Especificação Técnica: Filtro de Conteúdo Web

1. Objeto

1.1. Consulta pública para aquisição de solução de Filtro de conteúdo Web, Anti-Malware, inspeção de tráfego SSL e autenticação para acesso à Internet;

2. Especificação do Objeto a ser Contratado

2.1. Solução de Filtro de conteúdo Web, Anti-Malware, inspeção de tráfego SSL e autenticação para acesso à Internet, contemplando:

	Item	Descrição da solução	Quantidade
Grupo 01	1	HARDWARE de segurança corporativa com provimento de solução de Filtro de conteúdo Web, Anti-malware, Inspeção de tráfego SSL e autenticação, para acesso Internet, com licença para 102.000 usuários	01
	2	SOFTWARE de segurança corporativa com provimento de solução de Filtro de conteúdo Web, Anti-malware, Inspeção de tráfego SSL e autenticação, para acesso Internet, com licença para 102.000 usuários	01
	3	SERVIÇO DE SUBSCRIÇÃO DE BASE URL de segurança corporativa com provimento de solução de Filtro de conteúdo Web, Anti-malware, Inspeção de tráfego SSL e autenticação, para acesso Internet, com licença para 102.000 usuários, gerenciamento e logs para monitoração.	60 meses

2.2. Os equipamentos que compõe a Solução devem ser instalada em 3 localidades, sendo estas:

2.2.1.1.1. Regional Rio De Janeiro/RJ – Horto: Rua Pacheco Leão, Nº 1.235 Fundos, Bairro Horto Florestal – Rio De Janeiro/RJ, CEP: 22.460-030; CNPJ: 33.683.111/0008-75; Inscrição Estadual: 10.004.799; Inscrição Municipal: 0.094.089-5;

2.2.1.1.2. Regional São Paulo/SP: Rua Olívia Guedes Penteado, Nº 941, Bairro Capela Do Socorro – São Paulo/SP, CEP: 04.766-001; CNPJ: 33.683.111/0009-56; Inscrição Estadual: 111.445.700.110; Inscrição Municipal: 8.242.433-0;

2.2.1.1.3. Regional Brasília/DF: SGAN Av. L2 Norte, Quadra 601 Módulo “G” – Brasília/DF, CEP: 70.836-900; CNPJ: 33.683.111/0002-80; Inscrição Estadual: 07334743/002-94; Inscrição Municipal: 07334743/002-94;

2.3. Características da Solução em cada localidade:

2.3.1. Em casa localidade a Solução deve possuir as seguintes características de conectividade: a) Suporte a LAN switching: VLAN (802.1q); b) Portas de Comunicação RJ-45, 1 Gbps (um gigabit por segundo);

2.3.2. Em casa localidade a Solução deve possuir as seguintes características de performance: a) 4 Gbps (quatro gigabits por segundo) de throughput Full Duplex; b) Total de 30.000 (trinta mil) novas requisições HTTP por segundo, ou superior; c) Total de 600.000 (seiscentas mil) conexões TCP simultâneas, ou superior;

2.3.3. A infraestrutura que suportará a solução, em cada localidade de instalação, deve possuir alta disponibilidade, ou seja, possuir redundância do hardware e software de modo a manter o perfeito funcionamento da solução mesmo em caso de falhas desses componentes, com a manutenção automática de todas as funcionalidades, mesmo com o não-funcionamento de um dos equipamentos da solução;

2.3.4. Deve ser possível a configuração em modo Failover e Balanceamento;

2.3.4.1. No modo Failover: o equipamento principal deverá assumir a carga e em caso de falha repassar toda as conexões para o equipamento secundário;

2.3.4.2. No modo de Balanceamento: o equipamento principal e secundário(s) estarão ativos e distribuindo a carga de conexões, e em caso de falha de um dos equipamentos, os restantes devem manter o sistema em funcionamento;

2.3.5. A quantidade de usuários efetivos em cada localidade será atribuída pelo SERPRO, por meio de redirecionamento de tráfego de saída Internet da Rede SERPRO. As três localidades deverão suportar, em capacidade de hardware, 51% do quantitativo pedido em 2.1;

2.3.6. Todos os equipamentos, produtos e itens que compõem a solução devem ser fornecidos com todas as licenças necessárias para o seu pleno funcionamento, independente do período de garantia, ou seja, as licenças deverão ser perpétuas;

2.3.7. A solução deverá suportar IPv4 e IPv6 nativamente;

2.3.8. A solução deve inserir uma latência de no máximo 30 ms (trinta milisegundos) às requisições dos usuários, a ser validado no processo de ateste da solução por ferramentas de tempo de medição de resposta apresentado pelo SERPRO;

2.3.9. A solução deve ser compatível com a infraestrutura atual de topologia do SERPRO e atuar como proxy transparente através do redirecionamento de conexões utilizando balanceador externo;

2.3.10. Possuir fonte redundante;

2.3.11. A solução deve ser fornecida em appliance;

2.3.11.1. No caso de máquina virtual, o fornecedor deverá entregar as licenças de uso permanentes necessárias e os equipamentos físicos onde as VMs (Virtual Machine) serão hospedadas;

2.3.12. Todas as funcionalidades descritas deverão estar em um único equipamento sem a necessidade de instalação de softwares adicionais em nenhuma outra máquina no ambiente, com exceção da gerência centralizada e da geração de relatórios de informações que não sejam de tempo real;

2.3.13. Todo e qualquer equipamento fornecido deve estar adaptado para colocação em rack padrão 19”;

2.4. **Funcionalidades da Solução:**

2.4.1. A solução deve prover as funcionalidades de Proxy HTTP/HTTPS, Filtro de Conteúdo Web, Anti-Malware, Inspeção de Tráfego SSL, autenticação e controle de Redes Sociais, com capacidade de criar regras para tratamento destes conteúdos e, no mínimo:

2.4.1.1. Permitir acesso a sites de redes sociais sem restrições;

2.4.1.2. Permitir o acesso a sites de rede sociais, mas com proibição de aplicações específicas como chat, envio de arquivos (fotos, vídeos) e jogos;

2.4.1.3. Permitir o acesso somente à leitura do site, proibindo post de mensagens e arquivos;

2.4.2. Possuir filtro de URL baseado em categorias;

2.4.3. Possuir função anti-malware;

2.4.4. Deverá ser provido todo o licenciamento de software e sistemas operacionais necessários para compor todas as funcionalidades descritas para a solução;

2.5. **Base de URLs:**

2.5.1. A solução deve estar baseada em um banco de dados de, no mínimo, 20 milhões de sites com pelo menos 60 (sessenta) categorias previamente definidas e possibilidade de criação, sem limitação, de categorias personalizadas;

2.5.2. A solução deve classificar os sites de acordo com o assunto, possuindo, no mínimo, categorias relacionadas aos assuntos: pornografia, nudez, sites maliciosos, hacking, spyware, phishing, software ilegal, p2p, anonymizers, apostas, jogos, instant messaging, chat, web mail, redes sociais, shareware/freeware, rádio e tv, streaming, download de mídia, sites de relacionamento, armazenamento pessoal de arquivos, compartilhamento de arquivos, acesso remoto e de governo;

2.5.3. Deve analisar em tempo real o conteúdo de sites HTTP e HTTPS ainda não categorizados na base de URLs e filtrá-los de acordo com o resultado da análise, possibilitando o envio automático do resultado ao fabricante, para a devida categorização;

2.5.4. A base de dados de URLs deve ser atualizada automaticamente pela solução, via Internet, através de downloads incrementais;

2.5.5. A solução deve permitir que qualquer site seja adicionado manualmente nas categorias customizadas, também sem limitação, diferente da original e de acordo com a necessidade;

2.5.6. A solução deve permitir consultar em qual categoria determinado site está incluído, seja via website do fabricante, ou interface local;

2.6. **Caching e Proxy:**

2.6.1. Deve suportar os protocolos HTTP, HTTPS;

2.6.2. Deve permitir a configuração da porta ou portas utilizadas para o serviço de proxy;

2.6.3. Capacidade de configurar as estações de trabalho, através de arquivos tipo PAC (Proxy Auto-config), contemplando, no mínimo, os seguintes Sistemas Operacionais:

2.6.3.1. Windows (a partir da versão XP);

2.6.3.2. Linux (a partir da distribuição Ubuntu 12.04)

2.6.3.3. Mac OS X (a partir da versão 10.6)

2.6.4. Possuir a capacidade armazenar o conteúdo Web acessado, em cache no próprio equipamento, e de eliminar este conteúdo (purge), caso necessário;

2.6.5. Capacidade de criar listas de um ou mais domínios que não deverão ser

processados;

2.6.6. Deve ser capaz de criar lista de destinos (Endereços IP e domínios) que podem pular as regras de proxy e políticas;

2.6.7. Possuir a capacidade de atuar como proxy explícito e transparente;

2.6.8. Ao se conectar com a Internet, deve manter o IP de origem da conexão no pacote TCP no modo transparente e não somente no cabeçalho HTTP, permitindo utilizar a função IP spoofing do switch balanceador;

2.6.9. Possuir Servidor Proxy compatível com os Sistemas Operacionais citados nos itens 2.6.4, 2.6.5 e 2.6.6 e com os navegadores:

2.6.10. Mozilla Firefox (a partir da versão 45.3.0)

2.6.11. Google Chrome (a partir da versão 58.0.3029.81)

2.6.12. Apple Safari (a partir da versão padrão do Mac OS X 10.6)

2.6.13. Microsoft Internet Explorer (a partir da versão padrão do Windows XP)

2.6.14. Microsoft Edge (a partir da versão padrão do Windows 10)

2.6.15. Suportar a configuração de múltiplos Upstream Proxy HTTP a fim de redirecionar o tráfego, se necessário, para outras camadas de Proxy, possibilitando configurações de failover, balanceamento ou condicional;

2.6.16. Permitir roteamento de Proxy baseado em:

2.6.16.1. Origem e destino;

2.6.16.2. User Agent;

2.6.16.3. Portas TCP/IP específicadas;

2.7. **Autenticação e Autorização de Usuários:**

2.7.1. A solução deve permitir que políticas diferentes possam ser definidas por usuários, grupos, endereços IPs e conjunto de endereços IPs;

2.7.1.1. Cada política poderá ter regras diferentes para liberação e bloqueio de acesso a sites e download de arquivos;

2.7.2. A solução deve permitir a integração com bases externas de usuários e grupos, para a autenticação e autorização de usuários e grupos baseados em diretório padrão Microsoft Active Directory e LDAP (X.500), tanto utilizando certificados digitais X.509, como userid & password;

2.7.3. Deve possuir capacidade para executar consultas recursivas nas bases externas, permitindo a associação de políticas às estruturas de diretórios citadas no item 2.7.2, com grupos e subgrupos;

2.7.4. A solução deve fazer a autenticação do usuário em modo transparente, via NTLM (NT LAN Manager), ou seja, utilizando usuário já autenticado em domínio Windows, sem pedir novamente a senha para usuário;

2.7.5. A solução deve ser capaz de utilizar um autenticador externo (captive portal), software de Single Sign-On (SSO), e servidor de concessão de ticket (SCT) para autenticação dos usuários em bases LDAP (X.500);

2.7.6. A solução deve permitir que seja acrescentado ao cabeçalho HTTP da requisição as informações do IP do cliente e do usuário que está autenticado;

2.7.7. A solução deve autorizar os usuários sem a necessidade de replicação da base de usuários do diretório AD e LDAP, ora citados no item 2.7.2, ou seja, prover o acesso remoto a um diretório AD ou LDAP existente;

2.7.8. A solução deve permitir a customização do tempo de sessão do usuário final;

2.7.9. A solução deve permitir a configuração de intervalo de revalidação do login nos diretórios citados no item 2.7.2;

2.7.10. A solução deve permitir que os usuários possam se reautenticar, e realizar novo login a partir de uma estação associada anteriormente a outro usuário;

2.8. **Liberação e Bloqueio:**

2.8.1. As regras para liberação e bloqueio de acesso devem se basear na requisição e resposta HTTP e HTTPS;

2.8.2. A solução deve permitir que as políticas possam, para cada categoria:

2.8.2.1. Permitir o acesso livremente;

2.8.2.2. Bloquear o acesso incondicionalmente;

2.8.2.3. Monitorar;

2.8.3. A solução deve permitir o bloqueio de download por tipos de arquivos;

2.8.3.1. A filtragem deve utilizar, no mínimo, as seguintes formas de bloqueio de arquivo:

2.8.3.1.1. Pela extensão do arquivo a ser recebido;

2.8.3.1.2. Pela verificação do tipo dos arquivos compactados;

2.8.3.1.3. Por Content-Type;

2.8.4. A solução deve possuir um conjunto de Content-Types cadastrados e deverá ser possível o cadastramento de novos Content-Types;

2.8.5. A solução deve possibilitar criação de políticas baseada em tempo (dias da semana, hora do dia, etc) para o Filtro de URL;

2.8.6. A solução deve detectar, monitorar e interceptar o acesso feito às páginas abertas dentro de servidores remotos, como:

2.8.6.1. Servidores de tradução;

2.8.6.2. Proxies anônimos;

2.8.7. As transações que forem detectadas, conforme o item anterior, devem estar de acordo com as políticas estabelecidas para a filtragem de conteúdo.

2.8.7.1. Os conteúdos não permitidos que forem acessados sob este mecanismo devem ser bloqueados e os que estiverem de acordo com as políticas, que permitem o acesso, devem ser acessados;

2.8.8. Deve permitir o controle de banda para aplicação de Streaming Media, a fim de limitar a banda de internet usada para aplicações do tipo vídeo que são tuneladas via HTTP e HTTPS;

2.8.9. Deve permitir a liberação, bloqueio e controle de banda para aplicativos, como:

2.8.9.1. Skype;

2.8.9.2. Gmail;

2.8.9.3. Facebook;

2.8.9.4. YouTube;

2.9. **Console de Administração e Monitoração:**

2.9.1. Toda configuração e administração dos equipamentos de filtro de conteúdo Web deve ser implementada a partir de uma console de gerenciamento centralizada, e que permita granularidade no nível de acesso, com perfis distintos aos dos administradores;

2.9.2. A solução deve permitir o acesso à console de monitoração, protegido por autenticação usuário e senha, sendo que o administrador poderá criar tanto usuários em bases de dados local quanto obtê-los de diretórios externos (389 Directory Server versão 1.2.11.15);

2.9.3. A console deve permitir a administração e monitoração de múltiplos equipamentos, assim como a configuração de diferentes políticas de acesso web para diferentes clientes (multi-tenant) em equipamentos exclusivos, ou num mesmo equipamento compartilhado;

2.9.4. A solução de gerenciamento deve permitir replicar as configurações relativas as políticas de acesso definidas entre os sites citados no item 2.2, ou seja, ao ser aplicada uma configuração em uma máquina, todos os outros nós da solução deverão receber essa atualização de configuração, ficando todas as máquinas com as mesmas definições de políticas;

2.9.5. A console de gerenciamento centralizada deve permitir que políticas específicas não sejam replicadas em todos os equipamentos, permitindo implementar uma determinada política em um determinado equipamento e site, a critério do SERPRO;

2.9.6. Se for necessária a utilização de equipamento separado para a console de gerenciamento centralizado, o mesmo deve ser fornecido bem como todas as licenças de software necessárias de uso perpétuo, conforme item 2.3.6;

2.9.7. A console de gerenciamento deve funcionar em alta disponibilidade, entre 2 (duas) das 3 (três) localidades citadas no item 2.2;

2.9.8. A atualização de todos os mecanismos de checagem deve ocorrer de forma regular e automática, efetuando o download de forma incremental;

2.9.9. Deve conter em sua console, ferramenta de Trace das políticas para que o Administrador possa testar as políticas e regras para Troubleshooting;

2.10. **Geração de Logs e Banco de Dados:**

2.10.1. A solução deve gerar log para todo e qualquer acesso, onde conste, no mínimo:

2.10.1.1. Data e hora do acesso;

2.10.1.2. Endereço IP da estação cliente;

2.10.1.3. Usuário;

2.10.1.4. URL de destino da requisição (site visitado);

2.10.1.5. Categoria do site;

2.10.1.6. Tamanho do objeto solicitado (em bytes);

2.10.1.7. Ação tomada pela solução (bloqueado, permitido, etc);

2.10.2. A solução deve gerar dados com estatísticas de acessos internet;

2.10.3. O fornecedor deve prover funcionalidade de geração de relatórios a partir da exportação dos logs de acesso para armazenamento externo e separado do ambiente de Filtragem de conteúdo, visando consolidação e armazenamento de eventos de todos os equipamentos em um único Banco de Dados;

2.10.4. A solução deve ser capaz de armazenar localmente os registros de eventos dos últimos 3 (três) meses;

2.10.5. A console deve registrar, em logs, todas as ações e alterações executadas pelos usuários administradores, para efeito de auditoria;

2.10.6. Possuir interface de relatórios com informações em tempo real;

2.10.7. A solução deve possuir console de monitoração do tráfego em tempo real que mostre, pelo menos, categorias, usuários e sites mais acessados;

2.10.8. Possuir no mínimo os seguintes relatórios:

2.10.8.1. Visão do sistema (utilização e carga de hardware: CPU, memória e interfaces);

2.10.8.2. Atividades do site (demais URLs acessadas a partir do mesmo);

2.10.8.3. Detalhes do site;

2.10.8.4. Atividades do usuário;

2.10.8.5. Volume de dados;

2.10.8.6. Detalhes do usuário;

2.10.8.7. Detalhes da categoria;

2.10.9. A interface de relatórios de informações que não são de tempo real deve possuir as seguintes funcionalidades:

2.10.9.1. Relatório de sites e categorias acessados (geral e por usuário);

2.10.9.2. Relatório de sites bloqueados (geral e por usuário);

2.10.9.3. Relatórios de malwares (geral e por usuário);

2.10.9.4. Definição de um intervalo de dia e hora para os relatórios;

2.10.9.5. Sites mais acessados;

2.10.9.6. Usuários com mais acessos;

2.10.9.7. Relatórios sobre as aplicações;

2.10.10. Todos relatórios devem ser passíveis de customização e conter ao menos os seguintes campos:

2.10.10.1. Login e IP do usuário;

2.10.10.2. Nome e IP do servidor;

2.10.10.3. Tempo;

2.10.10.4. Volume de dados;

2.10.10.5. Hits;

2.10.10.6. Categoria;

2.10.11. As páginas de notificação de termos de uso, de erro, e de bloqueio de acesso, devem ser personalizáveis de acordo com a política de acesso

2.10.11.1. Deve ser possível hospedar essas páginas em um servidor Web externo;

2.10.12. A solução deve possuir interface de geração de relatórios com informações de histórico, não necessariamente integrada ao equipamento;

2.10.12.1. Deve permitir a exportação dos dados dos relatórios para diversos tipos de arquivos contemplando, no mínimo, os formatos CSV, PDF e XML;

2.10.12.2. Deve permitir o co-relacionamento de informações, possibilitando a criação de relatórios personalizados;

2.10.13. A solução de relatórios deve possibilitar exportar e importar as suas configurações para backup e restore, e logs para arquivamento externo;

2.10.14. Deve ser possível exportar os logs e registros de eventos para servidores externos de syslog e arquivamento;

2.11. **Inspeção de Tráfego SSL:**

2.11.1. A solução deve ser capaz de inspecionar tráfego SSL;

2.11.2. A solução deve possuir a capacidade de decriptar conexões HTTPS baseado na categoria do site de destino e baseado na reputação do site de destino;

2.11.3. Deve ser possível o bloqueio de sites com má reputação e de categoria desconhecida;

2.11.4. O conteúdo descriptografado deve ser inspecionado pelo filtro de URL e pelo componente anti-malware;

2.11.5. A solução deve atuar como man-in-the-middle, e deve suportar certificados on-box, importando certificados válidos ou gerando certificados autoassinados;

2.11.6. A solução deve realizar a inspeção do tráfego SSL de forma compatível com os principais navegadores e aplicativos atuais;

2.11.7. A solução deve checar os certificados digitais do site acessado com HTTPS;

2.11.7.1. No caso de certificados digitais inválidos, a solução deve ser configurável para, de acordo com preferência do administrador, bloquear o acesso ao site;

2.11.8. Para verificar a validade dos certificados digitais, a solução deve permitir configurar quais são as Autoridades Certificadoras Raiz confiáveis;

2.12. **Anti-Malware:**

2.12.1. A solução deverá possuir análise de arquivos para detecção e bloqueio de malware;

2.12.2. Para detecção de malware, a ferramenta deve ter uma base de assinaturas de malwares conhecidos, que deverá ser atualizada automaticamente;

2.12.3. A ferramenta deverá descompactar arquivos compactados como '.zip', '.gzip', '.tar', '.arj' e '.rar', bem como analisar seu conteúdo;

2.12.4. Se a detecção de malware não for feita no mesmo equipamento fornecido para filtro de conteúdo web, a contratante deve fornecer os appliances (conjunto de hardware e software de mesmo fabricante) para compor a solução, observando-se os requisitos de alta disponibilidade;

2.12.5. O mecanismo de verificação de malware deve reconhecer códigos maliciosos;

3. Níveis de Serviço

3.1. Garantia, Suporte e Atualização de versão de software:

3.1.1. A garantia de hardware da Solução, bem como da atualização dos softwares e patches será de 60 (sessenta) meses, a partir do recebimento definitivo do SERPRO;

3.1.2. A garantia também englobará sanar dúvidas relacionadas com a instalação, configuração e softwares contratados;

3.1.3. A atualização de softwares deve englobar:

3.1.3.1. Fornecimento das versões, releases e patches mais recentes;

3.1.3.2. Fornecimento de versões mais recentes da base de conhecimento;

3.1.3.3. O serviço de atualização deve incluir correções na solução ou execução de quaisquer medidas necessárias para sanar falhas de funcionamento ou vulnerabilidades;

3.1.4. A cada nova versão instalada, a CONTRATADA deve apresentar as novas funcionalidades de acordo com a solicitação do SERPRO, sem ônus adicional;

3.1.5. A garantia de 60 (sessenta) meses contemplará atendimento técnico quanto à configuração e solução de problemas envolvendo o produto ofertado, bem como a atualização dos softwares;

3.1.6. Caso a solução de Filtro de Conteúdo Web fornecida seja descontinuada na linha de comercialização do fabricante, durante a vigência da garantia, a CONTRATADA deve manter as condições da garantia explicitadas nesta contratação, ou providenciar a substituição por outra Filtro de Conteúdo Web disponível que executem as mesmas funcionalidades exigidas no edital, sem ônus adicionais para o SERPRO;

3.1.7. Para Solução Filtro de Conteúdo Web ofertada, a CONTRATADA deve realizar, no exercício da garantia, intervenções preventivas, sendo de responsabilidade da CONTRATADA prover todas as correções e atualizações necessárias, de forma sistemática e programada, de acordo com a periodicidade e os procedimentos especificados na documentação do fabricante;

3.1.8. A CONTRATADA deve entregar um cronograma de manutenção preventiva para aprovação do SERPRO;

3.1.9. A CONTRATADA deve entregar, a cada intervenção preventiva realizada, relatório técnico contendo os procedimentos executados;

3.1.10. Nas intervenções preventivas ou corretivas, em que haja risco de indisponibilidade total ou parcial, o SERPRO deve ser previamente notificado para que se proceda a aprovação e o agendamento da operação em horário conveniente ao SERPRO;

3.2. Tabela de Níveis de Serviço e Sancionamentos:

3.2.1. O exercício da garantia para retorno de hardware e software à condição operacional da solução deve ser realizado conforme critérios abaixo:

3.2.1.1. O atendimento deve ser prestado 10 (dez) horas por dia, das 8 às 18 horas, de segunda-feira a sexta-feira, excluindo os feriados, exceto para os chamados de atividades programadas;

3.2.1.1.1. Os chamados de Severidade 4 – Baixa serão atendidos dentro do horário comercial, das 8 às 17 horas;

3.2.1.1.2. O atendimento aos chamados para o exercício da garantia deve obedecer à seguinte classificação quanto ao nível de severidade:

Níveis de Severidade e Sancionamento					
Severidade	**Descrição**	**Tipo**	**Tempo de Atendimento**	**Tempo de Solução**	**Penalidades**
1 – Crítica	Chamados referentes a situações de emergência ou problema crítico, caracterizados pela existência de ambiente paralisado	On-site	No máximo 4 (quatro) horas após a abertura do chamado, incluindo percurso do técnico até as instalações do SERPRO	No máximo 8 (oito) horas após o início do atendimento do chamado	O não atendimento dentro do prazo estabelecido para o chamado, ensejará em aplicação de multa à CONTRATADA no valor de 0,15% (zero vírgula quinze por cento) do valor contratual, por hora ou fração de hora de atraso
2 – Alta	Chamados associados a situações de alto impacto, incluindo os casos de degradação severa de desempenho	On-site	No máximo 6 (seis) horas após a abertura do chamado	No máximo 10 (dez) horas após o início do atendimento do chamado	O não atendimento dentro do prazo estabelecido para o chamado, ensejará em aplicação de multa à CONTRATADA no valor de 0,1% (zero vírgula um por cento) do valor contratual, por hora ou fração de hora de atraso
3 – Média	Chamados referentes a situações de baixo impacto ou para aqueles problemas que se apresentem de forma intermitente, incluindo os casos em que haja necessidade de substituição de componentes	On-site ou Remoto	No máximo 10 (dez) horas após a abertura do chamado	No máximo 24 (vinte e quatro) horas após o início do atendimento do chamado	O não atendimento dentro do prazo estabelecido para o chamado, ensejará em aplicação de multa à CONTRATADA no valor de 0,075% (zero vírgula zero setenta e cinco por cento) do valor contratual, por hora ou fração de hora de atraso
4 – Baixa	Chamados com objetivo de sanar dúvidas quanto ao uso ou à implementação do produto	Remoto	No máximo 24 (vinte e quatro) horas após a abertura do chamado	No máximo 72 (setenta e duas) horas após a abertura do chamado	O não atendimento dentro do prazo estabelecido para o chamado, ensejará em aplicação de multa à CONTRATADA no valor de 0,05% (zero vírgula zero cinco por cento) do valor contratual, por hora ou fração de hora de atraso

3.2.1. Será aberto um chamado técnico para cada problema reportado, sendo iniciada a contagem do tempo de atendimento a partir da hora de acionamento;

3.2.2. Durante o período de garantia, a CONTRATADA deverá fornecer informações sobre as correções a serem aplicadas ou a própria correção;

3.2.3. Deve fornecer orientações para diagnóstico de problemas e ajuda na interpretação de traces, dumps e logs;

3.2.4. Nos casos de problemas não documentados, os registros enviados pelo SERPRO

(tais como: traces, dumps e logs) devem ser encaminhadas aos laboratórios do responsável técnico, a fim de que sejam fornecidas as devidas correções;

3.3. Chamados, Registro e Início de Prazos:

3.3.1. O atendimento aos chamados deve obedecer à tabela de classificação quanto ao nível de severidade;

3.3.2. Será aberto um chamado para cada problema reportado;

3.3.3. A abertura do chamado na CONTRATADA pelo SERPRO poderá ser realizado através dos Canais de Atendimento Obrigatórios;

3.3.4. Os prazos para atendimento de chamados de qualquer severidade serão considerados a partir da hora em que o chamado é aberto;

3.3.4.1. O chamado será registrado na CONTRATADA, recebendo uma identificação para acompanhamento, controle e histórico;

3.3.4.2. A contagem de tempo de atendimento será inciada a partir da hora de acionamento;

3.4. Atendimento e Manutenções:

3.4.1. A CONTRATADA deve prover todas as correções e atualizações necessárias para os hardwares instalados incluindo firmware e microcódigos;

3.4.2. A CONTRATADA deve manter a solução compatível com os demais componentes de hardware e software dos Centro de Dados do SERPRO sem ônus adicional para o SERPRO;

3.4.3. A CONTRATADA deve prover acesso para suporte técnico de 2° e 3° níveis no suporte a firmware e microcódigos da solução, sem ônus adicional para SERPRO;

3.4.4. Para todos efeitos da contratação em espécie, vigoram os seguintes conceitos:

3.4.4.1. Suporte Técnico de Primeiro Nível: equipe treinada para atender diretamente os usuários em demandas referentes a diagnóstico e tratamento de problemas, configuração e administração do ambiente e esclarecimento de dúvidas em geral;

3.4.4.2. Suporte Técnico de Segundo Nível: equipe multidisciplinar treinada, certificada e com grande experiência em ambientes críticos e complexos, que exigem alta disponibilidade;

3.4.4.3. Suporte Técnico de Terceiro Nível: escalonamento obrigatório ao fabricante, devido à necessidade de retaguarda nas tecnologias suportadas;

3.5. As peças e componentes em substituição, instaladas pela CONTRATADA, serão incorporadas na solução, passando a ser de propriedade do SERPRO;

3.6. Canais de Atendimento Obrigatórios:

3.6.1. Atendimento por meio de canal telefônico gratuito 0800 ou tarifação reversa, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana;

3.6.2. Chamado técnico através de site na Internet, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana;

3.7. Escalação e Severidade:

3.7.1. Por necessidade de serviço ou criticidade do problema, o SERPRO poderá solicitar a escalação de chamado para níveis superiores ou inferiores de severidade ou seus respectivos prazos;

3.8. Entrega Mensal de Relatórios:

3.8.1. Mensalmente deverá ser entregue relatório constando os acionamentos técnicos abertos, em andamento e encerrados no período do exercício da garantia, por localidade;

3.8.2. O relatório deve conter no mínimo as seguintes informações: número de acionamento, descrição da ocorrência, severidade, nome do responsável do SERPRO pela abertura do chamado, data e hora de abertura do chamado, data e hora do início do atendimento, tipo do atendimento (remoto, on-site ou ambos), data e hora de encerramento ou aplicação de solução de contorno e descrição da resolução adotada;

3.8.3. O relatório deverá ser entregue mesmo quando não houver chamados no período;