PROCESSO Nº 016/2021

CONTRATO Nº 011/2021, QUE ENTRE SI CELEBRAM A AGÊNCIA BRASILEIRA GESTORA DE FUNDOS GARANTIDORES E GARANTIAS S.A - ABGF E A EMPRESA MULTIP REDES MULTISERVIÇOS LTDA.

A AGÊNCIA BRASILEIRA GESTORA DE FUNDOS GARANTIDORES E GARANTIAS S.A. – ABGF, empresa pública, vinculada ao Ministério da Economia, com sede Setor Comercial Norte, Quadra 02, Bloco A, 10° Andar, Sala 1002, Edifício Corporate Financial Center, Brasília-DF, CEP:70710-000, cadastrada no CNPJ/MF sob o nº 17.909.518/0001-45, representada por seu Presidente, _____, _____, _____, _____, portador do Registro Geral nº _____, inscrito no CPF sob o nº xxx.329.878-xx, eleito no dia 19 de dezembro de 2019, pelo Conselho de Administração, por sua Diretora de Garantias, **HELENA MULIM VENCESLAU,** _____, _____, _____, _____, portadora do Registro Geral nº _____, inscrita no CPF sob o nº xxx.979.301-xx, eleita no 29 de agosto de 2019, pelo Conselho de Administração, ambos domiciliados Setor Comercial Norte, Quadra 02, Bloco A, 10° Andar, Sala 1002, Edifício Corporate Financial Center, em Brasília – DF, doravante denominada **CONTRATANTE**, e do outro lado a empresa **MULTIP REDE MULTISERVIÇOS LTDA - EPP**,. Inscrita no CNPJ sob o nº 04.721.052/0001-08, sediada no SRTVN, Quadra 70T, Conj. C, nº 214, salas 210 e 212, Ala “A”, Asa Norte, Brasília/DF, CEP: 70719-903, doravante denominada **CONTRATADA**, neste ato, representada por seu (ua) _____, _____, _____, _____, portador(a) do Registro Geral nº _____, inscrito(a) no CPF sob o nº _____, resolvem celebrar o presente Contrato, em conformidade com o que consta do Processo Administrativo nº 016/2021-ABGF, referente à Dispensa de Licitação nº 015/2021, e com fundamento na Lei nº 13.303/2016, mediante as Cláusulas e condições seguintes:

CLÁUSULA PRIMEIRA – DO OBJETO

1.1. Contratação de empresa especializada para fornecimento de firewall e antivírus, como serviço, para atender às necessidades da Agência Brasileira Gestora de Fundos Garantidores e Garantias S.A. – ABGF.

CLÁUSULA SEGUNDA – DAS ESPECIFICAÇÕES TÉCNICAS DOS SERVIÇOS

2.1 Item 01 - Solução de firewall, como serviço, e suporte técnico especializado:

2.1.1 A contratação de solução de segurança de rede, compreende o fornecimento de equipamentos (hardwares), softwares e prestação de serviços.

2.1.2 Next-Generation Firewall (NGFW) para proteção de informação perimetral e de rede interna que inclui stateful firewall com capacidade para operar em alta disponibilidade (HA) em modo ativo-passivo ou ativo-ativo para controle de tráfego de dados por identificação de usuários e por camada 07 (aplicação), com controle de administração de largura de banda (QoS), VPN IPsec e SSL, IPS, prevenção contra ameaças de vírus, malwares, Filtro de URL, criptografia de e-mail, inspeção de tráfego criptografado e proteção de firewall de aplicação Web.

2.1.3 Deverá ser fornecido, **na modalidade de comodato**, o equipamento necessário para implantação da solução de segurança de rede e console de gerenciamento do equipamento.

2.1.3.1 Por cada *appliance* físico que compõe a plataforma de segurança, entende-se o hardware, software e as licenças necessárias para o seu funcionamento.

2.1.4 Por alta disponibilidade (HA) entende-se que, caso o *appliance* apresente problemas de *hardware*, a CONTRATADA deverá substituir o equipamento por outro igual ou superior, no mesmo prazo estabelecidos no item 5.2 para respostas de alta criticidade.

2.1.5 A solução deverá contemplar a totalidade das capacidades exigidas, sendo permitido o uso de mais de um para complementar a solução, caso o fabricante não possua todas as funções em um único equipamento.

2.1.6 Cada *appliance* deverá ser capaz de executar a totalidade das capacidades exigidas para cada função, não sendo aceitos somatórias para atingir os limites mínimos.

2.1.7 O hardware e o software fornecidos não podem constar, no momento da apresentação da proposta, em listas de *end-of-sale, end-of-support, end-of-engineering-support* ou *end-of-life* do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante.

2.1.8 Características específicas de desempenho e hardware do firewall:

a) Performance mínima de 14 Gbps de *throughput* para firewall;
b) Performance mínima de 2.5 Gbps de *throughput* de IPS;
c) Performance mínima de 1.5 Gbps de *throughput* para controle de Threat Protection;
d) Performance mínima de 1 Gbps de *throughput* de VPN;
e) Suporte a, no mínimo, 8.000.000 de conexões simultâneas;
f) Suporte a, no mínimo, 100.000 novas conexões por segundo;
g) Possuir o número irrestrito quanto ao máximo de usuários licenciados;
h) Possuir armazenamento interno de no mínimo 120 GB SSD para sistema operacional, quarentena local, logs e relatórios;
i) Possuir no mínimo 8 GB de memória RAM;
j) Possuir no mínimo 6 (seis) interfaces de rede 1000Base-TX; e
k) Possuir 1 (uma) interface do tipo console ou similar.

2.1.9 Características gerais do firewall:

a) A solução deve consistir de *appliance* de proteção de rede com funcionalidades de *Next Generation Firewall* (NGFW), e console de gerência, monitoração e logs;
b) Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
c) As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos *appliances* desde que obedeçam a todos os requisitos desta especificação;
d) A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 07 (aplicação);
e) O software deverá ser fornecido em sua versão mais atualizada;
f) Uma interface completa de comando de linha (*CLI command-line-interface*) deverá ser acessível através da interface gráfica e via porta serial;
g) A atualização de software deverá enviar avisos de atualização automáticos;
h) O sistema de objetos deverá permitir a definição de redes, serviços, *hosts* períodos de tempos, usuários e grupos, clientes e servidores;
i) O *backup* e o reestabelecimento de configuração deverão ser realizados localmente, via FTP ou e-mail com frequência diária, semanal ou mensal, podendo também ser realizado por demanda;
j) As notificações deverão ser realizadas via e-mail e SNMP;
k) Suportar SNMPv3 e Netflow;
l) O firewall deverá ser *stateful*, com inspeção profunda de pacotes;
m) As zonas deverão ser divididas pelo menos em WAN, LAN e DMZ, sendo necessário que as zonas LAN e DMZ possam ser customizáveis;
n) As políticas de NAT deverão ser customizáveis para cada regra;

o) A proteção contra *flood* deverá ter proteção contra DoS (*Denial of Service*), DdoS (*Distributed DoS*);
p) Proteção contra *anti-spoofing*;
q) Suportar IPv4 e IPv6;
r) IPv6 deve suportar os tunelamentos 6in4, 6to4, 4in6 e *IPv6 Rapid Deployment (6rd)* de acordo com a RFC 5969;
s) Suporte aos roteamentos estáticos, dinâmico (RIP, BGP e OSPF) e multicast (PIM-SM e IGMP);
t) Deve possuir tecnologia de conectividade SD-WAN;
u) Deve possibilitar o roteamento baseado em VPNs;
v) Deve suportar criar políticas de roteamento, sendo permitidas pelo menos as seguintes condições: Interface de entrada do pacote; IPs de origem; IPs de destino; Portas de destino; Usuários ou grupos de usuários; Aplicação em camada 7.
w) Deve ser possível escolher um gateway primário e um gateway de backup para as políticas de roteamento;
x) Deve suportar a definição de VLANs no firewall conforme padrão IEEE 802.1q e *tagging* de VLAN.
y) Deve suportar Extended VLAN;
z) O balanceamento de link WAN deve permitir múltiplas conexões de links Internet, checagem automática do estado de links, *failover* automático e balanceamento por peso.
aa) A solução deverá permitir port-aggregation de interfaces de firewall suportando o protocolo 802.3ad, para escolhas entre aumento de throughput e alta disponibilidade de interfaces;
bb) Deve permitir a configuração de jumbo frames nas interfaces de rede;
cc) Deve permitir a criação de um grupo de portas layer2;
dd) A solução deverá permitir configurar os serviços de DNS, *Dynamic* DNS, DHCP e NTP;
ee) O *traffic shapping (QoS)* deverá ser baseado em rede ou usuário;
ff) A solução deve permitir o tráfego de cotas baseados por usuários para upload/download e pelo tráfego total, sendo cíclicas ou não-cíclicas;
gg) Deve possuir otimização em tempo real de voz sobre IP; e
hh) Deve implementar o protocolo de negociação Link Aggregation Control Protocol (LACP).

2.1.10 Controle por política de firewall:

a) Deve suportar controles por: porta e protocolos TCP/UDP, origem/destino e identificação de usuários;
b) O controle de políticas deverá monitorar as políticas de redes, usuários, grupos e tempo, bem como identificar as regras não-utilizadas, desabilitadas, modificadas e novas políticas;
c) As políticas deverão ter controle de tempo de acesso por usuário e grupo, sendo aplicadas por zonas, redes e por tipos de serviços;

d) Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
e) Controle de políticas por países via localização por IP;
f) Suporte a objetos e regras IPV6; e
g) Suporte a objetos e regras *multicast*.

2.1.11 Prevenção de ameaças:

2.1.11.1 Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus, *Anti-Malware* e Firewall de Proteção Web (*WAF*) integrados no próprio *appliance* de Firewall ou entregue em múltiplos *appliances* desde que obedeçam a todos os requisitos desta especificação.

2.1.11.2 Deve realizar a inspeção profunda de pacotes para prevenção de intrusão (IPS) e deve incluir assinaturas de prevenção de intrusão (IPS).

2.1.11.3 As assinaturas de prevenção de intrusão (IPS) devem ser customizadas.

2.1.11.4 Exceções por usuário, grupo de usuários, IP de origem ou de destino devem ser possíveis nas regras

2.1.11.5 Deve suportar granularidade nas políticas de IPS Antivírus e *Anti-Malware*, possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens, com customização completa.

2.1.11.6 A proteção *Anti-Malware* deverá bloquear todas as formas de vírus, *web malwares*, *trojans* e *spyware* em HTTP e HTTPS, FTP e *web e-mails*.

2.1.11.7 A proteção Anti-Malware deverá realizar a proteção com emulação *JavaScript*.

2.1.11.8 Deve ter proteção em tempo real contra novas ameaças criadas.

2.1.11.9 Deve possuir pelo menos duas *engines* de antivírus independentes e de diferentes fabricantes para a detecção de *malware*, podendo ser configuradas isoladamente ou simultaneamente.

2.1.11.10 Deve permitir o bloqueio de vulnerabilidades.

2.1.11.11 Deve permitir o bloqueio de *exploits* conhecidos.

2.1.11.12 Deve detectar e bloquear o tráfego de rede que busque acesso a *command and control* e servidores de controle utilizando múltiplas camadas de DNS, *AFC* e firewall.

2.1.11.13 Deve incluir proteção contra-ataques de negação de serviços.

2.1.11.14 Ser imune e capaz de impedir ataques básicos como: *SYN flood, ICMP flood, UDP Flood*, etc.

2.1.11.15 Suportar bloqueio de arquivos por tipo.

2.1.11.16 Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo.

2.1.11.17 Os eventos devem identificar o país de onde partiu a ameaça.

2.1.11.18 Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas de segurança considerando uma das opções ou a combinação de todas elas: usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por usuários, grupos de usuários, origem, destino, zonas de segurança.

2.1.11.19 O firewall de aplicação Web (*WAF*) deverá ter a função de *reverse proxy*, com a função de *URL hardening* realizando *deep-linking* e prevenção dos ataques de *path traversal* ou *directory traversal*.

2.1.11.20 O firewall de aplicação Web (*WAF*) deverá realizar *cookie signing* com assinaturas digitais, roteamento baseado por caminho, autenticações reversas e básicas para acesso do servidor.

2.1.11.21 O firewall de aplicação Web (*WAF*) deverá possuir a função de balanceamento de carga de visitantes por múltiplos servidores, com a possibilidade de modificação dos parâmetros de performance do *WAF* e permissão e bloqueio de *ranges* de IP.

2.1.11.22 Deve possuir pelo menos duas *engines* de antivírus independentes e de diferentes fabricantes para a proteção da aplicação Web, podendo ser configuradas isoladamente ou simultaneamente.

2.1.11.23 Proteção pelo menos contra os seguintes ataques, mas não limitado a: *SQL injection* e *Cross-site scripting*.

2.1.12 Controle e proteção de aplicações:

2.1.12.1 Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações por assinaturas e camada 07 (aplicação), utilizando portas padrões (80 e 443), portas não padrões, *port hopping* e túnel através de tráfego SSL encriptado.

2.1.12.2 Deve ser possível inspecionar os pacotes criptografados com os algoritmos SSL 2.0, SSL 3.0, TLS 1.2 e TLS 1.3.

2.1.12.3 O motor de análise de tráfego criptografado deve reconhecer, mas não limitado a, pelo menos os seguintes algoritmos: curvas elípticas (ECDH, ECDHE, ECDSA), DH, DHE, Authentication, RSA, DSA, ANON, Bulk ciphers, RC4, 3DES, IDEA, AES128, AES256, Camellia, ChaCha20-Poly1305, GCM, CCM, CBC, MD5, SHA1, SHA256, SHA384.

2.1.12.4 O motor de inspeção dos pacotes criptografados deve ser configurável e permitir definir ações como não decriptografar, negar o pacote e criptografar para determinadas conexões criptografadas

2.1.12.5 Reconhecer pelo menos 2.300 aplicações diferentes, classificadas por nível de risco, características e tecnologia, incluindo, mas não limitado a tráfego relacionado a *peer-to-peer*, redes sociais, acesso remoto, *update* de software, serviços de rede, VoIP, streaming de mídia, proxy e tunelamento, mensageiros instantâneos, compartilhamento de arquivos, web e-mail e update de softwares.

2.1.12.6 Reconhecer pelo menos as seguintes aplicações: *4Shared File Transfer, Active Directory/SMB, Citrix ICA, DHCP Protocol, Dropbox Download, Easy Proxy, Facebook Graph API, Firefox Update, Freegate Proxy, FreeVPN Proxy, Gmail Video, Chat* Streaming, Gmail WebChat, Gmail WebMail, Gmail-Way2SMS WebMail, Gtalk Messenger, Gtalk Messenger File Transfer, Gtalk-Way2SMS, HTTP Tunnel Proxy, HTTPort Proxy, LogMeIn Remote Access, NTP, Oracle database, RAR File Download, Redtube Streaming, RPC over HTTP Proxy, Skydrive, Skype, Skype Services, skyZIP, SNMP Trap, TeamViewer Conferencing e File Transfer, TOR Proxy, Torrent Clients P2P, Ultrasurf Proxy, UltraVPN, VNC Remote Access, VNC Web Remote Access, WhatsApp, WhatsApp File Transfer e WhatsApp Web.

2.1.12.7 Deve realizar o escaneamento e controle de *micro app* incluindo, mas não limitado a: *Facebook (Applications, Chat, Commenting, Events, Games, Like Plugin, Message, Pics Download e Upload, Plugin, Post Attachment, Posting, Questions, Status Update, Video Chat, Video Playback, Video Upload, Website), Freegate Proxy, Gmail (Android Application, Attachment), Google Drive (Base, File Download, File Upload), Google Earth Application, Google Plus, LinkedIN (Company Search, Compose Webmail, Job Search, Mail Inbox, Status Update), SkyDrive File Upload e Download, Twitter (Message, Status Update, Upload, Website), Yahoo (WebMail, WebMail File Attach) e Youtube (Video Search, Video Streaming, Upload, Website)*

2.1.12.8 Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de *payload* para checagem de assinaturas de aplicações conhecidas pelo fabricante.

2.1.12.9 Atualizar a base de assinaturas de aplicações automaticamente.

2.1.12.10 Reconhecer aplicações em IPv6.

2.1.12.11 Limitar a banda usada por aplicações (*traffic shaping*).

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

2.1.12.13 Deve ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras.

2.1.12.14 Deve permitir o uso individual de diferentes aplicativos para usuários que pertencem ao mesmo grupo de usuários, sem que seja necessária a mudança de grupo ou a criação de um novo grupo. Os demais usuários deste mesmo grupo que não possuírem acesso a estes aplicativos devem ter a utilização bloqueada.

2.1.13 Controle e proteção web:

2.1.13.1 Deve permitir especificar política de navegação Web por tempo, ou seja, a definição de regras para um determinado dia da semana e horário de início e fim, permitindo a adição de múltiplos dias e horários na mesma definição de política por tempo. Esta regra de tempo pode ser recorrente ou em uma única vez.

2.1.13.2 Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs e redes.

2.1.13.3 Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via LDAP, *Active Directory*, *Radius*, *E-directory* e base de dados local.

2.1.13.4 Autenticação em 02 fatores em conjunto com a autenticação Radius.

2.1.13.5 Permitir popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório.

2.1.13.6 Possuir pelo menos 90 categorias de URLs.

2.1.13.7 Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL.

2.1.13.8 Deve ser capaz de forçar o uso da opção Safe Search em sites de busca.

2.1.13.9 Deve ser capaz de forçar as restrições do Youtube.

2.1.13.10 Deve ser capaz de categorizar as URLs a partir de base ou cache de URLs locais ou através de consultas dinâmicas na nuvem do fabricante, independentemente do método de classificação a categorização não deve causar atraso na comunicação visível ao usuário.

2.1.13.11 Suportar a criação categorias de URLs customizadas.

2.1.13.12 Suportar a opção de bloqueio de categoria HTTP e liberação da categoria apenas em HTTPS.

2.1.13.13 Deve ser possível reconhecer o pacote HTTP independentemente de qual porta esteja sendo utilizada.

2.1.13.14 Suportar a inclusão nos logs do produto de informações das atividades dos usuários.

2.1.13.15 Deve salvar nos logs as informações adequadas para geração de relatórios indicando usuário, tempo de acesso, bytes trafegados e site acessado.

2.1.13.16 Deve permitir realizar análise flow dos pacotes, entendendo exatamente o que aconteceu com o pacote em cada checagem.

2.1.13.17 Deve realizar *caching* do conteúdo web.

2.1.13.18 Deve realizar filtragem por mime-type, extensão e tipos de conteúdo ativos, tais como, mas não limitado a*: ActiveX, applets* e *cookies*.

2.1.13.19 Deve ser possível realizar a liberação de cotas de navegação para os usuários, permitindo que os usuários tenham tempos pré-determinados para acessar sites na internet.

2.1.13.20 A console de gerenciamento deve possibilitar a visualização do tempo restante para cada usuário, bem como reiniciar o tempo restante com o intuito de zerar o contador.

2.1.13.21 Deve possuir capacidade de alguns usuários previamente selecionados realizarem um bypass temporário na política de bloqueio atual.

2.1.14 Identificação de usuários:

2.1.14.1 Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticando via LDAP, *Active Directory, Radius, eDirectory, TACACS+* e via base de dados local, para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários.

2.1.14.2 Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (*Captive Portal*).

2.1.14.3 Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços.

2.1.14.4 Deve permitir autenticação em modos: transparente, autenticação proxy (NTLM e Kerberos) e autenticação via clientes nas estações com os sistemas operacionais Windows, MAC OS X e Linux 32/64.

2.1.14.5 Deve possuir a autenticação Single sign-on para, pelo menos, os sistemas de diretórios *Active Directory* e *eDirectory*.

2.1.14.6 Deve possuir portal do usuário para que os usuários tenham acesso ao uso de internet pessoal, troquem senhas da base local e façam o download de softwares para as estações presentes na solução.

2.1.15 Qualidade de Serviço QoS:

2.1.15.1 Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações.

2.1.15.2 A solução deverá suportar *Traffic Shaping* (Qos) e a criação de políticas baseadas em categoria web e aplicação por: endereço de origem; endereço de destino; usuário e grupo do LDAP/AD.

2.1.15.3 Deve ser configurado o limite e a garantia de upload/download, bem como ser priorizado o tráfego total e *bitrate* de modo individual ou compartilhado.

2.1.15.4 Suportar priorização *Real-Time* de protocolos de voz (VoIP).

2.1.15.5 Deve permitir aplicar prioridade mesmo após o roteamento, utilizando o protocolo DSCP.

2.1.16 Redes Virtuais Privadas – VPN:

2.1.16.1 Suportar VPN *Site-to-Site e Cliente-to-Site*.

2.1.16.2 Suportar IPsec VPN.

2.1.16.3 Suportar SSL VPN.

2.1.16.4 Suportar L2TP e PPTP.

2.1.16.5 Suportar acesso remoto SSL, IPSec e VPN Client para Android e iPhone/iPAD.

2.1.16.6 Deve ser disponibilizado o acesso remoto ilimitado, até o limite suportado de túneis VPN pelo equipamento, sem a necessidade de aquisição de novas licenças e sem qualquer custo adicional para o licenciamento de clientes SSL.

2.1.16.7 Deve possuir o acesso via o portal de usuário para o download e configuração do cliente SSL para Windows.

2.1.16.8 Deve possuir opção de VPN IPSEC com client nativo do fabricante.

2.1.16.9 Deve possuir um portal encriptado baseado em HTML5 para suporte pelo menos a: RDP, SSH, Telnet e VNC, sem a necessidade de instalação de clientes VPN nas estações de acesso.

2.1.16.10 A VPN IPsec deve suportar: DES e 3DES, Autenticação MD5 e SHA-1;*Diffie-Hellman Group 1, Group 2, Group 5 e Group 14*; Algoritmo Internet Key Exchange (IKE); AES 128, 192 e 256 (*Advanced Encryption Standard*); SHA 256, 384 e 512; Autenticação via certificado PKI (X.509) e *Pre-shared key* (PSK).

2.1.16.11 Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Dell SonicWALL, Fortinet, Huawei, Juniper, Palo Alto Networks e Sophos.

2.1.16.12 Deve permitir criar políticas de controle de aplicações, IPS, Antivírus, *Anti-Malware* e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL.

2.1.16.13 Suportar autenticação via AD/LDAP, *Token* e base de usuários local.

2.1.16.14 Permitir estabelecer um túnel SSL VPN com uma solução de autenticação via LDAP, *Active Directory, Radius, eDirectory, TACACS+* e via base de dados local.

2.1.17 Deverá possuir painel administrativo para gerenciamento do equipamento.

2.1.17.1 Deve possuir solução de gerenciamento, possibilitando o gerenciamento do equipamento através de uma única console central (painel), com administração de privilégios e funções.

2.1.17.2 O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelo firewall.

2.1.17.3 Deve possuir indicadores do estado DO equipamentos e rede.

2.1.17.4 Deve emitir alertas baseados em thresholds customizáveis, incluindo também alertas de expiração de subscrição, mudança de status de gateways, uso excessivo de disco, eventos ATP, IPS, ameaças de vírus, navegação, entre outros.

2.1.17.5 Deve ter controle de privilégios administrativos, com granularidade de funções (VPN admin, App e Web admin, IPS admin, etc).

2.1.17.6 Deve ter logs de auditoria de uso administrativo e atividades realizadas no equipamento.

2.1.18 Gerência de logs e relatórios:

2.1.18.1 Deve possuir solução de logs e relatórios.

2.1.18.2 Deverá prover relatórios baseados em usuários com visibilidade sobre acesso a aplicações, navegação, eventos ATP, downloads e consumo de banda, independente em qual rede ou IP o usuário esteja se conectando.

2.1.18.3 Deve conter relatórios pré-configurados, pelo menos de: aplicações, navegação, web server (WAF), IPS, ATP e VPN.

2.1.18.4 Deve fornecer relatórios históricos para análises de mudanças e comportamentos.

2.1.18.5 Deve conter customizações dos relatórios.

2.1.18.6 Deve permitir a geração de relatórios em PDF ou Excel.

2.1.18.7 Deve fornecer relatórios sobre os acessos de procura por URL.

2.1.18.8 Deve fornecer logs em tempo real, de auditoria e arquivados.

2.1.18.9 Deve ter acesso baseado em web com controles administrativos distintos.

2.1.19 Integração com solução de endpoint (antivírus):

2.1.19.1 A solução de firewall deve possibilitar a integração com a solução de Endpoint que será instalada no ambiente da CONTRATANTE.

2.1.19.2 A integração deve possibilitar a criação de regras de bloqueio de endpoints, com determinado status, dentro do Firewall de forma automática, sem que haja intervenção por parte do time da CONTRATANTE.

2.1.19.3 A integração deverá ser nativa entre o firewall e o endpoint, ou utilizando APIs de integração da solução de firewall.

2.1.19.4 Caso a integração não seja nativa, cabe a CONTRATADA:

2.1.19.4.1 Desenvolver completamente a solução de integração do Firewall e o Endpoint instalado;

2.1.19.4.2 O Software de integração deve realizar a criação das regras do Firewall com no máximo 02 (dois) minutos após o incidente detectado no Endpoint;

2.1.19.4.3 Possuir interface WEB, acessada por HTTP ou HTTPS, para definição dos objetos das regras a serem criados, com no mínimo origem, destino, status do endpoint e protocolos;

2.1.19.4.4 Possibilitar o envio de e-mails sobre as ações do software;

2.1.19.4.5 Entregar o software de integração em máquina virtual, Windows ou Linux, juntamente com as devidas licenças necessárias para sistemas operacionais, banco de dados, e etc;

2.1.19.4.6 A máquina virtual será instalada no ambiente da CONTRATANTE, não sendo permitido soluções em nuvem;

2.1.19.4.7 A máquina virtual não deverá ter qualquer acesso remoto que não seja acordado pela CONTRATADA;

2.1.19.4.8 A mesma não deverá enviar/receber pacotes TCP/UDP ou por qualquer outro meio de comunicação, que não sejam do Firewall especificado ou a console do endpoint da CONTRATANTE;

2.1.19.4.9 A gestão do sistema operacional da máquina virtual em questão será de inteira responsabilidade da CONTRATANTE, de modo a garantir que sejam realizados todos os updates, correções de patchs, segurança do sistema operacional, bem como com seus softwares, alterações de versões, e etc.

2.1.19.4.10 A máquina virtual deve ser utilizada única e exclusivamente para o fim proposto na solução, não sendo permitido que a máquina virtual realize qualquer outra função;

2.1.19.4.11 Permitir backup das configurações do software de integração, possibilitando o restore em outra máquina virtual de forma a não comprometer o ambiente;

2.1.19.4.12 Realizar manutenção/alteração total no software de integração, sem custo adicional, durante o período de vigência do suporte do Firewall; e

2.1.19.4.13 Realizar teste de bancada, afim de comprovar a efetividade da integração.

2.2 <u>Item 02 - Solução de endpoint (antivírus), como serviço, e suporte técnico especializado.</u>

2.2.1 O serviço deverá ser prestado por 12 (doze) meses.

2.2.2 Características gerais da solução de endpoint:

2.2.2.1 Todos os componentes que fazem parte da solução, de segurança para servidores, estações de trabalho deverão ser fornecidas por um único fabricante. Não serão aceitas composições de produtos de fabricantes diferentes.

2.2.2.2 A console de monitoração e configuração deverá ser feita através de uma central única, baseada em web, que deverá conter todas a fermentas para a monitoração e controle da proteção dos dispositivos.

2.2.2.3 A console deverá apresentar dashboard com o resumo dos status de proteção dos computadores e usuários, bem como indicar os alertas de eventos de criticidades alta, média e informacional.

2.2.2.4 Deve possuir mecanismo de comunicação via API, para integração com outras soluções de segurança, como por exemplo SIEM.

2.2.2.5 Deve possuir capacidade de realizar a integração com soluções de firewalls para criar políticas automáticas em caso de ataques em massa nos computadores e servidores.

2.2.2.6 A console deve permitir a divisão dos computadores, dentro da estrutura de gerenciamento em grupos.

2.2.2.7 Deve permitir sincronização com o Active Directory (AD) para gestão de usuários e grupos integrados às políticas de proteção.

2.2.2.8 Deve possuir a possibilidade de aplicar regras diferenciadas baseado em grupos ou usuários.

2.2.2.9 A instalação deve ser feita via cliente específico por download da gerência central ou também via e-mail de configuração. O instalador deverá permitir a distribuição do cliente via Active Directory (AD) para múltiplas máquinas.

2.2.2.10 Deve ser capaz, via console, de criar e editar diferentes políticas para a aplicação das proteções exigidas e aplicadas a nível de usuários, não importando em que equipamentos eles estejam acessando.

2.2.2.11 Fornecer atualizações do produto e das definições de vírus e proteção

contra intrusos.

2.2.2.12 Deve permitir exclusões de escaneamento para determinados websites, pastas, arquivos ou aplicações, tanto a nível geral quanto específico em uma determinada política.

2.2.2.13 A console de gerenciamento deve permitir a definição de grupos de usuários com diferentes níveis de acesso as configurações, políticas e logs.

2.2.2.14 Atualização incremental, remota e em tempo real, da vacina dos antivírus e do mecanismo de verificação (Engine) dos clientes.

2.2.2.15 Permitir o agendamento da varredura contra vírus com a possibilidade de selecionar uma máquina, grupo de máquinas ou domínio, com periodicidade definida pelo administrador.

2.2.2.16 Atualização automática das assinaturas de ameaças (malwares) e políticas de prevenção desenvolvidas pelo fabricante em tempo real ou com periodicidade definida pelo administrador.

2.2.2.17 Utilizar protocolos seguros padrão HTTPS para comunicação entre console de gerenciamento e clientes gerenciados.

2.2.2.18 As mensagens geradas pelo agente deverão estar no idioma em português ou permitir a sua edição.

2.2.2.19 Permitir a exportação dos relatórios gerenciais para os formatos CSV e PDF.

2.2.2.20 Recursos do relatório e monitoramento deverão ser nativos da própria console central de gerenciamento.

2.2.2.21 Possibilidade de exibir informações como nome da máquina, versão do antivírus, sistema operacional, versão da engine, data da vacina, data da última verificação, eventos recentes e status.

2.2.2.22 Capacidade de geração de relatórios, estatísticos ou gráficos, tais como:

a) Detalhar quais usuários estão ativos, inativos ou desprotegidos, bem como detalhes dos mesmos;
b) Detalhamento dos computadores que estão ativos, inativos ou desprotegidos, bem como detalhes das varreduras e dos alertas nos computadores;
c) Detalhamento dos periféricos permitidos ou bloqueados, bem como detalhes de onde e quando cada periférico foi usado;

d) Detalhamento das principais aplicações bloqueadas e os servidores/usuários que tentaram acessá-las;
e) Detalhamento das aplicações permitidas que foram acessadas com maior frequência e os servidores/usuários que as acessam;
f) Detalhamento dos servidores/usuários que tentaram acessar aplicações bloqueadas com maior frequência e as aplicações que eles tentaram acessar; e
g) Detalhamento de todas as atividades disparadas por regras de prevenção de perda de dados.

2.2.2.23 Deverá possuir um elemento de comunicação para mensagens e notificações entre estações e a console de gerenciamento utilizando comunicação criptografada.

2.2.2.24 Deve fornecer solução de gerenciamento de arquivos armazenados em nuvem, garantindo que um arquivo que foi feito um upload (exemplo Dropbox), tenha o processo monitorado e gerenciado, bem como realizar automaticamente o escaneamento do arquivo contra malwares.

2.2.2.25 As portas de comunicação deverão ser configuráveis. A comunicação deverá permitir QoS para controlar a largura de banda de rede.

2.2.2.26 A solução deverá permitir a seleção da versão do software de preferência, permitindo assim o teste da atualização sobre um grupo de PCs piloto antes de implantá-lo para toda a rede. Permitir ainda selecionar um grupo de computadores para aplicar a atualização para controlar a largura de banda de rede. A atualização da versão deverá ser transparente para os usuários finais.

2.2.2.27 O agente antivírus deverá proteger laptops, desktops e servidores em tempo real, sob demanda ou agendado para detectar, bloquear e limpar todos os vírus, trojans, worms e spyware. No Windows o agente também deverá detectar PUA, adware, comportamento suspeito, controle de aplicações e dados sensíveis. O agente ainda deve fornecer controle de dispositivos terceiros e, controle de acesso à web.

2.2.2.28 Deve possuir mecanismo contra a desinstalação do endpoint pelo usuário e cada dispositivo deverá ter uma senha única, não sendo autorizadas soluções com senha única válida para todos os dispositivos.

2.2.2.29 Deve prover no endpoint a solução de HIPS (Host Instrusion Prevention System) para a detecção automática e proteção contra comportamentos maliciosos (análise de comportamento) e deverá ser atualizado diariamente.

2.2.2.30 Deve prover proteção automática contra web sites infectados e maliciosos, assim como prevenir o ataque de vulnerabilidades de browser via web exploits.

2.2.2.31 Deve permitir a monitoração e o controle de dispositivos removíveis nos equipamentos dos usuários, como dispositivos USB, periféricos da própria estação de trabalho e redes sem fio, estando sempre atrelado ao usuário o controle e não ao dispositivo.

2.2.2.32 O controle de dispositivos deve ser ao nível de permissão, somente leitura ou bloqueio.

2.2.2.33 Os seguintes dispositivos deverão ser, no mínimo, gerenciados: HD (hard disks) externos, pendrives USB, storages removíveis seguras, CD, DVD, Blu-ray, floppy drives, interfaces de rede sem fio, modems, bluetooth, infra-vermelho, MTP (Media Transfer Protocol) tais como Blackberry, iPhone e Android smartphone e PTP (Picture Transfer Protocol) como câmeras digitais.

2.2.2.34 A ferramenta de administração centralizada deverá gerenciar todos os componentes da proteção para estações de trabalho e servidores e deverá ser projetada para a fácil administração, supervisão e elaboração de relatórios dos endpoint e servidores.

2.2.2.35 Deverá possuir interface gráfica web, com suporte a língua portuguesa (padrão brasileiro).

2.2.2.36 A Console de administração deve incluir um painel com um resumo visual em tempo real para verificação do status de segurança.

2.2.2.37 Deverá fornecer filtros pré-construídos que permitam visualizar e corrigir apenas os computadores que precisam de atenção.

2.2.2.38 Deverá exibir os PCs gerenciados de acordo com critérios da categoria (detalhes do estado do computador, detalhes sobre a atualização, detalhes de avisos e erros, detalhes do antivírus, etc), e classificar os PCs em conformidade.

2.2.2.39 Uma vez que um problema seja identificado, deverá permitir corrigir os problemas remotamente, com no mínimo as opções abaixo:

a) Proteger o dispositivo com a opção de início de uma varredura;
b) Forçar uma atualização naquele momento;
c) Ver os detalhes dos eventos ocorridos;
d) Executar verificação completa do sistema;
e) Forçar o cumprimento de uma nova política de segurança;
f) Mover o computador para outro grupo; e
g) Apagar o computador da lista.

2.2.2.40 Atualizar a políticas de segurança quando um computador for movido de um grupo para outro manualmente ou automaticamente.

2.2.2.41 Gravar um log de auditoria seguro, que monitore a atividade na console de gerenciamento para o cumprimento de regulamentações, auditorias de segurança, análise e solução de problemas forenses.

2.2.2.42 Deverá permitir exportar o relatório de logs de auditoria nos formatos CSV e PDF.

2.2.2.43 Deve conter vários relatórios para análise e controle dos usuários e endpoints.

2.2.2.44 Os relatórios deverão ser divididos, no mínimo, em relatórios de: eventos, usuários, controle de aplicativos, periféricos e web, indicando todas as funções solicitadas para os endpoints.

2.2.2.45 Fornecer relatórios utilizando listas ou gráficos, utilizando informações presentes na console, com no mínimo os seguintes tipos:

a) Nome do dispositivo;
b) Início da proteção;
c) Último usuário logado no dispositivo;
d) Último update;
e) Último escaneamento realizado;
f) Status de proteção do dispositivo; e
g) Grupo a qual o dispositivo faz parte.

2.2.2.46 Permitir a execução manual de todos estes relatórios nos formatos CSV e PDF.

2.2.3 Características gerais da solução para proteção das estações de trabalho:

2.2.3.1 Características básicas do agente de proteção contra malwares:

a) Pré-execução do agente para verificar o comportamento malicioso e detectar malware desconhecido;
b) O agente deve buscar algum sinal de malware ativo e detectar malwares desconhecidos;
c) O agente deve ter a capacidade de submeter o arquivo desconhecido à nuvem de inteligência do fabricante para detectar a presença de ameaças;
d) O agente deve realizar a atualização várias vezes por dia para manter a detecção atualizada contra as ameaças mais recentes;
e) A solução deve manter conexão direta com banco de dados de ameaças do fabricante para uso da rede de inteligência;
f) Deve realizar a verificação de todos os arquivos acessados em tempo real, mesmo durante o processo de boot;

g) Deve realizar a verificação de todos os arquivos no disco rígido em intervalos programados;
h) Deve realizar a limpeza do sistema automaticamente, removendo itens maliciosos detectados e aplicações potencialmente indesejáveis (PUA);
i) Deve proteger os navegadores Internet Explorer, Firefox, Chrome, Opera e Safari, bloqueando o acesso a sites infectados conhecidos e pela verificação dos dados baixados antes de serem executados;
j) Deve permitir a autorização de detecções maliciosas e excluir da varredura diretórios e arquivos específicos;
k) É requerida a proteção integrada, ou seja, em um único agente, contra ameaças de segurança, incluindo vírus, spyware, trojans, worms, adware e aplicativos potencialmente indesejados (PUAs);
l) Suportar máquinas com arquitetura 32-bit e 64-bit;
m) O cliente para instalação em estações de trabalho deverá ser compatível com os sistemas operacionais, Mac OS X 10.10, 10.11, 10.12, Microsoft Windows 7, 8 e 10;
n) Possuir a funcionalidade de proteção contra a alteração das configurações do agente, impedindo aos usuários, incluindo o administrador local, reconfigurar, desativar ou desinstalar componentes da solução de proteção; e
o) Permitir a utilização de senha de proteção para possibilitar a reconfiguração local no cliente ou desinstalação dos componentes de proteção.

2.2.3.2 Funcionalidade de Firewall e Detecção e Proteção de Intrusão (IDS\IPS):

2.2.3.2.1 Deverá possui atualização periódica de novas assinaturas de ataque.

2.2.3.2.2 Capacidade de reconhecer e bloquear automaticamente as aplicações em clientes baseando-se na impressão digital (hash) do arquivo ou dinamicamente através do nome da aplicação.

2.2.3.2.3 Capacidade de bloqueio de ataques baseado na exploração de vulnerabilidade conhecidas;

2.2.3.2.4 Possuir um sistema de prevenção de intrusão no host (HIPS), que monitore o código e blocos de código que podem se comportar de forma maliciosa antes de serem executados.

2.2.3.2.5 Ser capaz de aplicar uma análise adicional, inspecionando finamente o comportamento de códigos durante a execução, para detectar comportamento suspeito de aplicações, tais como buffer overflow.

2.2.3.2.6 Deve possuir técnicas de proteção, que inclui:

a) Análise dinâmica de código - técnica para detectar malware criptografado mais complexo;
b) Algoritmo correspondente padrão - onde os dados de entrada são comparados com um conjunto de sequências conhecidas de código já identificados como um vírus;
c) Emulação - uma técnica para a detecção de vírus polimórficos, ou seja, vírus que se escondem criptografando-se de maneira diferente cada vez que se espalham;
d) Tecnologia de redução de ameaças - detecção de prováveis ameaças por uma variedade de critérios, como extensões duplas (por exemplo. jpg.txt) ou a extensão não coincida com o tipo de arquivo verdadeiro (por exemplo, um arquivo executável ou arquivo .exe com a extensão .txt); e
e) Verificação de ameaças web avançadas**:** bloqueia ameaças verificando o conteúdo em tempo real e remontando com emulação de JavaScript e análise comportamental para identificar e parar o código malicioso de malware avançados.

2.2.3.3 Funcionalidade de Antivírus e AntiSpyware:

2.2.3.3.1 Proteção em tempo real contra vírus, trojans, worms, rootkits, botnets, spyware, adwares e outros tipos de códigos maliciosos.

2.2.3.3.2 Proteção anti-malware deverá ser nativa da solução ou incorporada automaticamente por meio de plug-ins sem a utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo mesmo fabricante.

2.2.3.3.3 As configurações do anti-spyware deverão ser realizadas através da mesma console do antivírus.

2.2.3.3.4 Permitir a configuração de ações diferenciadas para programas potencialmente indesejados ou malware, com possibilidade de inclusão de arquivos em listas de exclusão (whitelists) para que não sejam verificados pelo produto.

2.2.3.3.5 Permitir a varredura das ameaças da maneira manual, agendada e em tempo real na máquina do usuário.

2.2.3.3.6 Capacidade de detecção e reparo em tempo real de vírus de macro conhecidos e novos através do antivírus.

2.2.3.3.7 Capacidade de remoção automática total dos danos causados por spyware, adwares e worms, como limpeza do registro e pontos de carregamento, com opção de finalizar o processo e terminar o serviço da ameaça no momento de detecção.

2.2.3.3.8 A remoção automática dos danos causados deverá ser nativa do próprio antivírus; ou adicionada por plugin, desde que desenvolvido ou distribuído pelo mesmo fabricante.

2.2.3.3.9 Capacidade de bloquear origem de infecção através de compartilhamento de rede com opção de bloqueio da comunicação via rede.

2.2.3.3.10 Permitir o bloqueio da verificação de vírus em recursos mapeados da rede.

2.2.3.3.11 Antivírus de Web (verificação de sites e downloads contra vírus).

2.2.3.3.12 Controle de acesso a sites por categoria.

2.2.3.3.13 Proteger a navegação na web, mesmo aos usuários fora da rede, para todos os principais navegadores (IE, Firefox, Safari, Opera e Chrome), fornecendo controle da Internet independentemente do browser utilizado, como parte da solução de proteção a estações de trabalho, incluindo a análise do conteúdo baixado pelo navegador web, de forma independente do navegador usado, ou seja, sem utilizar um plugin, onde não é possível ser ignorada pelos usuários, protegendo os usuários de websites infectados e categorias específicas de websites.

2.2.3.3.14 O Controle da Web deve controlar o acesso a sites impróprios, com no mínimo 14 categorias de sites inadequados. Deve ainda permitir a criação de lista branca de sites sempre permitidos e lista negra de sites que devem ser bloqueados sempre.

2.2.3.3.15 Todas as atividades de navegação na Internet bloqueadas deverão ser enviadas para a console de gerenciamento, informando detalhes do evento e a razão para o bloqueio.

2.2.3.3.16 Capacidade de verificar somente arquivos novos e alterados.

2.2.3.4 Funcionalidade de detecção Pró-Ativa de reconhecimento de novas ameaças:

2.2.3.4.1 Funcionalidade de detecção de ameaças via técnicas de machine learning.

2.2.3.4.2 Funcionalidade de detecção de ameaças desconhecidas que estão em memória.

2.2.3.4.3 Capacidade de detecção, e bloqueio pró-ativo de keyloggers, Trojans e Worms entre outros malwares não conhecidos através da análise de comportamento de processos em memória (heurística).

2.2.3.4.4 Capacidade de analisar o comportamento de novos processos ao serem executados, em complemento à varredura agendada.

2.2.3.5 Funcionalidade de proteção contra ransomwares:

2.2.3.5.1 Funcionalidades especificas para prevenção contra a ação de ransomwares, tais como a capacidade de impedir a criptografia quando feita por aplicativos desconhecidos ou a capacidade de fazer backup de arquivos antes de serem criptografados para posteriormente permitir sua restauração.

2.2.3.5.2 Para estações de trabalho, dispor de capacidade de proteção contra ransomware não baseada exclusivamente na detecção por assinaturas.

2.2.3.5.3 Para estações de trabalho, dispor de capacidade de remediação da ação de criptografia maliciosa dos ransomwares.

2.2.3.5.4 Para servidores, dispor de capacidade de prevenção contra a ação de criptografia maliciosa executada por ransomwares, possibilitando ainda o bloqueio dos computadores de onde partirem tal ação.

2.2.3.5.5 A solução deverá prevenir ameaças e interromper que eles sejam executados em dispositivos da rede, detectando e limpando os malwares, além da realização de uma análise detalhada das alterações realizadas.

2.2.3.5.6 Deve possuir uma tecnologia anti-exploit baseada em comportamento, reconhecendo e bloqueando as mais comuns técnicas de malware, protegendo os endpoints de ameaças desconhecidas e vulnerabilidades *zero-day*.

2.2.3.5.7 Deve ser realizada a *detecção e o bloqueio de, pelo menos, as seguintes* técnicas de *exploit*:

a) DEP (*Data Execution Prevention*);
b) *Address Space Layout Randomization* (ASLR);
c) *Bottom Up ASLR*;
d) *Null Page*;
e) *Anti-HeapSpraying*;
f) *Dynamic Heap Spray*;
g) *Import Address Table Filtering (IAF)*;
h) *VTable Hijacking*;
i) *Stack Pivot and Stack Exec*;
j) *SEHOP*;
k) *Stack*-based ROP (*Return-Oriented Programming*);
l) *Control-Flow Integrity (CFI)*;
m) *Syscall*;
n) *WOW64*;
o) *Load Library*;
p) *Shellcode*;
q) *VBScript God Mode*;
r) *Application Lockdown*;
s) *Process Protection*;

t) *Network Lockdown*.

2.2.3.5.8 A solução deverá trabalhar silenciosamente na máquina do usuário e deverá detectar a criptografia maliciosa de dados (ransomware), realizando a sua interrupção. No caso de arquivos serem criptografados a solução deverá realizar o retorno destes arquivos ao seu estado normal. Deste modo a solução deve ser capaz de fazer a limpeza e remoção completa do ransomware na máquina do usuário.

2.2.3.5.9 Deve fornecer também uma análise detalhada das modificações realizadas pelo ransomware, realizando a correlação dos dados em tempo real, indicando todas as modificações feitas em registros, chaves, arquivos alvos, conexões de redes e demais componentes contaminados.

2.2.3.5.10 A console de monitoração e configuração deverão ser feitas através de uma central única, baseada em web, que deverá conter todas a ferramentas para a monitoração e controle da proteção dos dispositivos para a solução de anti-exploit e anti-ransomware.

2.2.3.5.11 A console deverá apresentar *Dashboard* com o resumo dos status de proteção dos computadores e usuários, bem como indicar os alertas de eventos de criticidades alta, média e informacional, bem como todas as identificações para o mapeamento instantâneo dos efeitos causados pelo ransomware nos endpoints.

2.2.3.6 Funcionalidade de controle de aplicações e dispositivos:

2.2.3.6.1 Possuir controle de aplicativos para monitorar e impedir que os usuários executem ou instalem aplicações que podem afetar a produtividade ou o desempenho da rede.

2.2.3.6.2 Atualizar automaticamente a lista de aplicativos que podem ser controlados, permitindo que aplicativos específicos ou categorias específicas de aplicações possam ser liberadas ou bloqueadas.

2.2.3.6.3 Verificar a identidade de um aplicativo de maneira genérica para detectar todas as suas versões. Permitir a solicitação de adição de novas aplicações nas listas de controle de aplicativos através de interface web.

2.2.3.6.4 Oferecer proteção para chaves de registro e controle de processos.

2.2.3.6.5 Proibir através de política a inicialização de um processo ou aplicativo baseado em nome ou no hash do arquivo.

2.2.3.6.6 Detectar aplicativo controlado quando os usuários o acessarem, com as opções de permitir e alertar ou bloquear e alertar.

2.2.3.6.7 Deve possuir a opção de customizar uma mensagem a ser mostrada ao usuário em caso de bloqueio de execução do aplicativo.

2.2.3.6.8 Gerenciar o uso de dispositivos de armazenamento USB (ex: pen-drives e HDs USB). Permitir, através de regras, o bloqueio ou liberação da leitura/escrita/execução do conteúdo desses dispositivos.

2.2.3.6.9 Controlar o uso de outros dispositivos periféricos, como comunicação infravermelha e modem externo.

2.2.3.6.10 As funcionalidades do Controle de Aplicações e Dispositivos deverão ser nativas do produto ou incorporadas automaticamente por meio de plug-ins sem utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo mesmo fabricante.

2.2.3.6.11 Capacidade de bloquear execução de aplicativo que está em armazenamento externo;

2.2.3.6.12 A gestão desses dispositivos deverá feita diretamente console de gerenciamento com a possibilidade de definir políticas diferentes por grupos de endpoints.

2.2.3.6.13 Permitir a autorização de um dispositivo com no mínimo as seguintes opções:

a) Permitir que todos os dispositivos do mesmo modelo;
b) Permitir que um único dispositivo com base em seu número de identificação único;
c) Permitir o acesso total; e
d) Permitir acesso somente leitura.

2.2.3.6.14 Permitir ainda o bloqueio de pontes entre duas redes, por exemplo, um laptop conectado ao mesmo tempo na LAN e se tornar um hotspot Wi-Fi, ou através de um modem.

2.2.4 Características gerais da solução de proteção para servidores:

2.2.4.1 Características básicas do agente de proteção contra malwares:

2.2.4.1.1 A solução deverá ser capaz de proteger servidores contra malwares, arquivos e tráfego de rede malicioso, controle de periféricos, controle de acesso à web, controle de aplicativos em um único agente instalado nos servidores.

2.2.4.1.2 Deve realizar a pré-execução do agente para verificar o comportamento malicioso e detectar malwares desconhecidos.

2.2.4.1.3 O agente host deve buscar algum sinal de malwares ativos e detectar malwares desconhecidos.

2.2.4.1.4 O agente deve realizar a atualização várias vezes por dia para manter a detecção atualizada contra as ameaças mais recentes.

2.2.4.1.5 A solução deve manter conexão direta com banco de dados de ameaças do fabricante para uso da rede de inteligência.

2.2.4.1.6 Deve realizar a verificação de todos os arquivos acessados em tempo real, mesmo durante o processo de boot.

2.2.4.1.7 Deve realizar a verificação de todos os arquivos no disco rígido em intervalos programados.

2.2.4.1.8 Deve realizar a limpeza do sistema automaticamente, removendo itens maliciosos detectados e aplicações potencialmente indesejáveis (PUA).

2.2.4.1.9 Deve proteger os navegadores Internet Explorer, Firefox, Chrome, Opera e Safari, bloqueando o acesso a sites infectados conhecidos e pela verificação dos dados baixados antes de serem executados.

2.2.4.1.10 Deve permitir a autorização de detecções maliciosas e excluir da varredura diretórios e arquivos específicos.

2.2.4.1.11 É requerida a proteção integrada, ou seja, em um único agente, contra ameaças de segurança, incluindo vírus, spyware, trojans, worms, adware e aplicativos potencialmente indesejados (PUAs).

2.2.4.1.12 O cliente para instalação em estações de trabalho deverá ser compatível com os sistemas operacionais abaixo:

a) Windows Server 2016;
b) Windows Server 2012 R2 (64 bit);
c) Windows Server 2012 (64 bit);
d) Windows Server 2008 R2 (64 bit);
e) Windows Server 2008 (32 or 64 bit);
f) Amazon Linux;
g) CentOS;
h) Novell Open Enterprise Server 2015 SP1;
i) Oracle Linux 6.2/7;
j) Red Hat Enterprise Linux 6/7;
k) SUSE 11/12; e
l) Ubuntu Server 14.04/16.04.

2.2.4.1.13 Deve suportar o uso de servidores usados para atualização em cache para diminuir a largura de banda usada nas atualizações.

2.2.4.1.14 Deve possuir integração com as nuvens da Microsoft Azure e Amazon Web Services para identificar as informações dos servidores instanciados nas nuvens.

2.2.4.1.15 Possuir a funcionalidade de proteção contra a alteração das configurações do agente, impedindo aos usuários, incluindo o administrador local, reconfigurar, desativar ou desinstalar componentes da solução de proteção.

2.2.4.1.16 Permitir a utilização de senha de proteção para possibilitar a reconfiguração local no cliente ou desinstalação dos componentes de proteção.

2.2.4.2 Funcionalidade de Firewall e Detecção e Proteção de Intrusão (IDS\IPS):

2.2.4.2.1 Possuir proteção contra exploração de buffer overflow.

2.2.4.2.2 Deverá possui atualização periódica de novas assinaturas de ataque.

2.2.4.2.3 Capacidade de reconhecer e bloquear automaticamente as aplicações em clientes baseando-se na impressão digital (hash) do arquivo ou dinamicamente através do nome da aplicação.

2.2.4.2.4 Capacidade de bloqueio de ataques baseado na exploração de vulnerabilidade conhecidas.

2.2.4.2.5 Possuir um sistema de prevenção de intrusão no host (HIPS), que monitore o código e blocos de código que podem se comportar de forma maliciosa antes de serem executados.

2.2.4.2.6 Ser capaz de aplicar uma análise adicional, inspecionando finamente o comportamento de códigos durante a execução, para detectar comportamento suspeito de aplicações, tais como buffer overflow.

2.2.4.2.7 Deve possuir técnicas de proteção, que inclui:

a) Análise dinâmica de código - técnica para detectar malware criptografado mais complexo;
b) Algoritmo correspondente padrão - onde os dados de entrada são comparados com um conjunto de sequências conhecidas de código já identificado como um vírus;
c) Emulação - uma técnica para a detecção de vírus polimórficos, ou seja, vírus que se escondem criptografando-se de maneira diferente cada vez que se espalham;
d) Tecnologia de redução de ameaças - detecção de prováveis ameaças por uma variedade de critérios, como extensões duplas (por exemplo. jpg.txt) ou a extensão não coincida com o tipo de arquivo verdadeiro (por exemplo, um arquivo executável ou arquivo .exe com a extensão .txt); e

e) Verificação de ameaças web avançadas**:** bloqueia ameaças verificando o conteúdo em tempo real e remontando com emulação de JavaScript e análise comportamental para identificar e parar o código malicioso de malware avançados.

2.2.4.3 Funcionalidade de Antivírus e AntiSpyware:

2.2.4.3.1 Proteção em tempo real contra vírus, trojans, worms, rootkits, botnets, spyware, adwares e outros tipos de códigos maliciosos.

2.2.4.3.2 Proteção anti-malware deverá ser nativa da solução ou incorporada automaticamente por meio de plug-ins sem a utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo mesmo fabricante.

2.2.4.3.3 As configurações do anti-spyware deverão ser realizadas através da mesma console do antivírus.

2.2.4.3.4 Permitir a configuração de ações diferenciadas para programas potencialmente indesejados ou malware, com possibilidade de inclusão de arquivos em listas de exclusão (whitelists) para que não sejam verificados pelo produto.

2.2.4.3.5 Permitir a varredura das ameaças da maneira manual, agendada e em tempo real nos servidores.

2.2.4.3.6 Capacidade de detecção e reparo em tempo real de vírus de macro conhecidos e novos através do antivírus.

2.2.4.3.7 Capacidade de detectar arquivos através da reputação dos mesmos.

2.2.4.3.8 Capacidade de remoção automática total dos danos causados por spyware, adwares e worms, como limpeza do registro e pontos de carregamento, com opção de finalizar o processo e terminar o serviço da ameaça no momento de detecção.

2.2.4.3.9 A remoção automática dos danos causados deverá ser nativa do próprio antivírus; ou adicionada por plugin, desde que desenvolvido ou distribuído pelo mesmo fabricante.

2.2.4.3.10 Capacidade de bloquear origem de infecção através de compartilhamento de rede com opção de bloqueio da comunicação via rede.

2.2.4.3.11 Deverá detectar tráfego de rede para comandar e controlar os servidores.

2.2.4.3.12 Proteger arquivos de documento contra-ataque do tipo ransomwares.

2.2.4.3.13 Proteger que o ataque de ransomware seja executado remotamente.

2.2.4.3.14 Permitir o envio de amostras de malwares para a nuvem de inteligência do fabricante.

2.2.4.3.15 Permitir o bloqueio da verificação de vírus em recursos mapeados da rede.

2.2.4.3.16 Antivírus de web (verificação de sites e downloads contra vírus).

2.2.4.3.17 Controle de acesso a sites por categoria.

2.2.4.3.18 Proteger a navegação na web, mesmo aos usuários fora da rede, para todos os principais navegadores (Internet Explore, Firefox, Safari, Opera e Chrome), fornecendo controle da Internet independentemente do browser utilizado sem utilizar um plugin, onde não é possível ser ignorada pelos usuários, protegendo os usuários de websites infectados e categorias específicas de websites.

2.2.4.3.19 O Controle da Web deve controlar o acesso a sites impróprios, com no mínimo 14 categorias de sites inadequados. Deve ainda permitir a criação de lista branca de sites sempre permitidos e lista negra de sites que devem ser bloqueados sempre.

2.2.4.3.20 Todas as atividades de navegação na Internet bloqueadas deverão ser enviadas para a console de gerenciamento, informando detalhes do evento e a razão para o bloqueio.

2.2.4.3.21 Capacidade de verificar somente arquivos novos e alterados.

2.2.4.3.22 Capacidade de habilitar mensagens de desktop para a Proteção contra Ameaças.

2.2.4.3.23 Capacidade de adicionar exclusão de varredura para arquivos, pastas, processos, sites, aplicativos e tipos de explorações detectadas.

2.2.4.4 Funcionalidade de proteção contra ransomwares:

2.2.4.4.1 Funcionalidades especificas para prevenção contra a ação de ransomwares, tais como a capacidade de impedir a criptografia quando feita por aplicativos desconhecidos ou a capacidade de fazer backup de arquivos antes de serem criptografados para posteriormente permitir sua restauração.

2.2.4.4.2 Deve dispor de capacidade de proteção contra ransomware não baseada exclusivamente na detecção por assinaturas.

2.2.4.4.3 Deve dispor de capacidade de remediação da ação de criptografia maliciosa dos ransomwares.

2.2.4.4.4 Deve dispor de capacidade de prevenção contra a ação de criptografia maliciosa executada por ransomwares, possibilitando ainda o bloqueio dos computadores de onde partirem tal ação.

2.2.4.5 Funcionalidade de Controle de aplicações e dispositivos:

2.2.4.5.1 Possuir controle de aplicativos para monitorar e impedir que os usuários executem ou instalem aplicações que podem afetar a produtividade ou o desempenho da rede.

2.2.4.5.2 Deve ser capaz de atualizar automaticamente a lista de aplicativos que podem ser controlados, permitindo que aplicativos específicos ou categorias específicas de aplicações possam ser liberados ou bloqueados.

2.2.4.5.3 Verificar a identidade de um aplicativo de maneira genérica para detectar todas as suas versões. Permitir a solicitação de adição de novas aplicações nas listas de controle de aplicativos através de interface web.

2.2.4.5.4 Oferecer proteção para chaves de registro e controle de processos.

2.2.4.5.5 Proibir através de política a inicialização de um processo ou aplicativo baseado em nome ou no hash do arquivo.

2.2.4.5.6 Detectar aplicativo controlado quando os usuários o acessarem, com as opções de permitir e alertar ou bloquear e alertar.

2.2.4.5.7 Deve possuir a opção de customizar uma mensagem a ser mostrada ao usuário em caso de bloqueio de execução do aplicativo.

2.2.4.5.8 Gerenciar o uso de dispositivos de armazenamento USB (ex: pen-drives e HDs USB). Permitir, através de regras, o bloqueio ou liberação da leitura/escrita/execução do conteúdo desses dispositivos.

2.2.4.5.9 Controlar o uso de outros dispositivos periféricos, como comunicação infravermelha e modem externo.

2.2.4.5.10 As funcionalidades do Controle de Aplicações e Dispositivos deverão ser nativas do produto ou incorporadas automaticamente por meio de plug-ins sem utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante.

2.2.4.5.11 Capacidade de bloquear execução de aplicativo que está em armazenamento externo.

2.2.4.5.12 A gestão desses dispositivos deverá feita diretamente console de gerenciamento com a possibilidade de definir políticas diferentes por grupos de endpoints.

2.2.4.5.13 Permitir a autorização de um dispositivo com no mínimo as seguintes opções:

a) Permitir que todos os dispositivos do mesmo modelo;
b) Permitir que um único dispositivo com base em seu número de identificação único;
c) Permitir o acesso total;
d) Permitir acesso somente leitura; e
e) Permitir ainda o bloqueio de pontes entre duas redes, por exemplo, um laptop conectado ao mesmo tempo na LAN e se tornar um hotspot Wi-Fi, ou através de um modem.

2.2.4.6 Funcionalidade de Proteção e Prevenção a Perda de Dados:

2.2.4.6.1 Possuir proteção a vazamento ou perda de dados sensíveis, considerando o seu conteúdo ou o seu tipo real, além da possibilidade de avaliar a extensão do arquivo e múltiplos destinos como colocado abaixo.

2.2.4.6.2 Permitir a identificação de informações confidenciais, como números de passaportes ou outras informações pessoais identificáveis e/ou informações confidenciais mesmo que os documentos não tenham sido corretamente classificados, utilizando CCLs (Lista de Controle de Conteúdo).

2.2.4.6.3 Possibilitar o bloqueio, somente registrar o evento na Console de administração, ou perguntar ao usuário se ele ou ela realmente quer transferir o arquivo identificado como sensível.

2.2.4.6.4 Deve possuir listas de CCLs pré-configurados com no mínimo as seguintes identificações:

a) Números de cartões de crédito;
b) Números de contas bancárias;
c) Números de Passaportes;
d) Endereços;
e) Números de telefone;
f) Códigos postais definidas por países como Brasil, França, Inglaterra, Alemanha, EUA, etc; e
g) Lista de e-mails.

2.2.4.6.5 Suportar adicionar regras próprias de conteúdo com um assistente fornecido para essa finalidade.

2.2.4.6.6 Permitir criar regras de prevenção de perda de dados por tipo verdadeiro de arquivo.

2.2.4.6.7 Possuir a capacidade de autorizar, bloquear e confirmar a movimentação de dados sensíveis e em todos os casos, gravar a operação realizada com as principais informações da operação.

2.2.4.6.8 Permitir o controle de dados para no mínimo os seguintes meios:

a) Anexado no cliente de e-mail (ao menos Outlook e Outlook Express);
b) Anexado no navegador (ao menos Internet Explorer, Safari, Firefox e Chrome);
c) Anexado no cliente de mensagens instantâneas (ao menos Skype); e
d) Anexado a dispositivos de armazenamento (ao menos USB, CD/DVD).

2.3 Item 03 - Treinamento para solução de firewall e endpoint (antivírus).

2.3.1 Transferência de tecnologia (12 horas) das soluções contratadas (firewall e endpoint), para 04 (quatro) funcionários e fornecimento de certificado.

CLÁUSULA TERCEIRA – DO QUANTITATIVO DOS SERVIÇOS

3.1 Os serviços relacionados no quadro a seguir, serão prestados no seguinte endereço: Setor Comercial Norte Quadra 02, Bloco A, nº 190, 10º andar, sala 1002 – Edifício Corporate Financial Center, CEP: 70712-900 – Brasília – DF.

Item	Descrição	Qtd.
01	Solução de firewall, como serviço, e suporte técnico especializado	12
02	Solução de endpoint (antivírus), como serviço, e suporte técnico especializado.	01
03	Treinamento para solução de firewall e endpoint (antivírus).	01

3.2 Para o item 01 está prevista a quantidade de 02 (duas) parcelas para o serviço, haja visto que item será pago semestralmente.

CLÁUSULA QUARTA – DA IMPLANTAÇÃO DA SOLUÇÃO DE SEGURANÇA

4.1 A **CONTRATADA** deverá implantar os serviços no prazo máximo de 15 (quinze) dias corridos para os itens 01 e 02, contados da data de emissão da Ordem de Serviço - Anexo I.

4.4.1 Dada a complexidade dos serviços, o prazo poderá ser prorrogado, a pedido da **CONTRATADA**, por igual período.

4.5 O item 03 será fornecido após a implantação dos itens 01 e 02.

4.6 Os recebimentos dos serviços especificados no Termo de Referência, e neste Contrato ocorrerão por meio de empregado designado para este fim, que acompanhará e fiscalizará as entregas, certificando-se das Notas Fiscais e tomando as providências cabíveis para correção, quando for o caso, ou emissão do Termo de

Recebimento Provisório – Anexo II.

4.7 O Fiscal do Contrato terá um prazo de 05 (cinco) dias úteis, a partir do recebimento provisório para realizar as verificações de conformidade do equipamento e, uma vez aprovadas, atestar a Nota Fiscal apresentada, emitindo o Termo de Recebimento Definitivo – Anexo III.

4.8 A **CONTRATADA** será responsável por toda configuração e implantação da nova solução de segurança no ambiente de ABGF e em caso de encerramento do Contrato, será responsável por reconfigurar a atual solução de segurança (Aker) usada pela ABGF.

CLÁUSULA QUINTA – DO ACORDO DE NÍVEIS DE SERVIÇOS

5.1 Durante a vigência do Contrato, o atendimento deve ser realizado por telefone, e-mail, remoto ou on-site (ilimitado).

5.2 A CONTRATADA deverá possuir atendimento 08 horas por dia, 05 dias por semana (8x5), durante toda vigência do Contrato e atender aos seguintes níveis de serviços:

5.2.1 **Criticidade Baixa –** Tempo de resposta de até 6 horas e até 48 horas para tempo de solução. Os casos definidos com criticidade baixa são: Falha na console de acesso Web do software de integração, alterações no funcionamento da ferramenta mediante solicitação da contratada, falhas no envio de emails por parte do software de integração.

5.2.2 **Criticidade Média -** Tempo de resposta de 4 horas e até 8 horas para tempo de solução. Os casos definidos com criticidade média são: Bloqueios inesperados realizados pelo software de integração, falha na identificação do status dos endpoints, falha no job de backup.

5.2.3 **Criticidade Alta –** Tempo de resposta de até 2 horas e até 6 horas para tempo de solução. Os casos definidos com criticidade alta são: Sistema operacional da máquina virtual do software de integração inoperante, com problemas durante o boot da VM, qualquer falha no software que comprometa o funcionamento da solução como um todo.

CLÁUSULA SEXTA – DAS OBRIGAÇÕES DA CONTRATANTE

6.1. Comunicar à **CONTRATADA** qualquer irregularidade observada na prestação dos serviços.

6.2. Efetuar o pagamento dos serviços, após apresentação da Nota Fiscal e o respectivo ateste, realizado pelo(s) representante(s) da **CONTRATANTE.**

6.3. Suspender o pagamento da Nota Fiscal se houver obrigação contratual pendente por parte da **CONTRATADA**, no tocante à inexecução ou a não prestação a contento do serviço, até a completa regularização.

6.4. Efetuar as retenções tributárias devidas sobre o valor da Nota Fiscal/Fatura fornecida pela **CONTRATADA.**

CLÁUSULA SÉTIMA – DAS OBRIGAÇÕES DA CONTRATADA

7.1 Prestar os serviços contratados nos prazos e condições pactuados.

7.2 Manter, durante a execução deste Contrato, todas as condições que o habilitaram e o qualificaram para a prestação do serviço.

7.3 Respeitar as normas e procedimentos de controle e acesso às dependências da **CONTRATANTE.**

7.4 Obedecer rigorosamente a todas as normas e procedimentos de segurança implementados no ambiente de TI do **CONTRATANTE.**

7.5 Zelar e responder pela privacidade e sigilo (vide Anexo IV) das informações, de modo a assegurar que as informações de propriedade da **CONTRATANTE** não sejam divulgadas ou distribuídas pelos empregados ou agentes sob sua responsabilidade.

7.6 Responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com os artigos 12, 13 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990).

7.7 Atender prontamente a quaisquer exigências da **CONTRATANTE**, inerentes ao objeto proposto.

7.8 Responsabilizar-se pelas despesas dos tributos, encargos trabalhistas, previdenciários, fiscais, comerciais, taxas, fretes, seguros, deslocamento de pessoal, prestação de garantia e quaisquer outras que incidam ou venham a incidir na execução deste Contrato.

7.9 A **CONTRATADA** deverá assinar a **Declaração de Vedação ao Nepotismo (Anexo V),** declarando que seus sócio(s), dirigente(s) ou administrador(es) não é(são) empregado(s) ou dirigente(a) não possui(em) vínculo familiar (cônjuge, companheiro ou parente em linha reta ou colateral, por consanguinidade ou afinidade, até o terceiro grau, nos termos dos artigos 1.591 a 1.595 da Lei nº 10.406/2002 – Código Civil).

CLAÚSULA OITAVA – DA FISCALIZAÇÃO DOS SERVIÇOS

8.1 O acompanhamento e a fiscalização da execução deste Contrato consistem na verificação da conformidade do recebimento dos serviços e licenças, bem como da alocação dos recursos necessários, de forma a assegurar o perfeito cumprimento do ajuste, devendo ser exercidos por um ou mais representantes da **CONTRATANTE.**

8.2 A verificação da adequação da prestação do serviço deverá ser realizada com base nos critérios previstos no Termo de Referência e neste Contrato.

8.3 O Fiscal do Contrato ou seu substituto exigirá o cumprimento dos serviços prestados na forma de execução, de acordo com o estabelecido neste Contrato.

8.4 O Fiscal do Contrato ou seu substituto deverá promover o registro das ocorrências verificadas, adotando as providências necessárias ao fiel cumprimento das cláusulas contratuais.

8.5 O Fiscal do Contrato ou seu substituto, ao verificar qualquer inconformidade deverá comunicar à Gerência Executiva Administrativa e Financeira - GEAFI, em tempo hábil, para que sejam adotadas as medidas convenientes e necessárias a cada caso, ensejando notificação à **CONTRATADA**, para a adequação contratual.

8.6 O descumprimento total ou parcial das demais obrigações e responsabilidades assumidas pela **CONTRATADA** ensejará a aplicação de sanções administrativas, previstas no Termo de Referência, neste Contrato, e na legislação vigente, podendo culminar em rescisão contratual.

8.7 A fiscalização de que trata este item não exclui nem reduz a responsabilidade da **CONTRATADA**, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas ou vícios redibitórios e, na ocorrência desta, não implica em corresponsabilidade da **CONTRATANTE** ou de seus agentes e prepostos.

CLÁUSULA NONA – DAS SANÇÕES ADMINISTRATIVAS

9.1 As sanções serão aplicadas em decorrência de atraso injustificado na execução do Contrato ou pela inexecução total ou parcial deste Contrato, garantida a prévia defesa, a **CONTRATANTE** poderá aplicar ao contratado as seguintes sanções:

a) advertência;
b) multa, na forma prevista no instrumento convocatório ou no contrato;
c) suspensão temporária de participação em licitação e impedimento de contratar com a **CONTRATANTE**, por prazo não superior a 2 (dois) anos.

9.2 A advertência e a suspensão poderão ser aplicadas juntamente com a

multa, devendo a defesa prévia do interessado, no respectivo processo, ser apresentada no prazo de 10 (dez) dias úteis.

9.3 As multas poderão ser de natureza moratória ou compensatória, e poderão ser aplicadas cumulativamente, desde que seja aberto processo administrativo para este fim.

9.4 Na aplicação das multas deverá ser observado o princípio da proporcionalidade estritamente necessário ao atendimento do interesse da **CONTRATANTE**, garantido o direito à ampla defesa e ao contraditório:

a) de 0,2% (dois décimos por cento) a 0,5% (cinco décimos por cento) ao dia sobre o valor da parcela inadimplida, por dia de atraso, no caso de multa moratória e, para multa compensatória, até o limite de 10% (dez por cento) sobre o valor inadimplido do Contrato.

9.5 Caso a multa seja superior ao valor da garantia prestada, além da perda desta, responderá a **CONTRATADA** pela sua diferença, a qual será descontada dos pagamentos eventualmente devidos pela à **CONTRATANTE** ou, ainda, quando for o caso, cobrada judicialmente.

9.6 Em consonância ao disposto no art. 84, da Lei nº 13.303/2016, as sanções previstas na alínea "c", do subitem 9.1 poderão ser aplicadas às empresas ou aos profissionais que:

a) tenham sofrido condenação definitiva por praticarem, por meios dolosos, fraude fiscal no recolhimento de quaisquer tributos;
b) tenham praticado atos ilícitos visando a frustrar os objetivos da contratação;
c) demonstrem não possuir idoneidade para contratar com a **CONTRATANTE** em virtude de atos ilícitos praticados.

9.7 Se a falha detectada ocorrer por comprovado impedimento ou por motivo de reconhecida força maior, devidamente justificado e aceito pela CONTRATANTE a empresa **CONTRATADA** ficará isenta das penalidades mencionadas no item anterior.

9.8 Em qualquer hipótese de aplicação de sanções serão assegurados à **CONTRATADA** o contraditório e a ampla defesa, no prazo estabelecido no item 9.2.

9.9 As sanções serão obrigatoriamente registradas no SICAF, e no caso de impedimento de licitar, a **CONTRATADA** será descredenciada pelo prazo de até 05 (cinco) anos, sem prejuízo das demais cominações legais.

CLÁUSULA DÉCIMA – DO VALOR

10.1 O valor total deste Contrato é de **R$ 32.001,89 (trinta e dois mil, um real e oitenta e nove centavos**, divididos da seguinte forma:

Item	Descrição	2021	2022
01	Solução do serviço de firewall com WAF e suporte técnico	R$ 6.600,00	R$ 6.600,00
02	Solução de antivírus por 12 (doze) meses com suporte técnico	R$ 17.801,89	
03	Treinamento para solução de firewall e antivírus	R$ 1.000,00	
		R$ 25.401,89	**R$ 6.600,00**

CLÁUSULA DÉCIMA PRIMEIRA - DA DOTAÇÃO ORÇAMENTÁRIA

11.1 As despesas decorrentes desta contratação correrão à conta do Programa de Dispêndios Globais – PDG 2021 e 2022, sob as Rubricas Orçamentárias: 2.205.010.000 - Tecnologia da Informação - Serviços de Terceiros.

CLÁUSULA DÉCIMA SEGUNDA - DA VIGÊNCIA

12.1 O prazo de vigência do Contrato será de 12 (doze) meses, contados a partir da data de sua assinatura, podendo ser prorrogado, por períodos sucessivos, observado o limite de 05 (cinco) anos, nos termos do Art. 71 da Lei nº 13.303/2016.

CLÁUSULA DÉCIMA TERCEIRA – DO REAJUSTE

13.1 O reajustamento tem como finalidade a manutenção da justa remuneração decorrente da suscetibilidade inflacionária dos Contratos.

13.2 Nos Contratos firmados pela **CONTRATANTE**, o reajuste em sentido estrito será concedido automaticamente e prescinde de prévio pedido administrativo pela **CONTRATADA**.

13.3 O valor do contrato será reajustado pelo Índice de Custos de Tecnologia da Informação - ICTI, mantido pela Fundação Instituto de Pesquisa Econômica Aplicada – IPEA, conforme orientação da IN 01/2019, Art. 24 – SGD/ME, utilizando-se o percentual acumulado dos últimos 12 (doze) meses, observando a última publicação do ICTI que antecede a data do reajuste.

13.4 Caso o índice de reajustamento estabelecido neste Contrato seja extinto ou de qualquer outra forma não possa mais ser utilizado, o reajustamento utilizará como expressão para cálculo o índice geral de preços mais vantajoso para a **CONTRATANTE**, apresentado por instituição oficial.

13.5 O intervalo de 12 (doze) meses completos necessários para o cálculo do reajuste terá como marco inicial a data da assinatura deste Contrato.

CLÁUSULA DÉCIMA QUARTA – DO PAGAMENTO

14.1 Para o item 01, serão realizados pagamentos semestrais e para os itens 02 e 03 serão realizados pagamento únicos.

14.1.1 Os itens contratados serão pagos após o recebimento definitivo dos serviços.

14.2 O pagamento será efetuado até o 15º dia, após a apresentação da Nota Fiscal/Fatura devidamente atestada pelo Fiscal do contrato, de acordo com as condições e preços ajustados no contrato, conforme determina a Instrução Normativa RFB nº 1.234, de 11.01.2012, publicada no Diário Oficial de 12.01.2012.

CLÁUSULA DÉCIMA QUINTA - DA ALTERAÇÕES CONTRATUAIS

15.1 Este Contrato poderá ser alterado, com as devidas justificativas, nos casos previstos no Artigo 81 da Lei nº 13.303/2016, e na vigente Instrução Normativa nº 05, de 26 de maio de 2017 – Anexo X.

CLÁUSULA DÉCIMA SEXTA – DA RESCISÃO

16.1 Este Contrato poderá ser rescindido por inexecução de quaisquer das obrigações estipuladas neste Contrato, sem prejuízo das sanções estabelecidas.

16.2 As Partes acordam que em razão da inclusão da **CONTRATANTE** no Programa Nacional de Desestatização - PND (Decreto nº 10.007, de 05/09/2019), o **Contrato** poderá ser rescindido a qualquer momento pela **CONTRATANTE**, bastando um simples comunicado para formalizar a rescisão.

16.3 Na hipótese de rescisão unilateral da **CONTRATANTE**, a **CONTRATADA** isenta integralmente a **CONTRATANTE** do pagamento de quaisquer multas ou encargos advindos da extinção antecipada do Contrato.

16.4 Os casos de rescisão contratual devem ser formalmente motivados nos autos do processo, assegurado o contraditório e a ampla defesa.

CLÁUSULA DÉCIMA SÉTIMA – DOS CASOS OMISSOS

17.1 Os casos omissos serão resolvidos com base na Lei 13.303/2016 e nos princípios do direito privado.

CLÁUSULA DÉCIMA OITAVA – DA VINCULAÇÃO

18.1 Este Contrato guarda conformidade com o Termo de Referente, com a Dispensa de Licitação nº 015/2021, vinculando-se, ainda, à Proposta da **CONTRATADA** e demais documentos constantes do Processo nº 016/2021-ABGF que, independente de transcrição, integram este Instrumento.

CLÁUSULA DÉCIMA NONA – DA SUBCONTRATAÇÃO E DA SUB-ROGAÇÃO

19.1 Não será permitida a subcontratação e a sub-rogação do objeto deste Contrato.

CLÁUSULA VIGÉSIMA – FORO

20.1 Fica eleito o foro da Seção Judiciária da Justiça Federal, em Brasília-DF, para dirimir quaisquer dúvidas oriundas do presente Contrato.

20.2 E, para firmeza e validade do que foi pactuado, lavrou-se o presente Contrato Administrativo em 2 (duas) vias de igual teor e forma, para um só efeito, as quais, depois de lidas e achadas conforme, serão assinadas pelos representantes das partes.

Brasília-DF, 28 de outubro de 2021.

Representante legal da **CONTRATANTE**

_____	_____
Helena Mulim Venceslau	**Octávio Luiz Bromatti**
Diretora de Garantias	Presidente

Representante legal da **CONTRATADA**

_____

Assinatura da Contratada

TESTEMUNHAS:

1._____	2._____
Nome	Nome
CPF	CPF

ANEXO I - Ordem de Serviço - OS

Ordem de Serviço nº xxx/2021

IDENTIFICAÇÃO	
Nº do Contrato:	
Objeto:	
Contratada:	

DESCRIÇÃO

PRAZO

OBSERVAÇÕES

Brasília-DF, xx de xxxxxxxxx de 2021.

_____

Nome do Fiscal

Fiscal de Contrato

Portaria nº xxx/2021 - ABGF

ANEXO II - Termo de Recebimento Provisório

Por este instrumento, atestamos que os serviços (ou bens) objetos da contratação, foram recebidos nesta data e serão objeto de avaliação quanto aos aspectos de qualidade, de acordo com os Critérios de Aceitação previamente definidos pela CONTRATANTE.

Ressaltamos que o recebimento definitivo **ocorrerá em até 02 (dois) dias úteis a partir do recebimento provisório**, desde que não ocorram problemas técnicos ou divergências quanto às especificações constantes do Termo de Referência correspondente ao Contrato supracitado.

IDENTIFICAÇÃO	
Nº do Contrato:	
Objeto:	
Contratada:	

DESCRIÇÃO DOS SERVIÇOS

OBSERVAÇÕES
Ordem de Serviço nº xxx/2021.

Brasília-DF, xx de xxxxxxxxx de **2021**.

_____

Nome do Fiscal

Fiscal de Contrato

Portaria nº xxx/**2021**- ABGF

ANEXO III - Termo de Recebimento Definitivo

Por este instrumento, atestamos o recebimento definitivo dos itens, de acordo com as condições e especificações especificadas no Contrato.

IDENTIFICAÇÃO	
Nº do Contrato:	
Objeto:	
Contratada:	

DESCRIÇÃO DOS SERVIÇOS

OBSERVAÇÕES
Ordem de Serviço nº xxx/2021.

Brasília-DF, xx de xxxxxxxxx de 2021.

_____

Nome do Fiscal

Fiscal de Contrato

Portaria nº xxx/2021 - ABGF

De acordo,

Brasília-DF, xx de xxxxxxxxx de 2021.

_____

Nome do Gerente da área demandante

Gerente de xxxxxx

ANEXO IV - Termo de Confidencialidade e Sigilo – Prestadores de Serviço

Pelo presente instrumento, a empresa **MULTIP REDE MULTISERVIÇOS LTDA - EPP**. Inscrita no CNPJ sob o nº 04.721.052/0001-08, sediada no SRTVN, Quadra 70T, Conj. C, nº 214, salas 210 e 212, Ala "A", Asa Norte, Brasília/DF, CEP: 70719-903, doravante denominada **CONTRATADA**, neste ato, representada por seu (ua) _____, _____, _____, _____, portador(a) do Registro Geral nº _____, inscrito(a) no CPF sob o nº _____, perante a Agência Brasileira Gestora de Fundos Garantidores e Garantias – ABGF, na qualidade de prestador de serviços, declara estar ciente e concordar com a **Política de Segurança da Informação** composta por suas Diretrizes Gerais, Normas, Procedimentos e Instruções, que foram apresentadas por ocasião da assinatura do contrato.

Declaramos, também, estar ciente de que todos os acessos realizados à internet, pelos funcionários por nossa empresa alocados na **CONTRATANTE**, bem como o conteúdo das mensagens enviadas através do Correio Eletrônico corporativo são monitoradas automaticamente.

Declaramos, ainda, que todos os funcionários de nossa empresa, alocados na **CONTRATANTE**, estão cientes das responsabilidades descritas nas normas da Política de Segurança da Informação e que, a não observância desses preceitos, implicará na aplicação das sanções previstas no Normativo de Ação Disciplinar.

Brasília, 28 de outubro de 2021.

_____

Assinatura da Contratada

ANEXO V
DECLARAÇÃO - VEDAÇÃO AO NEPOTISMO

A Contratada/Credenciada DECLARA, sob as penas da Lei, que:

1. Seus sócio(s), dirigente(s) ou administrador(es) não é(são) empregado(s) ou dirigente(a) da CONTRATANTE e não possui(em) vínculo familiar (cônjuge, companheiro ou parente em linha reta ou colateral, por consangüinidade ou afinidade, até o terceiro grau, nos termos dos artigos 1.591 a 1.595 da Lei nº 10.406/2002 – Código Civil) com:

- empregado(s) detentor(es) de cargo comissionado que atue(m) em área da **CONTRATANTE** com gerenciamento sobre o contrato ou sobre o serviço objeto do presente contrato/credenciamento;
- empregado(s) detentor(es) de cargo comissionado que atue(m) na área demandante da contratação/licitação/credenciamento;
- empregado(s) detentor(es) de cargo comissionado que atue(m) na área que realiza o credenciamento/licitação/contratação;
- autoridade da **CONTRATANTE** hierarquicamente superior às áreas supramencionadas.

2. Não tem e que não contratará prestador(es) para a execução de serviço objeto deste contrato/credenciamento, com vínculo familiar (cônjuge, companheiro ou parente em linha reta ou colateral, por consangüinidade ou afinidade, até o terceiro grau, nos termos dos artigos 1.591 a 1.595 da Lei nº 10.406/2002 – Código Civil) com empregado(s) **CONTRATANTE** que exerça cargo(m) em comissão ou função de confiança ou com dirigente(a) **CONTRATANTE**:

- em área da CONTRATANTE com gerenciamento sobre o contrato ou sobre o serviço objeto do presente credenciamento/contrato;
- na área demandante do credenciamento/contratação/licitação;
- na área que realiza o credenciamento/licitação/contratação.

Brasília, 28 de outubro de 2021.

_____

Assinatura da Contratada