

## Projeto Básico COGTI 00495/2016

### Título

### Consulta pública para aquisição de solução de análise e auditoria de dispositivos de segurança do tipo firewalls com funcionalidade work-flow

### 2ª Versão

#### Vinculação com Documento de Oficialização de Demanda

Número DOD	Título da Demanda	Número do Item	Nome do Objeto	Descrição
------------	-------------------	----------------	----------------	-----------

### 1.0 Objeto

1.1. Aquisição da solução de análise e auditoria de dispositivos de segurança do tipo firewalls, com funcionalidade de work-flow. Esta solução deve ser capaz de monitorar, analisar, gerenciar, otimizar e auditar dispositivos de segurança de rede do tipo firewall, fornecidos por diferentes fabricantes e plataformas. A interface de administração da solução deve oferecer visibilidade em tempo real de toda a infraestrutura de rede.

O gerenciamento deve ser feito de forma intrusiva, modificando as bases de regras nos dispositivos monitorados. A solução ofertada deve ser baseado em software, fornecida com garantia de 36 (trinta e seis) meses e contemplar: instalação, configuração, repasse de conhecimento e integração com as ferramentas de work-flow utilizadas pelo SERPRO.

### 2.0 Especificação do objeto a ser contratado

#### 2.1. DA SOLUÇÃO DE ANÁLISE E AUDITORIA DE DISPOSITIVOS DE SEGURANÇA DO TIPO FIREWALLS

2.1.1. Deve suportar firewalls dos tipos: appliance físico, appliance virtual, switches, roteadores, em cluster ou não;

2.1.2. Deve permitir administração via interface gráfica e linha de comando (CLI) utilizando protocolo seguro de comunicação;

2.1.3. A solução deve possuir interface de administração via web, de acesso seguro (HTTPS);

2.1.3.1. A interface deve ser compatível no mínimo com Internet Explorer, Google Chrome e Firefox;

2.1.3.2. Deve possuir botão de ajuda sensível ao contexto, trazendo informação da tela atual;

2.1.3.3. Deve exibir mapa da rede incluindo dispositivos monitorados e não monitorados;

2.1.3.4. Deve exibir painel com visualização instantânea da situação de segurança e conformidade;

2.1.3.5. Deve exibir painel de todos os firewalls, indicando se estão, conectado, desconectados ou desabilitados;

2.1.3.6. A solução deve executar o monitoramento, análise e otimização de regras e políticas de firewall;

2.1.4. A solução deve importar automaticamente a tabela de roteamento, inclusive roteamento dinâmico;(AMOSTRA)

2.1.5. Dada uma origem, destino e serviço, deve identificar: interfaces, rotas possíveis,

- regras de firewall e NAT (Network Address Translation) que um pacote atravessa; (AMOSTRA)
- 2.1.6. Deve analisar a consistência das configurações dos equipamentos, tais como redes, grupos e serviços definido com nomes diferentes em firewalls distintos;
- 2.1.7. Deve realizar correlação entre vulnerabilidades, políticas de firewall e configurações de roteamento, identificando quais regras e rotas comprometem a segurança; (AMOSTRA)
- 2.1.8. A solução deve ser capaz de representar no mapa de rede as rotas e/ou ACLs que tem impacto na segurança; (AMOSTRA)
- 2.1.9. Deve estabelecer pontuação customizável de risco, baseado na criticidade de cada firewall monitorados: (AMOSTRA)
- 2.1.9.1. Deve permitir visualização de risco global e por dispositivo; (AMOSTRA)
- 2.1.9.2. Deve destacar a eficácia das políticas aplicadas e os riscos envolvidos; (AMOSTRA)
- 2.1.9.3. Simular a redução do nível de risco caso um conjunto de correções sejam aplicadas;(AMOSTRA)
- 2.1.9.4. Permitir a configuração de políticas de regras específicas da empresa e analisar sua conformidade para validação de novas regras; (AMOSTRA)
- 2.1.9.4.1. A ferramenta deve manter registro destas regras caracterizando como exceção em uma white-list; (AMOSTRA)
- 2.1.10. Deve ter a capacidade de fazer sugestões detalhadas de otimização de regras, tais como: (AMOSTRA)
- 2.1.10.1. Identificar regras potencialmente vulneráveis de acordo com normas e política internas criadas pelo SERPRO na própria ferramenta; (AMOSTRA)
- 2.1.10.2. Informar quais endereços e serviços específicos foram trafegados num intervalo de tempo e sugerir regras baseadas na matriz de tráfego;(AMOSTRA)
- 2.1.10.3. Analisar uma base de regras fornecendo recomendações de posicionamento das mesmas, a partir das estatísticas de uso;(AMOSTRA)
- 2.1.10.4. Reduzir o escopo de regras excessivamente abrangentes;(AMOSTRA)
- 2.1.10.5. Destacar regras que podem ser agrupadas, regras redundantes, regras duplicadas e identificar os objetos não utilizados;(AMOSTRA)
- 2.1.11. Qualquer alteração na configuração e regras de firewall deve ser identificada em tempo real e destacar, no mínimo, os itens:(AMOSTRA)
- 2.1.11.1. Qual a mudança;(AMOSTRA)
- 2.1.11.2. Quem efetuou;(AMOSTRA)
- 2.1.11.3. A data e hora;(AMOSTRA)
- 2.1.12. Deve identificar, no mínimo, as mudanças nos seguintes componentes de configuração:(AMOSTRA)
- 2.1.12.1. Regras de segurança;(AMOSTRA)
- 2.1.12.2. Regras de NAT (Network Address Translation);(AMOSTRA)
- 2.1.12.3. Objetos de segurança;
- 2.1.12.4. Serviços;(AMOSTRA)
- 2.1.12.5. Usuários;(AMOSTRA)
- 2.1.12.6. Aplicações;
- 2.1.12.7. Configuração de interfaces de rede; (AMOSTRA)
- 2.1.12.8. Zonas de segurança;(AMOSTRA)
- 2.1.12.9. Rotas;(AMOSTRA)
- 2.1.12.10. Versão de sistema;
- 2.1.12.11. Monitorar e auditar ACL (Access Control List) em switches e roteadores; (AMOSTRA)

- 2.1.13. Deve permitir a criação de diferentes perfis de acesso e níveis de segurança, com escopo de visualização e permissões de atuação diferentes; (AMOSTRA)
- 2.1.14. Permitir a divisão de uma requisição em múltiplas requisições com níveis de segurança diferentes; (AMOSTRA)
- 2.1.15. Deve ter a capacidade de informar sobre a utilização de objetos e regras, no mínimo, contendo as seguintes informações:(AMOSTRA)
  - 2.1.15.1. Regras não usadas;(AMOSTRA)
  - 2.1.15.2. Regras mais usadas;(AMOSTRA)
  - 2.1.15.3. Percentual de utilização da regra em comparação as demais regras; (AMOSTRA)
  - 2.1.15.4. Última vez que uma regra foi usada;(AMOSTRA)
  - 2.1.15.5. Monitorar continuamente e sugerir otimização das regras dos firewalls; (AMOSTRA)
  - 2.1.15.6. Detecção de regras de menor prioridade e com alta percentagem de tráfego; (AMOSTRA)
  - 2.1.15.7. Objetos não contidos em regras;(AMOSTRA)
  - 2.1.15.8. Objetos contidos em regras, porém não usados;(AMOSTRA)
  - 2.1.15.9. Regras e objetos (IP, rede, serviço) redundantes, inativos, sem uso e ocultos; (AMOSTRA)
- 2.1.16. Deve permitir a monitoração de sistema operacional e performance de firewalls; (AMOSTRA)
- 2.1.17. Possuir a capacidade de pesquisar regras por bloqueio e permissões de acesso em um firewall específico e em um grupo de firewalls;(AMOSTRA)
  - 2.1.17.1. Esta pesquisa deve conter os critérios: IP de origem, IP de destino e serviço, além da combinação entre estes critérios;(AMOSTRA)
- 2.1.18. Deve identificar e distinguir redes diferentes e que utilizam o mesmo endereçamento IP;
- 2.1.19. Deve permitir a indicação e visualização de data de expiração de uma determinada regra:(AMOSTRA)
  - 2.1.19.1. Permitindo a administração centralizada de regras com prazo definido de expiração;(AMOSTRA)
  - 2.1.19.2. Deve fornecer informação sobre regras expiradas e prestes a expirar; (AMOSTRA)
  - 2.1.19.3. Deve enviar alertas configurável sobre regras a expirar; (AMOSTRA)
- 2.1.20. Deve emitir alertas em caso de alterações de configuração que contrariem os padrões e políticas corporativas vigentes;(AMOSTRA)
- 2.1.21. Deve manter o registro de todas as configurações e mudanças capturadas pela solução para futura referência e análise; (AMOSTRA)
- 2.1.22. Deve permitir a comparação entre configurações quaisquer de um mesmo equipamento, armazenadas no banco de dados da solução; (AMOSTRA)
- 2.1.23. Deve realizar auditorias agendáveis e personalizadas das configurações dos firewalls conectados; (AMOSTRA)
  - 2.1.23.1. Deve gerar trilha de auditoria completa do uso do sistema, associando cada alteração da configuração ao usuário que a realizou;(AMOSTRA)
  - 2.1.23.2. Deve ser capaz de fornecer lista de usuários da solução com filtros, no mínimo, baseados nos seguintes critérios:
    - 2.1.23.2.1. Data de criação;
    - 2.1.23.2.2. Lista de usuários de VPN;
    - 2.1.23.2.3. Grupos de usuários;
    - 2.1.23.2.4. Métodos de autenticação dos usuários;

- 2.1.23.2.5. Data de expiração dos usuários;
- 2.1.24. A comunicação entre a solução e os dispositivos de segurança deve ser autenticada e criptografada;
- 2.1.25. Deve suportar operação em alta disponibilidade (HA) mesmo em máquinas virtuais;
- 2.1.26. Deve suportar comutação automática em caso de falha para operação ininterrupta;
- 2.1.27. Deve possuir base de usuários local;
- 2.1.28. A solução deve ter suporte a certificados digital da ICP-Brasil;
- 2.2. GERAÇÃO DE RELATÓRIOS
  - 2.2.1. Fornecer relatórios e histogramas da frequência de uso de regra e objetos (IP, rede, serviço);(AMOSTRA)
    - 2.2.1.1. Estes relatórios deve conter, no mínimo, o horário da alteração e o usuário responsável;(AMOSTRA)
  - 2.2.2. Ter a capacidade de fornecer relatório no formato CSV e PDF informando as alterações que foram feitas no firewall, em um determinado intervalo de tempo;
  - 2.2.3. Deve manter registro detalhado do fluxo de aprovação e implementação de mudanças; (AMOSTRA)
  - 2.2.4. Deve permitir relacionar uma alteração aos usuários aprovadores; (AMOSTRA)
  - 2.2.5. Deve ser capaz de comparar a base de regras do firewall com baselines padrão de mercado e fornecer um relatório de conformidade com o padrão utilizado na comparação;
    - 2.2.5.1. Permitir a emissão de relatórios de conformidade com base nos padrões SOX (Sarbanes-Oxley), PCI-DSS e ISO 27001;
    - 2.2.5.2. Deve possuir informações de vulnerabilidades do padrão CVE (Common Vulnerabilities and Exposures);
  - 2.2.6. Deve ser capaz de migrar as regras e políticas de um dispositivo suportado para um substituto, mesmo que de modelo e fabricante diferentes; (AMOSTRA)
  - 2.2.7. Deve ser capaz de ler e armazenar arquivos de texto das configurações do sistema, quando fornecido pelo dispositivo;
- 2.3. FLUXO DE APROVAÇÃO
  - 2.3.1. Deve suportar criação de fluxo de aprovações para implementação de mudanças nos dispositivos monitorados;
  - 2.3.2. Deve possuir um assistente tipo wizard para auxiliar as solicitações;
  - 2.3.3. Dada uma origem, destino e serviço, a solução deve identificar quais os dispositivos de segurança do tipo firewall precisam ter as regras alteradas para viabilizar o acesso ou bloqueio; (AMOSTRA)
  - 2.3.4. Deve possuir, no mínimo, as seguintes etapas no fluxo de aprovação: (AMOSTRA)
    - 2.3.4.1. Solicitação: Recebimento da Solicitação;(AMOSTRA)
    - 2.3.4.2. Aprovação: Aprovação de Solicitação;(AMOSTRA)
    - 2.3.4.3. Implementação:(AMOSTRA)
      - 2.3.4.3.1. Criação da configuração solicitada;(AMOSTRA)
      - 2.3.4.3.2. Análise de risco da configuração a ser implementada com checagem de conformidade com normas e políticas de segurança pré-definidas pelo SERPRO; (AMOSTRA)
      - 2.3.4.3.3. Implementação da configuração solicitada no dispositivo monitorado a partir da própria interface de gerência da solução;(AMOSTRA)
    - 2.3.4.4. Verificação:(AMOSTRA)
      - 2.3.4.4.1. Verificação da efetividade da configuração realizada;(AMOSTRA)

- 2.3.4.4.2. Auditoria periódica para checagem de conformidade com normas e políticas de segurança pré-definidas pelo SERPRO;
- 2.3.5. Deve possuir fluxos de aprovação pré-definidos e permitir criação de fluxos customizados, com a adição ou remoção de etapas, formulários e configurações; (AMOSTRA)
  - 2.3.5.1. Deve suportar no mínimo 50 fluxos customizados no work-flow;
  - 2.3.5.2. Não deve ser cobrado hora adicional de consultoria para a criação dos fluxos;
  - 2.3.5.3. Os seguintes fluxos customizados devem ser entregues junto com a solução:
    - 2.3.5.3.1. Fluxo de criação de regra de firewall adaptado aos processos do SERPRO; (AMOSTRA)
    - 2.3.5.3.2. Fluxo de alteração de regra de firewall adaptado aos processos do SERPRO; (AMOSTRA)
    - 2.3.5.3.3. Fluxo de exclusão de regra de firewall adaptado aos processos do SERPRO; (AMOSTRA)
    - 2.3.5.3.4. Fluxo de análise Técnica adaptado aos processos do SERPRO; (AMOSTRA)
    - 2.3.5.3.5. Fluxo de bloqueio de Endereço adaptado aos processos do SERPRO; (AMOSTRA)
    - 2.3.5.3.6. Fluxo de configuração de Túnel VPN adaptado aos processos do SERPRO; (AMOSTRA)
    - 2.3.5.3.7. Fluxo de criação de segmento de rede-ZDM adaptado aos processos do SERPRO; (AMOSTRA)
    - 2.3.5.3.8. Fluxo de designação e Fixação de endereço IP adaptado aos processos do SERPRO; (AMOSTRA)
    - 2.3.5.3.9. Fluxo de levantamento de regras existentes adaptado aos processos do SERPRO; (AMOSTRA)
- 2.3.6. Permitir a validação de riscos e conformidade com as políticas definidas pelo SERPRO antes de executar uma mudança nos dispositivos de segurança do tipo firewall monitorados;(AMOSTRA)
- 2.3.7. Deve suportar número ilimitado de aprovadores;
- 2.3.8. Deve permitir a realização de backup do conjunto de regras na própria solução antes de executar uma mudança no dispositivo monitorado; (AMOSTRA)
- 2.3.9. Deve permitir executar rollback de configuração do dispositivo monitorado; (AMOSTRA)
- 2.3.10. Deve permitir a recepção de solicitação de mudanças por interface Web;(AMOSTRA)
- 2.3.11. Deve suportar envio de notificações em tempo real;(AMOSTRA)
- 2.3.12. Deve suportar envio de notificações via e-mail ao solicitante, informando a situação da solicitação, contemplando no mínimo os seguintes tipos de situação: (AMOSTRA)
  - 2.3.12.1. Aprovada;(AMOSTRA)
  - 2.3.12.2. Recusada;(AMOSTRA)
  - 2.3.12.3. Executada;(AMOSTRA)
- 2.3.13. Deve suportar o envio de e-mail automático ao fim de cada etapa;(AMOSTRA)
- 2.3.14. Deve documentar todas as informações relacionadas a uma solicitação de mudança;
- 2.3.15. Suportar o padrão BPMN (Business Process Model and Notation) do OMG (Object Management Group) para integração com soluções de gerenciamento de processos de negócios;
- 2.3.16. Deve prover recurso de busca por palavras nos arquivos de configuração dos dispositivos;

- 2.3.17. Deve coletar log diretamente dos dispositivos monitorados;
- 2.3.18. Notificar quando uma regra for criada com a opção de registro de log desativada;
- 2.3.19. Deve possuir dashboard para visualização de efetividade do processo de mudanças;
- 2.3.20. Em todas as notificações e alertas por e-mail, deve incluir os dados relacionados a mudança tanto no corpo do e-mail quanto em anexo nos formatos HTML, XML ou CSV;

#### 2.4. CARACTERÍSTICAS DE AUTOMAÇÃO

- 2.4.1. Deve possuir a capacidade de automatizar todo o ciclo de vida do processo de criação de regras, Incluindo análise de risco, implantação, validação e auditoria;(AMOSTRA)
- 2.4.2. Gerenciar automaticamente a comunicação entre as entidades, mediante as suas respectivas ações;
- 2.4.3. Ser capaz de identificar que uma solicitação de criação ou alteração de regra ou alteração que não é necessária e alertar o usuário;(AMOSTRA)
- 2.4.4. Atender às solicitações de criação de regra, sugerindo a criação, alteração de regras e rotas;(AMOSTRA)
- 2.4.5. Fornecer ao executor o planejamento detalhado da mudança quando autorizada, contendo no mínimo:(AMOSTRA)
  - 2.4.5.1. Dispositivos onde serão realizadas as mudanças;(AMOSTRA)
  - 2.4.5.2. Posição da nova regra nos dispositivos;(AMOSTRA)
  - 2.4.5.3. Campos exatos que devem ser alterados ou preenchidos;(AMOSTRA)
  - 2.4.5.4. Informação que deve conter no comentário da regra;(AMOSTRA)
  - 2.4.5.5. Rotas que devem ser criadas ou alteradas;(AMOSTRA)
  - 2.4.5.6. Possibilidade de alteração dos nomes dos objetos;(AMOSTRA)
- 2.4.6. Possuir work-flow nativo para solicitações de criação, alteração e remoção de regras definitivas e temporárias;
  - 2.4.6.1. Deve informar todos os chamados relacionados à regra que será removida bem como a informação do solicitante;
  - 2.4.6.2. Deve informar, aos requisitantes de criação da regra original, que a mesma será removida;
- 2.4.7. Detectar e listar inconsistências entre a configuração ativa nos equipamentos e a última configuração efetuada pela ferramenta;
- 2.4.8. Utilizar para a criação de regras a base de objetos existentes nos dispositivos do tipo firewalls instalados no SERPRO;(AMOSTRA)
- 2.4.9. Permitir a criação de regras múltiplas através de um arquivo de entrada: (AMOSTRA)
  - 2.4.9.1. Gerar requisição de mudança com base no arquivo de entrada;(AMOSTRA)
  - 2.4.9.2. Suportar no mínimo os seguintes arquivos de entrada:(AMOSTRA)
    - 2.4.9.2.1. Coma-separated text values (CSV);
    - 2.4.9.2.2. Microsoft Excel (Ambos XLS e XLSX);
    - 2.4.9.2.3. OpenOffice Spreadsheet (Ambos SXC e ODS);(AMOSTRA)
- 2.4.10. A solução deve possuir templates pré-definidos para solicitação de mudança e permitir a criação de novos pelo administrador;
- 2.4.11. Detectar e validar automaticamente a execução da mudança de acordo com a solicitação aprovada;(AMOSTRA)
  - 2.4.11.1. Caso a mudança tenha sido feita de acordo com o solicitado, encerrar a atividade e notificar os envolvidos;(AMOSTRA)
  - 2.4.11.2. Caso contrário notificar o aprovador;(AMOSTRA)

## 2.5. IMPLEMENTAÇÃO

- 2.5.1. A solução deve ser compatível para a instalação em ambientes virtuais;
- 2.5.2. A solução deve suportar IPv6 nativamente (Internet Protocol version 6);
- 2.5.3. Deve possuir API (Application Programming interface) que permita integração com sistemas externos de controle de chamados que permita a criação, provisionamento, aplicação de regras de firewall e demais fluxos customizados;
- 2.5.4. Deve possuir SDK que permita integração com dispositivos não suportados nativamente;
- 2.5.5. Deve suportar autenticação via AD, LDAP, RADIUS e TACACS;
- 2.5.6. Deve permitir a utilização de base AD e LDAP para a população da base de usuários local;
- 2.5.7. Permitir a integração, no mínimo, com os seguintes sistemas corporativos de acompanhamento de chamados (Change Management Systems):
  - 2.5.7.1. IBM SCCD (Smart Cloud Control Desk);
  - 2.5.7.2. BMC Remedy;
  - 2.5.7.3. HP Service Center;
  - 2.5.7.4. Service Manager;
- 2.5.8. A solução deverá ser entregue integrada com a ferramenta de work-flow SCCD do SERPRO, preparada para todos os fluxos definidos nesta especificação;
- 2.5.9. Os métodos de integração com acompanhamento de chamado deverão ser no mínimo via interface API REST;
- 2.5.10. Deve possuir compatibilidade, no mínimo, com os seguintes dispositivos de segurança do tipo firewall:
  - 2.5.10.1. Check Point Smart Center, VE, VPN-1, VSX, Firewall-1;
  - 2.5.10.2. Check Point Log Servers, P1 CMA, P1 MDS;
  - 2.5.10.3. Cisco ASA, PIX, FWSM;
  - 2.5.10.4. Cisco Routers, VPN Concentrator, CSM, CatOS, IOS;
  - 2.5.10.5. Dell Sonic Wall;
  - 2.5.10.6. BROCADE VDX;
  - 2.5.10.7. Fortinet FortiGate, VDOM;
  - 2.5.10.8. Fortinet FortiManager;
  - 2.5.10.9. Huawei Eudemon;
  - 2.5.10.10. IBM Proventia MFS;
  - 2.5.10.11. Juniper Net-screen, SRX, ScreenOS, VSYS;
  - 2.5.10.12. Juniper E/EX and M/MX routers, NSM with ScreenOS, SA VPN;
  - 2.5.10.13. McAfee Enterprise Firewall 8X, Sidewinder 7X;
  - 2.5.10.14. Palo Alto Networks PAN PA Series, VSYS, Panorama;
  - 2.5.10.15. Secui NXG, MF2;
  - 2.5.10.16. Stonesoft Management Center;
  - 2.5.10.17. IPTables;
- 2.6. CAPACIDADE E QUANTIDADES
  - 2.6.1. A solução deve possuir licenciamento de uso perpétuo para atender 20 (vinte) dispositivos de segurança do tipo firewall, sem nenhuma restrição por falta de licenciamento;
  - 2.6.2. A solução deve ser capaz de gerenciar as políticas de firewalls e roteadores e switches exercendo função análoga a firewall;
  - 2.6.3. As licenças da solução são de uso permanente do SERPRO;
    - 2.6.3.1. Não deve expirar com a alteração de topologia rede e com substituição ou upgrade de componentes e dos ativos monitorados;
  - 2.6.4. A solução deve atender, as três localidades do SERPRO:

2.6.4.1. Regional SERPRO de Brasília: Capacidade de monitorar, analisar e auditar, no mínimo, 5 (cinco) contextos de firewall virtualizados em cluster de dispositivos e 2 (dois) firewall físicos;

2.6.4.2. Regional SERPRO de São Paulo: Capacidade de monitorar, analisar e auditar, no mínimo, 5 (cinco) contextos de firewall virtualizados em cluster de dispositivos e 2 (dois) firewall físicos;

2.6.4.3. Regional SERPRO do Rio de Janeiro: Capacidade de monitorar, analisar e auditar, no mínimo, 5 (cinco) contextos de firewall virtualizados em cluster de dispositivos e 1 (hum) firewall físico;

2.6.5. A gerência da solução deve ser centralizada em uma das Regionais, agregando todos os dispositivos;(AMOSTRA)

2.6.5.1. Deve possuir coletores nas Regionais remotas a fim de melhorar de performance;

2.6.5.2. A gerência da ferramenta deve permitir limitar aos poderes dos administradores ao conjunto de equipamentos de uma determinada regional do SERPRO. (AMOSTRA)

### 3.0 Níveis de serviço e sancionamentos

3.1. O exercício da garantia para retorno do hardware à condição operacional da solução deverá ser realizado conforme critérios abaixo:

3.1.1. 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;

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

Severidade	Descrição	Tipo de Atendimento	Tempo de Atendimento	Tempo de Solução	Observações	Penalidades
1 – Altamente 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 o percurso do técnico até as instalações do SERPRO.	No máximo 6 (seis) horas após a abertura do chamado.	Os chamados classificados com Severidade 1 serão atendidos em horário comercial, ou seja, das 08:00 às 18:00, de segunda-feira a sexta-feira, horário local.	O não atendimento dentro do prazo estabelecido para o chamado, ensejará em aplicação de multa à contratada no valor de 0,2% (zero vírgula dois por cento) do valor contratual, por hora ou fração de hora de atraso.
2 – Crítica	Chamados associados a situações de alto impacto, incluindo os casos de degradação severa de desempenho.	On-site	No máximo 4 (quatro) horas após a abertura do chamado, incluindo o percurso do técnico até as instalações do SERPRO.	No máximo 8 (oito) horas após a abertura do chamado.	Os chamados classificados com Severidade 2 serão atendidos em horário comercial, ou seja, das 08:00 às 18:00, de segunda-feira a sexta-feira, horário local.	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



Severidade	Descrição	Tipo de Atendimento	Tempo de Atendimento	Tempo de Solução	Observações	Penalidades
						hora de atraso.
3 – Alta	Chamados referentes a situações de baixo impacto ou problemas que se apresentem de forma intermitente, incluindo casos em que haja necessidade de substituição de componentes que possuam redundância.	Remoto, com exceção das situações em que seja necessária intervenção física.	No máximo 6 (seis) horas após a abertura do chamado.	No máximo 10 (dez) horas após a abertura do chamado.	Os chamados classificados com Severidade 3 serão atendidos em horário comercial, ou seja, das 08:00 às 18:00, de segunda-feira a sexta-feira, horário local.	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.
4 – Média	Chamados com objetivo de solicitar acompanhamento técnico presencial para o desligamento e posterior ligação de equipamentos em virtude de atividade programada.	On-site	No máximo 24 (vinte e quatro) horas após a abertura do chamado.	Conforme agendamento.	O atendimento deverá ser realizado conforme o agendamento, mesmo que contemple períodos noturnos e dias não úteis. Os chamados classificados com Severidade 4 serão atendidos em horário comercial, ou seja, das 08:00 às 18:00, de segunda-feira a sexta-feira, horário local.	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 décimos por cento) do valor contratual, por hora ou fração de hora de atraso.
5 – 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.	Os chamados classificados com Severidade 5 serão atendidos em horário comercial, ou seja, das 08:00 às 18:00, de segunda-feira a sexta-feira, horário local.	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.

3.2.1. O exercício da garantia para retorno do software à condição operacional deverá 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;

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

Severidade	Descrição	Tipo de Atendimento	Tempo de Atendimento	Tempo de Solução	Observações	Penalidades
1 Altamente 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 6 (seis) horas após a abertura do chamado para resolução ou aplicação de solução de contorno	As soluções de contorno deve ser substituída por aplicação de solução definitiva no prazo máximo de 90 (noventa) dias corridos. Os chamados classificados com Severidade 1 serão atendidos em horário comercial, ou seja, das 08:00 às 18:00, de segunda-feira a sexta-feira, horário local.	O não atendimento dentro do prazo estabelecido para o chamado, ensejará em aplicação de multa à contratada no valor de 0,2% (zero vírgula dois por cento) do valor contratual, por hora ou fração de hora de atraso.
2 – Crítica	Chamados associados a situações de alto impacto, incluindo os casos de degradação severa de desempenho.	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 a abertura do chamado.	Os chamados classificados com Severidade 2 serão atendidos em horário comercial, ou seja, das 08:00 às 18:00, de segunda-feira a sexta-feira, horário local.	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.
3 – Alta	Chamados referentes a situações de baixo impacto ou problemas que se apresentem de forma intermitente, incluindo casos em que haja necessidade de	Remoto, com exceção das situações em que seja necessária intervenção física.	No máximo 6 (seis) horas após a abertura do chamado.	No máximo 10 (dez) horas após a abertura do chamado.	Os chamados classificados com Severidade 3 serão atendidos em horário comercial, ou seja, das 08:00 às 18:00, de segunda-feira a	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

Severidade	Descrição	Tipo de Atendimento	Tempo de Atendimento	Tempo de Solução	Observações	Penalidades
	substituição de componentes que possuam redundância.				sexta-feira, horário local.	hora ou fração de hora de atraso.
4 – Média	Chamados com objetivo de solicitar acompanhamento técnico presencial para o desligamento e posterior ligação de equipamentos em virtude de atividade programada.	On-site	No máximo 24 (vinte e quatro) horas após a abertura do chamado.	Conforme agendamento.	O atendimento deverá ser realizado conforme o agendamento, mesmo que contemple períodos noturnos e dias não úteis.  Os chamados classificados com Severidade 4 serão atendidos em horário comercial, ou seja, das 08:00 às 18:00, de segunda-feira a sexta-feira, horário local.	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.
5 – 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.	Os chamados classificados com Severidade 5 serão atendidos em horário comercial, ou seja, das 08:00 às 18:00, de segunda-feira a sexta-feira, horário local.	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.

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

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

3.2.5. Durante o período de garantia, a contratada deverá assistir remotamente na instalação e uso da solução ofertada;

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

3.2.7. Nos casos de problemas não documentados, as documentações enviadas 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. CANAIS DE ATENDIMENTO

3.3.1. Atendimento através de canal telefônico gratuito 0800 ou tarifação reversa, das 8 horas às 18 horas, de segunda a sexta, excluindo os feriados;

3.3.2. Chamado técnico através de site na Internet, das 8 às 18 horas, de segunda-feira a sexta-feira, excluindo os feriados e canal telefônico gratuito 0800 ou tarifação reversa;

### 3.4. GARANTIA

3.4.1. Para Solução ofertada, a CONTRATADA deverá 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;

3.4.1.1. Caso não haja recomendação específica quanto à periodicidade, a intervenção preventiva deverá ser realizada em intervalos não superiores a 6 (seis) meses, mediante solicitação formal do SERPRO;

3.4.2. A CONTRATADA deverá entregar, a cada intervenção preventiva e corretiva realizada, relatório técnico contendo os procedimentos executados;

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

3.4.4. Para os softwares ofertados, a CONTRATADA deverá prestar, durante o período de garantia, atendimento técnico observando os níveis de serviço especificados neste edital;

### 3.5. ENTREGA MENSAL DE RELATÓRIO

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

3.5.2. 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, data e hora do início de atendimento local se for o caso, data e hora de encerramento ou aplicação de solução de contorno e descrição da resolução adotada;

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

## 4.0 Especificação de valores e forma de pagamento

### 4.1. FORMA DE PAGAMENTO

4.1.1. O pagamento será efetuado no 1º (primeiro) dia útil, após o 20º (vigésimo) dia corrido da data do recebimento definitivo dos equipamentos, indicados nas respectivas notas fiscais e/ou entregues no Protocolo Geral do SERPRO ou através do endereço eletrônico a ser informado pelo Gestor do Contrato;

4.1.2. Constatando alguma incorreção nas notas fiscais ou faturas que desaconselhe o seu pagamento, o prazo será contado a partir da respectiva regularização. Carta de correção só será admitida para regularizar os dados cadastrais do SERPRO;

4.1.3. A Razão Social do SERPRO na nota fiscal e faturas deverá ser: SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS (SERPRO);

4.1.4. A contratada deverá informar o CNPJ que será utilizado na emissão das notas fiscais e faturas;

## **5.0 Justificativa da contratação**

5.1. Todo processo de Consulta Pública está autorizado pelo Diretor de Operações no Memorando Siscor no. DIOPE 009693/2016.

5.2. Realização de Consulta Pública junto ao mercado para verificação e validação das especificações técnicas e níveis de serviço.

## **6.0 Seleção do fornecedor**

6.1. Em atendimento ao estabelecido no Decreto 5.450/2005, por se tratar de serviço comum, assim entendido por decorrência dos padrões de desempenho e qualidade estarem objetivamente definidos por meio de especificações usuais do mercado, a aquisição deverá ser na Modalidade de Pregão, na forma Eletrônica e adjudicação pelo menor valor global;

6.2. Avaliação de Amostra:

6.2.1. Ao licitante classificado em primeiro lugar, a CONTRATANTE exigirá avaliação de amostra, que consiste na comprovação das funcionalidades descritas nas Especificações do objeto deste Termo de Referência;

6.2.2. Após o aceite da documentação comprobatória, cada LICITANTE deverá disponibilizar todos os recursos necessários para a realização de avaliação de amostra;

6.2.3. A entrega dos equipamentos e licenças necessárias à avaliação de amostra deverá ocorrer em até 10 (dez) dias corridos contados a partir da solicitação formal da CONTRATANTE;

6.2.4. O prazo de execução da avaliação de amostra será de 20 (vinte) dias corridos a contar da comunicação da CONTRATANTE;

6.2.4.1. O prazo de avaliação de amostra poderá ser prorrogado a critério do SERPRO;

6.2.5. A critério do SERPRO, as etapas de avaliação de amostra poderão ser dispensadas ou abreviadas para aqueles ativos que sejam de uso corrente no SERPRO ou em seus Clientes, integrando a plataforma instalada em produção;

6.2.6. A aceitação final da proposta de cada LICITANTE somente será realizada após a aprovação em testes de bancada, nas etapas da avaliação de amostra, descritas nesta seção;

6.2.7. A Avaliação prática das EMPRESAS LICITANTES CLASSIFICADAS E APTAS para as etapas da avaliação de Amostra, será realizada com testes de todas as características e funcionalidades exigidas no edital;

6.2.8. Esta etapa caberá às EMPRESAS LICITANTES CLASSIFICADAS E APTAS, para todos os itens e subitens especificados, comprovar na prática, por meio dos testes de bancada, nas etapas da avaliação de amostra, das características e funcionalidades exigidas;

6.2.9. Esta etapa será executada por prepostos do SERPRO em conjunto com os prepostos da EMPRESAS LICITANTES CLASSIFICADAS E APTAS no ITEM específico da aquisição;

6.2.10. Cada ITEM será avaliado em fase sequencial, conforme cronograma que será estabelecido entre as partes, que não poderá ultrapassar os prazos previstos em edital;

6.2.11. Os testes de bancada, nas etapas da avaliação de amostra, serão realizados nas dependências do SERPRO, endereço descrito no ITEM a seguir:

6.2.11.1. REGIONAL BRASÍLIA/DF, SGAN Av. L2 Norte Quadra 601 – Módulo G – Brasília/Distrito Federal, CEP: 70830-900, Telefone Geral: 0XX(61) 2021-9000, Fax: 0XX(61) 2021-9806, INSCRIÇÃO ESTADUAL: 07334743/002-94, INSCRIÇÃO

MUNICIPAL: 07334743/002-94 e CNPJ: 33.683.111/0002-80;

6.2.12. Somente após todos testes de bancada, nas etapas da avaliação de amostra, será definida a EMPRESA LICITANTE VENCEDORA do processo licitatório;

6.2.13. Todos os testes de bancada, nas etapas da avaliação de amostra, e relacionamento dos técnicos da EMPRESA LICITANTE com o SERPRO deverão ser efetuados no idioma português;

6.2.14. Ao fim de cada dia de testes de bancada, nas etapas da avaliação de amostra, deverá ser emitida, assinada e distribuída Ata de Atividades e Ocorrências a todos os presentes;

6.2.15. Se um subitem referente às especificações seja considerado não atendido, a proposta, em avaliação de amostra, será totalmente desclassificada, não sendo corrigidos nos prazos estabelecidos;

6.2.16. Para cada ITEM as licitantes deverão indicar previamente os nomes de, no máximo, 02 (dois) técnicos para participação integral durante a realização dos testes de bancada, nas etapas da avaliação de amostra, Esses técnicos deverão ser representantes legais da licitante, comprovado por meio de documentação de vínculo contratual ou procuração;

6.2.17. A critério de cada licitante, as etapas da avaliação de amostra poderão ser executadas com apoio de no máximo um técnico do fabricante;

6.2.18. Dos técnicos indicados pela licitante, com a solução em teste do respectivo ITEM, apenas um técnico poderá ser substituído após o início dos testes de bancada, nas etapas da avaliação de amostra, desde que seja comunicado formalmente ao SERPRO;

6.2.19. As empresas concorrentes do pregão poderão indicar técnicos (apenas um para cada empresa) para acompanhar os testes de bancada, nas etapas da avaliação de amostra. As indicações deverão ser realizadas com, no mínimo, 2 (dois) dias de antecedência e apenas serão permitidos questionamentos diretos aos técnicos do SERPRO;

6.2.20. No caso de ausência, em qualquer dos períodos durante a realização dos testes de bancada, nas etapas da avaliação de amostra, dos técnicos indicados pelas demais empresas concorrentes do pregão, não serão aceitos quaisquer questionamentos sobre sua realização;

6.2.21. Durante a realização dos testes de bancada, nas etapas da avaliação de amostra, serão permitidas somente 02 (duas) atualizações de software e sistema operacional da solução sob avaliação, visando a correção ou adaptação para atendimento aos requisitos do edital. Essas atualizações poderão corrigir mais de um item simultaneamente;

6.2.22. A critério do SERPRO os testes de bancada, nas etapas da avaliação de amostra, poderão ser reiniciados após atualização de versão;

6.2.23. Os testes deverão ser realizados no horário compreendido entre 09:00 e 17:00 de segunda-feira a sexta-feira;

6.2.24. Avaliação de amostra da solução será exigido:

6.2.24.1. Instalação da solução descrita no item 2.0 deste Termo de Referência, em equipamentos fornecidos pelo SERPRO exclusivamente para testes de homologação;

6.2.25. A CONTRATADA deverá demonstrar as funcionalidades;

6.2.26. A avaliação da amostra será analisada pela CONTRATANTE com o objetivo de aferir a adequação da solução ofertada nas Especificações Básicas do item 2.0;

6.2.27. A CONTRATANTE poderá rejeitar a avaliação de amostra, independentemente da informação contida na proposta, caso os testes de homologação, o equipamento ou software não sejam capazes de cumprir às especificações exigidas;

- 6.2.28. A CONTRATANTE se reserva ao direito de avaliar o contexto do não atendimento de um dos itens para aceitação da solução;
- 6.2.29. A não implementação de algum dos protocolos citados na especificação, poderão ser substituídos, a critério da CONTRATANTE, quando a opção ofertada pela LICITANTE comprovadamente não impactar na interoperabilidade com o legado e na funcionalidade primariamente pedida;
- 6.2.30. A avaliação de amostra da solução ofertada deverá ser instalada sem custo para a CONTRATANTE;
- 6.2.31. A licitante que for reprovada na avaliação de amostra não terá direito a qualquer indenização;
- 6.2.32. Será emitido um relatório sucinto descrevendo os exames realizados e contendo a aprovação ou não da avaliação de amostra;
- 6.3. A LICITANTE com a proposta de menor preço, deverá apresentar em até 2 (dois) dias úteis após solicitação do pregoeiro, documentação técnica do fabricante da solução comprovando o atendimento a todos os requisitos contidos na Especificação do objeto a ser contratado;
- 6.4. Documentação técnica do fabricante:
- 6.4.1. Nessa documentação, a LICITANTE deve fornecer uma planilha ponto-a-ponto indicando documento e página onde consta o cumprimento de cada um dos requisitos das especificações técnicas;
- 6.4.2. Não serão aceitas referências a futuros releases ou versões de produtos para comprovar a existência ou aderência à qualquer quesito desta especificação;
- 6.4.3. Cada documento apresentado deve descrever claramente a referência ao modelo apresentado na proposta, não sendo válidas referências genéricas;
- 6.4.4. Relação de componentes, que compõe a solução, contendo o código do produto (fabricante) e as respectivas quantidades em cada item;
- 6.5. Será aceita Carta do Fabricante, como comprovação de atendimento de requisitos técnicos e de compatibilidade especificados neste edital, apenas para os itens que não constarem na documentação da maioria dos fabricantes ou que não puderem ser mensurados;
- 6.6. Deverá apresentar declaração do fabricante com indicação de rede de assistência técnica autorizada nas localidades como segue, que será apresentada com a proposta comercial: Brasília (DF), Rio de Janeiro (RJ) e São Paulo (SP);
- 6.7. Caso a documentação apresentada, deixe de comprovar o atendimento de um único item da especificação técnica, a proposta será desclassificada, não passando para a etapa seguinte de testes das funcionalidades especificadas;
- 6.7.1. A CONTRATANTE se reserva ao direito de avaliar o contexto do não atendimento de um dos itens para aceitação da solução;
- 6.8. A proposta comercial a ser apresentada pela LICITANTE deverá discriminar os valores unitários e totais de todos os itens que compõem a solução ofertada, incluindo hardware se houver, software e acessórios;

## **7.0 Justificativa para aceitação de preços**

- 7.1. Não se aplica

## **8.0 Gerenciamento contratual**

- 8.1. Obrigações da Contratada:

8.1.1. Garantia, Suporte e Atualização de versão de software.

8.1.2. A garantia da solução de análise e auditoria de regra de firewall, bem como da atualização dos softwares e patches será de 36 (trinta e seis) meses, a partir do

recebimento definitivo do SERPRO;

8.1.3. A garantia engloba sanar dúvidas relacionadas com a instalação, configuração e softwares contratados;

8.1.4. A atualização deverá englobar:

8.1.4.1. Fornecimento de versão, release ou patches mais recentes;

8.1.4.2. Fornecimento de versão mais recente da base de conhecimento;

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

8.1.5. A garantia de 36 (trinta e seis) meses contemplará atendimento técnico quanto à configuração e solução de problemas envolvendo o produto ofertado, bem como a atualização dos softwares;

8.1.6. A garantia deverá cobrir a realização de testes de funcionalidade da solução, visando identificar problemas de interoperabilidade e incompatibilidade com os produtos de firewalls e work-flow existentes;

8.1.7. Caso a solução fornecida seja descontinuada na linha de comercialização do fabricante, durante a vigência da garantia, a contratada deverá manter as condições da garantia nesta contratação explicitada, ou providenciar a substituição por outra solução disponível que executem as mesmas funcionalidades exigidas no edital, sem ônus adicionais para o SERPRO;

8.1.8. Promover a instalação e configuração da solução, incluindo todos equipamentos do tipo firewall, roteadores e switches previstos no projeto, nos ambientes do SERPRO, deixando-os em perfeitas condições de uso;

8.1.9. Responsabilizar-se por toda e qualquer despesa, independente da sua natureza, decorrente das instalações supramencionadas;

8.1.10. A documentação, bem como os manuais necessários para a homologação, deverão estar disponíveis para os representantes do SERPRO;

## 8.2. REPASSE DE CONHECIMENTO

8.2.1. A CONTRATADA deve repassar o conhecimento para as equipes do SERPRO para que as mesmas desenvolvam adaptações evolutivas e manutenção da solução após a sua implantação;

8.2.2. A CONTRATADA deve repassar o conhecimento sem ônus adicional para o SERPRO, incluindo todo o material didático necessário;

8.2.3. O material de aula deverá abordar conteúdo teórico e prático, e deverá ser submetido ao SERPRO para aprovação antes da realização da capacitação;

8.2.4. Após a assinatura do contrato, a CONTRATADA deverá realizar o repasse do conhecimento da solução, que poderá ocorrer em paralelo a fase de instalação;

8.2.5. A CONTRATADA deve prover o repasse de conhecimento dos profissionais do SERPRO para configuração e operação da solução;

8.2.6. A CONTRATADA deve repassar o conhecimento através de profissionais habilitados e credenciados pelos fabricantes ou empresa credenciada para tal finalidade;

8.2.7. Deve ser entregues pela CONTRATADA antes do início do repasse de conhecimento todo o material didático;

8.2.8. A CONTRATADA deverá providenciar a capacitação para 4 (quatro) turmas, sendo 2(duas) turmas em São Paulo e 2(duas) turmas em Brasília, com 8 (oito) participantes cada turma, abordando toda solução ofertada envolvendo teoria e prática, em datas a serem negociadas entre o SERPRO e a CONTRATADA; Além dos participantes de Brasília e São Paulo, 1 (um) funcionário da Regional Porto Alegre, e 3 funcionários da Regional Orto, no Rio de Janeiro deverão ser deslocados para participar



das turmas em São Paulo.

8.2.8.1. A carga horária mínima para cada turma deverá ser de 40 (quarenta) horas;

8.2.8.2. O repasse de conhecimento deve ser prestado em local externo de responsabilidade da contratada, nas capitais de Brasília e São Paulo;

8.2.9. O conteúdo mínimo a ser abordado em cada repasse de conhecimento para a solução fornecida neste contrato, abortando todos itens desta especificação. Sendo que este conteúdo poderá ser modificado posteriormente, a critério do SERPRO:

8.2.9.1. Instruções de instalação, incluindo resolução de problemas;

8.2.9.2. Instruções de manuseio e operação, incluindo resolução de problemas;

8.2.9.3. Devem ser fornecidas as instruções de utilização também em formato de videoconferência;

8.2.9.4. O repasse de conhecimento deverá ser feito com material no idioma português;

8.2.10. A vencedora deverá apresentar uma ementa do repasse que será aprovada pelo SERPRO;

8.2.11. O repasse de conhecimento será avaliado pelos participantes do SERPRO e caso não será atingido a média de 70% pela avaliação das turmas, o repasse deverá ser revisto e realizado novamente;

8.2.12. O repasse de conhecimento deve abortar os módulos: operação básica e avançada da solução de auditoria de firewall, com conteúdo teórico e prático.

### 8.3. PRAZO DE ENTREGA E INSTALAÇÃO PRAZO DE INSTALAÇÃO

8.3.1. A CONTRATADA deverá entregar a solução em até 60 (sessenta) dias corridos a partir assinatura do CONTRATO;

8.3.2. Prazo para instalação é no máximo 30(trinta) dias corridos, contados a partir da data da entrega dos produtos;

8.3.3. A CONTRATADA deve comunicar a data da entrega da solução com no mínimo 5 (cinco) dias de antecedência;

8.3.4. Caso constata-se incoerência com a especificação técnica, falha em algum componente da solução ou problemas de licenciamento, o fornecedor deve providenciar solução em até 5 dias corridos;

8.4. A garantia desta contratação será pelo período de 36 (trinta e seis) meses a contar a data da emissão do Termo de Recebimento;

8.5. O prazo de vigência contratual será de 6 (seis) meses;

8.6. Os serviços a serem contratados não possuem a natureza de serviço continuado sem dedicação exclusiva de mão de obra;

8.7. O objeto da presente contratação está caracterizado como bens ou serviços de informática ou automação, conforme definição constante no Art. 16-A da Lei No. 8.248, de 23/10/1991;

8.8. Com relação a instrução Normativa SLTI/MPOG no 01 de 19 de janeiro de 2010, com relação a sustentabilidade, a contratada ficará responsável pelo devido recolhimento dos consumíveis utilizados, bem como dos resíduos dos processos de manutenção e limpeza dos equipamentos, que deverão ser tratados de forma ambientalmente adequada e respeitando os critérios da referida Instrução Normativa;

8.9. Todas as configurações descritas e que serão homologadas, além de estarem identificadas, garante não só ao FABRICANTE vencedor, como seus concorrentes mensurarem esses resultados, pois trata-se de BEM COMUM, onde todos oferecem as mesmas condições descritas para uso.

8.10. São de responsabilidade da contratada os seguintes itens: frete, seguro, embalagens, manuais, despesa de transporte ou quaisquer custos relacionados a entrega, instalação e repasse de conhecimento.

## 9.0 Considerações gerais

9.1. Projeto Basico para realização da Consulta Pública para aquisição da solução de Análise e Auditoria de Dispositivos de Segurança do tipo Firewalls.

9.2. Atendendo a recomendação da SUPGA não é necessário o envio do Projeto Basico para que seja efetuada a analise para aprovação e encaminhamento das ações necessárias. Neste momento, a solicitação da consulta pública deve ser encaminhada através de SISCOR.

## **Elaboração**

Data : 28/03/2016

BRAZ CANUTO HERMOGENES - 08085757

COGTI/CISPO/CISRE

## **Elaborador Adicional**

Data : 28/03/2016

HEITOR DE SA ALENCAR E MORAES - 21088748

COGTI/CISPO/CISRE

## **Anexos**

Arquivo: [SISCOR DE AUTORIZACAO PARA CONSULTA PUBLICA DA SOLUCAO ANALISE DE REGRAS FIREWALL](#)