessus, Qualys, Foundstone, etc);

1.31.22. Identificação de anomalia de rede observando o tráfego ou informações do flow de ativos da rede de forma nativa;

1.31.23. Análise do comportamento da rede, com o intuito de detectar ameaças com origem/destino a segmentos monitorados pelo IPS. Isto inclui a capacidade de estabelecer padrões "normais" de tráfego através de técnicas de análise de fluxo (por exemplo, IPfix) e a capacidade de detectar desvios dos padrões considerados normais;

1.31.23.1. Análise do comportamento da rede fornecendo visibilidade do uso do segmento monitorado para auxiliar na solução de falhas de rede ou degradação de desempenho, no mínimo as seguintes informações devem ser disponibilizadas: Fluxos de sessão dos hosts, Hora de início/fim, Quantidade de dados trafegados.

1.31.23.2. Coletar, armazenar e correlacionar as informações adquiridas passivamente, sobre hosts que trafegam pelos segmentos monitorados pelo(s) IPS. No mínimo as seguintes informações devem ser correlacionadas e armazenadas: Sistema operacional do Host, Serviços existentes no Host, Portas em uso no Host, Aplicações em uso no Host, Vulnerabilidades existentes no Host, Smart phones e tablets, Network flow, Anomalias de redes, Identidades de usuários, Tipo de arquivo e protocolo, Conexões maliciosas.

1.31.23.3. Suporte a criar uma lista com o "ambiente ideal esperado" e a cada mudança nesse ambiente, o sensor deverá no mínimo alertar a console de gerencia sobre a mudança identificada. Entendemos como "ambiente ideal esperado" o conjunto de informações pré-configuradas na gerencia dos sensores de IPS a respeito dos atributos dos hosts participantes desse segmento, deve ser configurado no mínimo os seguintes atributos: Sistema Operacional, Serviços vigentes nos hosts, Aplicações autorizadas a serem executadas nos hosts, Aplicações não autorizadas a serem executadas nos hosts.

1.31.24. Suporte a criar e importar regras no padrão OpenSource, essas regras, devem poder ser habilitadas para simples monitoramento ou para bloqueio de tráfego, não deve haver limite da quantidade de regras a serem criadas ou importadas e não deve haver limite de funcionalidade nas regras criadas ou a serem importadas;

1.31.25. Criação de regras para monitoramento e controle das aplicações e serviços nos segmentos monitorados, os sensores de IPS devem ser capazes de executar no mínimo as seguintes ações:

1.31.25.1. Uso irrestrito de uma ou mais aplicações, para um determinado grupo de usuários, negando totalmente o uso para os demais usuários. Usuários autenticados através de um servidor LDAP definido pelo administrador da solução;

1.31.25.2. Permitir o uso com restrições de funcionalidades de uma ou mais aplicações para um determinado grupo de usuários, negando totalmente o uso para os demais usuários. Todos esses usuários devem ser autenticados através de um servidor LDAP definido pelo administrador da solução;

1.31.25.3. Negar totalmente o uso de uma ou mais aplicações independentes do usuário;

1.31.26. Capacidade de criar assinaturas definidas pelo usuário com uso de expresses regulares;

1.31.27. Capacidade de modificar e alterar as assinaturas existente, podendo a critério do administrador, alterar o modificar o conteúdo da assinatura;

1.31.28. Capacidade de identificar o tipo de arquivo trafegado e permitir a criação de políticas de detecção e bloqueio de eventos baseados no tipo de arquivo;

1.31.28.1. A solução deverá detectar e bloquear as seguintes categorias de ataques e ameaças: Malwares, Port Scans, VoIP attacks; IPv6 attacks; DoS attacks; Buffer overflows; P2P attacks; Anomalias em protocolos e aplicações; Ameaças Zero-day; Pacotes malformados; Segmentação TCP e fragmentação IP.

1.31.29. O appliance deve ser fornecido com serviço de atualização permanente de filtros de ataques e vulnerabilidades por 03 (três) anos;

1.31.30. Os equipamentos deverão ser fornecidos com seu software com licença irrestrita, em sua versão mais atual e completa. O fornecimento deverá incluir todas as licenças de software necessárias para a implementação de todas as funcionalidades disponibilizadas pelo fabricante para os equipamentos fornecido.

1.32. SUBSISTEMA CONTRA MALWARE

1.32.1. Funcionalidades de inspeção inbound de Malware com filtro de ameaças avançadas e análise de execução em tempo real, inspeção outbound de command & control, resolução e call-backs;

1.32.2. Capacidade para monitoração em tempo real;

1.32.3. Deve permitir diariamente, semanalmente ou mensalmente informações a respeito das tendências de ataque e riscos do ambiente;

1.32.4. Identificar tráfego de rede gerado por dispositivos conectados no segmento monitorado, incluindo tráfego malware e ataques associados;

1.32.5. Capacidade nativa e sem necessidade de equipamentos tipo SIEM de correlacionar informações de alertas malwares com ataques detectados e condições de tráfego, para assim definir um tipo de alerta personalizado em tempo tempo real;

1.32.6. Controle em tempo real de: arquivos, bloqueio malwares, bloqueio de aplicações (protocolos, clientes e web),

1.32.7. Controle de acesso, controle de URL's;

1.32.8. Suportar em tempo real a detecção e prevenção (bloqueio imediato) de arquivos malwares e ataques para os protocolos (Inbound e Outbound) HTTP, SMTP, FTP, POP3, IMAP e adicionalmente permite em tempo real a detecção (Inbound ou outbound) e prevenção (bloqueio imediato, Inbound ou outbound) de ataques e tráfego malware do tipo: comunicações de comando e controle, identificação de backdoors, propagação de infecção, presença e uso de ferramentas malware, ataques de negação de serviço, comunicação e presença de keyloggers (troca de informações), identificar redirecionamentos, identificar a exploração de overflows;

1.32.9. Deve implementar e identifica existência de Malware em comunicações de entrada e saída, incluindo destinos de servidores do tipo Command and Control;

1.32.10. Mecanismos de detecção e bloqueio de vazamento de informações sensíveis no ambiente, ao permitir a identificação de dados em: arquivos Microsoft Word (não criptografados) sendo enviados ou recebidos via protocolos FTP e HTTP, números de cartões de crédito para até 8 tipos de protocolos diferentes, endereços e-mail para até 8 tipos de protocolos diferentes e dados customizados pelo administrador para até 8 tipos de protocolos diferentes;

Agência Goiana de Habitação S/A - Rua 18-A nº 541, Setor Aeroporto - Goiânia - Goiás - 74.070-060 - (62) 3096-5000

1.32.11. Capacidade de Implementar detecção de ataques e malwares que utilizem mecanismo de exploit em arquivos PDF;

1.32.12. Capacidade para detecção de explorações diretas, uso suspeito ou malicioso das aplicações;

1.32.13. Deve permitir que arquivos executáveis (MSEXE) identificados pelo sensor sejam automaticamente enviados para análise utilizando tecnologia de virtualização em nuvem;

1.32.14. Manter histórico dos resultados de avaliações prévias e utilizar esta informação para determinar de forma configurável que o arquivo seja considerado malware a partir de certo limite;

1.32.15. Virtualização para análise sobre sistemas operacional MS Windows;

1.32.16. Implementação rede de inteligência global, em tempo real, proprietária para cobrir ataques originados de qualquer localidade global, novas origens e destinos de comunicações e distribuição de malwares;

1.32.17. Configuração in-line (em linha) totalmente transparente que permita em tempo real a detecção (inbound e/ou outbound) e a prevenção através de bloqueio (inbound e/ou outbound) de ataques malwares sejam estes no formato de arquivos maliciosos, comunicações ou explorações diretas, caso seja necessário a solução suporta a utilização de configurações de proxies;

1.32.18. Capacidade automática e periódica para download e instalar atualizações de dados de reputação IP para identificação de tráfego associado a origens e destinos de malware, comando e controle, spam, bots, proxies abertos, relays abertos, phishing e TOR (the onion router);

1.32.19. Implementar 02 (dois) modos de operação: detecção passiva e inline sendo que no último a solução deve permitir implementar bloqueios em tempo real e inclusive especificar a terminação das conexões de ataques utilizando pacotes "tcp reset" ao detectar a transferência de arquivos maliciosos, atividade de comunicação, infecção e proliferação de malwares assim como outras categorias de explorações remotas e motivadores de ataques através da rede monitorada pela solução;

1.32.20. Funcionalidade de bloqueio em tempo real de arquivos maliciosos (detectados como malwares) e comunicações malwares conhecidas no modo inline;

1.32.21. Recurso de análise tipo "sandbox", para no mínimo arquivos executáveis (MSEXE) de modo a permitir a análise completa do comportamento do Malware ou código malicioso;

1.32.22. Recursos que permitem o envio de informações de eventos de ataques e malwares para ferramentas de SIEM de fabricantes terceiros, para servidores Syslog

1.32.23. Suporte a protocolo SNMP v1, v2 e v3 para atividades de gerenciamento;

1.32.24. Deve implementar atualização da base de dados da Rede de Inteligência de forma automático, permitindo o agendamento mínimo de 2 hora de intervalo;

1.32.25. Implementar via interface gráfica de gerenciamento todas as opções de análise e tratamento eventos de ataques de rede, Malware, detecção de tráfego e notificação de eventos em tempo real, adicionalmente implementa automáticamente a capacidade de traçar uma visão cronológica de eventos de forma gráfica permitindo identificar em tempo-real a trajetória de acesso ou propagação de ameaças malware de

Agência Goiana de Habitação S/A - Rua 18-A nº 541, Setor Aeroporto - Goiânia - Goiás - 74.070-060 - (62) 3096-5000

forma lateral no ambiente, identificando o nome do arquivo, tipo e categoria do arquivo, nível de ameaça quando disponível, sha-256, tipo de evento, protocolo de aplicação utilizado, aplicação cliente utilizada para transferência, quantidade de visualizações, dia e hora, origem e destino do tráfego;

1.32.26. Realizar toda detecção e bloqueio de ataques de rede e malwares em tempo real, não sendo uma solução que necessita de ou é exclusivamente dependentes de tecnologia de virtualização tipo "sandboxing" para detecção de arquivos maliciosos e presenção de malware na rede monitorada;

1.32.27. Os processos de detecção e determinação de malwares, ataques e tráfego assim como os bloqueios preventivos inclusive para os arquivos sendo transferidos pela rede pelos protocolos suportados são realizados de forma automatizada e em tempo real;

1.32.28. O recurso de execução em ambiente de virtualização disponibilizado (sandbox), permite a automatização do envio de arquivos suportados pela solução de rede para este tipo de solicitação de análise dinâmica;

1.32.29. A solução Implementa múltiplos motores (engines) para verificação de Malware e/ou códigos maliciosos, não dependendo somente da utilização de recursos de análise virtualizada (sandbox) como método de identificação de malwares em arquivos;

1.32.30. Suporte a mecanismo de definição de exceções do tipo whitelist de arquivos, endereços IP, aplicações;

1.32.31. Suporte a criação de regras de detecção e permitir a criação de detecções de arquivos maliciosos utilizando amostra de arquivo, hash SHA-256 único e lista de hash SHA-256;

1.32.32. Implementar mecanismo de whitelist e detecções customizadas de arquivos, permitindo definição de regras por VLAN, subrede, endereço IP para utilização das listas;

1.32.33. Identificação e capacidade de controle de acesso em tempo real para os seguintes tipos de arquivo:

1.32.33.1. MSEXE,9XHIVE,DMG,DMP,ISO,NTHIVE,PCAP,PGD,SYLKc,SYMANTEC,VMDK,DWG,IMG_PICT,MAYA,PSD,WMF,SCRENC,UUENCODED,PDF,EPS,AUTORUN,BINARY_DATA,BINHEX, EICAR, ELF, ISHIELD_MSI, MACHO, RPM, TORRENT, AMR, FFMPEG, FLAC, FLIC, FLV, IVR, MIDI, MKV, MOV, MPEG, OGG, PLS, R1M, REC, RIFF, RIFX, RMF, S3M, SAMI, SMIL, SWF, WAV, WEBM, 7Z, ARJ, BZ, CPIO_CRC, CPIO_NEWC, CPIO_ODC, JAR, LHA, MSCAB, MSSZDD, OLD_TAR, POSIX_TAR, RAR, SIS, SIT, ZIP, ZIP_ENC, ACCDB, HLP, MAIL, MDB, MDI, MNY, MSCHM, MSOLE2, MSWORD_MAC5, MWL, NEW_OFFICE, ONE, PST, RTF, TNEF, WAB, WP, WRI, XLW, XPS.

1.32.34. Implementar em tempo real a inspeção, detecção e bloqueio autónomo (prevenção sem a necessidade de integrar com outros sistemas terceiros para que seja feito o bloqueio da ameaça) na rede para os seguintes tipos de arquivos:

1.32.34.1. 7Z, ACCDB, ARJ, BINARY_DATA, BINHEX, BZ, CPIO_CRC, CPIO_NEWC, CPIO, ODC, EICAR, FLV, GZ, ISHIELD_MSI, JAR, JARPACK, LHA, MAIL, MDB, MDI, MNY, MSCAB, MSCHM, MSEXE, MSOLE2, MSWORD_MAC5, NEW_OFFICE, OLD_TAR, PDF, POSIX_TAR, PST, RAR, RTF, SIS, SIT, SWF, TNEF, WAB, WRI, XLW, XPS, ZIP, ZIP_ENC.

1.32.35. A solução ofertada deve ser totalmente do mesmo fabricante, com serviço de atualização permanente por 03 (três) anos;

1.33. **ARQUITETURA**

1.33.1. Deve ser montável em rack de 19 polegadas (devem ser fornecidos os kits de fixação necessários). O equipamento fornecido deve ocupar no máximo 02 (duas) unidades de rack (02U);

1.33.2. Deve ser fornecido com fonte internas ao equipamento e com 08 (Oito) interfaces 1 Gigabit Ethernet.

1.34. **DESEMPENHO**

1.34.1. Suportar 250.000 (Duzentas e cinquenta mil) conexões simultâneas em sua tabela de estados de Stateful Firewall;

1.34.2. Suporte a criação de 20.000 (Vinte mil) novas conexões TCP por segundo para a funcionalidade de Stateful Firewall;

1.34.3. Suportar taxa de encaminhamento de Stateful Firewall de 750.000 pps (pacotes por segundo);

1.34.4. Suportar a funcionalidade de Stateful Firewall com desempenho mínimo de 1.8 Gbps (Um Gbps e Oitocentos Mbps) para pacotes UDP;

1.34.5. Suportar a funcionalidade de Stateful Firewall com desempenho mínimo de 900 Mbps (Novecentos Mbps) para pacotes TCP multiprotocolo;

1.34.6. Suportar um throughput de, no mínino, 850 Mbps (Oitocentos e Cinquenta Mbps por segundo) com as funcionalidades de controle de aplicação e IPS habilitadas simultaneamente;

1.34.7. Suportar a terminação de pelo menos 50 (Cinquenta) túneis IPSEC VPN simultaneamente. Caso sejam necessárias licenças, as mesmas devem ser fornecidas;

1.34.8. Suporte a terminação simultânea de túneis IPSEC, de modo que se suporte um total de pelo menos 300 (Trezentos) usuários VPN, independentemente do tipo de sessão. Caso sejam necessárias licenças, as mesmas devem ser fornecidas;

1.34.9. Possuir desempenho de, no mínimo, 250 Mbps (Duzentos e Cinquenta Megabits por segundo) para tratamento de conexões IPSEC (padrões AES e 3DES). A criptografia deve ser realizada em hardware dedicado;

1.34.10. Não deve haver restrição de número de usuários simultâneos através do equipamento para a licença de software fornecida para a funcionalidade de Stateful Firewall;

1.34.11. Deve ser possível criar pelo menos 100 (Cem) interfaces lógicas associadas a VLANs;

1.34.12. Devem ser suportadas, através de licenças adicionais, instâncias virtuais de Firewall, sendo entregue com pelo menos 5(Cinco) instâncias virtuais;

1.34.13. Reconhecer mais de 1000 (mil) aplicações com atualizações automáticas e suportar pelo menos 80 categorias de URL;

1.35. SUBSISTEMA DE GERÊNCIA CENTRALIZADA

1.35.1. Deve ser fornecido na forma de appliance dedicado ou appliance virtual compatível com VMWARE, com licenças e capacidade suficientes para gerenciar a quantidade de dispositivos solicitada;

1.35.2. Deve permitir a instalação, monitoramento, configuração e atualização de múltiplos equipamentos, simultaneamente, estejam estes instalados localmente ou remotamente;

1.35.3. Suporte a monitorar, configurar, diagnosticar problemas e gerar relatórios de múltiplos equipamentos;

1.35.3.1. Possuir as seguintes opções de resposta automática às ameaças detectadas: Alertas automáticos, Remediações em firewall; Remediações em roteador; Scans de rede;

1.35.4. Permitir configurar o perfil de inspeção de tráfego independentemente do segmento associado (físico ou lógico) bem como a direção de inspeção dentro do segmento (somente de entrada, somente de saída ou ambos os sentidos);

1.35.5. Permitir aplicar um ou mais perfis de inspeção de tráfego a um segmento ou a um grupo de segmentos;

1.35.6. Suportar a aplicação de diversos perfis de inspeção de tráfego, trabalhando de maneira simultânea em diferentes segmentos físicos ou lógicos;

1.35.7. Permitir criar políticas de inspeção baseada em grupos, usando os seguintes parâmetros para montagem dos grupos: Sensores; Conjunto de Interfaces de um único equipamento; Conjunto de Interfaces de equipamentos distintos;

1.35.8. Permitir que toda alteração de política e definições na console de gerenciamento seja registrada;

1.35.9. Permitir a criação e aplicação de respostas a eventos, categorizar os eventos de acordo com a severidade;

1.35.10. Permitir configurar diferentes perfis de usuários com níveis de privilégios hierárquicos;

1.35.11. Possuir capacidade de atualização manual e automática das assinaturas dos subsistemas IPS gerenciados, atualização do firmware dos IPSs gerenciados;

1.35.12. Deve coletar passivamente informações de identidade do usuário, para correlacionar o endereçamento IP com o nome de usuário, e tornar esta informação disponível para efeitos de gestão/correlação de eventos;

1.35.13. Permitir identificar usuários da rede interna, através de diretório padrão LDAP e correlacioná-los com os eventos de rede, tanto de conformidade com a política de segurança como de intrusão, sem necessidade de solução externa;

1.35.14. A análise de comportamento de rede deve permitir correlacionar os nomes de usuários com eventos de segurança suspeitos;

1.35.15. Permitir monitorar as condições de "saúde" dos subsistemas IPS monitorados, apresentando informações em sua console gráfica de no mínimo seguintes informações:

1.35.15.1. Heartbeat dos subsistemas IPS, permitindo monitorar se os equipamentos gerenciados estão operantes;

1.35.15.2. Uso da CPU- Deve permitir monitorar o uso da CPU, com possibilidade de definir dois tipos diferentes de alertas, para diferentes níveis de uso da CPU;

1.35.15.3. Reset da interfaces - Deve permitir monitorar o reset nas interfaces de inspeção dos subsistemas IPS;

1.35.15.4. Uso de Disco- Permitir monitorar o uso do Disco, com possibilidade de definir dois tipos diferentes de alertas, para diferentes níveis de uso do Disco;

1.35.15.5. Taxa de eventos de IPS- Permitir monitorar a taxa de eventos de IPS recebida por segundo, com possibilidade de definir dois tipos diferentes de alertas, para diferentes níveis de eventos de IPS recebidos por segundo;

1.35.15.6. Uso de Memória - Permitir monitorar o uso da memória do appliance, com possibilidade de definir dois tipos diferentes de alertas, para diferentes níveis de uso de memória;

1.35.15.7. Sincronização de tempo – Monitoramento da diferença de tempo de dispositivos gerenciados;

1.35.15.8. Traffic Status - Permitir monitorar se as interfaces de inspeção dos sensores de IPS estão recebendo tráfego.

1.35.16. Suporte a gráficos em tempo real das estatísticas do tráfego, ataques filtrados, hosts de rede e serviços;

1.35.17. Deve ser gerenciado através de interface WEB (HTTPS) e toda a comunicação entre dispositivo de gerencia e sensor de IPS deve ser criptografada;

1.35.18. Possuir recurso de geolocalização. Localização geográfica da máquina do atacante;

1.35.18.1. Permitir criar no mínimo os relatórios descritos abaixo: Dos 10 ataques mais comuns; IP de Origem; IP de Destino; Ataques por severidade; Ataques por ação, por porta, por segmento, por protocolo.

1.35.19. Deve permitir gerar relatórios gráficos, permitindo a geração de relatórios periódicos de forma automática. A solução deverá permitir também o envio automático dos relatórios para e-mail escolhido pelo administrador da solução;

1.35.20. Deve exportar relatórios para no mínimo os seguintes formatos: HTML, PDF e CSV;

1.35.20.1. Possuir ferramenta interna de manutenção do banco de dados, capaz de realizar no mínimo as seguintes funções: Backup Manual e agendado dos dados e das configurações do sistema de gerenciamento, armazenar no disco local do sistema de gerenciamento o backup dos sensores e sistema de gerenciamento.

1.35.20.2. Assim que o backup for concluído o sistema de gerenciamento deve ser capaz de copiar através de protocolo de comunicação criptografado (nativo do equipamento) e sem intervenção humana o Backup realizado para um host diferente;

1.35.21. Possuir banco de dados interno para armazenamento dos logs, permitindo ao administrador da solução que redirecione o armazenamento dessa base de dados em um volume de disco remoto;

1.35.22. Deve manter os logs de ataques e de alarmes enviados pelos subsistemas IPS, permitir enviar as informações para um Syslog remoto;

1.35.23. Ser gerenciável via linha de comando através de acesso seguro utilizando o protocolo SSH;

1.35.24. Implementar nativamente (sem uso de ferramentas de terceiros) SNMPv3;

1.35.25. Permitir envio de eventos SNMP relativos ao desempenho e funcionamento do equipamento e deve implementar NTP ou SNTP.

CLÁUSULA SEGUNDA – DO TREINAMENTO

2.1. O treinamento será Hands-on (mão na massa), treinamento feito durante a própria implantação do sistema/ appliance, ou seja, o Sistema/ appliance está sendo instalado os técnicos da AGEHAB acompanham a implantação e são treinados ao mesmo tempo. Essa atividade resume-se em transferir as rotinas e conhecimentos necessários para a equipe técnica da CONTRATANTE.

2.2. O treinamento deverá ser de responsabilidade da CONTRATADA com carga horária não superior a 40 UST para capacitar de forma adequada os 02 (dois) técnicos da CONTRATANTE.

2.3. A CONTRATADA deve disponibilizar profissional certificado pelo fabricando da solução ofertada para realizar o treinamento junto a CONTRATANTE.

2.4. Todas as despesas relativas à execução do treinamento serão de exclusiva responsabilidade da CONTRATADA, incluindo os gastos com instrutores, seu deslocamento, hospedagem, alimentação, o fornecimento do material didático em língua portuguesa.

2.5. O treinamento Hands-on deverá ser marcado com a Gerência de Tecnologia da Informação no prazo mínimo de 03 (três) dias antes da data do treinamento.

2.6. Para efeito de cálculo e orientação da CGU (Controladoria Geral da União) será utilizada a unidade UST (Unidade de Serviço Técnico) que equivale a uma hora de trabalho.

CLÁUSULA TERCEIRA – DA GARANTIA, SUPORTE E SERVIÇOS DE ASSINATURA

3.1. Todos os itens deveram seguir os padrões abaixo. Os serviços de garantia, suporte técnico e serviços de assinaturas deverão ser fornecidos pelo fabricante do equipamento.

3.2. O serviço de suporte técnico durante o período de garantia de 36 (trinta e seis) meses atendendo as seguintes exigências:

3.2.1. O serviço de suporte técnico deverá ser 24x7x4 (vinte e quatro horas por dia, sete dias por semana, quatro horas de tempo de resposta), no local onde a solução se encontrar instalada (on-site), por técnicos devidamente habilitados e credenciados pelo fabricante, e sem qualquer ônus adicional;

3.2.2. O fabricante deverá disponibilizar canal de atendimento para abertura de chamados técnicos 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, mediante número 0800 ou número local em Brasília;

3.2.3. Para cada chamado técnico, deverá informar um número de controle (protocolo) para registro, bem como manter histórico de ações e atividades realizadas;

3.2.4. Todos os serviços baseados em assinaturas devem estar disponíveis por, no mínimo, 36 (trinta e seis) meses.

CLÁUSULA QUARTA – DO PRAZO, LOCAL DE ENTREGA E FORMA DE RECEBIMENTO

4.1. Todos os itens deverão seguir os padrões de prazo, local de entrega e forma de recebimento descritos abaixo:

4.1.1. Os equipamentos deverão ser entregues até 60 (sessenta) dias a contar da assinatura do contrato ou instrumento equivalente;

4.1.2. Entende-se por entrega as seguintes atividades: o transporte dos produtos embalados para o local determinado pela CONTRATANTE, a entrega dos volumes, a desembalagem, a verificação visual do produto e sua reembalagem se for o caso;

4.1.3. Os equipamentos deverão ser novos e sem uso e deverão ser entregues nas caixas lacradas pelo fabricante, não sendo aceitos equipamentos com caixas violadas;

4.1.4. No ato da entrega, a gerência responsável emitirá **TERMO DE RECEBIMENTO PROVISÓRIO** relacionando todos os produtos recebidos, nos termos da Nota Fiscal;

4.1.5. Os produtos serão objeto de inspeção, que será realizada por pessoa designada pela gerência de Tecnologia da Informação, conforme procedimentos a seguir:

4.1.5.1. Abertura das embalagens;

4.1.5.2. Comprovação de que o produto atende às especificações mínimas exigidas e/ou aquelas superiores oferecidas pela CONTRATADA;

4.1.5.3. Colocação do produto em funcionamento, se for o caso;

4.1.5.4. Teste dos componentes se for o caso;

4.1.5.5. O período de inspeção será de até 10 (dez) dias úteis;

4.1.6. Nos casos de sinais externos de avaria de transporte ou de mau funcionamento do produto, verificados na inspeção do mesmo, este deverá ser substituído por outro com as mesmas características, no prazo de até 30 (trinta) dias corridos, a contar da data de realização da inspeção;

4.1.7. Findo o prazo de inspeção e comprovada a conformidade dos produtos com as especificações técnicas exigidas no Edital e aquelas oferecidas pela CONTRATADA, bem como cumpridas as horas de treinamento previstas na Cláusula Segunda – DO TREINAMENTO, a gerência de Tecnologia da Informação emitirá o **TERMO DE RECEBIMENTO DEFINITIVO**;

4.1.8. Nos casos de substituição do produto, iniciar-se-ão os prazos e procedimentos estabelecidos nestas CONDIÇÕES DE RECEBIMENTO;

4.1.9. Correrão por conta da CONTRATADA as despesas com o frete, transporte, seguro e demais custos advindos da entrega dos produtos.

CLÁUSULA QUINTA – DAS OBRIGAÇÕES DA CONTRATADA

5.1. Além das resultantes da Lei 8.666/93 a adjudicatária se obriga, nos termos do Termo de Referência, a:

5.1.1. Prestar todos os esclarecimentos que forem solicitados pela fiscalização da contratante;

5.1.2. Manter durante toda a execução do termo respectivo, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na contratação.

5.2. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com os artigos 14 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990);

5.3. Manter atualizados, durante a vigência do contrato, para fins de pagamento, a Certidão Negativa de Débito – CND de Débito Trabalhista-CNDT, o Certificado de Regularidade - CRF do FGTS e certidão de regularidade junto à Fazenda Federal e municipal;

5.4. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do Contrato, observando o preconizado no Termo de Referência;

5.5. Efetuar treinamento para operacionalização e implantação do appliance de firewall e seus subsistemas, para equipe técnica da AGEHAB;

5.6. Entregar o objeto do contrato e conduzir os serviços de acordo com as normas do serviço e as especificações técnicas e, ainda, com estrita observância do instrumento convocatório, do Termo de Referência, da Proposta de Preços e da legislação vigente;

5.7. Prestar o serviço no endereço indicado pelo Contratante;

5.8. Prover os serviços ora contratados, com pessoal adequado e capacitado em todos os níveis de trabalho;

5.9. Iniciar e concluir os serviços nos prazos estipulados;

5.10. Comunicar ao Fiscal do contrato, por escrito e tão logo constatado problema ou a impossibilidade de execução de qualquer obrigação contratual, para a adoção das providências cabíveis;

5.11. Responder pelos serviços que executar, na forma do ato convocatório e da legislação aplicável;

5.12. Reparar, corrigir, remover, reconstruir ou substituir, no todo ou em parte e às suas expensas, bens ou prestações objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes de execução irregular ou do emprego ou fornecimento de materiais inadequados ou desconformes com as especificações;

5.13. Observado o disposto no artigo 68 da Lei nº 8.666/93, designar e manter preposto, no local do serviço, que deverá se reportar diretamente ao Fiscal/Gestor do contrato, para

Agência Goiana de Habitação S/A - Rua 18-A nº 541, Setor Aeroporto - Goiânia - Goiás - 74.070-060 - (62) 3096-5000

acompanhar e se responsabilizar pela execução dos serviços, inclusive pela regularidade técnica e disciplinar da atuação da equipe técnica disponibilizada para os serviços;

5.14. Elaborar relatório sobre a prestação dos serviços, dirigido ao fiscal/gestor do contrato, relatando todos os serviços realizados, eventuais problemas verificados e qualquer fato relevante sobre a execução do objeto contratual;

5.15. Cumprir todas as obrigações e encargos sociais e trabalhistas;

5.16. <u>São expressamente vedadas à CONTRATADA</u>:

5.16.1. A ceder, sob qualquer forma, os créditos oriundos deste contrato a terceiros;

CLÁUSULA SEXTA – DAS OBRIGAÇÕES DA CONTRATANTE

6.1. Prestar as informações e os esclarecimentos pertinentes que venham a ser solicitados pelos empregados da contratada ou por seu preposto;

6.2. Fornecer de toda a infraestrutura necessária para instalação e funcionamento dos equipamentos, como local físico, tomadas elétricas, pontos de acesso à rede, etc;

6.3. Efetuar o pagamento conforme execução dos serviços, desde que cumpridas todas as formalidades e exigências do contrato;

6.4. Exercer a fiscalização do contrato;

6.5. Comunicar oficialmente à contratada quaisquer falhas verificadas no cumprimento do contrato;

6.6. Convocar reunião inicial, quando necessário, com todos os envolvidos na contratação; e acompanhar e monitorar toda a execução dos serviços.

CLÁUSULA SÉTIMA – DO LOCAL DE ENTREGA

7.1. Todos os produtos serão entregues na sede da Agência Goiana de Habitação S/A - AGEHAB, situadas na Rua 18 A nº 541 – Setor Aeroporto – Goiânia – GO – CEP 74070-060.

7.2. A proposta comercial deverá considerar todos os custos relativos a logística e entrega dos equipamentos na cidade de Goiânia – GO.

CLÁUSULA OITAVA – DA VIGÊNCIA DO CONTRATO E DO PAGAMENTO

8.1. O presente contrato terá um prazo de vigência de 12 (doze meses) meses.

8.2. O pagamento dos itens contratados será procedido mediante a apresentação da **primeira via original da Nota Fiscal/fatura ou da Nota Fiscal de Serviços Eletrônica – NFSe,** após o fechamento do mês e a quitação até o décimo dia útil do mês seguinte.

8.3. As nota(s) fiscal (is)/faturas deverão conter no mínimo os seguintes dados:

a) Data de emissão;
b) Estar endereçada a Agência Goiana de Habitação - AGEHAB, situada a Rua 18-A nº 541, Setor Aeroporto - Goiânia/GO, CNPJ nº 01.274.240/0001-47;
c) Preços unitários;

8.4. O pagamento será efetuado após ateste pela Gerência de Tecnologia da Informação da AGEHAB, assim como das respectivas requisições da AGEHAB, desde que a Certidão Negativa de Débito – CND, o Certificado de Regularidade do FGTS – CRF, a prova de regularidade para com a Fazenda Federal e municipal.

8.5. Na ocorrência da rejeição de nota fiscal/fatura, motivada por erro ou incorreções, o prazo estipulado no subitem 8.2 passará a ser contado a partir da data da sua reapresentação, examinadas as causas da recusa.

8.6. No caso de serviços de prestação de mão de obra na sede da AGEHAB, apresentar nas solicitações de pagamentos mensais, se for o caso, os seguintes documentos:
a) Cópias autenticadas, legíveis e pagas das guias de recolhimento ao INSS e ao FGTS, juntamente com a relação da SEFIP dos funcionários que estiveram prestando serviços para a contratante, referente ao mês anterior ao do pagamento;
b) Cópia autenticada, legível da Folha de pagamento ou dos contracheques devidamente quitados pela contratada e assinados pelos empregados dela, executores dos serviços na AGEHAB, referente ao mês anterior ao do pagamento.

8.7. O pagamento do item 2.2 será mediante a apresentação de nota fiscal separada e de planilha com a quantidade de UST utilizada pela CONTRATADA para conclusão do treinamento.

CLÁUSULA NONA – DA GARANTIA DO CONTRATO

9.1. A CONTRATADA deverá apresentar à AGEHAB, no prazo máximo de até 15 (quinze) dias úteis, contados da data de assinatura do CONTRATO, comprovante de prestação de garantia correspondente ao percentual de 5% (cinco por cento) do valor total do contrato, nos termos do art. 56, da Lei nº 8.666, de 1993 e instruções complementares definidas no Edital.

9.2. Caso a opção seja por utilizar títulos da dívida pública, estes devem ter sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Fazenda.

9.3. Não serão admitidos, como garantia, os títulos da dívida pública, emitidos por pessoas jurídicas de direito público no período de 1850 a 1930, assim como aqueles de duvidosa liquidez, ao critério do CONTRATANTE, além de pedras preciosas, ainda que portadoras de certificado de conformação geológica.

9.4. A garantia, se prestada na forma de fiança bancária ou seguro-garantia, deverá ter validade durante a vigência do contrato.

9.5. Em se tratando de garantia prestada através de caução em dinheiro, o depósito deverá ser feito obrigatoriamente na Caixa Econômica Federal - CEF, conforme determina o art. 82 do Decreto nº 93872, de 23 de dezembro de 1986, sendo esta devolvida atualizada monetariamente, nos termo do §§ 4º, art. 56, da Lei nº 8.666/93.

9.6. No caso de garantia na modalidade de fiança bancária, deverá constar expressa renúncia do fiador aos benefícios do artigo 827 do Código Civil.

9.7. No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser readequada nas mesmas condições.

9.8. Se o valor da garantia for utilizado, total ou parcialmente, pela CONTRATANTE, para compensação de prejuízo causado no decorrer da execução contratual por conduta da CONTRATADA, esta deverá proceder à respectiva reposição no prazo de 10 (dez) dias úteis, contados da data em que tiver sido notificada.

9.9. A garantia prestada pela CONTRATADA será liberada, após o término da vigência do Contrato, depois de certificado pelo Gestor deste Contrato que o mesmo foi Totalmente realizado a contento, dentro do prazo de 10 (dez) dias úteis.

CLÁUSULA DÉCIMA – DA FISCALIZAÇÃO DO CONTRATO

10.1. Será gestor deste contrato o empregado Sr/Srª _____, conforme portaria nº _____. Este ficará responsável pelo acompanhamento da execução bem como pela fiscalização do presente instrumento, por meio de relatórios, inspeções, visitas, atestado da satisfatória realização do objeto e outros procedimentos que julgar necessário.

CLÁUSULA DÉCIMA PRIMEIRA – DOS RECURSOS FINANCEIROS

11.1. As despesas decorrentes do presente contrato correrão à conta de **Recursos do Convênio 003/2015, firmado entre a AGEHAB e a Secretaria de Estado de Meio Ambiente, Recursos Hídricos, Infraestrutura, Cidades e Assuntos Metropolitanos - SECIMA, conforme Plano de Trabalho, Ação 2, Atividade "C".**

CLÁUSULA DECIMA SEGUNDA – DAS PENALIDADES E MULTAS

12.1. Pela inexecução contratual, atraso injustificado na execução do contrato, sujeitará a Contratada, além das cominações legais cabíveis, à multa de mora, graduada de acordo com a gravidade da infração, obedecida os seguintes limites máximos:

12.1.1. 10% (dez por cento) sobre o valor do contrato em caso de descumprimento total da obrigação;

12.1.2. Multa de até 0,1% (um décimo por cento) por semana de atraso, calculado sobre a respectiva etapa do serviço de implantação;

12.2. No caso de atraso superior a 90 (noventa) dias, será aplicada penalidade adicional de até (um por cento) sobre a respectiva etapa do serviço de implantação, por mês, até o limite de 10 (dez) meses;

Agência Goiana de Habitação S/A - Rua 18-A nº 541, Setor Aeroporto - Goiânia - Goiás - 74.070-060 - (62) 3096-5000

12.3. No caso do não cumprimento ou cumprimento irregular dos serviços de Manutenção e Evolução Tecnológica dos Softwares ERPI; Suporte Técnico das Soluções Implementadas ERP; Treinamento nos softwares ERP será aplicada multa de até 0,2% (dois décimos por cento) sobre o valor total do Contrato, por dia de atraso, até o limite de 5% (cinco por cento);

12.4. 0,3% (três décimos por cento) ao dia, até o trigésimo dia de atraso, sobre o valor da parte do fornecimento não realizado;

12.5. 0,7% (sete décimos por cento) sobre o valor do fornecimento não realizado, por cada dia subseqüente ao trigésimo;

12.6. suspensão temporária do direito de participar em licitação e impedimento de contratar com a Administração Pública, por prazo não superior a 05 (cinco) anos;

12.7. declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação, perante a própria autoridade que aplicou a penalidade, que será concedida sempre que o contratado ressarcir a Administração pelos prejuízos resultantes e após decorrido o prazo da sanção aplicada com base no inciso anterior.

12.8. A multa será descontada dos pagamentos eventualmente devidos, ou ainda, quando for o caso, cobrada judicialmente.

12.9. Qualquer das penalidades aqui previstas e aplicadas será registrada junto ao CADFOR.

CLÁUSULA DECIMA TERCEIRA – DA RESCISÃO

13.1. A rescisão do presente contrato poderá ser:

13.1.1. Determinada por ato motivado da Administração, após processo regular, assegurado o contraditório e a ampla defesa, nos casos do artigo 78, incisos I a XII, XVII e parágrafo único e inciso XVIII, da Lei Federal nº 8.666 de 21/06/1993.

13.1.2. Amigável, por acordo entre as partes, reduzida a termo, desde que haja conveniência para a Contratante.

13.1.3. Judicial, nos termos da legislação.

CLÁUSULA DÉCIMA QUARTA – DAS DISPOSIÇÕES GERAIS

14.1. O presente contrato reger-se-á pelas suas cláusulas e normas consubstanciadas na Lei Federal nº 8.666/93.

14.2. Fica declarado competente o foro da Comarca de Goiânia, para dirimir quaisquer dúvidas referentes a este contrato.

14.3. Os casos omissos serão resolvidos de acordo com a Lei nº 8.666/93, e demais normas aplicáveis.

E por estarem justos e contratados, os representantes das partes assinam o presente instrumento, na presença de testemunhas conforme abaixo, em 02(duas) vias de igual teor e forma, para um só efeito.

Goiânia, 22 de fevereiro de 2017.

LUIZ ANTONIO STIVAL MILHOMENS
Presidente

FERNANDO JORGE DE OLIVEIRA
Diretor Administrativo

HYULLEY AQUINO MACHADO
Diretor Financeiro

GLAUCIO DA SILVA MELO
Core Serviços e Informática Ltda – Me

LORIVALDO XAVIER DE OLIVEIRA
Core Serviços e Informática Ltda - Me

Testemunhas:

1 - Francisco Hicário C. de Magalhães
CPF: 251.260.752-68

2 - _____
CPF: _____
Marcelle Diniz Moura Barros
CPF: 010.870.921-32

Jair José Ribeiro Filho
OAB/GO Nº 31.599
ASJUR - AGEHAB