

Projeto Básico SUPCD 00732/2010

Título

**CONSULTA PÚBLICA PARA CONTRATAÇÃO DE SOLUÇÃO DE MONITORAÇÃO E
AUDITORIA EM BANCOS DE DADOS DE PLATAFORMA AVANÇADA
1a Versão**

1.0 Objeto

Contratação de Solução de Monitoração e Auditoria de Segurança em Base de Dados de Plataforma Avançada.

2.0 Especificação do Objeto

2.1. Configuração Única - Solução de Monitoração e Auditoria de Segurança em Base de Dados de Plataforma Avançada que trabalhe em alta disponibilidade, ou seja, com todos os componentes redundantes e tolerantes à falhas, com as seguintes características técnicas:

2.1.1. Deve monitorar e registrar os seguintes eventos das bases de dados de plataforma avançada:

2.1.1.1 Alterações em Esquemas de Dados (CREATE, DROP, ALTER) – DDL (Data Definition Language);

2.1.1.2. Alterações em Dados (INSERT, UPDATE, DELETE) – DML (Data Manipulation Language);

2.1.1.3. Acessos a Dados (SELECT, EXECUTE) – DQL (Data Query Language);

2.1.1.4. Eventos de segurança (GRANT, REVOKE, DENY) – DCL (Data Control Language).

2.1.1.5. Logins válidos, inválidos e rejeitados;

2.1.1.6. Logout;

2.1.1.7. Tentativas de acesso ao repositório de auditoria;

2.1.1.8. Atividades de gerenciamento de contas de usuários (criação, alteração de senha, etc.);

2.1.1.9. Alterações nas configurações de segurança;

2.1.1.10. Registro de criação, exclusão e alocação de objetos físicos de bancos de dados;

2.1.1.11. Registro de log de mensagens do banco de dados;

2.1.1.12. Tentativas de acesso ao sistema operacional por comandos do banco de dados;

2.1.1.13. Finalização (shutdown), erros e reinicialização do banco de dados comandados por instruções SQL;

2.1.1.14. Backup e restore de banco de dados.

2.1.2. Monitorar e registrar métricas de uso de banco de dados incluindo comandos SQL

de longa duração de execução, usuários mais ativos e últimos relatórios acessados para os usuários e tabelas.

2.1.3. Deve independer da tecnologia de hardware de processadores e do sistema operacional e softwares básicos utilizados nos servidores de bancos de dados, tais como:

- * IBM AIX 5, AIX 6.1 e superior;

- * Windows 2000 Advanced Server, Windows 2003 Enterprise Edition R1, Windows 2003 R2 x64, Windows 2008;

- * VMWARE ESX, versão 3.0 e superior;

- * HP-UX 11 e superior;

- * Red Hat Enterprise LINUX Advanced Server, versão 2.1 e superior;

- * Suse LINUX Enterprise Server, versão 8 e superior;

- * CentOS 5 e superior.

2.1.4. Deve suportar os seguintes Softwares Gerenciadores de Banco de Dados, independente de tecnologia de Hardware e Sistemas Operacionais, inclusive operando em cluster com no mínimo, dois servidores ou partições em cada cluster:

- * Oracle ® 8.0.3, 8.1.7, 9.1, 9.2.0.1 & 10g ou superior;

- * IBM ® DB2 ® UDB 8.0 ou superior;

- * Microsoft ® SQL Server, 2000 & 2005 ou superior;

- * MYSQL 4.1 e 5.0 ou superior;

- * PostGreSQL 7.4, 8.1, 8.2, 8.3 ou superior.

2.1.5 Deve ser composta por conjunto de software e appliance dedicado e altamente seguro que trabalhe em modo invisível (stealth mode, IP-less);

2.1.5.1. O Appliance deve possuir sistema operacional especialmente configurado para este fim e que implemente recursos de segurança elevada, permitindo o acesso somente através da interface de gerenciamento da solução;

2.1.5.2. A utilização e administração do appliance não deve depender de acesso direto ao sistema operacional (através de usuário administrador/root, system ou qualquer outro que proporcione acesso ao sistema operacional) nem requerer conexões externas via Telnet e Ftp;

2.1.5.3. Toda a comunicação entre o appliance e os módulos clientes deve ser de forma criptografada;

2.1.5.4. O sistema de gerenciamento do appliance deve prover garantias de segurança, integridade e não-repúdio, dos arquivos ao histórico de auditoria, impedindo que usuários administradores eliminem registros, suspendam a gravação ou alterem dados armazenados;

2.1.5.5. O Appliance deve possuir certificação FCC classe A ou certificação de compatibilidade com a norma IEC-60950 ou similar emitida pelo INMETRO ou por laboratório credenciado pelo INMETRO;

2.1.6. Deve empregar mecanismo de captura de pacotes seguro que permita ao gestor garantir a monitoração e coleta de todos os comandos executados e assim garantir a geração de trilhas de auditoria fidedignas;

2.1.7. Deve ser de instalação simples e funcional, e requerer baixo esforço de manutenção;

2.1.8. Deve possuir recurso de gerenciamento centralizado, permitindo gerenciar o sistema de vários pontos da rede de forma segura e configurar políticas e regras de forma centralizada;

2.1.9. Deve ser dotado de arquitetura expansível, permitindo adicionar pontos de monitoração distribuída totalmente integrados (através do uso de um modelo concentrador);

2.1.9.1. Toda a transmissão de dados entre os componentes de um sistema distribuído deve ser criptografada e digitalmente assinada;

2.1.9.2. Deve permitir a administração e gerenciamento centralizado de múltiplas redes dispersas geograficamente e elevados volumes de processamento;

2.1.10. Deve registrar atividades executadas diretamente na console do banco de dados;

2.1.11. Deve operar sem a utilização de "triggers" nos bancos de dados, sem a necessidade de acessar os registros de transações dos bancos (transaction logs), sem comprometer a segurança e a performance do banco de dados, sem a necessidade do recurso de "audit" estar ligado, e ainda assim deve fornecer granularidade e 100% de visibilidade sobre toda a atividade do banco de dados, com mínimo impacto sobre a infraestrutura, os servidores de banco de dados, as aplicações e não depender de análise de logs de bancos de dados e aplicações ou de processos que se conectem ao banco de dados;

2.1.12. Deve possuir capacidade de monitorar e proteger o tráfego local (conexões via terminal services e/ou acesso físico ao servidor, bem como tráfego entre cliente e servidor localizados na mesma máquina física) às bases de dados através de tecnologia própria de forma segura e persistente, sem a necessidade de alterar configurações do sistema gerenciador de banco de dados;

2.1.13. Deve implementar funcionalidade que permita monitorar servidores de bancos de dados localizados no SERPRO e/ou escritórios remotos a partir de uma única plataforma e de forma segura e persistente, evitando sempre que possível a instalação de agentes intrusivos ao banco de dados;

2.1.14. Deve incorporar recursos (APIs e outros mecanismos) que permitam integrar informações de quaisquer sistemas de 3 (três) ou mais camadas à solução de monitoramento, permitindo o registro de atributos específicos do usuário final da aplicação e da função de negócio relacionada ao comando (chave de acesso, endereço IP, URL, entre outros);

2.1.15. Deve possuir repositório de dados de auditoria segregado e altamente seguro que não permita acesso de usuários administradores de sistema operacional e banco de dados (SYSTEM, DBA, etc.);

2.1.15.1. O repositório de armazenamento local, deve permitir manter todas as informações coletadas pelo período mínimo de 180 dias;

2.1.16. Deve possuir interface amigável, do tipo GUI, que permita implementar a separação de responsabilidades requeridas pelos auditores;

2.1.17. Deve possuir funcionalidade integrada para geração automática e programada de relatórios tipo painel de controle (Security Balanced Scorecard) com a visão instantânea de indicadores-chave da segurança do Banco de Dados, permitindo analisar constantemente as vulnerabilidades das bases de dados. Estas medições podem ser obtidas sistematicamente e automaticamente em tempo real e/ou em bases históricas, realizando uma comparação da segurança verificada no Banco de Dados em relação às políticas de segurança pré-estabelecidos(SLAS);

2.1.18. Deve disponibilizar recurso de mapa de acesso cliente-servidor, que forneça uma visão instantânea das interações das “Aplicações” e “Clientes” com o Banco de Dados de forma visual. O gráfico resultante deverá ter recursos de personalização variada permitindo visualizar comandos específicos executados nas bases monitoradas, identificando quais as aplicações, usuários e endereços IP que originaram as chamadas, permitindo ainda a utilização de “drill-down” automático a partir de qualquer entidade representada no gráfico;

2.1.19. Deve exportar relatórios para formato CSV, texto ou PDF para análises e apresentações independentes;

2.1.20. Deve implementar recursos de detecção, prevenção de intrusões e geração de alertas em tempo-real baseado em informações da rede, aplicação e banco de dados, podendo agir como um verdadeiro firewall de banco de dados e aplicação, através de políticas flexíveis implementadas pelo usuário, incluindo entre outras funcionalidades: Terminate session (cliente recebe mensagem indicando que a sessão foi terminada), Drop session (nenhuma resposta é enviada e o cliente tem a impressão de que a sessão travou);

2.1.21. Deve permitir implementar política de controle de abertura de sessões nos bancos de dados através de envio de comandos do tipo TCP RESET a fim de derrubar conexões que infrinjam a política vigente, mesmo em implementações onde o appliance é implementado em modo passivo;

2.1.22. Deve permitir a tradução (alias) seletiva de informações técnicas (endereços IP, nomes de tabelas e aplicações) para facilitar a leitura das informações por usuários não técnicos e permitir a proteção dos dados;

2.1.23. Deve possuir recurso de geração automática de registro de comportamento médio (baseline) para controle de acesso determinístico para qualquer atividade dos bancos de dados permitindo implementar políticas de controle de acesso com precisão, levando em conta o comportamento histórico dos usuários;

2.1.24. Deve permitir a configuração automática de DNS lookup a fim de traduzir endereços IP para formato texto;

2.1.25. Deve possuir aplicações de workflow e gerenciamento de auditoria de alto nível incorporadas à solução, permitindo a utilização do produto por um grupo de trabalho e conseqüente segregação de responsabilidades;

2.1.26. Deve monitorar e proteger em único equipamento múltiplos sistemas de bancos de dados simultaneamente conforme listado no item 2.1.4;

2.1.27. Deve implementar recursos de segurança adaptativa e baseada em rede com inteligência na camada de aplicação para prevenir acessos maliciosos ou não-autorizados à central de dados corporativos, tanto por usuários internos quanto externos;

2.1.28. Deve inspecionar em profundidade todo o tráfego de rede e realizar análises detalhadas do dialeto SQL a fim de detectar e bloquear comandos com base em política de acesso e armazenar histórico detalhado em formato relacional a fim de permitir flexibilidade e agilidade em processos de auditoria;

2.1.29. Deve permitir agendamento das tarefas para avaliação automática e contínua das exceções configuradas, permitindo gerenciar o fluxo de trabalho das equipes de auditoria através da geração de "to-do-list" para cada responsável e/ou envolvido no processo, automatizando a distribuição de informações (relatórios, assessments de segurança, trilhas de auditoria) e responsabilização dos envolvidos pelo uso de assinaturas eletrônicas;

2.1.30. Deve capturar e auditar todos os comandos SELECT, todas as operações DML (Data Manipulation Language) e DDL (Data Definition Language) realizadas, sendo capaz ainda de rastrear todas as alterações feitas nos objetos dos Bancos de Dados, incluindo "quem" as fez, "quando" foram executadas e informar com precisão o "que" foi alterado;

2.1.31. Deve capturar e auditar todos os erros (incluindo a descrição do código de erro) gerados pelos bancos de dados, permitindo detectar ameaças e ineficiências prontamente;

2.1.32. Deve capturar e gerar relatórios de todos os comandos SELECT executados, permitindo o seu completo rastreamento através do fornecimento de informações sobre o emissor do comando (usuários de sistema operacional, banco de dados e aplicação), a origem de sua execução, o exato comando realizado e os objetos de banco de dados relacionados ao comando;

2.1.33. Deve gerar alerta em tempo-real com base na execução de comandos SQL específicos (SELECT);

2.1.34. Deve realizar auditoria de acessos realizados aos bancos de dados, incluindo informações de logins, IP de origem e destino, data e hora, rede e programa fonte;

2.1.35. Deve executar auditorias completas manuais e automatizadas de usuários específicos, permitindo revisão de todos os comandos executados;

2.1.36. Deve ter a capacidade de fornecer uma interface com diversos relatórios, pré-moldados e personalizados em tempo de execução, que suportem diversos níveis de "drill-downs" para que se possa compreender facilmente por quem, em que, de onde e como se dão as atividades nos bancos de dados, e que possa ser acessado de forma segura a partir de qualquer ponto de rede;

2.1.37. Deve ter funcionalidade de agrupamento de objetos (tabelas e colunas sensíveis,

endereços IP) e atividades comuns para fins de relatórios e alertas;

2.1.38. Deve rastrear a execução de “stored procedures”;

2.1.38.1. Deve identificar quem executou a “stored procedure” ;

2.1.38.2. Deve identificar quando “stored procedure” foi executada;

2.1.38.3. Deve auditar a criação e alteração de "stored procedures";

2.1.38.4. Deve identificar "stored procedures" que potencialmente afetem determinados objetos considerados críticos e permitir;

2.1.39. Deve rastrear todas as alterações relacionadas a segurança das permissões de acesso;

2.1.39.1. Deve rastrear todas as alterações de usuários e direitos (roles), incluindo criação, deleção, modificação de usuários, cargos e de permissões específicas (grants), tais como comandos GRANT, SET ROLE, REVOKE, DBCC, BACKUP, RESTORE e KILL, assim como toda e qualquer atividade sobre estruturas do banco de dados;

2.1.40. Deve capturar e armazenar toda a atividade de login dos bancos;

2.1.40.1. Deve registrar todas as tentativas de login direcionadas aos bancos de dados, inclusive aquelas que ocorrerem sem sucesso, identificando os endereços IP, nomes de usuários e programas fonte associados ao login, além de permitir a geração de alertas em tempo real sempre que tais atividades ocorram;

2.1.41. Deve capturar e armazenar as informações sobre a origem do comando executado no banco de dados, o produto deve rastrear qual host foi usado, o usuário do sistema operacional (OS user) para este host e a aplicação que foi utilizada para submeter este comando ao banco de dados;

2.1.42. Deve ser capaz de realizar auditorias seletivas, como por exemplo, realizar a auditoria de somente alguns usuários específicos;

2.1.43. Deve prover funcionamento simultâneo com todos os tipos (fabricantes) de Bancos de Dados relacionais listados no item 2.1.4, e armazenar todas as informações em um único repositório;

2.1.44. Deve manter os dados monitorados armazenados em ambiente seguro, sem permissão de acesso aos administradores de banco de dados, devendo possuir ainda as funcionalidades de export/purge manual e automática a fim de gerenciar o armazenamento de longo prazo das informações;

2.1.45. Deve permitir o envio de alerta em tempo real quando algum parâmetro (threshold) for atingido ou quando algum evento específico acontecer, nestes casos o produto deve enviar e-mails de alerta ou traps SNMP ou eventos de syslog;

2.1.46. Deve permitir a criação de alertas personalizados que possam estar integrados à execução de rotinas e procedimentos automatizados definidos pelo usuário;

2.1.47. Deve detectar e reportar o uso de práticas de segurança inadequadas, como por exemplo, o compartilhamento de chaves de acesso entre vários usuários, acesso de

usuários tipo SYSTEM e administradores às bases de produção, acessos através de aplicações não autorizadas, entre outros;

2.1.48. Deve gerenciar o crescimento dos dados armazenados, fornecendo opções de armazenamento (archiving), e rotinas de archive e purge;

2.1.49. Deve possuir automação e integração do processo de backup das informações do repositório de auditoria com IBM Tivoli Storage Manager (TSM);

2.1.49.1. Todo o backup armazenado deve ser criptografado e digitalmente assinado;

2.1.49.2. O Backup somente poderá ser restaurado a partir do appliance;

2.1.50. Deve implementar recursos de detecção e prevenção de extrusões e geração de alertas em tempo-real das informações que são extraídas dos bancos de dados baseado em políticas que definem padrões de dados sensíveis e volume de registros consultados;

2.1.51. Deve possuir recurso de segurança e auditoria para rastrear alterações de objetos externos críticos ao banco dados tais como variáveis de ambiente e arquivos de configuração do SGBD a fim de que mudanças estruturais, permissões, dados e configurações sejam imediatamente detectadas e reportadas;

2.1.52. Deve implementar funcionalidade de monitoração de acesso a dados não-estruturados armazenados em servidores de arquivo compartilhados através da monitoração de protocolos de redes (compartilhamento de redes e FTP).

2.1.53. Requisitos de performance mínimos:

2.1.53.1. Não deverá causar impacto na performance das bases de dados monitoradas e da rede;

2.1.53.2. Analisar e inspecionar de forma bidirecional o conteúdo (payload) do acesso de, no mínimo, 10.000 (dez mil) transações simultâneas/seg;

2.1.53.3. Deve suportar, no mínimo, 200 (duzentas) máquinas servidoras com banco de dados relacionais instalado, listados no item 2.1.4, independente de plataforma.

2.1.53.4. Deverá operar em modo promíscuo, ou seja, não deverá ser intrusivo aos sistemas gerenciadores de banco de dados a fim de não acarretar aumento de consumo de processamento no SGBD.

2.1.54. Requisitos de Gerenciamento e Documentação da Infraestrutura de Segurança de Banco de Dados:

2.1.54.1. Permitir gerenciamento via interface gráfica (GUI – Graphical User Interface) e SSH (Secure Shell);

2.1.54.2. Permitir gerenciamento centralizado;

2.1.54.3. Permitir o gerenciamento de políticas (bloqueio de acesso inapropriado e construção de políticas);

2.1.54.4. Suportar dispositivos de gerenciamento redundante;

2.1.54.5. Permitir importação e exportação dos arquivos de configuração do dispositivo inteiro ou de aplicações individuais;

2.1.54.6 Permitir a atualização de updates sem necessidade de parada total do ambiente, ou seja, sem a parada total da solução e seus serviços atendidos;

2.1.54.7. Permitir updates via interface gráfica de gerenciamento da solução;

2.1.54.8. Suportar reverter para a versão anterior do software após um update, caso necessário;

2.1.54.9. Gerenciar backup e restore do banco de dados de auditoria e log;

2.1.54.10. Gerenciar espaço dedicado ao banco de dados de auditoria e log;

2.1.54.11. Ter funcionalidade de monitorar consumo de espaço em disco com objetivo de identificar necessidade de expansão;

2.1.54.12. Garantir a performance do repositório de auditoria e log;

2.1.54.13. Deve ter funcionalidade de gerência do ambiente da Solução adquirida neste edital, devendo ser gerenciados/monitorados percentuais de uso de placas de rede da solução, customização de alertas, análise de performance, incluindo o tratamento de dados históricos e uso de console local e remota;

2.1.55. Requisitos de Autenticação:

2.1.55.1. Deverá ser fornecido método para controle de autenticação para o acesso à interface da Solução;

2.1.55.2. Garantir que senhas utilizadas para autenticação do usuário na solução atendam aos requisitos mínimos de complexidade (tamanho, regras de uso, e composição);

2.1.55.3. A solução deverá gerar e disponibilizar registros/logs ou relatórios de uso e acessos;

2.1.55.4. Permitir autenticação das chaves de usuários através de mecanismos LDAP, Radius, RSA SecurID;

2.1.56. Requisitos de Notificação de Eventos Monitorados e Dados Armazenados:

2.1.56.1. Deve prover facilidade para configuração de Atividades suspeitas;

2.1.56.2. Deve gerar alertas em Tempo Real, através do envio de e-mails, traps SNMP ou eventos de syslog;

2.1.56.3. Deve garantir que nenhum alerta seja perdido;

2.1.56.4. Deve armazenar as seguintes informações:

* Quem (usuário do banco, usuário do sistema);

* Onde (tabelas, colunas, objetos);

- * Como (comandos, operações);
- * Quanto (quantidade de linhas);
- * Quando (data, horário, tempo decorrido);
- * De Onde (host/computador, endereço IP);
- * Com o Quê (ferramentas, aplicações).

2.1.56.5. Deve registrar a identificação de sucesso ou falha de qualquer interação via SQL com o banco de dados.

2.1.57. Deve possuir funcionalidade de mascaramento dos dados armazenados:

2.1.57.1. Deve prover facilidade para definição e criação de políticas de mascaramento;

2.1.58. Deve possuir funcionalidade para criptografia de dados armazenados:

2.1.58.1 Deve suportar os seguintes algoritmos de criptografia:

- * DES
- * 3 DES
- * AES
- * RC4

2.1.58.2. Deve criptografar os dados armazenados de forma transparente ao tráfego de dados do Banco de Dados, na realização das cópias de segurança e exportações de dados;

2.1.58.3. Deve ter funcionalidade para criptografar todo o Banco de Dados ou partes específicas (tabelas, colunas e etc);

2.1.58.4. Deve ser transparente para as aplicações que acessam os Banco de Dados criptografados, ou seja, não deverá ter necessidade de re-codificação de aplicativos;

2.1.58.5. Deve suportar a criptografia de dados do tipo BLOB - Binary Large Object e CLOB - Character Large Object

2.2. Análise do ambiente atual para implementação da Solução de Monitoração e Auditoria em Bases de Dados de Plataforma Avançada dos ambientes de Brasília e São Paulo para a solução ofertada:

2.2.1. Levantamento da Arquitetura Atual e elaboração de Relatório da Situação atual que contemple relação de todos os servidores, bases de dados, análise de segurança, bem como apresentação do ambiente e arquitetura proposta;

2.2.2. Desenho do ambiente reestruturado, considerando as melhores práticas de mercado;

2.2.3. Apresentação do ambiente sugerido para aprovação pelo SERPRO;

2.2.4. Criação e apresentação do projeto executivo e cronograma das migrações dos ambientes para a nova solução;

2.2.5. A Contratada deverá executar todo o serviço necessário à configuração nos ambientes solicitados observando todas as políticas de segurança hoje existentes no SERPRO;

2.2.6. Deverá ser entregue ao SERPRO um Relatório da Situação Final do ambiente com a solução implantada.

2.3. Local de entrega e instalação:

2.3.1. A Solução de Monitoração e Auditoria de Segurança em Base de Dados de Plataforma Avançada deverá ser entregue e instalada nas Regionais do SERPRO de Brasília e São Paulo, conforme endereços abaixo:

SERPRO Regional Brasília: SGAN Av. L2 Norte Quadra 601 Módulo G - Brasília - DF, CEP: 70.830-900; CNPJ: 33.683.111/0002-80;

SERPRO Regional São Paulo: Rua Olívia Guedes Penteado, 941 - Capela do Socorro, São Paulo - SP, CEP: 04.766-900; CNPJ: 33.683.111/0009-56.

2.4. Do prazo de entrega, da instalação e do aceite da solução:

2.4.1. Entrega total da Solução:

2.4.1.1. Os equipamentos e Softwares da Solução de Monitoração e Auditoria de Segurança em Base de Dados de Plataforma Avançada, bem como os cabos, trilhos e customizações necessárias deverão ser entregues em até 150 (cento e cinquenta) dias corridos, após a assinatura do contrato;

2.4.1.2. Entende-se por cumprimento do prazo de entrega o recebimento total da Solução. O não cumprimento rigoroso do prazo de entrega, ou entrega parcial, ou entrega de configuração inferior a solicitada implicará em rescisão do contrato a ser firmado entre o SERPRO e a contratada;

2.4.1.3. A falta de instalação de um ou mais equipamentos e/ou produtos constitui-se em motivo de suspensão de todos os compromissos financeiros. Enquanto perdurar a falta da instalação ou a instalação incompleta, permanecendo a situação por mais de 30 (trinta) dias corridos, o contrato poderá ser rescindido, ficando a critério do SERPRO;

2.4.1.4. A Solução, cabos, trilhos, softwares, documentações, bem como os demais equipamentos, deverão ser entregues acondicionados adequadamente em caixa(s) lacrada(s), de forma a resistir à armazenagem e permitir completa segurança durante o transporte;

2.4.1.5. Caso os equipamentos sejam diferentes das especificações ou apresentem defeitos serão considerados não entregues e a contagem do prazo de entrega não será interrompida devido à rejeição dos mesmos;

2.4.2. Serviços de Análise e Instalação da solução:

2.4.2.1. A contratada deverá, em até 45 (quarenta e cinco) dias corridos após a assinatura

do contrato, realizar serviço de instalação operacional da solução para posterior configuração e customização;

2.4.2.2. A contratada deverá, em até 60 (sessenta) dias corridos após a assinatura do contrato, realizar serviço para análise do ambiente conforme descrito no item 2.2.;

2.4.2.3. Os serviços de configuração e customização da Solução no ambiente de Brasília e de São Paulo deverão ser entregues em até 150 (cento e cinquenta) dias corridos, após a assinatura do contrato;

2.4.2.4. A contratada deverá garantir a presença de, no mínimo, um técnico (hardware/software) nos locais de instalação dos equipamentos, até que os mesmos sejam entregues para a produção de serviços.

2.4.3. Aceite da Solução:

2.4.3.1. O aceite será realizado em 3(três) etapas:

2.4.3.1.1. 1ª Etapa:

2.4.3.1.1.1. O aceite será feito em até 10 (dez) dias úteis após a entrega dos equipamentos e sua instalação, deixando-os em condições operacionais nas Regionais de Brasília e São Paulo conforme item 2.4.2.1;

2.4.3.1.2. 2ª Etapa:

2.4.3.1.2.1. O aceite será feito em até 10 (dez) dias úteis após a conclusão de todas as atividades previstas no item 2.4.2.2;

2.4.3.1.3. 3ª Etapa:

2.4.3.1.3.1. O aceite será feito em até 10 (dez) dias úteis após a conclusão de todas as atividades previstas no item 2.4.2.3;

2.4.3.2. Para todas as etapas o aceite somente será realizado depois de minucioso teste de funcionamento pela equipe do SERPRO e da contratada. Por meio desses testes, preceder-se-á a checagem das perfeitas condições físicas dos equipamentos e perfeito funcionamento dos softwares e hardwares, bem como do respectivo funcionamento e das especificações técnicas constantes no edital, considerando-se as características técnicas ofertadas pela contratada;

2.4.3.3. Para todas as etapas, deverá ser entregue, pela contratada, o Relatório de Instalação, contendo:

2.4.3.3.1. Confirmação de todos os equipamentos e perfeito funcionamento do hardware e do software;

2.4.3.3.2. Identificação de cada produto instalado (marca, modelo, versão, número de série, ano de fabricação, etc);

2.4.3.3.3. Registro de nome, matrícula, data e assinatura do técnico responsável pela contratada e do técnico do SERPRO;

2.4.3.4. Quando do aceite pelo SERPRO o mesmo deverá fazer anotações no próprio

relatório de instalação, o qual deverá ser repassado a contratada para que seja providenciada a correção necessária se houver, sem prejudicar o cronograma de instalação e sem gerar ônus ao SERPRO;

2.4.3.5. O relatório de instalação não isenta a contratada das responsabilidades sobre o pleno funcionamento dos produtos, o qual deverá ser estendido ao longo de todo o período de garantia da Solução, ou seja, 24 (vinte e quatro) meses.

2.5. Adequação da Solução ao Ambiente do SERPRO:

2.5.1. Execução do plano de implementação do ambiente apresentado e aprovado pelo SERPRO conforme cronograma do item 2.5.22;

2.5.2. A contratada deverá ainda executar todo o serviço necessário a disponibilização da solução (serviços de instalação, físicas, lógicas, análise de performance, implementação da segurança, regras, alertas), conforme solicitado no Edital;

2.5.3. A Contratada, após a conclusão dos serviços de instalação e configuração, deve realizar junto aos técnicos de segurança da SUPCD testes de funcionalidade para constatar que os produtos foram instalados e configurados de acordo com os requisitos técnicos e parâmetros de configuração solicitados;

2.5.4. Teste de funcionalidade dos produtos especificados, integrando ao ambiente de rede e equipamentos existentes, buscando solucionar os eventuais problemas que possam ocorrer;

2.5.5 A coleta de eventos das bases de dados monitoradas;

2.5.6. A geração de pelo menos 05 (cinco) alertas com base nas regras definidas no projeto de implantação;

2.5.7. A emissão de pelo menos 03 (três) relatórios definidos no projeto de implantação;

2.5.8. A emissão de pelo menos 01 (um) relatório customizado pela equipe do projeto;

2.5.9. A Contratada deverá providenciar todos os módulos de software e hardware da solução necessária à execução completa dos testes de homologação;

2.5.10. Após adequação da solução no ambiente do SERPRO o técnico da Contratada realizará o acompanhamento e otimização de regras e resolução de problemas operacionais;

2.5.11. Após adequação da solução no ambiente do SERPRO a Contratada deve elaborar Documentação Técnica, contendo todas as configurações efetuadas e as descrições das características e recursos utilizados;

2.5.12. A solução deverá prever a inclusão de novos equipamentos para futura escalabilidade da própria solução ofertada, sem a necessidade de paradas, inclusive dos serviços;

2.5.13. Durante o processo de implementação da solução nenhum servidor e/ou ambiente/aplicação poderá sofrer interrupção nos serviços, à exceção dos previamente acordados com o SERPRO. A contratada deverá entregar em sua análise, Relatório de Situação Atual e relação de todos os ambientes que necessitem de paradas com seus

respectivos tempos;

2.5.14. Deverá ser fornecida, em até 10 (dez) dias corridos após a assinatura do contrato, uma descrição completa com datas e recursos envolvidos da contratada e do SERPRO, para a realização dos serviços de instalação da solução, bem como todos os softwares ofertados (instalação, configuração, segurança, otimização de performance). Os recursos solicitados ao SERPRO deverão passar por processo de avaliação e aprovação;

2.5.15. Após a instalação e execução de todos os serviços o SERPRO terá um prazo de até 15 (quinze) dias corridos para realização de testes de funcionalidade e performance, sendo que as funcionalidades dos ambientes atuais deverão ser mantidas;

2.5.16. O SERPRO deverá emitir termo de aceite após a realização de testes, que deverá ser o documento de ateste para parte do pagamento, conforme descrito neste edital;

2.5.17. O resultado da análise, bem como todas as informações levantadas e serviços realizados, não poderão ser divulgados sem a prévia autorização do SERPRO. A contratada deverá fornecer, na assinatura do contrato, Termo de Confidencialidade assinado comprometendo-se a não divulgar nenhuma informação sobre a aquisição, implementação da solução e definição da solução. Ou seja, nenhuma informação poderá ser divulgada sem a expressa autorização do SERPRO através da equipe técnica de segurança da Superintendência Centro de Dados;

2.5.18. Em caso de impossibilidade de conexão dos "appliances" aos switches do SERPRO, causada por indisponibilidade de portas do tipo "Port Span", a licitante deverá fornecer mecanismos que viabilizem a conexão;

2.5.18.1. Em caso de necessidade de utilização de agentes, estes somente poderão ser utilizados após avaliação do SERPRO sem comprometer a segurança e performance dos servidores e do ambiente;

2.5.19. Em hipótese alguma será aceita a conexão dos "appliances" ofertados aos switches de redes do SERPRO através de dispositivos passivos do tipo HUB;

2.5.20. A Solução não deverá ter um único ponto de falha. Para os demais casos em que não se tenha o recurso necessário, o SERPRO deverá ser alertado, por escrito, para que seja providenciada a contratação do componente para compor a redundância ou a aprovação de que aquele equipamento em específico não deverá ter redundância no acesso. Será de responsabilidade do SERPRO o acionamento as equipes técnicas dos fabricantes dos equipamentos que fazem parte da rede SERPRO, caso sejam levantados durante a execução dos serviços problemas relativos à matriz de compatibilidade e características dos equipamentos e/ou atualizações de firmwares;

2.5.21. Será de responsabilidade da contratada a implementação da interoperabilidade da solução objeto deste Edital e os atuais, Switchs, Firewall, IDS, IPS, roteadores, Network Taps, Placas de rede. A compatibilidade e a operabilidade entre os novos equipamentos e os atuais serão sempre solicitadas pelo SERPRO, quando da aquisição de um novo equipamento, ficando a cargo da contratada entregar documentação atualizada da topologia do ambiente implantado e configurado conforme solicitação do edital (layout, nível de firmware, utilização e configuração de portas, ligações, regras).

2.5.22. Quadro resumo do cronograma de atividades da contratada após assinatura do contrato:

Itens	Dias corridos após assinatura do contrato (limite)	Atividades
01	10	Apresentar cronograma de atividades e necessidades de recursos envolvidos da contratada e do SERPRO (Ref. Item 2.5.14.)
02	45	Entrega dos equipamentos. (Ref. Item 2.4.2.1.)
03	60	Realizar serviço para análise do ambiente a ser implantada a solução. (Ref. Item 2.4.2.2.)
04	150	Iniciar a capacitação técnica. (Ref. Item 9.3.3.)
05	150	Configuração da Solução no ambiente de Brasília e de São Paulo. (Ref. Item 2.4.2.3.)

3.0 Níveis de Serviço

3.1. Suporte técnico ao(s) equipamento(s) ofertado(s):

3.1.1. Possuir suporte técnico para o(s) appliances ofertado(s), bem como para os demais acessórios integrantes da proposta, durante o período de vigência da garantia, assegurando prazos de atendimento compatíveis com a instalação, ou seja, 24 (vinte e quatro) horas por dia e sete (7) dias por semana (à exceção dos chamados de Severidade 4);

3.1.2. O atendimento aos chamados deverá obedecer a seguinte classificação quanto ao nível de severidade:

Severidade	Descrição	Tipo de Atendimento	Tempo de Atendimento	Tempo de Solução
1 - Crítica	Chamados referentes a situações de emergência ou problema crítico, caracterizados pela existência de ambiente paralisado	On-site	No máximo 2 (duas) 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
2 - Alta	Chamados associados a situações de alto impacto, incluindo os casos de degradação severa de desempenho	On-site	No máximo 2 (duas) 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
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 a necessidade de substituição de componente(s) que possua(m) redundância	Remoto, com exceção das situações em que seja necessária intervenção física	No máximo 4 (quatro) horas após a abertura do chamado	No máximo 10 (dez) horas após a abertura do chamado
4 - Baixa	Chamados com objetivo de sanar	Remoto	No máximo 24 (vinte e quatro)	No máximo 72 (setenta e duas)

	dúvidas quanto ao uso ou à implementação do produto		horas após a abertura do chamado	horas após a abertura do chamado

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

3.1.4. Tratamento dos chamados de Severidade 1:

* Os chamados de Severidade 1 serão atendidos on-site em no máximo 2 (duas) horas após a sua abertura, incluindo o percurso do técnico até as instalações do SERPRO e contarão com esforço concentrado da contratada com vistas a aplicar solução ou medida de contorno em até 6 (seis) horas após a abertura do chamado;

* O atendimento de Severidade 1 não poderá ser interrompido até o completo restabelecimento do produto envolvido, mesmo que se estenda por períodos noturnos e dias não úteis;

3.1.5. Tratamento dos chamados de Severidade 2:

* Os chamados de Severidade 2 serão atendidos on-site em no máximo 2 (duas) horas após a sua abertura, incluindo o percurso do técnico até as instalações do SERPRO e contarão com esforço concentrado da contratada com vistas a aplicar solução ou medida de contorno em até 8 (oito) horas após a abertura do chamado;

* O atendimento de Severidade 2 não poderá ser interrompido até o completo restabelecimento do produto envolvido, mesmo que se estenda por períodos noturnos e dias não úteis;

3.1.6. Tratamento dos chamados de Severidade 3:

* Os chamados de Severidade 3 serão atendidos em no máximo 4 (quatro) horas após a sua abertura e contarão com esforço concentrado da contratada com vistas a aplicar solução ou medida de contorno em até 10 (dez) horas após a abertura do chamado;

* Caso o problema não possa ser resolvido remotamente, a contratada deverá colocar à disposição do SERPRO, um especialista devidamente habilitado e credenciado que trabalhará o tempo que for necessário para a solução do problema, sendo que o ônus financeiro de tal providência será da contratada;

* Os chamados classificados com Severidade 3, quando não solucionados no tempo definido, serão automaticamente escalados para Severidade 2, sendo que os prazos de atendimento e de solução serão automaticamente escalados para o novo nível de severidade;

3.1.7. Tratamento dos chamados de Severidade 4:

* Os chamados de Severidade 4 serão atendidos em no máximo 24 (vinte e quatro) horas após a sua abertura e deverão ser concluídos em até 72 (setenta e duas) horas após a abertura do chamado;

* Os chamados classificados com Severidade 4 serão atendidos em horário comercial, ou seja, das 08:00 h. às 18:00 h., de segunda-feira a sexta-feira, horário de Brasília;

3.1.8. Por necessidade de serviço, o SERPRO poderá solicitar a escalção de chamado para níveis superiores de severidade. Os prazos dos chamados escalados passam a contar novamente do início;

3.2. Suporte técnico aos softwares ofertados:

3.2.1. Possuir suporte técnico remoto para os softwares ofertados, durante o período de vigência da garantia, assegurando prazos de atendimento compatíveis com a instalação, ou seja, 24 (vinte e quatro) horas por dia e sete (7) dias por semana (à exceção dos chamados de Severidade 3 e 4);

3.2.2. O atendimento aos chamados deverá obedecer a seguinte classificação quanto ao nível de severidade:

Severidade	Descrição	Tipo de Atendimento	Tempo de Atendimento	Tempo de Solução
1 - Crítica	Chamados referentes a situações de emergência ou problema crítico, caracterizados pela existência de ambiente paralisado	Remoto	No máximo 2 (duas) horas após a abertura do chamado	No máximo 6 (seis) horas após a abertura do chamado
2 - Alta	Chamados associados a situações de alto impacto, incluindo os casos de degradação severa de desempenho	Remoto	No máximo 2 (duas) horas após a abertura do chamado	No máximo 8 (oito) horas após a abertura do chamado
3 - Média	Chamados referentes a situações de baixo impacto ou para aqueles problemas que se apresentem de forma intermitente	Remoto	No máximo 4 (quatro) horas após a abertura do chamado	No máximo 72 (setenta e duas) horas após a abertura do chamado
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 120 (cento e vinte) horas após a abertura do chamado

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. Tratamento dos chamados de Severidade 1:

- * Os chamados de Severidade 1 serão atendidos em no máximo 2 (duas) horas após a sua abertura e contarão com esforço concentrado da contratada com vistas a aplicar solução ou medida de contorno em até 6 (seis) horas após a abertura do chamado;

- * Caso o problema não possa ser resolvido remotamente, a contratada deverá colocar à disposição do SERPRO, um especialista devidamente habilitado e credenciado que trabalhará o tempo que for necessário para a solução do problema, sendo que o ônus financeiro de tal providência será da contratada;

- * Se após 3 (três) horas de iniciado o atendimento remoto ao chamado, o ambiente afetado não tiver sido restabelecido, o atendimento on-site deverá ser iniciado em até 4 (quatro) horas do início do atendimento remoto;

- * O atendimento de Severidade 1 não poderá ser interrompido até o completo restabelecimento do produto envolvido, mesmo que se estenda por períodos noturnos e dias não úteis;

3.2.5. Tratamento dos chamados de Severidade 2:

- * Os chamados de Severidade 2 serão atendidos em no máximo 2 (duas) horas após a sua abertura e contarão com esforço concentrado da contratada com vistas a aplicar solução ou medida de contorno em até 8 (oito) horas após a abertura do chamado;

- * Caso o problema não possa ser resolvido remotamente, a contratada deverá colocar à disposição do SERPRO, um especialista devidamente habilitado e credenciado que trabalhará o tempo que for necessário para a solução do problema, sendo que o ônus financeiro de tal providência será da contratada;

- * Se após 4 (quatro) horas de iniciado o atendimento remoto ao chamado, o ambiente afetado não tiver sido restabelecido, o atendimento on-site deverá ser iniciado em até 5 (cinco) horas do início do atendimento remoto;

- * O atendimento de Severidade 2 não poderá ser interrompido até o completo restabelecimento do produto envolvido, mesmo que se estenda por períodos noturnos e dias não úteis;

3.2.6. Tratamento dos chamados de Severidade 3:

- * Os chamados de Severidade 3 serão atendidos em no máximo 4 (quatro) horas após a sua abertura e contarão com esforço concentrado da contratada com vistas a aplicar solução ou medida de contorno em até 72 (setenta e duas) horas após a abertura do chamado;

- * Caso o problema não possa ser resolvido remotamente, a contratada deverá colocar à disposição do SERPRO, um especialista devidamente habilitado e credenciado que trabalhará o tempo que for necessário para a solução do problema, sendo que o ônus financeiro de tal providência será da contratada;

* Os chamados classificados com Severidade 3, quando não solucionados no tempo definido, serão automaticamente escalados para Severidade 2, sendo que os prazos de atendimento e de solução serão automaticamente escalados para o novo nível de severidade;

* Os chamados classificados com Severidade 3 serão atendidos em horário comercial, ou seja, das 08:00 h. às 18:00 h., de segunda-feira a sexta-feira, horário de Brasília;

3.2.7. Tratamento dos chamados de Severidade 4:

* Os chamados de Severidade 4 serão atendidos em no máximo 24 (vinte e quatro) horas após a sua abertura e deverão ser concluídos em até 120 (cento e vinte) horas após a abertura do chamado;

* Os chamados classificados com Severidade 4 serão atendidos em horário comercial, ou seja, das 08:00 h. às 18:00 h., de segunda-feira a sexta-feira, horário de Brasília;

3.2.8. Por necessidade de serviço, o SERPRO poderá solicitar a escalação de chamado para níveis superiores de severidade. Os prazos dos chamados escalados passam a contar novamente do início.

3.2.9. Em quaisquer casos e quando necessário, a contratada deverá assistir remotamente na instalação e uso dos software(s) ofertado(s), fornecendo orientações para diagnóstico de problemas e ajuda na interpretação de traces, dumps e logs. Nos casos de defeitos não conhecidos, as documentações enviadas pelo SERPRO (tais como: traces, dumps e logs) deverão ser encaminhadas aos laboratórios dos produtos a fim de que sejam fornecidas as devidas correções;

3.2.10. Em quaisquer casos e quando necessário, a contratada deverá fornecer informações sobre as correções a serem aplicadas ou a própria correção.

3.3. Penalidades:

3.3.1. A interrupção do atendimento de um chamado por parte da contratada, que não tenha sido previamente autorizada pelo SERPRO, ensejará aplicação de multa, conforme o nível de severidade do mesmo:

Severidade 1 – 0,5% (cinco décimos por cento) do valor constante no contrato para o item (equipamento ou software) correspondente, por hora ou fração de hora de interrupção;

Severidade 2 – 0,5% (cinco décimos por cento) do valor constante no contrato para o item (equipamento ou software) correspondente, por hora ou fração de hora de interrupção;

3.3.2. O não atendimento dentro do prazo estabelecido para o chamado ensejará aplicação de multa à contratada, conforme o nível de severidade do mesmo:

Severidade 1 – 0,5% (cinco décimos por cento) do valor constante no contrato para o item (equipamento ou software) correspondente, por hora ou fração de hora de atraso;

Severidade 2 – 0,5% (cinco décimos por cento) do valor constante no contrato para o item (equipamento ou software) correspondente, por hora ou fração de hora de atraso;

Severidade 3 – 0,2% (dois décimos por cento) do valor constante no contrato para o item

(equipamento ou software) correspondente, por hora ou fração de hora de atraso;

Severidade 4 – 0,1% (hum décimo por cento) do valor constante no contrato para o item (equipamento ou software) correspondente, por hora ou fração de hora de atraso;

3.4. Canais de atendimento:

3.4.1. Atendimento através de canal telefônico gratuito 0800, 24 horas por dia, 7 dias por semana;

3.4.2. Chamado técnico através de site na Internet, 24 horas por dia, 7 dias por semana e/ou canal telefônico gratuito 0800;

3.4.3. Acionamento automático do fornecedor no caso de falha de quaisquer dos componentes do(s) equipamento(s) ofertado(s).

4.0 Estimativa de Valor

Não se aplica.

5.0 Justificativa da Contratação

6.0 Justificativa da Dispensa ou Inexigibilidade

7.0 Pesquisa de Mercado

8.0 Acompanhamento da Licitação

O processo será acompanhado pelos empregados da SUPCD relacionados abaixo:

- João Henrique de Almeida Lara #61 2021-8467, e-mail: joao-henrique.lara@serpro.gov.br

- Fernando Elisio da Silva Alexandre #61 2021-7620, e-mail: fernando.alexandre@serpro.gov.br

9.0 Considerações Gerais

9.1. Da comprovação e documentação:

9.1.1. A proposta comercial a ser apresentada pelo fornecedor deverá discriminar os valores do(s) equipamento(s) e do(s) software(s) ofertado(s), bem como dos seus acessórios;

9.1.2. Fornecer junto com a proposta, descrição detalhada do(s) equipamento(s), software(s) e acessório(s) ofertado(s), que permita verificação do cumprimento dos requisitos técnicos e de compatibilidade especificados neste edital;

9.1.3. Fornecer documentação, caso o fornecedor não seja o fabricante da Solução ofertada, de que possui ou possuiu sob contrato de manutenção, equipamento similar ao ofertado em instalações de mesmo porte ou superior às do SERPRO;

9.1.4. Fornecer, junto com a proposta, em papel timbrado, declaração garantindo que o(s) equipamento(s) ofertado(s) nunca foi(ram) usado(s) e que não será(ão) descontinuado(s)

até, pelo menos, a data de licitação;

9.1.5. Fornecer, junto com a proposta, em papel timbrado, Termo de Confidencialidade assinado, pelo qual o fornecedor se comprometa a não divulgar informações relativas aos ambientes operacionais do SERPRO.

9.2. Da instalação e configuração:

9.2.1. O(s) equipamento(s) e seus acessórios deverão ser entregues pelo fornecedor em perfeitas condições de operação;

9.2.2. O(s) equipamento(s) e seus acessórios deverão ser entregues acondicionados adequadamente, em caixa lacrada, de forma a resistir à armazenagem e permitir a completa segurança durante o transporte. Deverá ser observado o limite da capacidade dos elevadores do SERPRO para o transporte do(s) equipamento(s). Na Regional São Paulo, o elevador suporta 950 Kg (novecentos e cinquenta quilogramas) e a dimensão da sua porta é de 100 cm (cem centímetros) de largura por 200 cm (duzentos centímetros) de altura;

9.2.3. Caberá ao fornecedor a responsabilidade pelo deslocamento, alimentação e estadia do seu técnico ao/no local da instalação do(s) equipamento(s), bem como pela retirada e entrega do mesmo, de peças de reposição e demais componentes necessários, com todas as despesas de transporte, frete e seguro correspondentes;

9.2.4. Deverá ser fornecida, com antecedência mínima de 10 (dez) dias da entrega do(s) equipamento(s), relação dos requisitos necessários à instalação física do(s) mesmo(s), tais como: medidas de layout, consumo de BTUs, circuitos elétricos, padrão das tomadas, necessidade de linhas telefônicas e portas de rede;

9.2.5. O SERPRO poderá solicitar mudança do local de instalação do(s) equipamento(s), juntamente com os softwares e demais acessórios ofertados, pelo menos 2 (duas) vezes durante o período de vigência da garantia, para suas instalações do Rio de Janeiro, São Paulo e de Brasília;

9.2.5.1 Qualquer mudança será comunicada ao fornecedor em tempo hábil para sua execução. As despesas com transporte e seguro do(s) equipamento(s) serão de responsabilidade do SERPRO. Caberá ao fornecedor a responsabilidade pelo deslocamento do seu técnico ao local de desinstalação/instalação do(s) equipamento(s) para a realização das mudanças solicitadas, sem ônus para o SERPRO e sem perda da garantia e das manutenções descritas neste edital.

9.3. Da garantia e manutenção:

9.3.1. O fornecedor deverá garantir o funcionamento da Solução, hardwares, softwares e demais acessórios ofertados, a partir do aceite pelo SERPRO, durante o período de 36 (trinta e seis) meses;

9.3.2. O fornecedor deverá garantir a atualização dos micro-códigos, firmwares, drivers e softwares instalados, provendo o fornecimento de novas versões por necessidade de correção de problemas ou por implementação de novos releases, a partir do aceite pelo SERPRO, durante o período de 36 (trinta e seis) meses;

9.3.3. O fornecedor deverá manter, no local de instalação do(s) equipamento(s), estoque de peças para seus componentes mais críticos, tais como: ventiladores, memórias, fontes

de alimentação, interfaces, HDs e processadores;

9.3.3.1. Todas as peças de reposição deverão ser novas e sem uso;

9.3.3.2. Em caso de troca de HDs, quando não formatados em RAID-5 ou RAID-6, os HDs substituídos deverão permanecer em poder do SERPRO;

9.3.4. Deverá ser fornecida documentação que comprove o licenciamento dos softwares ofertados;

9.3.5. Deverá estar contemplado na proposta do fornecedor Suporte Presencial, prestado por técnicos especializados em cada um dos segmentos. O Suporte Presencial será limitado a 600 (seiscentas) horas, que serão utilizadas pelo SERPRO dentro do prazo de garantia da Solução, durante o horário comercial. As requisições para o Suporte Presencial serão agendadas previamente com o fornecedor, sendo que este deverá disponibilizar os especialistas em um prazo máximo de 5 (cinco) dias úteis após a requisição, sem ônus adicional para o SERPRO. O intervalo mínimo que será considerado para um chamado de Suporte Presencial será de 16 (dezesesseis) horas. As requisições para a Suporte Presencial poderão ser executadas nas Regionais do SERPRO de São Paulo e Brasília, onde a Solução será instalada. Na proposta deverá estar discriminado o valor da hora de Suporte Presencial.

9.4. Das obrigações da contratada:

9.4.1. Para a Solução ofertada, o fornecedor deverá realizar manutenção preventiva, tanto do hardware quanto do firmware e dos softwares instalados, sendo de responsabilidade do fornecedor prover todas as correções e/ou atualizações necessárias, de forma sistemática e programada, de acordo com a periodicidade e os procedimentos especificados no(s) manual(is) do fabricante;

9.4.1.1. Caso não haja recomendação específica quanto à periodicidade, a manutenção preventiva deverá ser realizada em intervalos não superiores a 4 (quatro) meses;

9.4.2. No caso de manutenções, preventivas ou corretivas, em que haja risco de indisponibilidade total ou parcial da Solução, o SERPRO deverá ser previamente notificado para que se proceda a aprovação e o agendamento da manutenção em horário conveniente ao SERPRO;

9.4.3. Para a Solução ofertada, o fornecedor deverá prestar, durante o período de garantia, suporte técnico, tanto do hardware quanto do firmware e dos softwares instalados, observando os níveis de serviço descritos no item 3.0 e seus sub-itens;

9.5. Documentação técnica:

9.5.1. Deverá ser entregue juntamente com a Solução ofertada, relação detalhada do(s) equipamento(s), software(s) e acessório(s) entregues, em que constem: modelos, features, configurações, versões do sistema operacional e dos software(s) licenciados, etc.;

9.5.2. Deverá ser entregue juntamente com a Solução todos os CDs de instalação do(s) software(s) licenciado(s) e suas respectivas licenças;

9.5.3. Deverá ser entregue juntamente com a Solução toda a documentação técnica, composta por manuais de instalação, configuração e operação, em CD/DVD-ROM.

9.6. Da capacitação:

9.6.1. Capacitação, sem ônus para o SERPRO, a ser realizada durante o prazo de vigência do contrato, que contemple os conhecimentos necessários para efetuar as configurações e o gerenciamento da Solução ofertada, com carga horária mínima de 40 (quarenta) horas;

9.6.1.1. A capacitação deverá ser realizada em São Paulo e Brasília, onde a Solução será instalada, totalizando 80 (oitenta) horas. Em São Paulo e Brasília, deverá ser realizada nas dependências do fornecedor, podendo ser realizada nas dependências do SERPRO, caso haja disponibilidade de infra-estrutura;

9.6.1.2. A capacitação deverá ser realizada em 2 (duas) turmas (manhã e tarde) de 12 (dez) pessoas cada, em cada uma das localidades;

9.6.1.3. A data de início da capacitação bem como o local de realização serão definidos pelo SERPRO de acordo com suas necessidades. O SERPRO deverá comunicar formalmente o fornecedor com uma antecedência mínima de 5 (cinco) dias;

9.6.2. A capacitação deverá ser ministrada por profissional(ais) certificado(s) e/ou autorizado(s) pelo fabricante da Solução;

9.6.2.1. O fornecedor deverá apresentar com antecedência de, no mínimo, 15 (quinze) dias do início da capacitação, os certificado(s) solicitado(s) bem como declaração de que a empresa está autorizada pelo fabricante a prestar a capacitação;

9.6.3. O conteúdo programático bem como o material da capacitação deverão ser entregues ao SERPRO com antecedência de, no mínimo, 15 (quinze) dias do seu início, para avaliação prévia e aprovação;

9.6.4. Todas as despesas com material, equipamentos, instrutores, deslocamento de instrutores e demais itens serão de responsabilidade do fornecedor;

9.6.5. Após cada capacitação deverá ser emitido certificado para cada participante, obedecendo a critérios de frequência previamente negociados com o SERPRO;

9.7 Da Prova de Conceito:

9.7.1. A Solução de Monitoração e Auditoria de Segurança em Base de Dados de Plataforma Avançada da empresa que apresentar o menor preço no certame licitatório, será avaliada por meio de uma Prova de Conceito previamente à adjudicação, com o objetivo de certificar o atendimento das especificações técnicas definidas neste edital;

9.7.2. A prova de conceito da solução será realizado no SERPRO/Regional São Paulo: Rua Olívia Guedes Penteado, 941 – Capela do Socorro - São Paulo - SP, previamente à adjudicação do certame licitatório, em até 7 (sete) dias corridos da convocação da Licitante com menor preço, com duração de 15 (quinze) dias, após a solicitação formal do SERPRO, com o objetivo de certificar a total compatibilidade com as funcionalidades e requisitos e tipificação, distribuição geográfica e volumetria das bases a serem monitoradas. O grupo de avaliação será formado por 4 (quatro) técnicos definidos pelo SERPRO/SUPCD;

9.7.3. Caberá à empresa fornecedora:

9.7.3.1 Disponibilizar todos os recursos de hardware e de software minimamente necessários para compor um ambiente de testes para realização da Prova de Conceito, em até 10 (dez) dias úteis, a partir da comunicação da empresa com menor preço. O não cumprimento do prazo estipulado desclassificará a empresa fornecedora;

9.7.3.2 Disponibilizar técnico(s) com os conhecimentos necessários para execução dos testes e das medições de desempenho;

9.7.3.3 Disponibilizar ferramentas para coleta e tratamento de dados que permitam a avaliação do desempenho da Solução ofertada;

9.7.3.4 Fornecer valores de referência, do próprio fabricante e/ou de entidade independente (IDC, Gartner Group, etc.), constante em literatura técnica especializada, para o dimensionamento da Solução a partir dos dados coletados nos testes.

9.7.4. Caberá ao SERPRO:

9.7.4.1 Preparar local e infra-estrutura para a instalação dos recursos de hardware e software a serem disponibilizados pela empresa fornecedora, em até 7 (sete) dias úteis, a partir da comunicação da empresa com menor preço;

9.7.4.2 Disponibilizar técnico para acompanhamento dos testes.

9.7.5. Dos testes:

9.7.5.1 A fase de execução dos testes deverá ser iniciada em até 3 (três) dias úteis após a fase de instalação dos recursos de hardware e de software disponibilizados pela empresa fornecedora;

9.7.5.2 Os técnicos do SERPRO e da empresa fornecedora disporão de até 10 (dez) dias úteis para realização dos testes, que deverão ocorrer no horário entre 08:00 e 17:00 horas;

9.7.5.3 A Prova de Conceito constituir-se-á de testes funcionais e de desempenho para validação do atendimento das especificações técnicas definidas nos itens 2.3 e 2.4 deste edital, sendo considerada apta a Solução que atendê-las satisfatoriamente;

9.7.5.4 Ao final da Prova de Conceito deverá ser elaborado um relatório pelos técnicos do SERPRO, onde deverão ser registrados os resultados dos testes, bem como a aprovação ou reprovação da Solução avaliada.

9.8. Os equipamentos e os softwares deverão ser faturados com suas respectivas alíquotas de imposto;

9.9. O prazo de vigência do contrato será de 6 (seis) meses;

9.10. A modalidade de aquisição será por pregão eletrônico;

9.11. Demais condições devem obedecer ao padrão dos contratos do SERPRO;

9.12. Gestor do contrato: Sr. .x.x.x.x.x.x.x.x.x, CPF: .x.x.x.x.x.x.x., matrícula: .x.x.x.x.x.x., lotação: COOGC, e-mail: .x.x.x.x.x.x.x.x, telefone: #.x.x.x.x.x.x.x.;

9.13. Considerando que os padrões de desempenho e de qualidade estão efetivamente descritos no presente Termo de Referência e que as especificações estabelecidas são usuais de mercado, entendemos que a Solução aqui descrita é caracterizada como "Bem Comum".