TERMO DE REFERÊNCIA

DLP – DATA LOSS PREVENTION

DIRETORIA DE INFRAESTRUTURA E TECNOLOGIA

Novembro / 2020

EMPRESA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DO MUNICÍPIO DE SÃO PAULO - PRODAM-SP S/A
Av. Francisco Matarazzo, 1500 - Torre Ary Antenor de Barros - CEP 05001-100 - São Paulo - SP
Tel.: (11) 3396-8000 - Fax: (11) 3396-8001
www.prodam.sp.gov.br

TERMO DE REFERÊNCIA

1. OBJETO

Abertura de processo para Ata de Registro de Preços para para futura aquisição de licenças de solução de prevenção contra perda de dados DLP (Data Loss Prevention) com gerenciamento centralizado; fornecimento de suporte, manutenção especializada e garantia, fornecimento de serviço de instalação e configuração de toda a solução objeto deste contrato e ainda treinamento específico para a Prodam-SP e para a Prefeitura Municipal de São Paulo.

1.1 Tabela de Composição de Itens:

ITEM	DESCRIÇÃO	UNID.	QUANT.	VALOR UNITARIO (R$)	VALOR TOTAL (R$)
01	**Licenças para Solução de Prevenção Contra Perda de Dados (Data Loss Prevention – DLP)**	**UN**	**XXXX**		
02	**Gerenciamento Centralizado**	**UN**	**X**		
03	**Suporte Técnico, Manutenção e Garantia (12 Meses)**	**UN**	**X**		
VALOR PARA 3 ANOS – SUBTOTAL 1					
ITEM	**DESCRIÇÃO**	**UNID.**	**QUANT.**	**VALOR UNITÁRIO (R$)**	**VALOR TOTAL (R$)**
04	**Serviço de Instalação e Configuração**	**UN**	**X**		
05	**Treinamentos**	**UN**	**X**		
SUBTOTAL 2					
VALOR TOTAL = (SUBTOTAL 1 + SUBTOTAL 2) – VALOR A SER POSTADO NO COMPRASNET					

1.2 Vigência do Contrato:

1.2.1 O contrato terá vigência de 12 (doze) meses, a contar da data de assinatura do Termo de Aceite, previsto no item Aceite deste

documento, podendo ser prorrogado até o limite de 5 anos, conforme dispõe o artigo 71, da Lei Federal nº 13.303/2016.

1.2.2 Durante o período de vigência, estarão inclusas todas as atualizações necessárias para o perfeito funcionamento da solução.

2. ESPECIFICAÇÃO TÉCNICA

Solução de Prevenção Contra Perda de Dados (Data Loss Prevention – DLP) com licenças por subscrição;

2.1 Resposta a incidentes:

2.1.1 Deve possuir notificações personalizáveis através de e-mail em caso de violação de política previamente estabelecida;

2.1.2 A solução deve permitir ao administrador acrescentar quais detalhes sobre o incidente serão enviados nas notificações;

2.1.3 Deve permitir tomar ações automáticas pré-definidas na detecção de incidentes, para no mínimo:

2.1.3.1 Permitir o envio, deletar anexos, quarentenas ou criptografar e-mails;

2.1.3.2 Permitir ou bloquear tráfego de dados sensíveis via FTP;

2.1.3.3 Permitir ou bloquear tráfego de dados sensíveis via HTTP/ HTTPs;

2.1.3.4 Através do agente, permitir, bloquear ou solicitar justificativa para o tráfego em pelo menos: Qualquer tipo de aplicação executada pelo Sistema operacional, cópia para armazenamentos de rede, impressão de arquivos, E-mails enviados, upload para páginas Web e cópias para dispositivos USB.

2.1.3.5 Permitir a possibilidade de busca ou não de detalhes sobre o incidente durante o registro;

2.1.3.6 Execução de atividades customizadas;

2.1.3.7 Enviar mensagens para servidores de Syslog;

2.1.3.8 Enviar notificações por e-mail;

2.1.3.9 Manipular arquivos durante a descoberta de rede.

2.1.3.10 Deve permitir vários botões de reposta na interface gráfica dos incidentes totalmente configuráveis.

2.1.3.11 Os botões de resposta na interface gráfica dos incidentes devem possibilitar no mínimo:

2.1.3.12 Designar o incidente para resposta de alguém específico;

2.1.3.13 Modificar o status do incidente;

2.1.3.14 Modificar a severidade do incidente;

2.1.3.15 Ignorar o incidente;

2.1.3.16 Adicionar TAG no incidente;

2.1.3.17 Adicionar comentários no incidente;

2.1.3.18 Fazer Download do incidente;

2.1.3.19 Deletar o incidente;

2.1.3.20 Acionar scripts ou tarefas customizadas;

2.1.3.21 Escalar o incidente para o gerente do usuário envolvido;

2.1.3.22 Escalar o incidente para uma pessoa específica.

2.1.3.23 Deve exibir todos os detalhes do incidente em uma única página.

2.1.3.24 Deve permitir exibir partes específicas da mensagem ou arquivo que violou as políticas previamente estabelecidas, através de uma visualização rápida na tela do incidente, sem a necessidade de usar software externo.

2.1.3.25 Deve permitir armazenar a mensagem e o arquivo original que gerou o incidente.

2.1.3.26 Deve exibir todo o histórico do incidente, incluindo alterações, edições e respostas executadas automaticamente e manualmente.

2.2 Relatórios

Deve ser capaz de restringir regras de proteção de dados a grupos de usuários do Active Directory;

2.2.1 Ação aplicada;

2.2.2 Responsável pela análise;

2.2.3 Nome da aplicação;

2.2.4 Departamento;

2.2.5 Canal de detecção;

2.2.6 Nível de classificação da informação;

2.2.7 Destino de tráfego da informação;

2.2.8 Tipo estação (Desktop ou Laptop);

2.2.9 ID do incidente

2.2.10 Hora do incidente

2.2.11 Nome do arquivo trafegado;

2.2.12 Histórico do incidente;

2.2.13 Incidentes marcados como ignorados;

2.2.14 TAGs de incidentes;

2.2.15 Quantidade de informação sensível trafegada;

2.2.16 Propriedades do arquivo;

2.2.17 Política acionada;

2.2.18 Nome da regra adicionada:

2.2.19 Severidade do incidente;

2.2.20 Origem do incidente;

2.2.21 Status do incidente;

2.2.22 Tamanho da transação;

2.2.23 Dados relacionados as violações encontradas;

2.2.24 Deve exportar relatórios para os formatos HTML, PDF e CSV;

2.2.25 Deve apresentar um painel para visualização de relatórios;

2.2.26 Deve possuir API para permitir que aplicações de terceiros extraiam dados de incidentes da base de dados do DLP;

2.2.27 Deve ter a capacidade para configurar, salvar relatórios e painéis personalizados por usuário;

2.2.28 Deve possuir painéis (Dashboards) para, no mínimo os seguintes itens:

2.2.28.1 Incidentes criados nos últimos X dias;

2.2.28.2 Políticas mais acionadas;

2.2.28.3 Incidentes por severidade;

2.2.28.4 Incidentes por ação tomada;

2.2.28.5 Incidentes por canais de detecção;

2.2.28.6 Incidentes por origem/destino;

2.2.28.7 Usuários que mais violam políticas.

2.3 Módulo da Área de Armazenamento

2.3.1 Deve verificar existência de conteúdo confidencial em file systems sem a necessidade de agentes de coleta (agent-less) para no mínimo CIFS, NFS, SMB e NT FS.

2.3.2 Deve permitir a análise dos file systems através de agentes ou sem agentes em sistemas operacionais, para no mínimo:

2.3.2.1 Windows Server 2008 R2;

2.3.2.2 Windows Server 2012;

2.3.2.3 Windows Server 2016;

2.3.2.4 Red Hat Enterprise Linux 6 e demais releases da versão;

2.3.2.5 Red Hat Enterprise Linux 7 e demais releases da versão.

2.3.3 Deve analisar conteúdo sigiloso armazenado em ambientes complexos, para no mínimo:

2.3.3.1 Microsoft Sharepoint;

2.3.3.2 Lotus notes;

2.3.3.3 Microsoft SQL Server;

2.3.3.4 Oracle;

2.3.3.5 MySQL

2.3.3.6 Microsoft Exchange Online;

2.3.3.7 Microsoft Office365;

2.3.4 Deve possuir a capacidade de verificar arquivos Microsoft "PST", possibilitando executar varreduras tanto nas mensagens, assim como, nos arquivos anexos as mensagens;

2.3.5 Possibilidade de mover para quarentena arquivos que violam políticas de segurança.

2.3.6 Deve manter o arquivo no local original, substituindo seu conteúdo por uma mensagem customizável, como aviso e orientação para o usuário;

2.3.7 Permitir a remoção do arquivo que está em quarentena e restaurá-lo de volta ao local original;

2.3.8 Deve permitir coleta automática de arquivos que violem políticas para análise legal (evidência);

2.3.9 Permitir a criação de respostas personalizadas para incidentes;

2.3.10 Exibir detalhes, no incidente, dos arquivos que violam as políticas;

2.3.11 Permitir a visualização das permissões do arquivo;

2.3.12 Deve possibilitar notificação através de e-mail e alerta Syslog em caso de violação de política;

2.3.13 Deve permitir agendamento de varreduras automáticas;

2.3.14 Possuir mecanismo de verificação incremental, na qual apenas arquivos novos, ou alterados, sejam verificados;

2.3.15 Deve permitir configurar janelas de tempo para verificações, interrompendo o processo automaticamente ao fim do período configurado;

2.3.16 Preservar os atributos originais do arquivo, inclusive o atributo "Acessado em", enquanto realiza a verificação;

2.3.17 Possuir capacidade de pausar, manualmente, a verificação;

2.3.18 Deve utilizar técnicas de paralelismo e controle de banda;

2.3.19 Permitir o controle da velocidade das verificações para limitar o uso da largura de banda da rede;

2.3.20 Deve ter a capacidade de reutilizar uma única credencial (nome de usuário/senha) em múltiplos alvos a serem verificados;

2.3.21 Permitir a verificação simultânea em várias fontes distintas;

2.3.22 Permitir limitar quais portas de comunicação serão utilizadas entre o sistema-alvo e o servidor que faz a verificação;

2.3.23 Deve permitir aplicar filtros para verificar na varredura de arquivos de um determinado tipo ou em certo diretório;

2.3.24 Deve permitir aplicar filtros para verificar na varredura de arquivos a idade e/ou o seu tamanho.

2.4 Módulo Terminal de Usuário

2.4.1 Capacidade de descobrir fuga de informações sensíveis, por meio de agente;

2.4.2 Possibilidade de aplicação de políticas mesmo quando o agente não tem comunicação com o servidor de gerenciamento;

2.4.3 Possibilidade de armazenamento em cache, dos arquivos que causaram o incidente até que o usuário se conecte, novamente, à rede corporativa;

2.4.4 A solução deve possuir a funcionalidade de OCR em arquivos do tipo imagem, no mínimo para:

2.4.4.1 Jpeg;

2.4.4.2 Bmp;

2.4.4.3 Png;

2.4.4.4 Gif;

2.4.4.5 Tiff;

2.4.5 Monitorar e bloquear dados copiados para dispositivos de armazenamento removível (USB);

2.4.6 A solução deverá possuir capacidade de analisar arquivos menos de 1 kbyte;

2.4.7 Possibilidade de criptografar dados sensíveis a serem definidos nessa contratação copiados para dispositivos USB, sem a necessidade de soluções adicionais;

2.4.8 Permitir a monitoração e bloqueio para dados copiados para CD/DVD;

2.4.9 Permitir a monitoração e bloqueio para dados enviados a qualquer tipo de impressora local e de rede;

2.4.10 Permitir a monitoração e bloqueio para ações de copiar e colar;

2.4.11 Permitir a monitoração e bloqueio de dados sensíveis definidos nessa contratação trafegados via e-mail corporativo on-premises ou nuvem (Outlook/Office365);

2.4.12 Permitir a monitoração e bloqueio para transmissões HTTPS pelo menos nos seguintes navegadores:

2.4.12.1 Internet Explorer;
2.4.12.2 Microsoft Edge;
2.4.12.3 Mozilla Firefox;
2.4.12.4 Google Chrome;
2.4.12.5 Safari.

2.4.13 Permitir a monitoração e bloqueio para transmissões HTTP;

2.4.14 Permitir a monitoração e bloqueio para transmissões via FTP;

2.4.15 Permitir a monitoração e bloqueio para uso de dados confidenciais a serem definidos nessa contratação por qualquer aplicativo, incluindo programas de criptografia não autorizados;

2.4.16 Permitir a monitoração e bloqueio para dados copiados para compartilhamentos de rede pelo Windows Explorer;

2.4.17 A Solução deve possuir monitoramento, por padrão, para pelo menos os seguintes aplicativos:

2.4.17.1 Chrome;
2.4.17.2 Firefox;
2.4.17.3 Internet Explorer (IE);
2.4.17.4 Microsoft Edge;
2.4.17.5 Opera;

2.4.17.6 Safari;

2.4.17.7 Tor;

2.4.17.8 Torch;

2.4.17.9 Acoustica MP3 CD Burner;

2.4.17.10 Alcoh01 120%;

2.4.17.11 CD-Mate;

2.4.17.12 Disk Utility;

2.4.17.13 iTunes;

2.4.17.14 Nero Burning ROM;

2.4.17.15 Roxio — Easy Media Creator;

2.4.17.16 Windows Media Player;

2.4.17.17 Amazon Cloud Drive;

2.4.17.18 Box;

2.4.17.19 Dropbox;

2.4.17.20 Egnyte;

2.4.17.21 Google Drive;

2.4.17.22 iCloud;

2.4.17.23 OneDrive;

2.4.17.24 Salesforce Files;

2.4.17.25 ShareFile;

2.4.17.26 Syncplicity;

2.4.17.27 Watch Dox;

2.4.17.28 Apple Mail;

2.4.17.29 Eudora;

2.4.17.30 Lotus Notes;

2.4.17.31 MailMate;

2.4.17.32 Microsoft Outlook;

2.4.17.33 Microsoft Outlook Express;

2.4.17.34 Mozilla Thunderbird;

2.4.17.35 Pegasus Mail;

2.4.17.36 Postbox;

2.4.17.37 Sparrow;

2.4.17.38 Windows Live Mail;

2.4.17.39 Windows Mail;

2.4.17.40 DK2 Network Server Remote Monitor - DK2 DESkey;

2.4.17.41 File Encryption XP;

2.4.17.42 Windows Privacy Tray (WinPT);

2.4.17.43 Core FTP LE;

2.4.17.44 Cute FTP Home 8.2;

2.4.17.45 File Transfer Program (Microsoft Utility);

2.4.17.46 FileZilla FTP Client;

2.4.17.47 Flash FXP 3.6 build 1240;

2.4.17.48 FTP Voyager 15;

2.4.17.49 Ipswitch WS FTP Home;

2.4.17.50 Leech FTP;

2.4.17.51 Serv-U;

2.4.17.52 Smart FTP Client;

2.4.17.53 Adium;

2.4.17.54 AlM

2.4.17.55 Apple Messages;

2.4.17.56 Camfrog;

2.4.17.57 Cisco WebEx;

2.4.17.58 GoT0Meeting;

2.4.17.59 ICQ;

2.4.17.60 Jabber Messenger;

2.4.17.61 ManyCam;

2.4.17.62 Microsoft Lync 2010;

2.4.17.63 Miranda 1M;

2.4.17.64 ooVoo;

2.4.17.65 Pidgin;

2.4.17.66 Skype for Business;

2.4.17.67 TeamViewer;

2.4.17.68 Teccent QQ;

2.4.17.69 Trillian;

2.4.17.70 Viber;

2.4.17.71 Yahoo! Instant Messenger;

2.4.17.72 Adobe Reader;

2.4.17.73 Bean;

2.4.17.74 Eclipse;

2.4.17.75 Emacs;

2.4.17.76 Evernote;

2.4.17.77 Keynote;

2.4.17.78 LibreOffice/Apache OpenOffice;

2.4.17.79 Mellel;

2.4.17.80 Microsoft Office Access;

2.4.17.81 Microsoft Office Excel;

2.4.17.82 Microsoft Office InfoPath;

2.4.17.83 Microsoft OneNote;

2.4.17.84 Microsoft Office PowerPoint;

2.4.17.85 Microsoft Office Project;

2.4.17.86 Microsoft Office Publisher;

2.4.17.87 Microsoft Office Visio;

2.4.17.88 Microsoft Office Word;

2.4.17.89 Notepad;

2.4.17.90 Numbers;

2.4.17.91 OpenOffice.org Calc;

2.4.17.92 OpenOffice.org Draw;

2.4.17.93 OpenOffice.org Math;

2.4.17.94 OpenOffice.org Writer;

2.4.17.95 Pages;

2.4.17.96 Reminders;

2.4.17.97 Stickies;

2.4.17.98 TextEdit;

2.4.17.99 WordPad;

2.4.17.100 AllegianceMD;

2.4.17.101 eClinicalWorks;

2.4.17.102 ECLIPSYS;

2.4.17.103 INGENIX;

2.4.17.104 inteGreat;

2.4.17.105 Sequel;

2.4.17.106 Ares;

2.4.17.107 Azureus;

2.4.17.108 BearShare;

2.4.17.109 BitComet;

2.4.17.110 BitLord;

2.4.17.111 BitTornado;

2.4.17.112 BitTorrent;

2.4.17.113 eMule;

2.4.17.114 FrostWire;

2.4.17.115 Kazaa Lite;

2.4.17.116 LimeWire;

2.4.17.117 Pando;

2.4.17.118 Transmission;

2.4.17.119 uTorrent;

2.4.17.120 7-Zip File Manager;

2.4.17.121 iArchiver;

2.4.17.122 WinRAR;

2.4.17.123 WInZip;

2.4.17.124 Bluetooth Stack COM Server - BTStackServer;

2.4.17.125 Fsquirt;

2.4.17.126 iTunes;

2.4.17.127 Wireless Link File Transfer App — Irftp;

2.4.17.128 WCESMgr;

2.4.17.129 Aplicor (online);

2.4.17.130 CRM.com;
2.4.17.131 HostAnalytics;
2.4.17.132 Intacct;
2.4.17.133 NetSuite;
2.4.17.134 Oracle CRM on demand;
2.4.17.135 RightNow;
2.4.17.136 Salesforce;
2.4.17.137 WorkDay;
2.4.17.138 FoxPro;
2.4.17.139 Ld;
2.4.17.140 MSTSC;
2.4.17.141 NT backup tool;
2.4.17.142 Vista backup tool;
2.4.17.143 VMWare.

2.4.18 A solução deve permitir a criação de qualquer aplicativo existente que não venha cadastrado por padrão;

2.4.19 Definir dispositivos removíveis individuais, ou grupos de dispositivos, como confiáveis e criar exceções de políticas para esses dispositivos;

2.4.20 0 agente deverá suportar, no mínimo, Windows 7 (32 e 64 bits), Windows 2008 R2 Enterprise (64bit), Windows 10, Windows Server 2012, Windows Server 2016 e Apple MacOS;

2.4.21 Todas as funções devem ser executadas por um único agente;

2.4.22 Permitir a desativação do agente pela console de gerenciamento;

2.4.23 Possuir mecanismo que reinicie o agente caso o usuário tente interromper o serviço;

2.4.24 Possuir proteção contra desinstalação do agente;

2.4.25 Capacidade de apresentar as mensagens de notificações em português;

2.4.26 Possuir a capacidade de envio de notificação automática, por e-mail, para o usuário e administrador durante a ocorrência de um incidente;

2.4.27 Possuir a capacidade de gerenciamento da saúde dos agentes.

2.4.28 Deve permitir a distribuição do agente através de GPO ou por ferramenta de terceiros;

2.4.29 Deve ter a capacidade de permitir ao usuário justificar a movimentação de conteúdo confidencial, a partir do alerta em "pop-up", escolhendo opções de justificativa configuráveis pelo administrador da ferramenta;

2.4.30 O agente deve executar varredura local para verificar se a estação do usuário possui conteúdo confidencial;

2.4.31 Deve permitir realizar verificações incrementais, apenas em arquivos novos e alterados;

2.4.32 Permitir a instalação do agente de modo oculto ou em modo de interação com o usuário;

2.4.33 Quando utilizado em modo interativo, permitir sincronização de políticas de forma manual, através de acionamento de botão no agente;

2.4.34 Alimentar a console de gerenciamento, com pelo menos, as seguintes informações do agente:

2.4.34.1 Nome do computador;

2.4.34.2 IP Address;

2.4.34.3 Usuário logado;

2.4.34.4 Última vez que o agente se comunicou com a o servidor central;

2.4.34.5 Identificador do grupo de políticas utilizados;

2.4.34.6 Campo que informa se o agente está em sincronismo com as últimas políticas/configurações disponibilizadas pelo administrador;

2.4.34.7 Versão do agente;

2.4.34.8 Versão da política instalada;

2.4.34.9 Deve possuir agentes para smartphones, compatíveis com Android e IOS.

2.5 Módulo de rede

2.5.1 Permitir a monitoração/bloqueio do e-mail corporativo, evitando que e-mails com dados sigilosos definidos por essa contratação sejam enviados para fora da organização, inclusive em smartphones e tablets;

2.5.2 Possibilidade de colocar mensagens de correio eletrônico em quarentena para análise;

2.5.3 Permitir a monitoração/bloqueio de tráfego WEB, evitando que dados sigilosos definidos por essa contratação saiam da organização por este canal, inclusive em smartphones e tablets;

2.5.4 Capacidade de monitorar/bloquear o tráfego de informações sensíveis em posts de redes sociais;

2.5.5 Permitir a monitoração de qualquer protocolo baseado em TCP, como o SMTP, inclusive anexos; HTTP, inclusive arquivos de upload; FTP ativo e passivo;

2.5.6 Capacidade de monitorar o vazamento de dados por meio de softwares de Mensagens Instantâneas desde que de uso coorporativo;

2.5.7 Permitir a classificação dos protocolos, mesmo quando executados em portas que não são padrão;

2.5.8 Capacidade de filtrar o tráfego da rede para inspeção, segundo o protocolo, faixa de IP e remetente/destinatário de e-mail;

2.6 Módulo de Classificação da informação

2.6.1 Solução deve ser capaz de implementar em no mínimo:

2.6.1.1 Windows 7;

2.6.1.2 Windows 8;

2.6.1.3 Windows 8.1;

2.6.1.4 Windows 10;

2.6.1.5 MacOS 10.10, 1 0.1 1 e 10.12;

2.6.2 A solução deve ter integração nativa com a solução de Data Loss Prevention fornecida;

2.6.3 A solução deve ter a capacidade de automaticamente classificar arquivos no mínimo para os seguintes tipos de arquivo:

2.6.3.1 Word, Excel, PowerPoint e Project Microsoft Office;

2.6.3.2 Open Office, PDF;

2.6.3.3 ZIP;

2.6.3.4 MSG, TIF e EML files;

2.6.3.5 JPEG;

2.6.3.6 HTML;

2.6.4 A solução deve ter a capacidade de proporcionar ao usuário a possibilidade de classificar a informação recém-criada de forma que as soluções integradas possam usufruir desta classificação e incluí-las de forma automática dentro de políticas previamente criadas e definidas por essa contratação;

2.6.5 A solução deve possibilitar a CUSTOMIZAÇÃO DE GRAUS DE SIGILO/CATEGORIAS PARA a classificação da informação pelo usuário, possibilitando classificar a informação recém-criada em no mínimo:

2.6.5.1 Informação Pública;

2.6.5.2 Informação Restrita;

2.6.5.3 Informação Interna;

2.6.5.4 Informação Confidencial

2.6.5.5 Informação Pessoal.

2.6.6 A solução deve possibilitar classificar tanto a informação recém-criada, quanto as já existentes;

2.6.7 A solução deve ter integração para classificação da informação pelo usuário para no mínimo:

2.6.7.1 Word, Excel, PowerPoint e Project Microsoft Office;

2.6.7.2 Open Office;

2.6.7.3 PDF;

2.6.7.4 ZIP;

2.6.8 A solução deve ser capaz de analisar o comportamento malicioso do usuário, priorizando alertas correlacionados com diversas soluções de segurança em produção, contendo desta forma as ameaças, possibilitando a partir de um único relatório indicar um possível ataque;

2.6.9 A solução deve ter a capacidade de analisar as informações em conformidade com normas e regulamentações, para no mínimo GDPR, PCI, DSS, SOX, HIPAA;

2.6.10 A solução deve basear o coeficiente comportamental de risco, indicando a priorização das ações e identificando se o comportamento malicioso é interno ou se é externo, correlacionando para isso informações de no mínimo:

2.6.10.1 Incidentes recebidos da solução de DLP fornecida;

2.6.10.2 Incidentes recebidos pela solução de criptografia, na tentativa de acesso aos dados sensíveis;

2.6.10.3 Incidentes de classificação de documentos/informação por parte do usuário final;

2.6.10.4 Incidentes recebidos da rede de inteligência mundial do fabricante da solução;

2.6.11 A solução deve ser capaz de identificar os usuários expostos aos maiores níveis de risco e possibilitar a partir desta informação refinar as políticas de proteção dos dados;

2.6.12 A solução deve ter a capacidade de calcular a pontuação de risco de cada usuário a partir do comportamento do passado e do presente;

2.6.13 A solução deve ter a capacidade de criar relatórios de risco, baseados nos maiores infratores;

2.6.14 A solução deve ter a capacidade de criar políticas de alerta e bloqueio definidos por essa contratação, conforme segue:

2.6.14.1 **Políticas de Alerta**: É enviado um alerta ao usuário, no entanto, é possível ao usuário salvar o arquivo e enviá-lo por e-mail;

2.6.14.2 **Políticas de Bloqueio**: É enviado um alerta ao usuário, independentemente do nível de classificação do arquivo, onde não será possível salvar, nem tão pouco enviar o arquivo;

2.6.15 A solução deverá possibilitar no mínimo formas de:

2.6.15.1 Descoberta de Informações;

2.6.15.2 O fluxo da informação;

2.6.15.3 Proteger contra a exfiltração da informação, quer seja intencional, quer seja inadvertida;

2.6.15.4 Assegurar conformidade com as políticas de acesso e políticas de segurança definidos por essa contratação;

2.6.15.5 Possibilitar a manutenção da trilha de auditoria por razões de controle e conformidade;

2.6.15.6 Possibilitar alertar aos usuários quando da criação de informações, sobre as políticas de gerenciamento da informação;

2.6.15.7 Possibilitar o rastreio de "onde" os dados não estruturados estão sendo criados e "quem" os estão criando;

2.6.16 A solução deve permitir forçar a aplicação de políticas antes que os dados saiam da gerência do Órgão, para no mínimo:

2.6.16.1 Políticas de TAG;

2.6.16.2 Políticas de introdução de cabeçalhos (append headers);

2.6.16.3 Políticas de inclusão de metadados (add metadata);

2.6.17 A solução deve ser capaz de implementar gráficos comparativos de risco comportamental entre no mínimo:

2.6.17.1 Usuários sob o mesmo Gerente;

2.6.17.2 Usuários do mesmo departamento;

2.6.17.3 Comportamento dos endpoints;

2.6.17.4 Comportamento das informações marcadas com TAG de dados sensíveis;

2.6.17.5 Frequência com que as políticas de proteção dos documentos são violadas;

2.6.17.6 f) Envio de informações sensíveis por e-mail e web.

2.7 Características do módulo de gerenciamento:

2.7.10 Toda infraestrutura necessária para gerenciamento da solução do DLP, como servidores, sistemas operacionais, banco de dados, entre outros serviços e equipamentos necessários, deve ser disponibilizado em nosso datacenter pela CONTRATADA com as devidas licenças;

2.7.11 A solução de gerenciamento deve ser fornecida em modo de alta disponibilidade;

2.7.12 A solução de gerenciamento deve suportar, no mínimo, 1 ano de armazenamento de logs;

2.7.13 Deve suportar a instalação nos seguintes sistemas operacionais:

2.7.13.1 Windows Server 2016 ;

2.7.13.2 Windows Server 2012 Release 2;

2.7.13.3 Windows Server 2012 ;

2.7.14 A arquitetura dos Sistemas Operacionais deve ser 64-bits;

2.7.15 Deve suportar a instalação em Cluster Microsoft;

2.7.16 Deve suportar Ipv4 e Ipv6;

2.7.17 Deve suportar a virtualização do sistema operacional com base nos seguintes hypervisors:

2.7.17.1 Vmware ESX;

2.7.17.2 Citrix Xen Server;

2.7.17.3 Microsoft Hyper-V;

2.7.17.4 Deve possuir suporte a base de dados:

2.7.17.5 SQL Server 2012 ou superior;

2.7.17.6 Não serão aceitas soluções que usam SQL Express ou Base de dados embutidas;

2.7.18 A console de gerência deve ser acessada via WEB;

2.7.19 Deve possuir compatibilidade com os seguintes browsers:

2.7.19.1 Google Chrome;

2.7.19.2 Firefox;

2.7.19.3 Internet Explorer 7 ou superior;

2.7.19.4 Edge

2.7.19.5 Safari 6.0 ou superior;

2.7.20 Deve suportar o uso do SQL Server em ambientes SAN;

2.7.21 Permitir a instalação dos Módulos da Solução a partir de um único servidor;

2.7.22 Permitir a alteração das configurações dos recursos instalados nas estações (clientes) de maneira remota;

2.7.23 Deve possuir uma solução de gerenciamento única para estações de trabalho, instalada em um único servidor de aplicação, afim de prover uma única console de gerenciamento centralizado;

2.7.24 Suporte a múltiplos usuários, com diferentes níveis de acesso e permissões ao produto gerenciado;

2.7.25 Criação de grupos de máquinas baseadas em regras definidas em função do endereço IP do cliente;

2.7.26 Forçar a instalação do agente DLP nos clientes;

2.7.27 Deve ser possível realizar a customização dos relatórios gráficos gerados;

2.7.28 Exportação dos relatórios para os seguintes formatos: HTML, CSV, PDF, XML;

2.7.29 A solução de gestão deve possuir dashboards no gerenciamento da solução;

2.7.30 Ter a capacidade de gerar registros/logs para auditoria;

2.7.31 A solução de gerenciamento deve ter a capacidade de atribuir etiquetas as máquinas, facilitando assim a distribuição automática dentro dos grupos hierárquicos na estrutura de gerenciamento;

2.7.32 A solução de gerenciamento deve permitir acesso a sua console via web;

3. REQUISITOS DE PROJETO E DE IMPLEMENTAÇÃO

3.1. A empresa vencedora da licitação deverá apresentar um projeto para implementação da solução DLP para toda a Rede PMSP e para a Prodam.

3.1.1. O projeto deverá ser conduzido em fases:

3.1.1.1. **INICIAÇÃO:** a Prefeitura Municipal de São Paulo deverá apresentar todo o mapeamento dos dados e análises de riscos, bem como as informações de ambiente a fim de que se possa iniciar o projeto.

3.1.1.2. a CONTRATADA deverá criar a visão do projeto e definirá o escopo de trabalho necessário para trazê-la para a realidade, após as informações prestadas pela Prefeitura Municipal de São Paulo por intermeio da CONTRATANTE;

3.1.1.3. **PLANEJAMENTO:** deverá consistir na elaboração dos processos detalhados a serem utilizados na implantação do projeto, com base nas informações, políticas definidas pela Prefeitura Municipal de São Paulo, estrutura organizacional e relatório operacional de tratamento;

3.1.1.4. **EXECUÇÃO**: consistirá na execução das atividades definidas na fase de planejamento, podendo ser dividida em sub-bases para melhor controle;

3.1.1.5. **ESTABILIZAÇÃO:** a solução deverá ser disponibilizada aos usuários do ambiente de produção, sendo efetuados os ajustes necessários para a estabilização da mesma;

3.1.1.6. **ENCERRAMENTO:** deverá ser entregue a documentação do projeto, e coletada a aprovação formal do cliente;

3.1.2. Da inicialização e planejamento

3.1.2.1. Reunião de startup:

3.1.2.1.1. Apresentação de cronograma;

3.1.2.1.2. Levantamento de requisitos;

3.1.2.1.3. Informações de ambiente;

3.1.2.1.4. Configuração de políticas para planejamento de implementação e configurações.

3.1.2.2. Levantamento de informações do ambiente pertinentes ao projeto de implementação;

3.1.2.3. Alinhamento de requisitos necessários para implementação das soluções;

3.1.2.4. Definição de papeis e responsabilidades;

3.1.2.5. Levantamento de políticas e regras para a solução DLP;

3.1.2.6. Definição e alinhamento de cronograma para implementação das soluções;

3.1.2.7. Após assinado o contrato, a PREFEITURA deverá entregar em até 90 (noventa) dias os documentos necessários para a iniciação do projeto e implementação.

3.1.2.8. O prazo para entrega da CONTRATADA do planejamento de implementação das 12.000 licenças de DLP será de até 25 (vinte e cinco) dias da entrega dos documentos dispostos no item 3.1.2.7 e a CONTRATANTE tem 05 (cinco) dias para dar o aceite no projeto;

3.1.2.9. Não serão considerados responsabilidade da CONTRATADA implementação de agentes em equipamentos fora de pré-requisitos estabelecidos pelo fabricante, sem conectividade com a console central de administração da solução.

3.1.3. Responsabilidade do Fabricante da solução vencedora:

3.1.3.1. Compete a PRODAM acompanhar 30% de implementação em suas dependências com a equipe de analistas de segurança da informação em conjunto com a do fabricante;

3.1.3.2. Deverão executar Health Check (saúde das consoles) na solução de DLP;

3.1.3.3. Deverão ofertar vouchers de treinamento oficial da solução de DLP, realizado pelo próprio fabricante nas dependências do mesmo no Município de São Paulo;

3.1.3.4. Os profissionais deverão ter um contrato de trabalho com o CNPJ do mesmo no Brasil.

3.1.4. Implementação da solução de DLP:

3.1.4.1. Serviço inicial de instalação, devendo a CONTRATADA fornecer mão de obra especializada e própria para realizar as seguintes atividades no início do contrato, sendo que a CONTRATADA e o FABRICANTE deverão apresentar relação contendo os nomes dos empregados que trabalham na execução do contrato e copias de registros dos mesmos junto a empresa, devidamente anotado na carteira de trabalho e previdência social – CTPS;

3.1.4.2. Instalação de consoles de gerenciamento;

3.1.4.3. O serviço de implementação preferencialmente será realizado em horário comercial, das 08h00 às 17h00, de segunda a sexta-feira, excetuando-se feriados nacionais, estaduais e municipais da cidade de São Paulo, exceto horários que poderão ser estabelecidos fora de horário comercial e nos finais de semana, a critério da contratante;

3.1.4.4. Criação de políticas em conjunto com as equipes técnicas e de segurança da informação e infraestrutura da PRODAM, em conjunto com a Prefeitura Municipal de São Paulo.

3.1.5. O prazo para implementação da solução de DLP por parte da CONTRATADA, será de 60 (cento e oitenta) dias corridos a partir do aceite do projeto.

3.1.6. Fase de homologação (Fase Piloto):

3.1.6.1. Para homologação das soluções, o projeto de implementação deverá possuir uma fase inicial (fase piloto) contemplando a instalação dos agentes em 1% (um por cento) do número de total de estações de trabalho, definidas por escopo, contemplando infraestruturas diversificadas, assim como sistemas operacionais, proteção de endpoint e equipamentos de hardwares diferentes nos ambientes da PRODAM.

3.1.6.2. O prazo máximo para homologação da fase piloto será de até 15 dias corridos após a aprovação do projeto.

3.1.7. Fase de Rollout

3.1.7.1. A instalação das soluções ocorrerá em estações de trabalho e servidores instalado na Rede da Prefeitura Municipal de São Paulo administrados pela PRODAM;

3.1.7.2. Deverá ser utilizada como método de instalação (deploy) dos agentes em desktops e notebooks, a instalação remota via console da solução contratada ou solução de distribuição similiar sem custos adicionais. A PRODAM fornecerá os pré-requisitos para viabilidade da instalação remota via console da solução;

3.1.7.3. A instalação (deploy) dos agentes deve ser realizada pela CONTRATADA nas dependências da PRODAM, de forma presencial e nas demais localidades pro meio remoto ou presencial desde que seja comprovada a necessidade técnica ou acordo com a equipe técnica da PRODAM;

3.1.7.4. Será considerada concluída a implementação dos agentes nas estações de trabalho e servidores quando o número de computadores for igual ou superior a 100% do volume de

computadores identificados no levantamento inicial do projeto de implementação:

3.1.7.4.1. Instalação (deploy) dos agentes da solução em servidores físicos e virtuais (sobre a plataforma Microsoft Hyper-V);

3.1.7.4.2. Instalação (deploy) dos agentes da solução em desktop e notebooks, que fazem parte do domínio local (Active Directory), incluindo remoção dos agentes existentes quando aplicável;

3.1.7.4.3. Instalação (deploy) dos agentes da solução em desktop e notebooks, que não fazem parte do domínio local (Active Directory), porem possuem comunicação de rede com a rede principal da PRODAM;

3.1.7.4.4. Geração de pacotes de instalação (deploy) em agentes, para a equipe da PRODAM, e a equipe da PRODAM realizará a instalação (deploy) da solução nos desktops e notebooks que não fazem parte do domínio local (Active Directory), bem como que não possuem comunicação de rede com a rede principal da PRODAM;

3.1.7.4.5. Durante a fase de rollout a CONTRATADA deverá disponibilizar técnicos capacitados para acompanhamento em cada uma das equipes de implementação, com objetivo de resolver problemas de acesso físico e logico às localidades;

3.1.7.4.6. À CONTRATADA ficará a cargo de efetuar a remoção previa dos agentes em servidores devido a criticidade do ambiente;

3.1.7.4.7. Instalação de console centralizada para gestão de todos os itens da solução ofertada no lote desta licitação;

3.1.7.4.8. Intregração de todos os itens que compõem a solução de modo a permitir a visão e o gerenciamento em uma única console;

3.1.7.4.9. Serviço inicial de instalação, devendo a CONTRATADA fornecer mão de obra especializada e própria para realizar as seguintes atividades no início do contrato.

3.1.8. Execução

3.1.8.1. Embora conste previsto que os trabalhos terão o acompanhamento por parte da equipe técnica da CONTRATANTE, cabe intensificar o entendimento que a CONTRATADA terá exclusiva responsabilidade quando à entrega dos serviços destacados, uma vez que estejam em plenas condições de operação munidos de todos os requisitos fornecidos pelo CONTRATANTE e de acordo com os prazos estabelecidos;

3.1.8.2. As condições de execução remota das ações da CONTRATADA visam agilizar e facilitar o projeto, no entanto, eventuais visitas presenciais de técnicos nas unidades da Prefeitura de São Paulo deverão ocorrer sem qualquer ônus para a CONTRATANTE;

3.1.8.3. A CONTRATANTE acompanhará a CONTRATADA em suas localidades de áreas de difícil acesso e/ou risco;

3.1.8.4. A comunicação às unidades da Prefeitura de São Paulo, bem como o agendamento dos trabalhos deverão ser articulados por equipe própria de gestão do projeto da CONTRATANTE.

4. SERVIÇO DE SUPORTE TÉCNICO E GARANTIA

4.1. Os serviços de suporte técnico e garantia abrangem:

4.1.1. Manutenção preventiva, manutenção corretiva, esclarecimento de dúvidas e reparação de problemas na solução;

4.1.2. Elaboração de relatórios, estudos e diagnósticos sobre o ambiente monitorado;

4.2. Os serviços de suporte técnico e garantia abrangem todas as soluções fornecidas pela contratada no âmbito dessa contratação.

4.3. Os serviços de suporte técnico e garantia de toda a solução deverão ser prestados por um período de 12 (doze) meses e deverão ser iniciados a partir da data Emissão do Termo de Aceite da solução.

4.4. Os serviços de suporte técnico poderão ser prestados de forma remota ou presencial no endereço da CONTRATANTE.

4.5. Os bens e produtos adquiridos devem ser licenciados de forma que o suporte e a garantia permitam as atualizações dos sistemas e ferramentas durante a vigência do contrato. Deverão estar incluídas tanto as atualizações de segurança, quanto as atualizações para novas versões dos softwares licenciados, quando disponibilizadas, independente da política de comercialização do fabricante.

4.6. Todas os sistemas ou ferramentas que fazem parte da solução deverão ser disponibilizados na versão mais recente disponibilizada pelo fabricante.

4.7. A CONTRATADA deve garantir que todas as personalizações e configurações realizadas sejam automaticamente portadas para novas versões em caso de atualização, reinstalação ou upgrade, dispensando a necessidade de migrações ostensivas e onerosas.

4.8. Detalhamento de um plano de ação para correção dos problemas identificados, que será executado pela equipe interna da CONTRATANTE, por meio de orientações da Prefeitura.

4.9. A CONTRATADA deverá elaborar, a cada 4 meses, a partir do início do serviço de suporte técnico, relatório sobre a saúde do ambiente da CONTRATANTE utilizando informações fornecidas pela solução

contratada. O relatório deve contemplar, no mínimo, as seguintes informações:

4.9.1. Saúde do ambiente de diretório;

4.9.2. Saúde do ambiente de correio;

4.9.3. Saúde do ambiente de servidores de arquivos;

4.9.4. Análise de dados coletados para identificar e documentar áreas de risco e vulnerabilidades do ambiente;

4.9.5. Evolução em relação a informações de relatórios anteriores.

4.10. O relatório descrito no item anterior deverá ser confeccionado e finalizado durante mês em que se completa cada quadrimestre.

5. PENALIDADES

5.1. Caso haja atraso na entrega da solução, conforme especificado no item 2.7.1, haverá multa de 1,5% por dia de atraso, calculado sobre o valor do contrato;

5.2. Caso haja atraso na disponibilização de profissionais certificados, conforme previsto no item 7.2, haverá multa de 1% ao dia de atraso, calculado sobre o valor do contrato;

5.3. Caso haja atraso na entrega da Inicialização e Planejamento do Projeto de Implementação da Solução, conforme descrito no item 3.1.2, haverá multa de 1,5% por dia de atraso, calculado sobre o valor do contrato;

5.4. Caso haja atraso na fase de homologação (3.1.6), haverá multa de 1% por dia de atraso calculado sobre o valor do contrato.

5.5. Caso haja atraso na implementação, conforme especificado no item 3.1.5, haverá multa de 1,5% por dia de atraso, calculado sobre o valor do contrato;

5.6. Caso o tempo para atendimento ultrapasse as 4 horas, contadas a partir da abertura do chamado, conforme item 7.12, haverá multa de 1% por hora de atraso, calculado sobre o valor mensal do contrato;

5.7. Caso o tempo para a solução de um chamado de manutenção ultrapasse as 6 horas, contatadas a partir da abertura do chamado, conforme item 7.12, haverá multa de 0,5% por hora de atraso, calculado sobre o valor mensal do contrato;

5.8. Caso haja atraso na substituição do equipamento avariado por um novo após 120 horas da abertura do chamado sem solução, conforme item 7.14, será cobrada multa de 5% por dia de atraso, calculado sobre o valor do contrato.

5.9. Caso haja atraso na entrega dos treinamentos conforme especificado no edital, haverá multa de 2% por dia de atraso, calculado sobre o valor do item treinamento;

6. OBRIGAÇÕES DA CONTRATANTE

6.1. Nomear gestor e fiscal do contrato para acompanhar e fiscalizar a execução do contrato;

6.2. Encaminhar formalmente à Contratada a demanda de acordo com os critérios técnicos estabelecidos no Termo de Referência;

6.3. Comunicar formalmente à Contratada quaisquer ocorrências relacionadas a execução do contrato;

6.4. Disponibilizar recursos de infraestrutura e logística quando forem necessários a execução ou entrega do objeto;

7. OBRIGAÇÕES DA CONTRATADA

7.1. A Contratada deverá oferecer garantia, suporte e licenças da solução e suas funcionalidades contratadas por um prazo mínimo de 12 meses, a contar da data de sua efetiva instalação; durante o período de cobertura, a CONTRATADA devera prestar Serviços de Manutenção “On Site”, para todos os componentes do objeto deste edital, incluindo configuração técnica do produto;

7.2. Disponibilizar profissionais certificados pelos fabricantes da solução;

7.3. Instalar, configurar e acompanhar os testes de funcionamento antes da entrada de produção dos equipamentos;

7.4. Orientar tecnicamente os responsáveis pela operação dos equipamentos, fornecendo os esclarecimentos necessários ao seu perfeito funcionamento;

7.5. Disponibilizar número de telefone (local ou DDG) para suporte telefônico (24x7x365) e abertura de chamados técnicos;

7.6. Ao final da abertura de cada atendimento de suporte, a CONTRATADA deverá emitir um ticket do chamado técnico contendo, no mínimo:

7.6.1. Número do chamado;

7.6.2. Data e hora de abertura do chamado;

7.6.3. Previsão de conclusão do atendimento;

7.6.4. Severidade do erro;

7.6.5. Descrição da solicitação.

7.7. A CONTRATADA deverá disponibilizar relatórios de chamados por período, contendo, no mínimo, as seguintes informações:

7.7.1. Número do chamado;

7.7.2. Data e hora de abertura do chamado;

7.7.3. Data e hora do início do tratamento do chamado;

7.7.4. Data e hora de resolução do chamado;

7.7.5. Prazo Total de Início do Tratamento do Chamado (ITC);

7.7.6. Prazo Total de Resolução do Chamado (PRC)

7.7.7. Início do Tratamento do Chamado (ITC) cumprido (Sim/Não);

7.7.8. Prazo para Resolução do Chamado (PRC) cumprido (Sim/Não);

7.7.9. Contato do técnico atendente;

7.7.10. Responsável pelo registro do chamado;

7.7.11. Severidade do chamado;

7.7.12. Descrição da solicitação;

7.7.13. Solução aplicada;

7.8. Depois de concluído o chamado, a CONTRATADA comunicará o fato à equipe técnica da CONTRATANTE e solicitará autorização para o

fechamento deste. Caso a CONTRATANTE não confirme a solução definitiva do problema, o chamado permanecerá aberto até que seja efetivamente solucionado pela CONTRATADA. Nesse caso, a CONTRATANTE fornecerá as pendências relativas ao chamado aberto.

7.9. A CONTRATANTE poderá registrar um número ilimitado de chamados de suporte durante a vigência do Contrato.

7.10. Toda infraestrutura necessárias para o pleno funcionamento da solução, como servidores, sistemas operacionais, banco de dados, licenças, entre outros hardwares e softwares necessários, deve ser disponibilizado em nosso datacenter pela CONTRATADA;

7.11. Proceder à entrega dos equipamentos, devidamente embalados, de forma a não serem danificados durante a operação de transporte e de carga e descarga, com as especificações detalhadas para conferência;

7.12. O modelo do equipamento (solução) ofertado deverá estar em linha normal de produção e sem previsão de encerramento;

7.13. O tempo máximo de atendimento para os chamados de defeitos deverá ser de 4 hs (quatro horas) e de solução em até 6 h (seis horas) a contar do registro de abertura do chamado no Centro de Atendimento Técnico da Contratada, realizando testes e corrigir defeitos, inclusive com a sua substituição quando necessário, sem ônus para a CONTRATANTE, durante o período de garantia;

7.14. A cada visita técnica realizada nas dependências da CONTRATANTE a CONTRATADA deverá emitir um relatório de execução das atividades, relacionando os serviços executados e lista de equipamentos que eventualmente sejam deixados ou retirados das dependências da CONTRATANTE;

7.15. Caso a Contratada não consiga recuperar o equipamento em até 72 horas após a abertura do chamado, o appliance com problema deverá ser substituído por outro novo em até 120 horas após a abertura do chamado;

7.16. A Contratada deverá acompanhar com pessoal in loco o primeiro dia útil de operação do ambiente em produção.

8. CONDIÇÕES DE FATURAMENTO

8.1. O valor será faturado mensalmente e o encaminhamento da Nota Fiscal de Eletrônica de Serviços deverá ser realizado através de Solicitação de Pagamento, a partir do 1º (primeiro) dia subsequente ao mês da efetiva prestação dos serviços e autorização do Gestor do Contrato.

8.1.1. O primeiro faturamento está condicionado à emissão do Termo de Aceite Final, conforme previsto no item 15.3.

8.2. O valor relativo à Instalação/configuração e treinamentos será faturado a partir da emissão dos respectivos Termo de Aceite de Entrega e Instalação e Termo de Aceite de Conclusão de Treinamento, previstos nos itens 15.1 e 15.2 e o encaminhamento da Nota Fiscal Eletrônica de Serviços deverá ser realizado através de Solicitação de Pagamento, a partir do 1º (primeiro) dia subsequente à emissão dos termos acima e autorização do Gestor do Contrato.

9. PROPOSTA PARA CONDIÇÕES DE PAGAMENTO

9.1. A Nota Fiscal Eletrônica de Serviços deverá ser emitida e encaminhada à CONTRATANTE, através do setor de Expediente, por meio do endereço gfl@prodam.sp.gov.br.

9.1.1. Após o recebimento da Nota Fiscal de Serviços, a CONTRATANTE disporá de até 05 (cinco) dias úteis para emissão do Termo de Aceite de Pagamento, aprovando os serviços prestados.

9.1.2. O pagamento será realizado por intermédio de crédito em conta corrente ou por outra modalidade que possa vir a ser determinada pela Gerência de Planejamento e Controle Financeira (GFP), em 30

(trinta) dias corridos a contar da data de emissão do Termo de Aceite de Pagamento.

9.2. Caso a Nota Fiscal Eletrônica de Serviços contenha divergências com relação ao estabelecido no Instrumento Contratual, a CONTRATANTE ficará obrigada a comunicar a empresa CONTRATADA, formalmente, o motivo da não aprovação no prazo de 05 (cinco) dias úteis. A devolução da Nota Fiscal Eletrônica de Serviços, devidamente, regularizada pela CONTRATADA, deverá ser efetuada em até 05 (cinco) dias úteis da data de comunicação formal realizada pela CONTRATANTE.

9.3. Em caso de atraso de pagamento dos valores devidos à CONTRATADA, mediante requerimento formalizado por esta, incidirão juros moratórios calculados utilizando-se o índice oficial de remuneração básica da caderneta de poupança e de juros simples no mesmo percentual de juros incidentes sobre a caderneta de poupança, para fins de compensação da mora (TR + 0,5% "*pro-rata tempore*"), observando-se para tanto, o período correspondente à data prevista para o pagamento e aquela data em que o pagamento efetivamente ocorreu.

10. QUALIFICAÇÃO TÉCNICA

10.1. A LICITANTE deverá apresentar, em seu nome, atestado (s) de capacidade técnica, emitido (s) por pessoa jurídica de direito público ou privado, comprovando a execução de atividade pertinente e compatível em características e quantidades, com o objeto a ser contratado, relativo ao fornecimento de 6.000 licenças DLP (50% do objeto)

10.2. Comprovação de que o licitante possui autorização do fabricante para comercializar, instalar e prestar suporte no Brasil para o produto especificado. A comprovação deverá ser feita por meio de declaração do fabricante e destinada a PRODAM e com referência explícita a este processo de aquisição.

10.3. A licitante deverá comprovar a capacitação técnico-profissional, demonstrando possuir em seu quadro permanente de pessoal, na data da licitação, 2 (dois) profissionais técnicos nível pleno, com formação superior em ciência da computação, análise de sistemas, processamento de dados, engenharia, áreas exatas, ou MBA ou especialização na área de TI; possuir experiência em prestação de serviços de segurança da informação e conter no mínimo suporte em ambiente Microsoft Windows e Linux do software de prevenção contra perda de dados - DLP.

11. TREINAMENTO

11.1. Deverão ser fornecidos treinamentos para as soluções de DLP, ministrados por instrutor certificado e autorizado pelo fabricante, para 6 funcionários, dividido em turmas de no máximo 2 funcionários, agendadas em datas distintas a critério da CONTRATANTE, e em acordo com a CONTRATADA;

11.2. Os treinamentos poderão ser fornecidos em turmas abertas;

11.3. Os treinamentos deverão ser finalizados em até 180 dias após assinatura do contrato e em acordo entre as partes.

11.4. O treinamento deverá ser ministrado dentro do município de São Paulo em ambiente próprio e dedicado para este fim, caso o treinamento seja realizado fora do município de São Paulo, a CONTRATADA será responsável pelas despesas de transporte, hospedagem e alimentação;

11.5. No caso de excepcionalidade de permanência do isolamento social, o treinamento poderá ser fornecido de forma remota distribuído conforme item 11.1.

11.6. Os treinamentos deverão ser em idioma português do Brasil;

11.7. O material didático poderá ser em idioma português ou idioma inglês;

11.8. O treinamento deverá ser capaz de instruir os alunos administrar e operar as soluções adquiridas;

11.9. Os treinamentos deverão ter no mínimo carga horaria igual ou superior a 32 horas cada;

11.10. Ao final dos treinamentos, deverá ser emitido certificado de participação;

11.11. O aceite para pagamento dos treinamentos somente será emitido após a finalização da capacitação dos 6 funcionários.

12. PRAZO DE ENTREGA

12.1. O prazo máximo de entrega de todo hardware/software/licenças que compõem a a solução será de 30 (trinta) dias corridos, contados a partir da data de assinatura do contrato.

12.2. Toda a solução deverá ser entregue e instalada no Município de São Paulo;

12.3. Prazo máximo para instalação e configuração do gerenciamento da solução será de 30 (trinta) dias corridos contados a partir da entrega dos equipamentos, devendo obrigatoriamente ser realizada em finais de semana ou feriados, conforme agendamento da contratante.

12.4. Prazo máximo para ativação da solução contratada (conforme item 3.1.5) será de até 180 dias corridos contados a partir da assinatura do contrato.

13. DOCUMENTAÇÃO TÉCNICA

13.1. Deverão ser fornecidos juntamente com a solução, os manuais técnicos de referência, contendo todas as informações sobre os produtos com as instruções para instalação, configuração e operação, preferencialmente em Português (Brasil), ou, na inexistência de tradução em Português, podem ser escritos em Língua Inglesa;

14. CONFIDENCIALIDADE

14.1. A CONTRATADA deverá zelar pelo sigilo de quaisquer informações referentes à estrutura, sistemas, usuários, contribuintes, topologia, e ao modo de funcionamento e tratamento das informações da CONTRATANTE, durante e após fim do contrato, salvo se houver autorização expressa da Contratante para divulgação;

14.2. Não haverá nenhum tipo de facilidade de acesso remoto, tão menos envio de forma automática ou controlada de informações (backdoor) originadas de software/hardware contratado ou adquirido sem o conhecimento e formal autorização da Contratante. A não observância desse fato poderá ser considerada espionagem e será motivo de processo civil e criminal conforme legislação vigente.

15. ACEITE

15.1. Após a instalação e configuração da solução de gerencimento, a equipe técnica da PRODAM emitirá o Termo de Aceite de Entrega e Instalação da solução em até 5 (cinco) dias úteis após a formalização pela CONTRATADA da finalização do processo de instalação/configuração (operação) e que todos os quesitos estão sendo cumpridos conforme o Edital.

15.1.1. Entende-se pela instalação e configuração, tanto a parte física da solução, configuração lógica de todos os produtos/serviços e testes de todas as regras e procedimentos necessárias à operação do serviço.

15.2. Após a conclusão do treinamento, conforme especificado no item 11, a equipe técnica da PRODAM emitirá o Termo de Aceite de Conclusão de Treinamento da solução em até 5 (cinco) dias úteis após a formalização pela CONTRATADA de sua conclusão, conforme o Edital;

15.3. Após a instalação do agente em 100% das estações identificadas no levantamento inicial, conforme previsto no item 3.1.7.4, a equipe

técnica da PRODAM emitirá o “TERMO DE ACEITE FINAL” da solução em até 5 (cinco) dias úteis após a formalização pela CONTRATADA da finalização do processo de instalação/configuração e confirmação de que todos os quesitos estão sendo cumpridos conforme o Edital, iniciando os pagamentos mensais;

São Paulo, 20 de outubro de 2020.

WAGNER KANAGUSUKO
Gerência de Segurança Operacional

TERMO DE ACEITE DE PAGAMENTO

CONTRATADA: <nome completo da empresa contratada>

CONTRATO: <número do contrato>

OBJETO: <breve definição do objeto de contratação>

ATESTAMOS, para os devidos fins, que a empresa <**nome da empresa**>, procedeu com a prestação dos serviços de <**apontar os serviços prestados**>, discriminados na Nota Fiscal de Serviços n.º <inserir número>, emitida em __ / __ / 20_, referente ao <inserir o número do CO-00.00/000, <**dentro ou fora**> do prazo previsto, não havendo em nossos registros nenhum fato que desabone a conduta da empresa, respeitando as formalidades legais e cautelas de estilo, motivo pelo qual assinamos o presente termo.

São Paulo,___ de _____ de 20__.

NOME DO GESTOR DA CONTRATAÇÃO
Cargo ou Função
Gerência <detalhar> (XXX)

NOME DO FISCAL DA CONTRATAÇÃO
Cargo ou Função
Gerência <detalhar> (XXX)

TERMO DE ACEITE DE ENTREGA E INSTALAÇÃO

CONTRATADA: <nome completo da empresa contratada>

CONTRATO: <número do contrato>

ORDEM DE SERVIÇO Nº: <número da Ordem de Serviço>

OBJETO: <breve definição do objeto de contratação>

A documentação gerada pela empresa <CONTRATADA> e elencada como produtos entregues do período de __/__/____ até __/__/____ no documento “Confirmação de recebimento de produtos”, parte integrante deste processo, estão disponíveis para consulta e/ou reprodução a qualquer momento no servidor corporativo da PRODAM, identificado no link a seguir:
Todos os produtos foram entregues à equipe de projeto da PRODAM e constam da documentação do sistema atualizada.

Através deste documento, a PRODAM formaliza o recebimento dos itens listados previstos em contrato para o referido período e também atesta que nada consta contra qualidade dos itens apresentados, confirmando-se assim a entrega da versão final e consequente autorização do faturamento do período em questão deste contrato e ordem de serviço.

São Paulo, __ de _____ de 20__.

NOME DO GESTOR DA CONTRATAÇÃO
Cargo ou Função
Gerência <detalhar> (XXX)

NOME DO FISCAL DA CONTRATAÇÃO
Cargo ou Função
Gerência <detalhar> (XXX)