Ferramenta de Gerenciamento, Controle de Demanda e Implementação Restrições Parametrizadas a Fluxos de Informação

ANEXO I

TERMO DE REFERÊNCIA

1. Objeto

Ferramenta de Gerenciamento, Controle de Demanda e Implementação Restrições Parametrizadas a Fluxos de Informação

2. Justificativa

Projeto com referência a centralização das demandas de sistemas do SESC/DF, com objetivo de otimizar performance gerenciar de forma centralizada as requisições e executar filtragem de segurança necessita ao trafego

3. Relação de Itens

Item	Descrição	UND	Quantitativo
1	Ferramenta de Gerenciamento, Controle de Demanda e Implementação Restrições Parametrizadas a Fluxos de Informação 12 meses	MES	12
2	Instalação, Configuração e Customização de Aplicações Envolvidas	UND	01
3	Suporte Técnico 12 meses	MES	12
4	Operação Assistida	HORA	8064

4. Caraterísticas de Validade Contratual

4.1. Os produtos e serviços ofertados devem ser validos pelo período de 12 meses, assim como contratos de suporte manutenção

4.2. A Renovação do Contrato será executada de forma automática e obrigatória cada 12 meses, pelo período mínimo de 36 meses, e período máximo facultativo de mais 24 meses, em duas renovações anuais, totalizando 60 meses.

5. Especificação Técnica da Ferramenta de Ferramenta de Gerenciamento, Controle de Demanda e Implementação Restrições Parametrizadas a Fluxos de Informação

5.1. O VIRTUAL APPLIANCE deverá ser compatível com a plataforma operacional que será disponibilizada pelo SESC/DF de acordo com o subitem enumerado a seguir:

5.2. Sistema de Virtualização VMWARE 6.7 ou versões superiores, a critério do SESC/DF;

5.3. O SESC/DF disponibilizará os equipamentos (ou ambiente Virtual) que atuara como servidor físico hospedeiro para os VIRTUAL APPLIANCES;

5.4. O VIRTUAL APPLIANCE deverá ser capaz de balancear o tráfego de entrada e saída para a Internet de 1 Gbps (um gigabits por segundo) ou superior, de tráfego IP oriundo de clientes externos e internos em enlaces de comunicação de redes distintas, de diferentes operadoras de telecomunicações, sem a necessidade da utilização do protocolo BGP ou qualquer outro protocolo de roteamento;

5.5. O VIRTUAL APPLIANCE PODERA operar de forma redundante em topologia de alta disponibilidade, ou seja, na eventualidade da falha de um dos VIRTUAL APPLIANCES, outro APPLIANCE deverá automaticamente assumir, de forma transparente, todas as funções executadas pelo APPLIANCE defeituoso, com sincronismo de configurações e sem perda das sessões que estiverem em curso;

5.6. Todos os VIRTUAL APPLIANCES fornecidos deverão estar em linha na data de sua entrega, não sendo aceitos VIRTUAL APPLIANCES que tenham sido descontinuados ou com data de descontinuidade anunciada;

5.7. Todos os softwares integrantes das soluções ofertadas, inclusive firmware e sistema operacional dos VIRTUAL APPLIANCES, deverão ser fornecidos na versão mais nova comercializada na data da abertura das Propostas;

5.8. Deverão ser fornecidos em conjunto com as soluções ofertadas, todos os acessórios, softwares e opcionais necessários para o correto funcionamento do VIRTUAL APPLIANCE;

5.9. Suportar e garantir a instalação em ambiente de alta disponibilidade;

5.10. Assegurar que a solução deverá ser capaz de trabalhar no modo Ativo/Standby, com virtual appliance da mesma marca e modelo;

5.11. Fornecer uma solução que opere no modo Ativo/Ativo, mantendo o status das conexões. Aceita-se como Ativo/Ativo a utilização de dois endereços Virtuais, onde cada endereço fica ativo em um elemento e standby no outro;

5.12. Assegurar que a operação da solução de 2 ou mais appliances virtuais, quando implementada em ambiente redundante suporte sincronismo de sessão entre os dois membros. A falha do virtual appliance principal não deverá causar a interrupção das sessões balanceadas;

5.13. A solução deve possuir escalabilidade, podendo crescer na forma de cluster adicionando novos appliances virtuais ou físicos inclusive de modelos diferentes;

5.14. Possuir suporte a IPv6;

5.15. A solução deve suportar múltiplas tabelas de rotas independentes;

5.16. Possuir capacidade para gerenciar os recursos disponíveis de acordo com as funções habilitadas nos equipamentos SLB, GSLB, Aceleração Web, etc.

5.17. A solução deve possuir múltiplos domínios de roteamento em IPv4 e IPv6;

5.18. Possuir ferramenta online web gratuita na qual seja possível carregar as configurações e receber diagnóstico da solução com informações sobre atualizações, melhores práticas, estado da solução e informações preventivas.

5.19. Possuir suporte à funcionalidade de VXLAN, essencial para integração com o ambiente de virtualização (Software Defined Network).

Gerenciamento

5.20. Implementar uma configuração de endereçamento IP estático ou dinâmico (DHCP/BOOTP) para o gerenciamento;

5.21. Implementar o SNTP (Simple Network Time Protocol) ou NTP (Network Time Protocol);

5.22. Permitir acesso in-band via SSH;

5.23. Manter internamente múltiplos arquivos de configurações do sistema;

5.24. Utilizar SCP ou HTTPS como mecanismo de transferência de arquivos de configuração e Sistema Operacional;

5.25. Possuir auto-complementação de comandos na CLI;

5.26. Possuir ajuda contextual;

5.27. Interface por linha de comando (CLI – Command Line Interface) que possibilite a configuração dos equipamentos;

5.28. Possuir, no mínimo, Três níveis de usuários na GUI – Super-Usuário, Usuário com permissões reduzidas, e usuário Somente Leitura;

5.29. Os usuários de gerência deverão poder ser autenticados em bases remotas. No mínimo RADIUS, LDAP e TACACS+ deverão ser suportados;

5.30. Deverá ser possível receber da base RADIUS, LDAP e TACACS+ o nível de acesso (Grupo ou Permissões);

5.31. Possuir Interface Gráfica via Web;

5.32. A interface Gráfica deverá permitir a atualização do sistema operacional e/ou a instalação de patches ou Hotfixes sem o uso da linha de comando;

5.33. A interface gráfica deverá permitir a configuração de qual partição o equipamento deverá dar o boot;

5.34. Possuir um comando, via CLI, que mostre o tráfego de utilização das interfaces (bps e pps);

5.35. Suportar a rollback de configuração e imagem;

5.36. Possuir e fornecer MIBs compiláveis na plataforma HP Open View Network Node Manager;

5.37. Possuir e fornecer geração de mensagens de syslog para eventos relevantes ao sistema;

5.38. Possuir configuração de múltiplos syslog servers para os quais o equipamento irá enviar as mensagens de syslog;

5.39. Possuir armazenamento de mensagens de syslog em dispositivo interno ao equipamento;

5.40. A interface Gráfica deverá permitir a reinicialização do equipamento;

5.41. Reinicialização do equipamento por comando na CLI;

5.42. Possuir recurso de gerência via SNMP e implementar SNMPv1, SNMPv2c e SNMPV3;

5.43. Possuir traps SNMP;

5.44. Possui suporte a monitoração utilizando RMON através de pelo menos 4 grupos: statistics, history, alarms e events

5.45. Os logs de sistema devem ter a opção de ser armazenados internamente ao sistema ou em servidor externo;

5.46. Implementar Debugging: CLI via console e SSH;

5.47. Deve possuir suporte a Link Layer Discovery Protocol (LLDP);

5.48. Deve ser possível enviar, pelo menos, as seguintes informações via LLDP: Port ID, TTL, Port Description, System Name, System Description, Management Address, Port VLAN ID, Port and Protocol VLAN ID, VLAN Name, Protocol Identity, Link Aggregation, Maximum Frame Size;

5.49. A Solução deve ter a capacidade de permitir a criação de MIBs customizadas;

5.49.1. A Solução deve ter suporte a sFlow;

5.49.2. Distribuição de carga e otimização das aplicações

5.49.3. Suportar todas as aplicações comuns de um Switch Layer 7, como:

5.49.4. Server Load-Balancing;

5.49.5. Firewall Load-Balancing;

5.49.6. Proxy Load-Balancing;

5.50. Suportar Balanceamento apenas em direção ao servidor, onde a resposta do servidor real é enviada diretamente ao cliente;

5.51. A solução deve permitir o encapsulamento, em camada 3, do tráfego entre o balanceador e o servidor para tráfego IPv4 e IPv6, quando o balanceamento é realizado apenas em direção ao servidor, onde a resposta do servidor real é enviada diretamente ao cliente;

5.52. Permitir a clonagem de pools, de forma que a solução envie uma cópia do tráfego para um pool adicional, como por exemplo um pool de IDSs ou Sniffers, para fins de análise de tráfego de rede ou mesmo para identificação de padrões de acesso não permitidos ou indicações de atividade maliciosas ou ataques de rede;

5.53. Possuir recursos para balancear servidores com qualquer hardware, sistema operacional e tipo de aplicação;

5.54. A solução deve possuir recurso de ativação de grupo prioritário, no qual o administrador pode especificar a quantidade mínima de servidores que devem estar disponíveis em cada grupo e a prioridade dos grupos.

5.55. Caso o número de servidores disponíveis fique menor do que o estipulado pelo administrador, a solução deve automaticamente distribuir o tráfego para o próximo grupo com maior prioridade não afetando o serviço.

5.56. Caso o número de servidores disponíveis volte ao valor mínimo estipulado pelo administrador, a solução deve automaticamente retirar o grupo com menor prioridade de balanceamento, voltando ao estado original.

5.57. Possuir capacidade de abrir um número reduzido de conexões TCP com o servidor e inserir os HTTP requests gerado pelos clientes nestas conexões,

reduzindo a necessidade de estabelecimento de conexões nos servidores e aumentando a performance do serviço;

5.58. Suportar os seguintes métodos de balanceamento:

5.58.1. Round Robin;

5.58.2. - Least Connections;

5.58.3. - Weighted Percentage (por peso);

5.58.4. Servidor ou equipamento com resposta mais rápida baseado no tráfego real;

5.58.5. Weighted Percentage dinâmico (baseado no número de conexões)

5.58.6. Dinâmico, baseado em parâmetros de um determinado servidor ou equipamento, coletados via SNMP ou WMI;

5.59. A solução deve permitir aplicar criptografia de cookies para a proteção dos cookies utilizados pela aplicação web;

5.60. Possuir recursos para balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência de sessão dos seguintes tipos:

5.60.1. Por cookie: inserção de um novo cookie na sessão;

5.60.2. - Por cookie: utilização do valor do cookie da aplicação, sem adição de cookie;

5.60.3. - Por endereço IP destino;

5.60.4. - Por endereço IP origem;

5.60.5. - Por sessão SSL;

5.60.6. - Através da análise da URL acessada.;

5.60.7. - Através da análise de qualquer parâmetro no header HTTP;

5.60.8. - Através da análise do MS Terminal Services Session (MSRDP)

5.60.9. - Através da análise do SIP Call ID ou Source IP;

5.60.10. - Através da análise de qualquer informação da porção de dados (camada 7);

5.61. A solução deve utilizar Cache Array Routing Protocol (CARP) no algoritmo de HASH;

5.62. O equipamento oferecido deverá suportar os seguintes métodos de monitoramento dos servidores reais:

5.63. - Layer 3 – ICMP;

5.64. - Conexões TCP e UDP pela respectiva porta no servidor;

5.65. - Devem existir monitores predefinidos para, no mínimo, os seguintes protocolos: ICMP, HTTP, HTTPS, Diameter, FTP, SASP, SMB, RADIUS, MSSQL, NNTP, ORACLE, RPC, LDAP, IMAP, SMTP, POP3, SIP, Real Server, SOAP, SNMP e WMI;

5.66. Possuir recursos para balanceamento de carga de servidores SIP para VoIP (equipamento SIP PROXY);

5.67. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor real;

5.68. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor virtual;

5.69. Possuir recursos para limitar o número de sessões estabelecidas com cada grupo de servidores;

5.70. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor físico:

5.71. Realizar Network Address Translation (NAT);

5.72. Realizar Proteção contra Denial of Service (DoS);

5.73. Realizar Proteção contra Syn flood;

5.74. Realizar Limpeza de cabeçalho HTTP;

5.75. A solução deve permitir o controle da resposta ICMP por servidor virtual;

5.76. Possuir recursos para que a configuração seja baseada em perfis, permitindo uma fácil administração;

5.77. Possuir capacidade de geração e gestão de perfis hierarquizados, permitindo maior facilidade na administração de políticas similares;

5.78. Permitir a criação de Virtual Servers com endereço IPv4 e os servidores reais com endereços IPv6;

5.79. Possuir recursos para executar compressão de conteúdo HTTP, para reduzir a quantidade de informações enviadas ao cliente;

5.80. Deve permitir compressão tipo GZIP e Deflate;

5.81. Definir qual tipo de compressão será habilitada (gzip1 a gzip9, deflate);

5.82. Possuir capacidade para definir compressão especificamente para certos tipos de objetos;

5.83. Possuir recursos para fazer aceleração de SSL, onde os certificados digitais são instalados no equipamento e as requisições HTTP são enviadas aos servidores sem criptografia;

5.84. Deve possuir capacidade de importação dos certificados e chaves criptográficas, para transações seguras entre cliente/servidor, podendo assim operar em modo “man in the middle”, ou seja, descriptografar, otimizar e re-criptografar o tráfego SSL sem comprometer a segurança da conexão SSL estabelecida previamente entre cliente/servidor. Caso haja falha na leitura da conexão SSL, esta deverá, se assim definido, prosseguir em regime de passthrough.

5.85. A solução deve possuir a funcionalidade de espelhamento de conexões SSL.

5.86. A solução deve possuir a capacidade de redirecionar o SSL Offload (troca de chaves) de determinado serviço para outro appliance virtual que tenha mais capacidade para tratamento SSL. Dessa forma deve ser possível otimizar recursos executando tarefas que exigem muito desempenho para serem tratadas em hardware especializado.

5.87. Possuir recursos para configurar o equipamento para recriptografar em SSL a requisição ao enviar para o servidor, permitindo as demais otimizações em ambiente 100% criptografado;

5.88. Todas as funcionalidades de inspeção, proteção e aceleração de tráfego criptografado através de SSL/TLS especificadas neste edital devem estar disponíveis quando a conexão segura for estabelecida usando:

5.89. Autenticação do servidor por parte do cliente, através da verificação da validade do certificado digital fornecido pelo lado servidor durante o processo de estabelecimento do túnel SSL/TLS;

5.90. Autenticação do cliente por parte do servidor, através da solicitação e verificação da validade do certificado digital fornecido pelo cliente durante o processo de estabelecimento do túnel SSL/TLS;

5.91. Ambas as autenticações acima mencionadas ocorrendo de forma simultânea;

5.92. Ao realizar inspeção, proteção, OffLoad e aceleração de tráfego criptografado através de SSL/TLS, a solução deverá ser capaz de:

5.93. Encaminhar ao servidor real via cabeçalho HTTP ou de forma transparente, todo o certificado digital utilizado pelo lado cliente para se autenticar perante o servidor durante o processo de estabelecimento do túnel SSL/TLS;

5.94. Encaminhar ao servidor real via cabeçalho HTTP campos específicos do certificado digital utilizado pelo cliente para se autenticar perante o servidor durante o processo de estabelecimento do túnel SSL/TLS;

5.95. A solução deve permitir aplicar criptografia de cookies para a proteção dos cookies utilizados pela aplicação web;

5.96. Possuir recursos para fazer aceleração de SSL, onde os certificados digitais são instalados no equipamento e as requisições POP3S, IMAPSe SMTPS são enviadas aos servidores sem criptografia;

5.97. A solução deve possuir diversos recursos relacionados ao uso de criptografia com o objetivo de otimizar e minimizar o impacto na performance das aplicações. Dentre eles deve ser possível configurar parâmetros como:

5.98. SSL session cache Timeout;

5.99. Session Ticket;

5.100. OCSP (Online Certificate Status Protocol) Stapling;

5.101. Dynamic Record Sizing;

5.102. ALPN (Application Layer Protocol Negotiation);

5.103. Perfect Forward Secrecy;

5.104. Suportar a utilização de memória RAM como cache de objetos HTTP, para responder às requisições dos usuários sem utilizar recursos dos servidores;

5.105. Possuir capacidade, no uso do recurso de cache, em definir quais tipos de objeto serão armazenados em cache e quais nunca devem ser cacheados;

5.106. Garantir que o recurso de cache possa ajustar quanta memória será utilizada para armazenar objetos;

5.107. Suporte a otimização do protocolo TCP para ajustes a parâmetros das conexões clientes e servidor;

5.108. A solução deve suportar Internet Content Adaptation Protocol (ICAP);

5.109. Deve ser capaz de realizar DHCP relay;

5.110. Deve possuir relatórios das aplicações, com pelos menos os seguintes gráficos:

5.111. - Tempo de resposta da aplicação;

5.112. - Latência;

5.113. - Conexões para conjunto de servidores, servidores individuais;

5.114. - Por URL;

5.115. A ferramenta de relatórios deve possuir pelo menos os seguintes filtros para a geração dos gráficos:

5.116. Servidores virtuais

5.117. Servidores balanceados

5.118. URLs

5.119. Países de origem, baseados em geolocalização (GEOIP)

5.120. Dispositivos de origem do cliente (user agent)

5.121. Deve possuir framework unificado para configuração da aplicação

5.122. Deve possuir criptografia IPSEC para comunicação entre os balanceadores;

5.123. Quando licenciada, a solução deve ter a capacidade de realizar cache transparente das respostas DNS;

5.124. A Solução deve ter a capacidade de permitir a criação de MIBs customizadas;

5.125. A Solução deve ter suporte a sFlow;

5.126. A solução deve possuir múltiplos domínios de roteamento em IPv4 e IPv6;

5.127. A solução deve permitir que cada domínio de roteamento utilize BGP, OSPF e RIP em IPv4 e IPv6;

5.128. A solução deve suportar Equal Cost Multipath (ECMP);

5.129. A solução deve realizar Bidirectional Forward Detection (BFD);

5.130. A solução deve ter suporte a Stream Control Transmission Protocol (SCTP);

5.131. Deve ter suporte a Transport Layer Security (TLS) Server Name Indication (SNI);

5.132. A solução deve possuir monitor HTTP/HTTPS com autenticação NTLM embutida, que permita verificar se o HTTP/HTTPS está operando assim como a plataforma de autenticação;

5.133. A solução deve ter suporte a TLS 1.2, SHA 2 Cipher e SHA256 hash;

5.134. A solução deve ter suporte a criptografia Perfect Forward Secrecy não apenas para troca de chaves RSA.

5.135. A solução deve ser capaz de colocar em fila as requisições TCP que excedam a capacidade de conexões do grupo de servidores ou de um servidor. O

balanceador não deverá descartar as conexões que excedam o número de conexões do servidor ou do grupo de servidores:

5.136. - Deve ser possível configurar o tamanho máximo da fila;

5.137. - Deve ser possível configurar o tempo máximo de permanência na fila;

5.138. A solução deve realizar Controle de Banda Estático para grupos de aplicações e rede;

5.139. A solução deve realizar Controle de Banda Dinâmico por aplicação e usuário;

5.140. A solução deve realizar Controle de Banda baseado em domínio de roteamento;

5.141. Permitir tráfego por parâmetros de QoS (Quality of Service) ou rate-shaping, com pelo menos 2 (duas) filas para priorização de tráfego baseada na camada de aplicação;Através dessa priorização de tráfego e restrição de largura de banda deverá ser possível permitir um melhor nível de serviço para clientes preferenciais em detrimento dos demais clientes.A solução deve permitir a priorização de tráfego de entrada para determinadas aplicações.

5.142. A solução deve permitir a criação de túneis IP por domínio de roteamento utilizando GRE, IPIP, EtherIP, PPP;

5.143. A solução deve permitir a criação de túneis IP transparente utilizando GRE e IPIP;

5.144. Fornece recursos para o uso de servidores (reals) no mesmo Virtual Server;

5.145. Possuir suporte ao protocolo SPDY e HTTP 2.0;

5.146. O equipamento deve possuir suporte ao espelhamento de conexões FTP, Telnet, HTTP, UDP, SSL.

5.147. O equipamento deverá permitir a sincronização das configurações:

5.147.1. De forma automática;

5.147.2. Manualmente, forçando a sincronização apenas no momento desejado;

5.148. Permitir a configuração das interfaces de alta disponibilidade do cluster (heartbeat), com opções para:

5.148.1. Compartilhar a rede de heartbeat com a rede de dados

5.148.2. Utilizar uma rede exclusiva para o heartbeat

5.149. Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar a distribuição dinâmica de tráfego e aumentar a proteção contra-ataques;

5.150. A solução deve possuir linguagem de programação open-source que permita a manipulação do tráfego de entrada e saída, viabilizando assim a alteração de parâmetros no cabeçalho e no corpo das mensagens.

5.151. Essa linguagem de programação deve permitir a importação de pacotes, garantindo assim que a agilidade e flexibilidade no compartilhamento dos scripts.

5.152. Permitir a criação de políticas através de interface gráfica web para manipulação de tráfego através de lógica para pelo menos os seguintes operadores:

5.153. GEOIP, http-basic-auth, http-cookie, http-header, http-host, http-method, http-referer, http-set-cookie, http-status, http-uri e http-version.

5.154. Deve ser possível tomar as seguintes ações através dessas políticas:

5.154.1. Bloqueio de tráfego

5.154.2. Reescrita e manipulação de URL

5.154.3. Registro de tráfego (log)

5.154.4. Adição de informação no cabeçalho HTTP

5.154.5. Redirecionamento do tráfego para um membro específico

5.154.6. Selecionar uma política específica para Aplicação Web

5.154.7. A solução deverá ser capaz de fazer log de todas as sessões, onde os registros deverão conter:

5.154.8. Endereço IP de origem;

5.154.9. Porta TCP ou UDP de origem;

5.154.10. Endereço IP de destino;

5.154.11. Porta TCP ou UDP de destino;

5.154.12. Protocolo de camada 4 (TCP ou UDP);

5.154.13. Data e hora da mensagem;

5.154.14. URL acessada;

5.155. A solução deve possuir políticas de uso de senhas administrativas tais como: nível de complexidade, período de validade e travamento de conta devido a erros múltiplos de login de forma nativa ou no mínimo integrado a uma base Active Directory.

5.156. A solução deve suportar controle de versão da política de configuração de forma a permitir fazer roll back de políticas aplicadas.

5.157. A solução deve ser capaz de analisar a performance de aplicações web.

5.158. A solução deve possuir relatórios das aplicações.

5.159. Deve prover métricas de aplicações como: Transações por Segundo; Tempo de latência do cliente e servidor; Throughput de requisição e resposta; Sessões

5.160. A solução deverá gerar informações para permitir análises históricas e auxiliar nos processos de manutenções preventivas, de troubleshooting, de planejamento de capacidade e de análise da experiência dos usuários finais no acesso das aplicações.

5.161. As informações coletadas deverão permitir a análise dos dados por aplicações, por URL's, por clientes e por servidores, permitindo assim a identificação mais precisa dos eventuais ofensores do tráfego suportado pela solução.

5.162. A solução deverá gerar informações estatísticas de acesso identificando para cada aplicação os métodos de acesso HTTP (GET e Post), o tipo de sistema operacional utilizado pelos clientes, e os browsers utilizados.

5.163. A geração de informações históricas deverá permitir:

5.164. O detalhamento do tempo de resposta total de carregamento de uma URL e ou Página;

5.165. Permitir a correlação de métricas de uso de rede com o comportamento das aplicações.

5.166. Proteção contra-ataques de aplicação:

5.167. A solução deve operar nos modos ativo-ativo e ativo-standby;

5.168. O equipamento oferecido deverá proteger a infraestrutura web de ataques contra a camada de aplicação (Camada 7);

5.169. Deve possuir tecnologia para mitigação de DDoS em camada 7 baseado em analise comportamental, usando o aprendizado.

5.170. Não deve haver a necessidade de intervenção de usuário para configurar thresholds DoS pois esses valores devem ser autoajustáveis e adaptativos de acordo com mudanças.

5.171. A solução deve possuir a capacidade de automaticamente capturar tráfego no formato TCP Dump relativos a ataques DoS L7, Web Scraping e força bruta permitindo uma análise mais aprofundada por parte do administrador.

5.172. A solução deve suportar o uso de firewall camada 3-4 junto com firewall camada 7 no mesmo equipamento/appliance para evitar problemas com o aumento da latência.

5.173. O equipamento oferecido deverá possuir a certificação ICSA para Firewall de Aplicação (Web Application Firewall);

5.174. Permitir a utilização de um modelo positivo de segurança para proteger contra-ataques conhecidos aos protocolos HTTP e HTTPS e às aplicações web acessíveis através destes.

5.175. Possuir política de segurança de aplicações web pré-configurada na solução.

5.176. Permite a criação de políticas diferenciadas por aplicação e por URL, onde cada aplicação e URL poderão ter políticas totalmente diferentes;

5.177. Permitir a criação de políticas diferenciadas por aplicação.

5.178. Permite configurar de forma granular, por aplicação protegida, restrições de métodos HTTP permitidos, tipos ou versões de protocolos, tipos de caracteres e versões utilizadas de cookies;

5.179. A solução deverá se integrar a soluções de análise (Scanner) de vulnerabilidade do site. O resultado desta análise deve ser utilizado para configurar as políticas do equipamento;

5.180. A solução deve permitir a integração com soluções de análise de vulnerabilidades (Scanner) de terceiros como por exemplo: Trustwave App Scanner (Cenzic), White Hat Sentinel, IBM AppScan, Qualys, Quotium Seeker, HP Webinspect.

5.181. A solução deve permitir a inspeção de upload de arquivos para os servidores de aplicação;

5.182. Essa inspeção pode ser feita via integração ICAP. Deve ser possível integrar com diferentes softwares de Antivírus;

5.183. Deve se integrar com o software de Antivírus diversos

5.184. Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar e aumentar a proteção contra-ataques recentes;

5.185. Permitir a integração com Firewall de Database de outros fabricantes.

5.186. A solução deve se integrar com outras soluções de segurança e análise de logs de outros fabricantes.

5.187. O fabricante da solução deve disponiibilizar também a comercialização como serviço na nuvem (WAFaaS), incluindo o serviço de migrar as regras/políticas existentes do Datacenter para a nuvem.

5.188. Deve possuir tecnologia de detecção de anomalias baseado nos IDs dos dispositivos, permitindo a detecção de DoS, ataques de força bruta e ataques de sequestro de sessão. Deve ser possível filtar relatórios por IDs de dispositivos.

5.189. A solução deve permitir incluir em blacklist os endereços IPs que repetidamente falharem a desafios no browser. Portanto o sistema não precisa usar recursos para mitigar trafego enviado por esses endereços Ips. Ao entrar em

Blacklist o sistema automaticamente bloqueia os pacotes enviados por esse endereço por um período.

5.190. A solução deve suportar e fazer a proteção do tráfego em cima de protocolo WebSocket.

5.191. A solução deve possibilitar o uso de múltiplas formas de logging remoto ao mesmo tempo para a mesma aplicação. Portanto dever ser possível por exemplo logar os requests válidos num servidor de SIEM e os requests inválidos em outro servidor de SIEM de outra marca e modelo.

5.192. A solução deverá possuir funcionalidade de proteção positiva e segura contra-ataques, como:

5.192.1. Acesso por Força Bruta;

5.192.2. Ameaças Web AJAX/JSON;

5.192.3. DoS e DDoS camada 7;

5.192.4. Buffer Overflow;

5.192.5. Cross Site Request Forgery (CSRF);

5.192.6. Cross-Site Scripting (XSS);

5.192.7. SQL Injection;

5.192.8. Parameter tampering

5.192.9. Cookie poisoning;

5.192.10. HTTP Request Smuggling;

5.192.11. Manipulação de campos escondidos;

5.192.12. Manipulação de cookies;

5.192.13. Roubo de sessão através de manipulação de cookies;

5.192.14. Sequestro de sessão;

5.192.15. Força bruta no browser

5.192.16. XML bombs/DoS

5.192.17. Checagem de consistência de formulários;

5.192.18. Checagem do cabeçalho do “user-agent” para identificar clientes inválidos.

5.193. A solução deve suportar o uso de páginas de login AJAX/JSON tanto com configuração manual como descoberta automática

5.194. Deverá ser capaz de identificar e bloquear ataques através de:

5.195. Regras de verificação personalizadas – política de segurança configurada.

5.196. Assinaturas, com atualização periódica da base pelo fabricante;

5.197. As assinaturas devem ser atualizadas durante o período do contrato sem que seja necessário nenhum custo a mais por parte da CONTRATANTE na aquisição de novas licenças ou subscrições. Deve fazer parte da solução de WAF ofertada.

5.198. Prevenir contra vazamento de dados sensíveis (mensagens de erro HTTP, códigos das aplicações, entre outros) dos servidores de aplicação, retirando os dados ou mascarando a informação nas páginas enviadas aos usuários.

5.199. Permitir a customização da resposta de bloqueio.

5.200. Permitir a liberação temporária ou definitiva (white-list) de endereços IP bloqueados por terem originados ataques detectados pela solução.

5.201. Deve permitir limitar o número de conexões e requisições por IP de origem para cada endereço IP Virtual.

5.202. Deve permitir adicionar, automaticamente e manualmente, em uma lista de bloqueio, os endereços IP de origem que ultrapassarem o limite estabelecido, por um período determinado através de configuração.

5.203. Deve permitir criar lista de exceção (white list) por endereço IP específico ou faixa de sub-rede.

5.204. A solução deve suportar o modelo de segurança positiva definido pelo OWASP, pelo menos o que consta no TOP 10.

5.205. Permitir o uso do parâmetro HTTP X-Forwarded-For como parte da política de controle.

5.206. Deverá implantar, no mínimo, as seguintes funcionalidades:

5.206.1. Proteção contra Buffer Overflow;

5.206.2. Checagem de URL;

5.206.3. Checagem de métodos HTTP utilizados (GET, POST, HEAD, OPTIONS, PUT, TRACE, DELETE, CONNECT);

5.206.4. Proteção contra envios de comandos SQL escondidos nas requisições enviadas a bases de dados (SQL Injection);

5.206.5. Proteção contra Cross-site Scripting;

5.206.6. Funcionalidade de Cookie Encryption;

5.206.7. Checagem de consistência de formulários;

5.206.8. Checagem do cabeçalho “user-agent” para identificar clientes inválidos.

5.207. Implementar Cloaking – Proteção contra exposição de informações do ambiente e servidores internos como:

5.207.1. Sistema operacional e servidor web com impressão digital;

5.207.2. Esconder qualquer mensagem de erro HTTP dos usuários;

5.207.3. Remover as mensagens de erro às páginas que serão enviadas aos usuários;

5.207.4. Permitir a utilização de uma página HTML informativa e personalizável como HTTP Response aos bloqueios.

5.208. Deve ser possível verificar o endereço de origem do pacote IP no cabeçalho IP e no parâmetro X-forwarded-for (XFF).

5.209. Deve suportar a criação de políticas por geo-localização, permitindo que o tráfego de determinado(s) País/Países seja(m) bloqueado(s).

5.210. Possuir mecanismo de aprendizado automático capaz de identificar todos os conteúdos das aplicações, incluindo URLs, parâmetros URLs, campos de formulários, o que se espera de cada campo (tipo de dado, tamanho de caracteres), cookies, arquivos XML e elementos XML.

5.211. A ferramenta oferecida deverá possuir uma funcionalidade de criação automática de políticas, onde a política de segurança é criada e atualizada automaticamente baseando-se no tráfego real observado à aplicação;

5.212. O perfil aprendido de forma automatizada pode ser ajustado, editado ou bloqueado;

5.213. A ferramenta oferecida deverá possuir proteção baseada em assinaturas para prover proteção contra ataques conhecidos. Deverá ser possível desabilitar algumas assinaturas específicas em determinados parâmetros, como uma exceção a regra geral;

5.214. A atualizações de assinaturas deverão passar por um período configurável de testes, ondes nenhuma requisição que viole a assinatura será bloqueada, apenas informada no relatório. Este processo deve ser automatizado, não sendo necessário criar regras específicas a cada atualização de assinatura;

5.215. A ferramenta oferecida deverá permitir o bloqueio de ataques DoS na camada 7, possuindo também a opção de apenas registrar o ataque, sem tomar nenhuma ação de bloqueio;

5.216. A ferramenta oferecida deverá possuir as seguintes formas de detecção de ataques DoS na camada de aplicação:

5.216.1. Número de requisições por segundo enviados a uma URL específica;

5.216.2. Número de requisições por segundo enviados de um IP específico;

5.216.3. Detecção através de código executado no cliente com o objetivo de detectar interação humana ou comportamento de robôs (bots);

5.216.4. Número máximo de transações por segundo (TPS) de um determinado IP;

5.216.5. Aumento de um determinado percentual do número de transações por segundo (TPS);

5.216.6. Aumento do stress do servidor de aplicação;

5.217. A ferramenta oferecida deverá permitir o bloqueio de ataques de força bruta de usuário/senha em páginas de acesso (login) que protegem áreas restritas. Este bloqueio deve limitar o número máximo de tentativas e o tempo do bloqueio deverá ser configurável;

5.218. A ferramenta oferecida deverá permitir o bloqueio de determinados endereços IPs que ultrapassarem um número máximo de violações por minuto. O período de bloqueio deverá ser configurável e durante este período todas as requisições do cliente serão bloqueadas automaticamente;

5.219. A ferramenta oferecida deverá permitir o bloqueio de robôs (bots) que acessam a aplicação através de detecção automática, não dependendo de cadastros manuais. Robôs conhecidos do mercado, como Google, Yahoo e Microsoft Bing deverão ser liberados por padrão;

5.220. A ferramenta oferecida deverá permitir o cadastro de robôs que podem acessar a aplicação;

5.221. Possuir política de segurança de aplicações pré-configuradas na ferramenta para pelo menos as seguintes aplicações:

5.221.1. Microsoft ActiveSync v1.0, v2.0;

5.221.2. Microsoft OWA in Exchange 2003, 2007, 2010;

5.221.3. Microsoft SharePoint 2003, 2007, 2010;

5.222. A ferramenta oferecida deverá implementar proteção ao JSON (JavaScript Object Notation);

5.223. Possuir firewall XML integrado – suporte a filtro e validação de funções XML específicas da aplicação;

5.224. Implementar a segurança de web services, através dos seguintes métodos:

5.224.1. Criptografar/Decriptografar partes das mensagens SOAP;

5.224.2. Assinar digitalmente partes das mensagens SOAP;

5.224.3. Verificação de partes das mensagens SOAP;

5.225. Prevenir o vazamento de informações, permitindo o bloqueio ou a remoção dos dados confidenciais;

5.226. Prevenir que erros de aplicação ou infraestrutura sejam mostrados ao usuário;

5.227. Deverá ter integração, via ICAP, com servidor de anti-vírus para verificação dos arquivos a serem carregados nos servidores;

5.228. Permitir o uso do parâmetro HTTP X-Forwarded-For como parte da política de controle;

5.228.1. Deverá proteger o protocolo FTP com pelo menos os seguintes métodos:

5.228.2. Determinar os comandos FTP permitidos;

5.228.3. Requests FTP anônimos;

5.228.4. Checar compliance com o protocolo FTP;

5.228.5. Proteger contra-ataques de força bruta nos logins;

5.229. Deverá proteger o protocolo SMTP com pelo menos os seguintes métodos:

5.229.1. A comunicação deve ser aderente a RFC 2821;

5.229.2. Limitar o número de mensagens;

5.229.3. Validar registro SPF do DNS;

5.229.4. Determinar quais métodos SMTP podem ser utilizados;

5.229.5. Deverá armazenar os log localmente ou exportar para Syslog server;

5.229.6. Deverá proteger contra atraques CSRF (Cross-Site Request Forgery), podendo ser possível especificar quais URLs serão examinadas;

5.230. Deverá possuir controle de fluxo por aplicação permitindo definir o fluxo de acesso de uma URL para outra da mesma aplicação. Dessa forma qualquer

tentativa de acesso a um determinado site que não siga o fluxo passando pelas URLs pré-definidas deverá ser bloqueado como uma tentativa de acesso ilegal.

5.231. A solução deve fornecer relatórios consolidados de ataques com pelo menos os seguintes dados: Resumo geral com as políticas ativas, anomalias e estatísticas de tráfego, Ataques DoS, Ataques de Força Bruta, Ataques de Robôs, Violações, URL, Endereços IP, Países, Severidade e PCI Compliance.

5.232. Deverá permitir o agendamento de relatórios a serem entregues por email;

5.233. Fornecer os seguintes Gráficos de alertas por:

5.233.1. Política de segurança;

5.233.2. Tipos de ataques;

5.233.3. Violações;

5.233.4. URL;

5.233.5. Endereços IP;

5.233.6. Países;

5.233.7. Severidade;

5.233.8. Código de resposta;

5.233.9. Métodos;

5.233.10. Protocolos;

5.233.11. Vírus;

5.233.12. Usuário;

5.233.13. Sessão;

5.234. Deverá exportar as requisições que contém os ataques, pelo menos nos formatos PDF e binário

5.235. Deve possuir relatório em tempo real sobre ataques DoS L7, atualizado automaticamente.

5.236. A solução deve mostrar o impacto de ataques DoS L7 na performance e memória do servidor.

5.237. Os logs devem indicar o momento de início e final de um ataque DoS L7.

5.238. Possuir método de mitigação de DoS L7 baseado em: CAPTCHA ; Descarte de todas as requisições de um determinado IP e/ou país suspeito; Geolocalização, incluindo a prevenção com CAPTCHA para países suspeitos que ultrapassarem os thresholds; Defesa proativa contra Bot, através da injeção de um desafio JavaScript para detectar se é um usuário legítimo ou robô;

5.239. A solução deve permitir que ao detectar um falso positivo, o administrador aceite a requisição e atualize a política automaticamente.

5.240. A solução ao se integrar com um Scanner de vulnerabilidade deve mostrar quais a vulnerabilidades podem ser resolvidas automaticamente (pela própria solução de WAF) e quais podem ser resolvidas manualmente, pelo próprio administrador. No caso de resolução manual, deve ainda mostrar um guia com os passos necessários para resolver aquela vulnerabilidade, inclusive com a avisos de possíveis consequências na aplicação Web.

5.241. A solução deve classificar o nível de violação de uma requisição, possuindo pelo menos 5 níveis, onde o nível 5 é referente a violação mais grave e, portanto, deve ter prioridade.

5.242. A solução deve possuir proteção de DDoS L7 baseado em análise comportamental, sem precisar de nenhuma configuração manual.

5.243. Suportar os protocolos HTTP/1.0, HTTP/1.1 e HTTP/2.0.

5.244. Suportar codificação HTML "application/x-www-form-urlencoded".

5.245. Suportar Cookies v0 e v1.

5.246. Suportar codificação fragmentada (chunked encoding) em requisições e respostas.

5.247. Suportar compressão de requisições e respostas.

5.248. Suportar validação de protocolo, como:

5.249. Possibilidade de restringir uso de métodos;

5.250. Possibilidade de restringir protocolos e versões de protocolos;

5.251. Strict (per-RFC) Request Validation;

5.252. Validar caracteres URL-encoded; e

5.253. Validação de codificação fora de padrão %uXXYY.

5.254. Suportar restrições de HTML, como:

5.255. Tamanho do nome de parâmetros;

5.256. Tamanho dos valores de parâmetros; e

5.257. Combinação de tamanho de parâmetros (nome e valores).

5.258. Suportar POST no upload de arquivo.

5.259. Permitir configurar ou oferecer restrições para tamanho individual de arquivo.

5.260. Permitir customizar a lógica na inspeção de upload de arquivos.

5.261. Suporte para os métodos Basic, Digest e NTLM para autenticação.

5.262. Suporte para autenticação por back end tipo LDAP e Microsoft Active Directory.

5.263. Capacidade de filtrar cabeçalhos, corpo e status de respostas.

5.264. Suportar as seguintes técnicas de detecção:

5.265. URL-decoding;

5.266. Terminação Null Byte String;

5.267. Paths auto-referenciados;

5.268. Case de caracteres misturados;

5.269. Uso excessivo de espaços em branco;

5.270. Remoção de comentários;

5.271. Decodificação de entidades HTML; e

5.272. Caracteres de escape.

5.273. Possuir registro de logs com as seguintes características:

5.274. Em cada registro de log de acesso deve ser inserido um identificador de transação HTTP que deve ser único, envolvendo o par requisição/resposta;

5.275. Os registros de log de acesso e eventos devem ser armazenados em arquivo ou em banco de dados que permita a exportação ou em outro formato aberto como CSV ou TXT, podendo ainda serem armazenados localmente ou carregados (upload) em servidor de log via FTP ou SCP ou armazenados em servidor externo de banco de dados;

5.276. Permitir configurar a retenção dos logs por tempo e volume; e

5.277. Ter capacidade para detecção, remoção ou codificação de dados sensíveis do log.

5.278. A solução deverá gerar relatórios com as seguintes características:

5.279. Permitir a filtragem por data ou hora, endereço IP e tipo de incidente;

5.280. Permitir a geração de relatórios sob demanda ou pré-programados periodicamente (diário e semanal); e

5.281. Permitir a geração de relatórios em formatos PDF/A (versão aberta) e HTML.

5.282. Possuir as seguintes características de gerenciamento:

5.283. Facilidade para liberação de regras aprendidas automaticamente que estejam gerando grande quantidade de falso positivo;

5.284. Facilidade para transformar um ataque detectado e considerado falso positivo como regra do firewall;

5.285. Facilidade para aplicar diferentes regras para diversas aplicações;

5.286. Capacidade para customizar regras de negação de serviço;

5.287. Capacidade para combinar detecção e prevenção na construção das regras; e

5.288. Capacidade para desfazer a aplicação de uma regra.

5.289. Possuir mecanismos que garantam a capacidade de gerenciamento da ferramenta sob condições de alto tráfego.

5.290. A solução deve apresentar perfil de aprendizagem automática com:

5.291. Capacidade de aprendizagem automática sem intervenção humana; e

5.292. Capacidade de inspeção das regras criadas automaticamente.

5.293. Permitir o gerenciamento da configuração com as seguintes características:

5.294. Gerenciamento por autenticação dos usuários e as autorizações baseadas em perfis (roles); e

5.295. Capacidade de gerenciamento remoto das ferramentas.

5.296. Apresentar logs e relatórios administrativos com as seguintes características:

5.297. Capacidade para identificar e notificar falhas do sistema ou perda de performance;

5.298. Capacidade de agregação de informações para simplificar a revisão das atividades do dispositivo; e

5.299. Capacidade para gerar estatísticas de serviço e sistema.

5.300. Possuir suporte a XML:

5.301. Para proteção de WebServices;

5.302. Em conformidade com a especificação WS-I básico; e

5.303. Com capacidade de restringir métodos do WebService via definição em WSDL.

5.304. Suportar funções de camuflagem (cloaking), como:

5.305. Esconder qualquer mensagem de erro http dos usuários; e

5.306. Remover as mensagens de erro das páginas que serão enviadas aos usuários.

5.307. Proteger a aplicação Web contra robôs sofisticados através da combinação de desafios enviados ao browser do usuário e técnicas avançadas de análise comportamental.

5.308. A solução deve encriptar dados e credenciais na camada de aplicação, sem ter a necessidade de atualizar a aplicação.

5.309. Essas informações devem ser encriptadas para proteger o login e as credenciais dos usuários e com isso os dados da aplicação.

5.310. Deve aprender automaticamente o comportamento da aplicação e combinar o comportamento heurístico do tráfego com o stress do servidor de aplicação para determinar uma condição de DDoS.

5.311. Ao detectar uma condição de DDoS, assinaturas dinâmicas devem ser automaticamente criadas e implementadas em tempo real para proteção da aplicação.

5.312. Deve possuir uma proteção proativa contra-ataques automatizados por robôs e outras ferramentas de ataque.

5.313. Deve proteger informações sensíveis e confidenciais da interceptação por terceiros, através da criptografia de dados quando ainda no browser do usuário.

5.314. Deve proteger esses dados criptografados de malwares e keyloggers.

5.315. Deve possuir proteção contra-ataques DDoS, através da análise de comportamento de tráfego usando técnicas de análise de dados e Machine Learning.

5.316. Através da análise contínua de carga e monitoração de saúde de servidores, deve ser possível identificar anomalias e mitigá-las.

5.317. Deve ajudar a prevenir contra-ataques de Credential Stuffing, onde bases de credenciais expostas na Internet são usados para tentativa de acesso de outras aplicações Web.

5.318. Deve possuir lista dinâmica de endereços IP globais com atividades maliciosas:

5.319. Deve ser possível verificar o endereço de origem do pacote IP no cabeçalho IP e no parâmetro X-forwarded-for (XFF)

5.320. Deve possuir, pelo menos, as seguintes categorias de endereços IP: Windows Exploits, Web Attacks, Botnets, Scanners, Denial of Service, Reputation, Phishing Proxy, Anonymous Proxy

6. Instalação, Configuração e Customização de Aplicações Envolvidas

6.1. Serão contemplados todos os serviços de instalação física de todos os componentes adquiridos.

6.2. Deverá ser fornecido documentação de toda a implementação e configuração dos produtos adquiridos.

6.3. Após no máximo 10 (dez) dias da assinatura do contrato, deverá ser realizada uma reunião presencial no Contratante, com a participação de no mínimo 1 (um) preposto da Contratada e os representantes da equipe do Contratante, com o objetivo de elaborar o plano de migração.

6.4. A Contratada deverá apresentar, para aprovação do Contratante, o plano detalhado de instalação, especificando os procedimentos e cronograma a serem adotados.

6.5. O Contratante fará análise e validação do plano detalhado de migração, em até 5 (cinco) dias úteis, apontado as devidas correções no documento, ficando a Contratada responsável por ajustar o plano em até 7 (sete) dias úteis, conforme as alterações apontadas pela Contratante.

6.6. Fica a critério do Contratante, definir o horário de instalação e configuração das ferramentas, podendo tais procedimentos serem executados em feriados ou finais de semana e em horário noturno.

6.7. A Contratada não poderá realizar terceirização dos serviços objeto deste termo de referência, sendo responsável pela execução do serviço objeto desta contratação.

7. Garantia e Suporte Técnico

7.1. Os serviços poderão ser prestados pela CONTRATADA ou por representante indicada pela CONTRATADA ou pelo fabricante da solução, sem

prejuízo a responsabilidade integral da CONTRATADA quanto aos atendimento dos níveis de serviço;

7.2. Entende-se por “Garantia” ou ”“Suporte” ou “Manutenção”, doravante denominada unicamente como “Garantia”, toda atividade do tipo “corretiva” não periódica que variavelmente poderá ocorrer, durante todo o período de garantia. A mesma possui suas causas em falhas e erros no Software e trata da correção dos problemas atuais e não iminentes de fabricação dos mesmos. Esta “Garantia” inclui os procedimentos destinados a recolocar em perfeito estado de operação os serviços e produtos ofertados, tais como:

7.3. Do software: desinstalação, reconfiguração ou reinstalação decorrente de falhas de desenvolvimento do software, atualização da versão de software, correção de defeitos de desenvolvimento do software, de acordo com os manuais e as normas técnicas específicas do fabricante para os recursos utilizados;

7.4. Quanto às atualizações pertinentes aos softwares: Entende-se como “atualização” o provimento de toda e qualquer evolução de software, incluindo correções, “patches”, “fixes”, “updates”, “service packs”, novas “releases”, “versions”, “builds”, “upgrades”, englobando inclusive versões não sucessivas, nos casos em que a solicitação de atualização de tais versões ocorra durante o período de garantia do contrato.

7.5. Substituir, temporária ou definitivamente, o produto defeituoso por outro de mesma marca e modelo e com as mesmas características técnicas, novo e de primeiro uso, quando então, a partir de seu efetivo funcionamento, ficará suspensa a contagem do prazo de reparo, nos casos em que não seja possível o reparo dentro dos prazos máximos estipulados acima.

7.6. Devolver, em perfeito estado de funcionamento, no prazo máximo de 30 (trinta) dias corridos, a contar da data de retirada das ferramentas, os ferramentas que necessitem ser temporariamente retirados para conserto, ficando a remoção, o transporte e a substituição sob inteira responsabilidade da CONTRATADA.

7.7. A CONTRATADA fornecerá e aplicará pacotes de correção, em data e horário a serem definidos pelo Contratante, sempre que forem encontradas falhas de laboratório (bugs) ou falhas comprovadas de segurança em software ou firmware dos aparelhos que integrem o objeto do contrato. O atendimento deste

requisito está condicionado a liberação pelo fabricante dos pacotes de correção e/ou novas versões de software.

7.8. Deverá fornecer, ainda, serviços de configuração, instalação, transferência de conhecimento, com licenciamento e garantia durante o período de contrato, ao longo do qual deverão ser fornecidas sem custo adicional todas as correções (patches) e atualizações, inclusive de “firmware”, da solução, sempre que houver adição de novas funcionalidades ou correções.

7.9. É facultado a Contratada a execução, ao seu planejamento e disponibilidade, de “Garantia” do tipo “preventiva” que pela sua natureza reduza a incidência de problemas que possam gerar “Garantia” do tipo “corretiva”. As manutenções do tipo “preventiva” não podem gerar custos ao Contratante.

7.10. A manutenção técnica do tipo “corretiva” será realizada sempre que solicitada pelo Contratante por meio da abertura de chamado técnico diretamente à empresa CONTRATADA (ou a outra informada pela CONTRATADA) via telefone (com número do tipo “0800 ou Internet ou e-mail ou fac-símile ou outra forma de contato;

7.11. Os serviços de “Garantia” incluem:

7.12. Solução de problemas relativos à indisponibilidade da solução decorrentes de problemas de fabricação, desenvolvimento ou ocasionada pelo uso normal das ferramentas;

7.13. Solução de falhas ou defeitos no funcionamento, incluindo a instalação de arquivos para correção dos erros;

7.14. Esclarecimento de dúvidas sobre o funcionamento e operação da solução;

7.15. Instalação de novas versões ou atualizações e patches;

7.16. A CONTRATADA deve disponibilizar a central atendimento 24 horas por dia, 7 dias da semana (incluindo feriados) e equipe com conhecimentos sólidos no funcionamento e operação da solução de gestão.

7.17. O serviço de “Garantia” deve disponibilizar o seguintes tipos de atendimento:

7.18. Nível I - Atendimento Telefônico (Help Desk): chamados abertos através de ligação telefônica ou e-mail ou outro forma de contato, em regime de 24x7: 24 horas por dia, 7 dias da semana (incluindo feriado). Esse serviço deve atender demandas dos usuários referentes ao funcionamento da solução, que decorram de problemas de funcionamento.

7.19. Nível II - Atendimento Remoto: atendimento remoto de chamados de suporte técnico através de tecnologia disponibilizada pelo Contratante, mediante prévia autorização e seguindo os padrões de segurança, objetivando análise e solução remota dos problemas apresentados.

7.20. Nível III - Atendimento Presencial (On-Site): atendimentos técnicos realizados nas dependências do CONTRATANTE, através de visita de técnico especializado, com a finalidade de resolver demandas abertas no Help Desk e não solucionadas pelo Atendimento Telefônico e/ou Remoto.

7.21. Toda “Garantia” deve ser solicitada inicialmente via Help Desk (Nível I), ficando a transferência do atendimento para o Atendimento Remoto (Nível II)

7.22. Toda “Garantia” solicitada inicialmente via Help Desk (Nível I), deve ser transferido para o Atendimento Presencial (Nível III) quando o atendimento do Help Desk não for suficiente para solução do problema sem a intervenção presencial de um técnico.

7.23. Os prazos para a prestação dos serviços devem garantir a observância ao atendimento da seguinte SEVERIDADE:

7.24. SEVERIDADE URGENTE – Solução totalmente inoperante.

7.25. Prazo máximo de início de atendimento de até 04 horas úteis contadas a partir do horário de abertura do chamado;

7.26. Prazo máximo de resolução do problema de até 24 horas úteis contadas a partir do início do atendimento.

7.27. SEVERIDADE IMPORTANTE – Solução parcialmente inoperante – Necessidade de suporte na solução com a necessidade de interrupção de funcionamento da solução.

7.28. Prazo máximo de início de atendimento de até 24 horas úteis contadas a partir do horário de abertura do chamado;

7.29. Prazo máximo de resolução do problema de até 48 horas úteis contadas a partir do início do atendimento.

7.30. SEVERIDADE NORMAL – Solução não inoperante, mas com problema de funcionamento – Necessidade de suporte na solução sem a necessidade de interrupção de funcionamento da solução.

7.31. Prazo máximo de início de atendimento de até 48 horas úteis contadas a partir do horário de abertura do chamado;

7.32. Prazo máximo de resolução do problema de até 96 horas úteis contadas a partir do início do atendimento.

7.33. SEVERIDADE EXTERNO – Solução inoperante, de forma parcial ou total, fruto de falha de elemento de hardware e/ou software não fornecido pela Contratada. Neste caso, ficam suspensos todos os prazos de atendimento até que o Contratante resolva os problemas externos que provocam a inoperância da solução. Após disponibilizar o ambiente de forma estável para a reativação da solução, a Contratada realizará avaliação da extensão do dano a solução e as partes definirão em comum acordo o prazo para a reativação da solução.

7.34. SEVERIDADE INFORMAÇÃO – Solicitações de informações diversas ou dúvidas sobre a solução.

7.35. Prazo máximo de resposta de até 03 dias úteis, contados a partir da data de abertura da ocorrência.

7.36. Um chamado técnico somente poderá ser fechado após a confirmação do responsável da CONTRATANTE e o término de atendimento dar-se-á com a disponibilidade do recurso para uso em perfeitas condições de funcionamento no local onde o mesmo está instalado;

7.37. Na abertura de chamados técnicos, serão fornecidas informações, como Número de série (quando aplicável), anormalidade observada, nome do responsável pela solicitação do serviço e versão do software utilizada e severidade do chamado.

7.38. A severidade do chamado poderá ser reavaliada quando verificado que a mesma foi erroneamente aplicada, passando a contar no momento da reavaliação os novos prazos de atendimento e solução;

7.39. A CONTRATADA poderá solicitar a prorrogação de qualquer dos prazos para conclusão de atendimentos de chamados, desde que o faça antes do seu vencimento e devidamente justificado.

8. Operação Assistida

8.1. A contratada deverá disponibilizar, sob demanda, horas de serviços técnicos especializados em segurança da informação, de forma a atender aos seguintes requisitos:

8.1.1. Execução de até 8.064 (oito mil e sessenta e quatro) horas; 6.1.2. os serviços elegíveis a serem executados irão se limitar, exclusivamente, aos seguintes casos:

8.1.1.1. Elaboração de pareceres em segurança da informação;

8.1.1.2. Elaboração de relatórios gerenciais;

8.1.1.3. Análise de segurança em elementos que sejam de propriedade da contratada ou que não estejam no escopo desse projeto;

8.1.1.4. Suporte aos planos de melhoria na infraestrutura de segurança do SESC/DF/DF; 6.1.2.5. suporte a mudanças de arquitetura do ambiente do SESC/DF, sobretudo aos aspectos de segurança envolvidos;

8.1.1.5. Avaliação de incidentes, incluindo a indicação de atualizações ou procedimento necessários para mitigar possíveis vulnerabilidades;

8.1.1.6. Apoio na definição e implementação de mecanismos futuros de monitoramento de segurança;

8.1.1.7. Configuração de segurança e atualização de versão de softwares da solução contratada;

8.1.1.8. Orientação quanto a procedimentos de auditoria no ambiente computacional do SESC/DF/DF;

8.1.1.9. Elaboração, em conjunto com o SESC/DF, de planos de conscientização de usuários que proporcionem maior grau de segurança;

8.1.1.10. Quaisquer serviços ou procedimentos realizados deverão ser previamente aprovados pela CONTRATANTE por meio de Ordem de Serviço, em comum acordo entre o SESC/DF e a contratada, sendo que o tempo necessário ao atendimento deverá ser previamente definido na respectiva Ordem de Serviço;

8.1.1.11. A prorrogação do prazo de execução de uma Ordem de Serviço somente será possível mediante apresentação, pela contratada, de relatório de impacto contendo justificativas plausíveis, devidamente aceitas pela CONTRATANTE, ou por interesse desta, em caso de impedimento devidamente justificado que dificulte ou não permita a execução dos serviços;

8.1.1.12. As ordens de serviço só serão consideradas concluídas após a entrega da documentação dos procedimentos e da configuração resultante nas bases e nos padrões definidos pelo SESC/DF (incluindo documento asbuilt);

8.1.1.13. Para recebimento dos serviços será preenchido o Termo de Recebimento de Serviços.

8.1.1.14. O SESC/DF deve avaliar os serviços entregues em até 10 (dez) dias úteis contados da entrega dos serviços exigidos;

8.1.1.15. A contratada deverá reapresentar o serviço corrigindo eventuais observações feitas pelo SESC/DF em até 10 (dez) dias úteis, a contar da comunicação;

8.1.1.16. Estando todos os elementos necessários, a CONTRATANTE fará o recebimento definitivo dos serviços no prazo máximo de 15 (quinze) dias úteis;

8.1.1.17. Para a recebimento definitivo será preenchido o Termo de Recebimento de Serviços. o SESC/DF somente autorizará o pagamento das faturas emitidas após o recebimento definitivo dos serviços, realizado mensalmente, de acordo com os níveis mínimos de serviço estabelecidos.

8.1.2. a contratada deverá fornecer mensalmente os relatórios abaixo descritos:

8.1.2.1. dados, informações, indicadores e métricas que permitam quantificar o percentual de disponibilidade da central de atendimento da contratada, detalhados para a central de atendimento telefônico e para o portal na Internet;

8.1.2.2. atividades de suporte e manutenção, com pelo menos descrição de: problemas, correções, aplicações de patches, mudanças de configuração e eventos ocorridos no período;

8.1.2.3. chamados abertos no período, ações corretivas tomadas, tempos para execução das atividades;

8.1.2.4. diagnóstico dos ambientes monitorados, obtido por meio do cruzamento das informações obtidas nos logs coletados; relatórios analíticos contendo dados, informações, indicadores e métricas que permitam avaliar a qualidade e desempenho dos serviços prestados em relação ao atingimento ou não dos níveis mínimos de serviço.

8.1.2.4.1. Níveis Mínimos de Serviços (SLA

8.1.2.4.2. Serão estabelecidos os seguintes prazos máximos de conclusão das atividades, os indicadores utilizados na mensuração da qualidade dos serviços e os respectivos fatores de abatimento pelo descumprimento dos níveis mínimos de serviço associados:

8.1.2.4.2.1. Atividade Nivel minimo de serviço IndMeta Indicador para NMS Fator de peso da atividade (FPA)

8.1.2.4.2.2. Gerenciamento de regras e políticas 120 minutos após abertura de chamado 120 minutos regra implementada 0,5 2- Alteração de configurações 240 minutos após abertura de chamado 240 minutos configuração implementada 0,5

8.1.2.4.2.3. Chamados Emergenciais (limitados a 20 por mês e relacionados apenas a gerenciamento de regras ou alteração de configurações) 20 minutos após abertura do chamado 20 min chamado concluído 1

8.1.2.4.2.4. Verificação e filtragem de logs 24 horas após a abertura do chamado 24 horas Arquivo de Log enviado ao requisitante 0,2

8.1.2.4.2.5. atualização de plataformas por meio da implementação de patches e fixes 5 dias após a liberação das atualizações pelo fabricante. 5 dias Patch e fix instalados 0,5

8.1.2.4.2.6. registro de incidentes se segurança pela contratada 10 minutos após primeiro registro ou sintoma relacionado ao evento 10 min chamado aberto 0,1

8.1.2.4.2.7. Início de atuação para resolução de incidentes 15 minutos após a abertura de chamado pelo cliente ou pela contratada] 15 min registro das ações tomadas no chamado pelo responsável pela resolução 0,5

8.1.2.4.2.8. Resolução de incidentes que provoquem indisponibilidade dos serviços e que não necessitem substituição de peças 60 minutos após a abertura do chamado pelo cliente ou contratada 60 min chamado concluído 1,5

8.1.2.4.2.9. resolução de incidentes que não provoquem indisponibilidade dos serviços 240 minutos após abertura de chamado 240 minutos chamado concluído 0,5

8.1.2.4.2.10. Resolução de incidentes que provoquem indisponibilidade dos serviços e que necessitem de substituição de partes e peças 2 dias úteis após a abertura do chamado pelo cliente ou contratada 3 dias úteis chamado concluído 2 1. os Fatores de Abatimento por Desempenho de Serviço (FADS) serão calculados com base na comparação dos resultados alcançados na execução das atividades com os níveis de serviço definidos.

8.1.2.4.2.11. O FADS será calculado como somatório das ocorrências realizadas para cada uma das atividades definidas, conforme fórmula a seguir: FADSK = [(n*FPAK)/100]*VMCK FADS é o Fator de Abatimento por Desempenho de Serviço; k é o item de serviço contratado n é a quantidade de ocorrências da atividade que não atenderam o NMS definido; FPA é o Fator de Peso da Atividade; VMC valor mensal do contrato;