SERVIÇO PÚBLICO FEDERAL
MINISTÉRIO DA FAZENDA
SUPERINTENDÊNCIA DE SEGUROS PRIVADOS – SUSEP
DIRETORIA DE ADMINISTRAÇÃO
COORDENAÇÃO-GERAL DE TECNOLOGIA DA INFORMAÇÃO

TERMO DE REFERÊNCIA – CGETI Nº 01/2015 /PROJETO BÁSICO

1 – DEFINIÇÃO DO OBJETO

Contratação de empresa para prestação de serviços continuados de DATA CENTER, incluindo os serviços de hospedagem, armazenamento, processamento e comunicação de dados ponto-a-ponto com capacidade para prover tráfego de dados entre as unidades que compõem a Susep (Sede – Rio de Janeiro, São Paulo, Brasília, Rio Grande do Sul e Minas Gerais) e fornecimento de contas de correio eletrônico para esta Autarquia, pelo prazo de 36 meses.

2 – FUNDAMENTAÇÕES DA CONTRATAÇÃO

2.1 – RELAÇÃO DEMANDA X NECESSIDADE

Id	Demanda Prevista
1	Serviço de Hospedagem *de Sistemas e Gerenciamento do Centro de Dados*
2	Serviço de Fornecimento e Administração de Rede de Longa Distância
3	*Serviço de Correio Eletrônico*

2.2 – MOTIVAÇÃO

No atual contexto de atuação da Susep (fiscalizar a constituição, organização, funcionamento e operação das Sociedades Seguradoras, de Capitalização, Entidades de Previdência Aberta e Resseguradores, zelar pela defesa do interesse dos consumidores junto ao mercado supervisionado, monitorar a estabilidade, liquidez e solvência deste mesmo mercado etc.) configura-se como grande desafio da Coordenação Geral de Tecnologia da Informação - CGETI estruturar adequadamente informações e dados para compor a visão estratégica da organização, procurando alinhar a missão e os objetivos da instituição com os objetivos estratégicos desta mesma CGETI. Acrescente-se ainda a necessidade de atender às boas práticas de Governança de TI, conforme acórdão 2746/2010 do TCU, apoiar a crescente demanda da população usuária de sistemas da Susep. Amparado ainda pelo Art. 10, do Decreto-Lei 200/67, cujo objetivo é concentrar esforços na gestão em detrimento da execução de tarefas, julgamos como melhor alternativa a contratação de empresa dotada de recursos tecnológicos e humanos adequados.

Com efeito, a demanda de processamento de dados desta Autarquia tem aumentado significativamente nos últimos anos e, assim como acontece no mercado, novos serviços são criados para atender às necessidades internas da Administração bem como para as entidades supervisionadas. Para suportar este crescimento, a área de Tecnologia de Informação (TI) também precisou evoluir, aumentando a quantidade de equipamentos e sistemas nesta Instituição. Com isso, aumentou também a complexidade e, consequentemente, a responsabilidade por manter todo ambiente operacional e os sistemas/serviços disponíveis. Anote-se ainda que a manutenção de todo este aparato tecnológico internamente demandaria grande quantidade de pessoal em turnos variáveis, do contrário poderia haver falhas e problemas técnicos constantes.

Visando superar a problemática de um ambiente sensível a falhas, composto por equipamentos únicos, sejam servidores, sejam equipamentos para conexões de rede, a Susep optou pela hospedagem da infraestrutura de servidores e armazenamento em Centros de Dados externos (decisão esta corroborada pelo Comitê de Tecnologia da Informação). Analisando-se detidamente o elevado montante de recursos necessários para implantação e manutenção de um ambiente de Centro de Dados interno que atenda às necessidades da Susep, verifica-se a premente necessidade de contratação destes serviços junto a empresas especializadas. Melhor explicando: os Centros de Dados (*Data*

Centers) hospedam recursos críticos de tecnologia da informação em ambiente altamente controlado e gerenciado diuturnamente para suportar aplicações empresarias ou governamentais. O projeto em tela contempla, ainda, um ambiente corporativo voltado para a qualidade nos serviços e agilidade no atendimento às demandas por sistemas, reduzindo custos internos de desenvolvimento e aquisição de licenças de software. Funcionalmente, o Centro de Dados (data Center) opera como um elo entre a rede Internet e o *backbone* constituído pelos canais de comunicação que interligam as diversas unidades da CONTRATANTE. Esta abordagem vem sendo adotada com sucesso pela Autarquia desde 2008, quando da contratação do Serviço Federal de Processamento de Dados (Serpro) e posteriormente com a contratação por pregão eletrônico da Level 3 Comunicações do Brasil, cujo contrato se encerra em 20 de junho de 2015. A presente contratação visa dar continuidade ao modelo atual, ampliando a flexibilidade e escalabilidade do ambiente, o que certamente levará a uma maior eficiência na utilização dos recursos.

Permanece a necessidade de uma solução integrada de rede de comunicações, com o objetivo de prover tráfego ininterrupto de dados, voz e imagem entre as unidades da Susep (Sede, no Rio de Janeiro, e suas Regionais – SP, RS, MG, RJ2 e BSB). Esta integração via rede de comunicações objetiva oferecer acesso aos diversos Sistemas internos da Susep (FIP/SAPIEMS/SES e demais aplicações) às Regionais citadas, para o regular cumprimento de suas funções institucionais, bem como acesso seguro aos arquivos eletrônicos internos. Ademais, a solução em questão compreenderá o fornecimento, a instalação, a manutenção, o gerenciamento e a monitoração de porta de comunicação com a Rede mundial de computadores e ainda serviços de borda com a Internet, tais como: firewall, DNS, VPN e Proxy.

Igualmente importante é o serviço de correio eletrônico para os colaboradores desta Casa. Devido à forte integração entre a infraestrutura de centro de dados, os sistemas de informação internos e o correio eletrônico, os ganhos com a unificação de diretório de usuários, bem como à possibilidade de redução de custos pelo compartilhamento de enlaces de dados, consideramos imprescindível que este serviço (correio eletrônico) seja parte integrante e indissociável deste certame, integrado à solução de segurança e disponibilidade do Centro de Dados (*data Center*).

Há que se destacar que a decisão estratégica desta Coordenação Geral de Tecnologia da Informação de manter em ambiente externo à Susep o Centro de Dados foi corroborada unanimemente pelo Comitê de TI desta Autarquia, no dia 13 de fevereiro de 2012. Contribuíram à época para a tomada de decisão do referido comitê principalmente os altos custos de manutenção de um centro de dados interno bem como eventual alocação de recursos públicos em ativos fixos cujas depreciação e defasagem tecnológica são constantes.

Ressalta-se ainda a necessidade de aquisição conjunta dos serviços citados, a saber: centro de dados (*data Center*), rede WAN e correio eletrônico. Preliminarmente, sublinhe-se que os serviços a serem licitados formam um conjunto harmônico e com configurações técnicas interdependentes. Dividir os itens seria temerário, pois dificilmente identificaríamos a responsabilidade técnica por alguma instabilidade ou inoperância dos serviços, haja vista a complementaridade dos mesmos. Diante do exposto, decidiu-se contratar todos os serviços mencionados em regime de menor preço global.

Por fim, faz-se necessário salientar que os custos internos e externos, bem como os prazos necessários à migração de dados descrita no item 4 do presente Termo de Referência, se mostram incompatíveis com prazos contratuais inferiores aos 36 meses aqui propostos. Ademais, estudos realizados quando do planejamento de contratação de solução semelhante, no ano de 2012, demonstraram que o custo mensal é sobremaneira onerado para contratos com prazos de 12 (doze) e 24 (vinte e quatro) meses~~)~~. Estes estudos estão descritos no Processo Susep nº 15414.001808/2012-61 e resumidos no documento de Estratégia de Contratação relativo àquele certame.

2.3 – RESULTADOS A SEREM ALCANÇADOS

Id	Tipo	Resultado
1	Redundância	A PROPONENTE deve prover mecanismos de redundância e contingência para evitar e/ou minimizar os impactos de paralisações inesperadas, tanto no que tange ao fornecimiento dos enlaces (links) quanto às informações armazenadas no Centro de Dados (Data Center).
2	Segurança	Implantação de controles que minimizem riscos de acesso indevido, físico ou lógico, às informações armazenadas e trafegadas pela CONTRATADA. Mais: responder a tentativas de interrupções de serviços, invasões e ataques externos através da proteção da infraestrutura, das aplicações e dos dados com segurança elevada.
3	Gerenciamento	Oferecer recursos de gerenciamento centralizado e criar um domínio de gestão unificado baseados em melhores práticas de Governança de TI, como, por exemplo, os padrões Cobit e Itil.
4	Escalabilidade	Permitir a ampliação e retração da infraestrutura de acordo com a demanda da autarquia, obtendo benefício da hospedagem em um ambiente de larga escala e aumentando a eficiência na alocação de recursos.

2.4 – JUSTIFICATIVA DA SOLUÇÃO ESCOLHIDA

Id	Necessidade	Benefício	Tipo
1	Diminuição de investimentos em ativos fixos.	Desnecessidade de consideráveis investimentos em equipamentos, evitando assim a obsolescência dos mesmos em médio prazo e mantendo a instituição atualizada tecnologicamente.	Administrativo
2	Segurança: Alta disponibilidade para arquivos armazenados e Sistemas em Produção.	Proteger aplicativos e sistemas de informação da Susep contra inatividade planejada ou não através da automação da recuperação de aplicativos em ambientes físicos e virtuais na maioria dos servidores e plataformas de armazenamento.	Técnico
3	Redução de Custos Operacionais.	Redução de custo tendo em vista a consolidação dos diversos servidores e equipamentos de interconexão de rede em um único sítio, entretanto com estrutura tecnológica superior.	Administrativo

4	Monitoração e avaliação contínua do desempenho das aplicações.	Monitorar transações executadas pelos usuários das aplicações e componentes de infraestrutura de forma pró-ativa em um único ambiente de gerenciamento, altamente especializado.	Técnico

3 – DESCRIÇÃO DA SOLUÇÃO DE TI (Requisitos Técnicos Mínimos)	
ITEM	**DESCRIÇÃO**
1	***Serviço de Hospedagem de Sistemas e Gerenciamento do Centro de Dados*** O objetivo do Serviço de Hospedagem *de Sistemas e Gerenciamento do Centro de Dados* é prover toda a infraestrutura necessária para abrigar os ambientes operacionais de hospedagem (*hosting*) de sistemas em produção, homologação e desenvolvimento da Susep. **A) Das Características Físicas do Centro de Dados (Data Center):** A.1 Ambiente do Centro de Dados restrito, monitorado por CFTV, controlado e com registro de acesso físico, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana; A.2 Rede elétrica estabilizada e com mais de uma entrada de alimentação; A.3 Grupo-gerador redundante (N+1) e independente, com comando automático para suprimento na eventualidade de interrupção no fornecimento de energia comercial e autonomia mínima de 72 (setenta e duas) horas; A.4 Sistema redundante de baterias para garantir a transição entre o fornecimento normal de energia e o grupo gerador; A.5 Temperatura ambiente controlada por sistemas de Climatização redundantes (N+1); A.6 Sistema de monitoração para controle de temperatura, umidade relativa do ar e filtros contra poeira; A.7 Piso suspenso com, no mínimo, 2 (duas) camadas de cabeamento, com vias independentes para cabos de energia, cabos UTP e cabos óticos; A.8 Sistema de detecção e combate a incêndio com uso de sensores de fumaça e fogo distribuídos pela área do Centro de Dados e uso de gás inerte para extinção (FM200 ou equivalente); A.9 Sistema de detecção de fumaça, extintores manuais e brigada de incêndio; A.10 Devido à importância para a CONTRATANTE, a mesma poderá auditar as instalações relativamente ao item anterior por meio de vistorias e testes acordados com a PROPONENTE. **B) Descrição geral dos Serviços de Hospedagem de Sistemas e Gerenciamento do Centro de Dados**

B.1 O serviço de hospedagem de sistemas será prestado no Centro de Dados da PROPONENTE e contemplará a instalação, configuração, manutenção de recursos de hardware e software, acesso à internet, armazenamento, segurança, gerenciamento e processamento dos dados da CONTRATANTE.

B.2 A CONTRATADA deverá providenciar e manter equipe técnica qualificada para a prestação dos serviços requisitados no presente edital, que serão responsáveis pela administração do ambiente de infraestrutura da Susep.
B.3 Qualquer alteração a ser efetuada no ambiente da Susep pela CONTRATADA deverá ser acordada com a equipe técnica da Autarquia, de acordo com um processo de gerência de mudanças. A proposta de prestação de serviços a ser apresentada pela PROPONENTE e aprovada pela CONTRATANTE deverá detalhar estes procedimentos.
B.4 O Centro de Dados contemplará infraestrutura conjugada de hardware e software, responsável pela prestação dos serviços de firewall, Proxy *cache*, serviço de resolução de nomes (DNS), detecção e prevenção de intrusão, distribuição e filtragem de e-mails (*mail relay*), filtragem de conteúdo web e VPN.
B.5 O DNS deve ser configurado em pelo menos dois servidores distintos por questões de contingência. Deve haver um servidor mestre com autoridade sobre uma determinada zona cujos dados são derivados dos arquivos locais e outro equipamento distinto utilizado como secundário (*slave*).
B.6 A CONTRATADA deverá disponibilizar serviço de *relay* SMTP (*Simple Mail Transfer Protocol*), permitindo que aplicações efetuem o envio de e-mails para endereços internos e externos, de acordo com as regras a serem definidas para cada aplicação.
B.7 A CONTRATADA deverá disponibilizar serviço de NTP (*Network Time Protocol*) para a sincronização de horário dos equipamentos servidores fornecidos para a Susep. O serviço deverá sincronizar com outros servidores NTP disponíveis na internet.
B.8 Os equipamentos disponíveis no Centro de Dados da PROPONENTE deverão ser gerenciados e monitorados pela MESMA, 24 horas por dia, 7 (sete) dias por semana.
B.9 A PROPONENTE deverá empenhar-se em manter atualizados tecnologicamente todos os equipamentos destinados à execução dos serviços disponíveis no Centro de Dados, configurando as últimas versões/atualizações/correções recomendadas (hardware/software), de modo a assegurar a plena integridade do ambiente.
B.10 A PROPONENTE deverá dimensionar, inicialmente, os equipamentos destinados à execução dos serviços disponíveis no Centro de Dados para suportar, sem perda de desempenho, acesso simultâneo de até 600 (seiscentas) estações de trabalho à internet.
B.11 A PROPONENTE deverá manter a capacitação de seus funcionários e colaboradores em técnicas e metodologias de gerenciamento de serviços e data Center.
B.12 A PROPONENTE deverá observar as práticas de gerenciamento de serviços de tecnologia definidas pela biblioteca de serviços ITIL (*Information Technology Infrastructure Library*).
B.13 A PROPONENTE deverá se utilizar de processos de monitoramento, gerência

de falhas e de mudanças, além de possibilitar a verificação dos NÍVEIS MÍNIMOS DE SERVIÇO (NMS) objeto desta contratação.
B.14 A PROPONENTE deverá submeter à aprovação da CONTRATANTE as paradas programadas de equipamentos ou serviços com antecedência mínima de 3 (três) dias úteis.
B.15 Em caso de paradas emergenciais, a qualquer tempo, a PROPONENTE deverá realizar os serviços de manutenção corretiva, quando possível, em finais de semana ou em dias úteis após as 19h00, mitigando a indisponibilidade dos sistemas e acesso à internet. Tais paradas deverão ser previamente aprovadas pela CONTRATANTE.
B.16 O serviço de hospedagem de sistemas e gerenciamento do centro de dados, contemplará ainda as seguintes rotinas:

- Operação de servidores, fitotecas, equipamentos de interconexão de rede e periféricos em geral.
- Administração e manutenção das bases de dados da CONTRATANTE.
- Monitoração de servidores, disponibilidade de serviços (Sistema Operacional, Banco de Dados e aplicações web).
- Administração do diretório de usuários.

B.17 A CONTRATADA deverá manter disponível ferramenta para a abertura de chamados e consultas técnicas, reporte de incidentes e abertura de solicitações de serviço, via web, telefone e e-mail, durante 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana.
B.18 A CONTRATADA disponibilizará, mensalmente, relatório gerencial dos incidentes e solicitações abertas, para que a Susep possa atestar o provimento dos serviços. Além disso, para fins de controle e auditoria, a CONTRATADA deve disponibilizar as informações supracitadas para a equipe técnica da Susep, a qualquer tempo, através de sistema informatizado.
B.19 Todas as ferramentas de gerenciamento e monitoração a serem fornecidas pela CONTRATADA deverão permitir acesso de leitura para a equipe técnica da Susep para a verificação e validação das atividades executadas, além de relatórios gerenciais para a aferição dos serviços prestados.
B.20 Em relação à Segurança da Informação do Centro de Dados (Data Center), especifica-se:

- O ambiente de uso exclusivo da Susep deverá possuir as seguintes funcionalidades de segurança mínimas, porém não exaustivas, em face da evolução contínua das boas práticas deste tipo de serviço:
    - Firewall com s*tateful packet inspection*.
    - Controle de Aplicação;
    - Filtro de Conteúdo Web;
    - Sistema de Prevenção de Intrusão (IDS/IPS);
    - *Antimalware* / Antivírus;
    - VPN IPSEC (*Client-to-Site* e *Site-to-Site*) e SSL para 150 usuários simultâneos;
    - Suporte a qualidade de serviço (QoS) com traffic shaping;
- As funcionalidades acima descritas deverão ser implementadas pela CONTRATADA através de hardwares dedicados com fim específico (*appliances*), podendo duas ou mais funções serem agregadas em equipamentos do tipo UTM (*Unified Threat Management*).

- As políticas dos dispositivos de segurança citados acima serão implementadas pela CONTRATADA, que deverá possuir pessoal qualificado à operação do ambiente descrito, de acordo com as regras definidas pela Susep.
- Todo o tráfego de entrada e saída da rede da Susep deverá passar pelos equipamentos de segurança aqui descritos, de modo que seja possível, a critério da CONTRATANTE, definir os controles e restrições necessários, com a colaboração da equipe da CONTRATADA.
- Os equipamentos que atenderão aos serviços acima deverão ser estruturados em cluster, de forma redundante, permitindo balanceamento de carga e/ou *failover* completo na ocorrência de falhas.
- O firewall em questão deve permitir filtragem de pacotes através da análise do endereço de origem, endereço de destino, serviço (TCP, UDP, ICMP, etc.). As configurações de regras e filtros a serem implementadas nos equipamentos de firewall deverão ser estabelecidas de acordo com as políticas de Segurança do CONTRATANTE.
- As solicitações de alterações, exclusões e inclusões de novas regras, como, por exemplo, filtros de pacotes, bloqueios de endereço IP e fixação de endereço IP e NAT, deverão ser avaliadas e efetivamente operacionalizadas pela PROPONENTE, em um prazo máximo de 24 (vinte e quatro) horas.
- A CONTRATADA deverá:
  - Adotar controles físicos e lógicos inerentes à execução dos serviços, de forma a garantir a integridade, a confidencialidade, a disponibilidade e autenticidade dos dados e informações.
  - Utilizar-se de melhores práticas e tecnologias reconhecidas pelo mercado no sentido de gerir e operacionalizar a segurança da informação e comunicação, bem como de prevenir incidentes.
  - Utilizar software para detecção e remoção de códigos maliciosos (antivírus / anti-malware) de amplo reconhecimento e utilização pelo mercado.
  - Tratar Incidentes de Segurança (Vírus, SPAM/Phishing e outros) em conjunto com a Equipe de Tratamento de Incidentes de Rede - ETIR da Susep.
  - Consolidar relatórios mensais de ataques e incidentes para apresentação à CONTRATANTE.
  - Proteger todos os componentes da solução CONTRATADA (hardware e software) contra vulnerabilidades conhecidas e que venham a ser divulgadas pelos fabricantes.
  - Nos casos de resposta a ataques e vulnerabilidades que ensejarem intervenção na infraestrutura, a CONTRATANTE deverá ser consultada (excetuando-se as emergências fora do horário comercial, sendo obrigada a PROPONENTE a relatar prontamente tais alterações).
  - Manter a capacitação de seus funcionários e colaboradores em técnicas e metodologias de gerenciamento de segurança da informação e comunicação.
  - Adotar controles e métodos presentes nas normas ISO família 27000.

C) Recursos a serem providos para as soluções de TIC:

C.1 Nenhum dos equipamentos utilizados no atendimento dos serviços (servidores de rede, roteadores, firewalls etc.) poderá estar descontinuado pelo fabricante.
C.2 Os servidores de rede deverão ser fornecidos em ambiente virtualizado.
C.3 A solução tecnológica apresentada deverá possuir estrutura de rede local exclusiva para a CONTRATANTE e as conexões entre todos os servidores dos ambientes de homologação, produção e desenvolvimento deverão ter banda garantida igual ou superior a 1(um) Gbps (Gigabits por segundo) em método full duplex cada.
C.4 A configuração e manutenção da infraestrutura de hardware dos servidores, de acordo com os requisitos mínimos definidos serão de responsabilidade da CONTRATADA e deverão seguir diretrizes definidas pela SUSEP.
C.5 O pagamento mensal do contrato será apurado consoante utilização dos recursos (memória/disco/núcleos virtuais de processador), de todos os AMBIENTES.
C.6 A CONTRATADA deverá fornecer um pool de recursos, a serem utilizados de acordo com as necessidades definidas pela equipe técnica da Susep, nos limites estabelecidos no quadro abaixo:

Estimativas de Utilização de Recursos de Tecnologia da Informação			
Ambientes	**Elementos**	**Mínimo Mensal**	**Máximo Mensal**
Ambiente de Produção	Memória (GB)	50	190
	Disco (GB)	4000	17000
	Núcleo de Processador virtual (VCPU)	20	80
Ambientes de Homologação e Desenvolvimento	Memória (GB)	0	240
	Disco (GB)	0	23000
	Núcleo de Porcessador virtual (VCPU)	0	70

C.7 A SUSEP garante contratar pelo menos os valores estipulados na coluna Mínimo Mensal.
C.8 Os ambientes (produção/homologação/desenvolvimento) devem ser segregados, impedindo-se a comunicação entre as máquinas localizadas em ambientes distintos. Esta segregação deve ser feita através de firewall ou protocolo 802.1q de modo que seja possível, a critério da CONTRATANTE, controlar através de listas de controle de acesso (ACLs) o tráfego entre as diversas máquinas hospedadas, de acordo com as sub-redes de origem e destino e os protocolos utilizados (ICMP, TCP e UDP e respectivas portas).
C.9 Os recursos deverão ser fornecidos em ambiente virtualizado, redundante e tolerante à falha.
C.10 Deverão ser fornecidos, no mínimo, 3 (três) servidores físicos, para fins de

redundância e redução do risco de indisponibilidade, de arquitetura x86 de 64 bits, com as seguintes características mínimas:

- Os núcleos dos processadores disponíveis deverão possuir velocidade mínima 2.4 Ghz cada, com suporte a instruções de 32 e 64 bits (x86 e x86_64) e suporte à virtualização por hardware;
- A velocidade mínima do barramento de memória dos hosts físicos deverá ser de 1333 Mhz;
- As interfaces de rede ethernet deverão suportar, no mínimo, as velocidades 10/100/1000 mbps;
- As interfaces para o equipamento de armazenamento deverão suportar, no mínimo, a velocidade de 8 (oito) Gbps. Caso estas interfaces sejam para rede ethernet (iSCSI), as mesmas deverão possuir suporte ao recurso TOE (TCP Offline Engine) nativamente;
- Os equipamentos deverão possuir fontes redundantes.

C.11 Os hosts físicos de virtualização disponibilizados pela CONTRATADA não deverão ultrapassar o limite de 70% (setenta por cento) de utilização média diária em cada um dos seus recursos (processador, memória, vazão de rede).
C.12 A Susep deverá pagar somente os valores referentes aos serviços demandados por ela e disponibilizados pela CONTRATANTE, durante o mês de apuração.
C.13 A Susep poderá demandar acréscimo ou decréscimo de QUANTITATIVOS DE RECURSOS COMPUTACIONAIS (memória/disco/núcleo de processador) a qualquer momento e sem limite de demanda mensal.
C.14 A Susep poderá demandar a instalação de softwares clientes de sua propriedade destinados à gestão de ativos, monitoramento e outras soluções ligadas à gestão de TI. À CONTRATADA é reservado o direito de solicitar a remoção de determinado software, somente em situações nas quais fique comprovada a incompatibilidade do mesmo com o bom funcionamento do serviço.

D) Da plataforma de virtualização:

A plataforma de virtualização a ser utilizada deverá possuir as seguintes características mínimas:

D.1 Criar máquinas virtuais em equipamentos físicos dotados de processadores baseados na tecnologia X86_64 ou compatíveis.
D.2 Deverá permitir a alocação de 32 processadores virtuais por máquina virtual.
D.3 Deverá permitir a alocação de até 1 TB de memória por máquina virtual.
D.4 Isolar totalmente as máquinas virtuais, impedindo a comunicação entre elas a não ser pelo ambiente de rede em que serão inseridas.
D.5 Suportar máquinas virtuais coexistindo no mesmo equipamento com quaisquer dos sistemas operacionais: Windows Server 2003 R2, ou superior; Windows 7, ou superior; RedHat Enterprise Linux 5 ou superior; Debian 6; CentOS versão 5 ou superior, Ubuntu versão 8 ou superior.
D.6 Possibilitar a instalação em servidor físico sem disco físico local, podendo

ser iniciado através de uma SAN (Storage Area Network) utilizando o conceito de "diskless".
D.7 Suportar extensão do tamanho do disco virtual enquanto a máquina virtual permanece ligada.
D.8 Armazenar em "storage" somente o espaço em disco que a máquina virtual estiver utilizando.
D.9 Permitir a formação de um ou mais clusters, com emprego de dois ou mais hosts físicos para manutenção de disponibilidade.
D.10 Permitir a criação de switches virtuais locais em cada host físico ou distribuído pelo cluster, e que suportem VLANs.
D.12 Acessar a SAN ("Storage Area Network") por mais de um caminho ("multipath") e tolerante a falha ("failover").
D.13 Ter sistema de arquivos que permita ser configurado em "storage" compartilhado, onde mais de um servidor físico consiga acessar o mesmo compartilhamento simultaneamente.
D.14 Criar ambiente de alta disponibilidade, por meio de "cluster" ou tecnologia superior, entre as máquinas virtuais, mesmo que estas estejam em servidores físicos diferentes.
D.15 Permitir o balanceamento de carga gerado pelas máquinas virtuais com a movimentação destas máquinas entre os servidores físicos sem causar indisponibilidade do serviço.
D.16 Permitir integração com o software de backup fornecido pela CONTRATADA para que seja possível o restore completo das imagens das máquinas virtuais e de arquivos dentro destas imagens.
D.17 Permitir integração do ambiente de virtualização com os principais fornecedores de antivírus do mercado (Mcafee, Symantec, Trend, etc.).
D.18 Emitir alertas parametrizáveis por e-mail e traps SNMP.
D.19 Possibilitar a integração com o serviço de diretório Microsoft Active Directory sem a necessidade de alterar o esquema do serviço de diretório.
D.20 Deverá ser disponibilizado acesso de leitura para que a equipe técnica da Susep tenha visibilidade da console de virtualização a qualquer tempo, além de relatórios gerenciais mensais de disponibilidade para a aferição da prestação de serviços.

E) Do acesso ao serviço de acesso remoto (SAR) ou *Virtual Private Network* (VPN)

E.1 O SAR deve estar disponível 24 horas por dia e possibilitar ao usuário devidamente credenciado acesso à intranet da CONTRATANTE, por meio de túneis virtuais criptografados.

E.2 O túnel deve ser implementado utilizando IPsec ou SSL, a critério da CONTRATANTE, e os dados a serem trafegados deverão ser cifrados utilizando

AES com no mínimo 192 bits ou 3 DES com no mínimo 128 bits.

E.3 A chave simétrica deve ser trocada, obrigatoriamente, por meio de algoritmo de criptografia assimétrica para cada sessão estabelecida.

E.4 A autenticação de usuários deve ser, a critério da CONTRATANTE, realizada utilizando-se tokens One Time Password (OTP) ou por meio de Certificado Digital padrão ICP-Brasil, podendo este último ser armazenado em *tokens* ou *smartcards*.

E.5 A PROPONENTE deverá manter a monitoração constante, controle e armazenamento dos eventos relativos ao serviço de acesso remoto (SAR), obrigando-se a disponibilizá-los à CONTRATANTE em tempo real.

E.6 O Serviço de Acesso Remoto poderá utilizar como meio de comunicação os acessos do tipo banda larga residencial, rede celular ou rede local corporativa, desde que conectadas à internet. Deverá haver a possibilidade de utilização através de firewall com NAT, através de protocolos normalmente permitidos por estes equipamentos, como, por exemplo, HTTPS (túnel SSL).

E.7 Deverá haver controle dos acessos ao serviço, registrando-se, no mínimo, os eventos de hora de conexão, hora de desconexão, endereço IP (internet protocol) válido e nome do usuário.

E.8 A CONTRATANTE, mediante acordo prévio, poderá definir perfis de acesso ao serviço, bem como restrições a portas ou serviços após o fechamento do túnel e o estabelecimento de conexão segura.

E.9 As mesmas políticas de segurança utilizadas internamente pela CONTRATANTE devem ser aplicadas aos usuários conectados por meio deste serviço.

F) Dos Subsistemas de Armazenamento de Dados da PROPONENTE

A CONTRATADA deverá disponibilizar sistema de armazenamento de dados para os ambientes computacionais contratados que suportem as necessidades da Susep. A tecnologia utilizada para o armazenamento de dados deverá ser rede de armazenamento SAN (*Storage Area Network*) e possuir as seguintes características mínimas:

F.1 Sistema de armazenamento em disco externo, com tecnologia SAN com suporte a iSCSI e/ou FC para alta disponibilidade – sem ponto único de falha, acesso aos dados por mais de um canal de I/O, com cache espelhado, para instalação das bases de dados multiplataforma.

F.2 Controladoras redundantes, com memória cache de 04 (quatro) GB cada uma, bateria própria para autonomia e garantia dos dados.

F.3 02 (duas) portas para conexões FC – *Fiber Channel* de 08 Gbps ou 02 (duas) portas para conexões iSCSI de 10 Gbps por controladora.
F.4 Balanceamento dinâmico de carga entre discos e controladoras.
F.5 Detecção e isolamento de falhas, devendo abranger a automonitoração e geração de relatórios (*logs*) de erros, bem como acionamento automático de disco de reposição (*disk spare*).
F.6 Possibilitar o gerenciamento de conexões simultâneas dos servidores que utilizam o espaço total em disco disponibilizado para a Susep.
F.7 Permitir a alteração (aumento ou diminuição) do tamanho do(s) volume(s) lógico(s) nativo(s) executada de forma online e transparente para as aplicações e dados armazenados nestes mesmos volumes.
F.8 Implementar mecanismos de mapeamento (*mapping*), mascaramento (*masking*) de volumes lógicos, de forma que seja possível restringir o acesso apenas para servidores de rede autorizados.
F.9 Deverá suportar discos SSD, FC, SAS, NL-SAS e SATA no mesmo sistema de armazenamento.
F.10 Implementar mecanismo de tierização automática de discos, onde a proporção do nível 0 (discos SSD) não deverá ser menor do que 5% (cinco por cento) e o nível 1 (discos SAS ou FC 15000 rpm) não poderá ser menor do que 35% (trinta e cinco por cento) do volume útil requerido.
F.11 Deverão ser disponibilizadas múltiplas Logical Units (LUNs) para acesso dos servidores da Susep.

G) Do Serviço de Diretório

G.1 A CONTRATANTE possui um serviço de diretório baseado em Microsoft Active Directory em Windows Server 2003 R2 com um único domínio. A CONTRATADA deverá implantar e administrar em suas dependências um controlador de domínio.
G.2 A CONTRATADA assumirá responsabilidade sobre a administração do domínio, ficando encarregada de sua operação diária e da execução das tarefas de manutenção e backup. A gestão das diretrizes de funcionamento permanecerá sob a responsabilidade da CONTRATANTE, que deverá ser consultada previamente a respeito das alterações necessárias, de acordo com a metodologia de gestão de mudanças.
G.3 A delegação da operação do domínio por parte da CONTRATANTE não ensejará perda dos direitos administrativos sobre os sistemas em questão. Caso a CONTRATADA deseje se resguardar de possíveis falhas operacionais ocasionadas por ação da equipe técnica da CONTRATANTE, esta poderá implantar os métodos de rastreabilidade que julgar necessários, desde que sejam previamente aprovados por ambas as partes. Da mesma forma, a CONTRATANTE se resguarda o direito de auditoria nas operações realizadas em seus ativos.
G.4 Pedidos de inclusão, exclusão e modificação de atributos de usuários; inclusão, exclusão e alteração de grupos; inclusão, exclusão de *scripts* de *login* e inicialização; bloqueio, desbloqueio e redefinição de senhas serão tratados como solicitações de serviço e deverão ser atendidos em um prazo de 24 horas.

H) Da configuração dos servidores de aplicação a serem hospedados no ambiente da CONTRATADA

Os servidores de aplicação a serem hospedados no ambiente da CONTRATADA serão utilizados inicialmente para:
H.1Hospedagem do sítio internet da Susep, constituído de aplicações web e páginas de conteúdo publicadas através da solução de gerenciamento de conteúdo Zope/Plone.
H.2 Hospedagem do sítio intranet da Susep, constituído de aplicações web e páginas de conteúdo publicadas através da solução de gerenciamento de conteúdo Joomla.
H.3 Execução de sistemas do tipo Cliente/Servidor.
H.4 A configuração inicial de software dos servidores deverá possuir os seguintes componentes:

#	*Categoria*	*Componente*	*Versão*
1	Servidor de Aplicação	IIS	7 ou acima
2	Servidor de Aplicação	Apache	2.2.X
3	Framework	.Net Framework	1.1
4	Framework	.Net Framework	4.5.x
5	Extensão IIS	Web Deploy	3.5 ou acima
6	Extensão IIS	Application Initialization[1]	1.0
7	Extensão IIS	PHP Manager for IIS 7	1.2
8	Acesso a dados	SQL Server Client Tools	2008 R2
9	Acesso a dados	SQL Server Client Tools	2012
10	Acesso a dados	Microsoft Access Database Engine	2010
11	Utilitário	Microsoft Web Platform Installer	5.0 ou acima
12	Motor de Linguagem	PHP	5.3.6
13	Motor de Linguagem	Python	2.4.6
14	Gerenciamento de Conteúdo	Joomla	1.5.22
15	Gerenciamento de Conteúdo	Zope	2.10.11
16	Gerenciamento de Conteúdo	Plone	3.3.5
17	Framework	Python Image Library (PIL)	1.1.7
18	Banco de Dados	MySQL	5.1
19	Banco de Dados	PostgreSQL	8.4.x

20	Software Aplicativo	SysAid Server	14.3.12
21	Sistemas da Contratante	Aplicações Cliente/Servidor	N/D
22	Gerenciamento de Conteúdo	Plugins do Plone para gerenciamento de conteúdo do Portal Susep	N/D

[1] Não necessário caso a versão do servidor de aplicação IIS seja 8.0 ou superior

H.5 A CONTRATADA deverá prover ambientes de produção, homologação e desenvolvimento. Tais ambientes poderão sofrer alterações ao longo do contrato, observados os limites mínimo e máximo de utilização de recursos computacionais, conforme item C.6.
H.6 A relação de componentes especificada no item H.4 , bem como suas respectivas versões, poderá ser aditivada e/ou alterada, a pedido da CONTRATANTE, a qualquer momento.
H.7 Nas situações em que a licença do componente seja livre / pública, ou de propriedade da CONTRATANTE, esta terá plenos poderes para realizar as alterações necessárias, observando o Processo de Gerência de Mudanças em vigor na CONTRATANTE.
H.8 Nas situações em que a licença do componente seja de propriedade da CONTRATADA as mesmas deverão permitir sua atualização para versões mais recentes e/ou downgrade para versões anteriores, a critério da CONTRATANTE. Tais atualizações serão de responsabilidade da CONTRATADA, com suporte da CONTRATANTE, observando o Processo de Gerência de Mudanças em vigor na CONTRATANTE.
H.9 A aplicação de atualizações de segurança / fix / patches em qualquer dos componentes mencionados será de responsabilidade da CONTRATADA, observadas as janelas operacionais acordadas e observando o Processo de Gerência de Mudanças em vigor na CONTRATANTE.
H.10 A instalação dos frameworks e sua configuração básica, de acordo com parâmetros fornecidos pela CONTRATANTE, será de responsabilidade da CONTRATADA. O suporte e a manutenção permanecerão sob a responsabilidade da CONTRATANTE.
H.11 É responsabilidade da CONTRATADA disponibilizar as licenças de softwares comerciais previstas neste Termo.
H.12 A licença, bem como a instalação, configuração e manutenção do software aplicativo SysAid Server serão de responsabilidade da CONTRATANTE.
H.13 Os sistemas da CONTRATANTE (Aplicações Cliente/Servidor) são aplicações desenvolvidas e/ou mantidas pela CONTRATANTE e disponibilizadas no sistema de arquivos dos servidores, através de mapeamento de rede, juntamente com seus arquivos de configuração e/ou arquivos de trabalho. Essas aplicações, em princípio, não são instaláveis. Todavia, caso surja a necessidade de instalação de alguma aplicação desenvolvida pela CONTRATANTE, esta será realizada

observando o Processo de Gerência de Mudanças em vigor na CONTRATANTE.
H.14 A CONTRATADA deverá instalar certificado SSL fornecido pela CONTRATANTE em todos os servidores.

I) Das atividades de administração de dados sob a responsabilidade da CONTRATADA
I.1 A critério da CONTRATANTE, a CONTRATADA será responsável pela execução das seguintes atividades de administração de dados, com seus respectivos NMS (Nível Mínimo de Serviço).
I.2 Restauração de bases de dados, a partir de um backup especificado ou a partir de qualquer dos servidores hospedados no datacenter (copy only), entre os diferentes servidores da solução, em até 24h corridas após a solicitação da CONTRATANTE. Exemplos: restauração do último backup full do banco ABC no servidor B1 para o banco ABC no servidor B2; cópia do banco ABC do servidor B3 para o banco ABC no servidor B4.
I.3 Emitir alertas de monitoração das bases de dados, via e-mail e/ou SMS, para os destinatários informados pela CONTRATANTE, sempre que ocorrerem eventos de interesse desta. A definição dos eventos que irão gerar tais alertas será feita durante a 2ª etapa da instalação do ambiente, conforme definido no item 3. Estes eventos serão selecionados a partir dos eventos gerados automaticamente pelo SGBD Sql Server.
I.4 Subsidiar a Susep quanto à aquisição, funcionamento, melhoria e atualização dos diversos sistemas gerenciadores de Bancos de Dados (SGBDs), existentes no ambiente da Susep.
I.5 Prover migração de dados entre SGBDs distintos, conforme solicitação e planejamento estabelecidos pela Susep.
I.6 Criar os ambientes de banco de dados, de acordo com boas práticas de mercado, apoiando a Susep na elaboração de Normas Internas.
I.7 Participar, quando solicitado, de reunião com os gerentes e participantes dos projetos de desenvolvimento, manutenção e administração de dados, a fim de apoiar a elaboração de soluções para projetos/atividades em andamento.
I.8 Seguir processos do ITIL, nas disciplinas de Gerenciamento de incidentes, problemas, configuração, mudança e liberação.
I.9 Instalar e configurar SGBDs e produtos correlatos.
I.10 Manter os SGBDs em produção, garantindo a sua estabilidade, confiabilidade, desempenho e disponibilidade.
I.11 Apoiar a equipe técnica da Susep na elaboração das políticas de replicação e de backup dos dados e configurações armazenados em Bancos de Dados (BD), implantando os agentes e realizando as configurações necessárias para o funcionamento correto das soluções, caso necessário.
I.12 Avaliar o tempo de resposta das consultas via SQL e sugerir melhorias para aumento de desempenho dos SGBDs.
I.13 Configurar os parâmetros necessários para o correto funcionamento, utilizando todos os recursos disponíveis nos servidores de BD.
I.14 Administrar e configurar os SGBDs seguindo as práticas de segurança, conforme determinação da Susep.
I.15 Monitorar o desempenho, capacidade e continuidade dos SGBDs de forma a detectar e corrigir eventuais problemas.
I.16 Gerar relatórios sobre a disponibilidade do serviço e possíveis pontos de falha, inclusive prevendo o crescimento das bases e quando deverá ser alocado

mais espaço para tais dados.
I.17 Sugerir a implantação de soluções de alta disponibilidade, cluster, balanceamento de carga, migração de dados e tolerância a falhas para os serviços críticos.
I.18 Manter documentação completa da instalação e funcionamento dos SGBDs, inclusive topologias dos nós de clusters e sistemas de balanceamento de carga.
I.19 Aplicar patches de correção e/ou atualização necessários para redução no risco de falhas e vulnerabilidades e disponibilização de melhorias nos SGBDs.
I.20 Configurar , quando solicitado, perfis de acesso para os usuários clientes que farão acesso a bases de dados, mantendo documentação atualizada, garantindo a segurança lógica do banco de dados.
I.21 Atender solicitações e requisições da equipe técnica da Susep presencialmente, por e-mail e/ou telefone.
I.22 Subsidiar a equipe técnica da Susep na elaboração de projetos para a melhoria dos serviços da área
I.23 Elaborar relatórios técnicos que subsidiem A Susep no gerenciamento de contratos de serviços de TI e homologação de equipamentos e softwares.
I.24 Coordenar a criação, verificação, atualização e implementação dos scripts de solução de problemas na área de Bancos de Dados.
I.25 Produzir, conferir e executar scripts nos SGBDs – SQL, shell scripts, DDL ou DML necessários ao funcionamento e implantação de funcionalidades aos bancos de dados, quando solicitado.
I.26 Elaborar auditorias de dados, consultas às bases de logs de transações, relatórios diversos que não estejam implantados nas aplicações existentes.
I.27 Dar suporte à Equipe de Tratamento de Incidentes de Redes – ETIR.
I.28 A delegação da operação do domínio por parte da CONTRATANTE não ensejará perda dos direitos administrativos sobre os sistemas em questão. Caso a CONTRATADA deseje se resguardar de possíveis falhas operacionais ocasionadas por ação da equipe técnica da CONTRATANTE, esta poderá implantar os métodos de rastreabilidade que julgar necessários, desde que sejam previamente aprovados por ambas as partes. Da mesma forma, a CONTRATANTE se resguarda o direito de auditoria nas operações realizadas em seus ativos.

J) Da configuração dos servidores de banco de dados
J.1 A CONTRATADA deverá prover ambientes dedicados para o SGBD SQL Server em produção, homologação e desenvolvimento. Tais ambientes poderão sofrer alterações ao longo do contrato, observados os limites mínimo e máximo de utilização de recursos computacionais, conforme item C.6.
J.2 A configuração inicial dos ambientes mencionados no item C.6 consistirá dos seguintes servidores de aplicação:

- Produção – Operacional
- Produção – Dados Gerenciais
- Homologação
- Desenvolvimento

J.3 A instalação dos SGBDs em todos os servidores e sua configuração básica, de acordo com parâmetros fornecidos pela CONTRATANTE, será de responsabilidade da CONTRATADA.
J.4 As licenças para execução de todos os SGBDs serão de responsabilidade da CONTRATADA.

K) Monitoração dos serviços e soluções de TIC

K.1 A CONTRATADA será responsável pelo fornecimento de ferramenta de monitoração de todos os recursos e serviços de TIC utilizados no ambiente da Susep (equipamentos servidores, de rede, de armazenamento, aplicações web, SGBDs).
K.2 A ferramenta de monitoração deverá se integrar à de abertura de chamados para o reporte e acionamento das equipes de tratamento de incidentes da CONTRATADA.
K.3 A ferramenta deverá suportar monitoração de equipamentos através da utilização de agentes e do protocolo SNMP.
K.4 A CONTRATADA deverá monitorar e gerenciar os recursos de hardware dos equipamentos hospedados em seu ambiente e informar a CONTRATANTE qualquer evento detectado, por meio de chamado técnico.
K.5 Deverá ser disponibilizado acesso de leitura para que a equipe técnica da Susep tenha visibilidade da console de gerenciamento a qualquer tempo, além de relatórios gerenciais mensais de disponibilidade para a aferição da prestação de serviços.
K.6 A ferramenta disponibilizada pela CONTRATADA deverá fornecer à CONTRATANTE relatórios on-line, com segurança de acesso e em formato HTML, com informações de desempenho e ocupação dos recursos computacionais fornecidos, demonstrando em gráficos históricos as tendências e horários de maior e menor utilização.

L) Dos Procedimentos de Cópia de Dados Armazenados no Centro de Dados da PROPONENTE:

L.1 A política de cópia de segurança (backup) a ser adotada pela PROPONENTE deverá contemplar as seguintes características:

- Cópia de segurança completa *(Backup full)* com as seguintes periodicidades: Semanal (retenção por 10 semanas), Mensal (retenção por 60 meses) – Apenas para o ambiente de produção.
- Cópia de segurança diferencial com periodicidade diária e retenção por pelo menos 30 dias – Para os três ambientes: Produção, Homologação e desenvolvimento.
- A tecnologia utilizada para a realização das cópias de segurança deverá permitir a realização do *backup* de todos os dados, inclusive os que estiverem sendo utilizados dentro do horário de realização das cópias.
- Todas as licenças de uso de todos os softwares necessários para a solução de contingência (*backup/restore*) deverão ser fornecidas pela PROPONENTE.
- O licenciamento dos softwares mencionados deve permitir atualização de versão durante toda vigência do contrato, sendo mantidas as condições contratuais, sem custo adicional.
- As solicitações de exclusões e inclusões de novas áreas de armazenamento nas cópias de segurança deverão ser avaliadas e efetivamente operacionalizadas pela PROPONENTE, em um prazo máximo de 24 (vinte e quatro) horas.

- As solicitações de restauração de dados previamente armazenados em cópias de segurança deverão ser avaliadas e efetivamente operacionalizadas pela PROPONENTE, em um prazo máximo de 24 (vinte e quatro) horas, para o caso de dados inclusos no backup diário (que poderão estar localizados no datacenter), e de 72 (setenta e duas) horas para os dados de fitas localizadas fora do datacenter.
- Em caso de falha na realização da cópia de segurança, a PROPONENTE deverá comunicar a CONTRATANTE e iniciar uma nova execução das tarefas que tenham falhado imediatamente após a sua detecção. A critério da CONTRATANTE, esta nova execução poderá ser interrompida ou adiada, caso venha a impactar o desempenho dos demais serviços.

L.2 Armazenamento de cópia de segurança dos dados da CONTRATANTE em local distinto do Centro de Dados da PROPONENTE (no mínimo, a 5 km de distância) em local tecnicamente adequado para este fim e que tenha a segurança física compatível. Caso sejam utilizadas mídias removíveis, tanto no centro de dados principal, quanto no local de armazenamento remoto, estas deverão ser armazenadas em um cofre específico para este fim. Somente o backup diário poderá ser mantido no local do centro de dados. Em hipótese alguma, os dados pertencentes à CONTRATANTE deverão trafegar fora das dependências do Centro de Dados, seja em mídia física, ou em enlace de dados, sem que seja utilizada criptografia aprovada pela própria.

L.3 Ao término do contrato, as mídias removíveis utilizadas para salvaguarda dos dados deverão ser entregues a CONTRATANTE.

L.4. A CONTRATADA deverá assumir a custódia das mídias que compõem o histórico de cópias de segurança da CONTRATANTE, gravados através da ferramenta Symantec Netbackup. Estas mídias deverão ser armazenadas em local distante do centro de dados, conforme o item L.2.

L.5 Caso seja necessário restaurar algum destes arquivos, a solicitação será feita de acordo com os procedimentos já descritos. Se a CONTRATADA desejar converter estas cópias para outro formato de sua conveniência, deverá solicitar a aprovação da Susep.

L.6 O transporte de fitas deverá ser feito por empresa especializada neste tipo de serviço e com controle de custódia por todas as etapas de trânsito.

L.7 Será aceita a subcontratação para a execução dos serviços do transporte e armazenamento de fitas citados acima, entretanto, a empresa CONTRATADA será responsável total e exclusivamente pela prestação integral dos serviços realizados, não sendo aceito, sob qualquer pretexto, a transferência de responsabilidade da CONTRATADA a terceiros.

M) Da Replicação de Dados de Servidores de Arquivos

M.1 Haverá replicação de dados entre servidores de arquivos localizados nas dependências da CONTRATANTE e um servidor análogo localizado no Centro de Dados.

M.2 A solução adotada deverá permitir a definição das áreas de armazenamento a serem replicadas, com possibilidade de especificação de quais localidades remotas receberão determinados arquivos. Por exemplo, deve ser possível fazer com que uma determinada pasta seja replicada entre todas as localidades, enquanto outras são replicadas apenas entre a Sede e o Centro de Dados.

M.3 Os arquivos replicados deverão manter as listas de controle de acesso (ACL) idênticas aos originais, que estarão no padrão Microsoft NTFS (*New Technology File System*).
M.4 Para fins de cálculo de Nível Mínimo de Serviço, será considerada como falha qualquer defasagem maior do que 30 minutos entre arquivos análogos de localidades diferentes.

N) Das Atualizações de Software

N.1 A CONTRATADA deverá acompanhar as notas divulgadas pelos fornecedores dos softwares por ela administrados de modo a realizar a correção de falhas e vulnerabilidades de forma eficaz.
N.2 O processo de atualização deve ser dado em 3 etapas, com a instalação sucessiva nos ambientes de desenvolvimento, homologação e produção, necessariamente nesta ordem e com uma diferença mínima de uma semana.
N.3 Quando da aplicação de correções no ambiente de desenvolvimento, deve ser dada ciência à CONTRATANTE em um prazo de 24 horas. A atualização dos demais ambientes dependerá de aprovação expressa.
N.4 Qualquer atualização crítica ou de segurança deve ser aplicada em até 30 dias após a sua divulgação. Casos excepcionais, para os quais haja a recomendação de aplicação de correções em prazos mais curtos, deverão ser analisados pela CONTRATADA e submetidos à aprovação da CONTRATANTE.

O) Dos Níveis Mínimos de Serviço:

O.1 A PROPONENTE deverá prover disponibilidade, entendida como tempo em que cada um dos servidores - físicos ou virtuais - equipamentos e serviços descritos acima permanecem utilizável em condições normais de funcionamento, de 98,00 %.
O.2 Será considerado como indisponibilidade todo o incidente que inviabilize, total ou parcialmente, a utilização de determinado servidor, e o tempo será contado a partir da abertura do chamado por parte da CONTRATANTE ou da detecção da falha pelo sistema de monitoramento, o que ocorrer primeiro.
O.3 Haverá glosa de pagamento no caso de descumprimento da disponibilidade prevista no item anterior segundo a fórmula:

Desc = [1 – (Ia / Ic)] * Vs , onde :

Desc= valor do desconto
Ia= indicador aferido
Ic = indicador contratual (vide item O.1)
Vs= valor mensal pago relativo ao equipamento em questão.

Excetua-se do cálculo previsto neste item a indisponibilidade:

- Para fins de manutenção preventiva, desde que previamente autorizada pela CONTRATANTE com, no mínimo, 48 (quarenta e oito) horas;
- Períodos de manutenção de interesse da SUSEP;
- Motivos de calamidade pública e força maior conforme legislação em vigor;

- Incidentes que, após analisados, sejam descaracterizados como indisponibilidade do serviço, desde que comprovados e aceitos pela CONTRATANTE;

O.4 Percentuais de disponibilidade do ambiente do Centro de Dados inferiores a 90%, ensejarão a glosa de 50% do custo mensal dos serviços disponíveis no Centro de Dados (data Center).
O.5 Percentuais de disponibilidade do ambiente do Centro de Dados inferiores a 70%, ensejarão a glosa de 100% dos serviços disponíveis no Centro de Dados (data Center).

P) Da prestação de contas

Deverão ser enviados relatórios periódicos que evidenciem o devido cumprimento das exigências do presente termo. Sem prejuízo de outros documentos que a CONTRATADA deseje gerar, esta deverá observar os relatórios e periodicidades mínimas listados abaixo:

P.1 Relatório de utilização de recursos de hardware
Periodicidade: Mensal
Conteúdo mínimo: Capacidade de armazenamento alocada, capacidade de armazenamento utilizada, quantidade de memória RAM alocada total e por servidor, gráfico histórico de utilização de memória por servidor, quantidade de CPUs alocada total e por servidor, gráfico histórico de percentual de utilização de CPUs por servidor.

P.2 Relatório de incidentes e solicitações
Periodicidade: Mensal
Conteúdo mínimo: Relação de solicitações e registros de incidentes, com o nome do responsável pela abertura, horário de registro, horário de encerramento, duração, e classificação e o número de identificação fornecido pela CONTRATANTE.

P.3 Relatório de incidente grave
Periodicidade: Em até 48 horas à conclusão de qualquer incidente que gere a indisponibilidade de um dos serviços listados nos itens A a J.
Conteúdo mínimo: Nome do responsável pela abertura, horário de registro, horário de encerramento, duração, e classificação e o número de identificação fornecido pela CONTRATANTE, soluções de contorno e solução definitiva adotadas ou previstas.

P.4 Relatório de backup
Periodicidade: Diário
Conteúdo mínimo: Tipo de backup realizado, nome das pastas que sofreram cópias de segurança, horário de início, horário de término.
Em caso de falhas, totais ou parciais, estas deverão estar explícitas em relatório extra.

P.5 Relatório de atualizações de software
Periodicidade: Mensal

	Conteúdo mínimo: Relação de atualizações instaladas por servidor, relação de atualizações aplicáveis não instaladas por servidor (com justificativa). P.6 Relatório do sistema de prevenção de intrusão Periodicidade: Mensal Conteúdo mínimo: Principais tipos de ataque, principais origens de ataques, principais alvos de ataques. P.7 Relatório de usuários de VPN Periodicidade: Mensal Conteúdo mínimo: Relação de usuários habilitados, alterados ou desabilitados para o serviço durante o período, e número da solicitação de serviço correspondente. P.8 Relatório de acessos VPN Periodicidade: Mensal Conteúdo Mínimo: Nome do usuário, hora de conexão, hora de desconexão e endereço IP (internet protocol) válido.
2	***Serviço de Administração de Rede de Longa Distância:*** O objetivo do serviço de administração de redes de longa distância é prover tráfego ininterrupto de dados entre as unidades da Susep (Sede e suas Regionais – SP, RJ , RS, MG e BSB) e destas com o Centro de Dados do item anterior, bem como acesso à internet. Para cada unidade, a PROPONENTE deverá fornecer um ou mais roteadores, interligando a LAN da localidade a um *backbone MPLS*. Será aceita a subcontratação para a execução apenas dos serviços de comunicação de dados deste certame, sendo, no entanto, a empresa CONTRATADA responsável total e exclusivamente pela prestação integral dos serviços realizados, não sendo aceito, sob qualquer pretexto, a transferência de responsabilidade da CONTRATADA a terceiros. **A) Das Características dos Equipamentos de Interconexão de Rede:** A.1 Fornecer roteador tipo corporativo, para todas as localidades contempladas (Sede e Regionais da Susep), durante todo período do contrato, com capacidade de executar serviços SNMP (que deverá estar habilitado para utilização pelo CONTRATANTE apenas para leitura dos dados); A.2 Todos os equipamentos instalados nas unidades da SUSEP deverão ser de um mesmo fabricante e deverão estar disponíveis para acesso de leitura por parte da CONTRATANTE; A.3 Os circuitos a serem disponibilizados para a Susep deverão suportar o padrão IEEE 802.1p, e ainda, permitir a configuração dos parâmetros de qualidade (QoS);

A.4 Todos os roteadores da rede (*backbone* da PROPONENTE e os instalados nas unidades da SUSEP), deverão ter capacidade para suportar o tráfego com banda completamente ocupada, sem exceder a 75% de utilização de CPU e memória;
A.5 À Susep será concedida credencial de acesso para cada um dos equipamentos dispostos nas suas dependências, com privilégios de leitura exclusivamente (*read only*).

B) Descrição Geral dos Serviços de Fornecimento e Administração de Rede de Longa Distância

B.1 A PROPONENTE deve ser um Sistema Autônomo (***A****utonomous* ***S****ystem*), grupo de Redes IP gerenciados por mais de uma operadora de telecomunicações que possuam entre si uma política independente de roteamento. Deverá ser alocado para a CONTRATANTE um bloco contínuo de 16 endereços IP.
B.2 A solução em questão compreenderá fornecimento, instalação, manutenção, monitoração de:
· Porta de Comunicação com a Rede Internet;
· Backbone MPLS, constituído por canais de comunicação interligando todas as unidades da Susep e o próprio Centro de Dados fornecido pela PROPONENTE.
B.3 No caso específico do ponto de acesso da Sede (RJ) deve ser empregada necessariamente a técnica da "dupla abordagem" com dois enlaces (*links*) provenientes de operadoras de telecomunicações distintas, sem qualquer compartilhamento de meio físico.
B.4 Devido à importância para a CONTRATANTE, a mesma poderá auditar a solução apresentada relativamente ao item anterior por meio de vistorias e testes acordados com a PROPONENTE.
B.5 O provimento de acesso à Internet às unidades da Susep, bem como a interligação de dados entre estas deve ser fornecido 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.
B.6 Para cada unidade da Susep, o *backbone* deve prover estrutura lógica que proporcione conectividade completa entre estas unidades e destas com o Centro de Dados do item anterior. Assim, a divulgação de rotas deverá possibilitar que cada unidade atinja diretamente todas as outras.

B.7 O serviço em questão deve contemplar a capacidade de administração de alto tráfego a ser provido pelo *backbone* da rede e suportar classes de serviços e IEEE 802.1p.

B.8 O serviço de administração de rede de longa distância deve suportar transações CLIENTE-SERVIDOR, correio eletrônico, aplicativos Web, dados de gerenciamento (SNMP) e futuras aplicações de videoconferência e telefonia IP.

B.9 A PROPONENTE deverá responder pela elaboração e manutenção do mapa de endereçamento IP utilizado no *BACKBONE* MPLS e na rede IP de acesso. Tais endereços devem ser plenamente compatíveis com o plano de endereçamento das redes LAN.

B.10 A PROPONENTE deverá disponibilizar sistema WEB em tempo real para monitoramento, gerência de falhas e de mudanças, além de possibilitar a verificação dos NÍVEIS MÍNIMOS DE SERVIÇOS (NMS) dos links e pontos de acesso objeto desta contratação.

B.11 Em relação à filtragem dos acessos à Internet, a PROPONENTE deverá observar o seguinte:

- Controle de acesso à internet por horários e por dia da semana;
- Controle de acesso à internet por domínio;
- Bloqueio de *download* de arquivos por extensão, nome de arquivo e tipo de arquivo;
- Bloqueio de *download* de arquivos por tamanho;

  Possuir pelo menos 60 categorias para classificação de sítios *web*, dentre as quais devem constar:
  - Proxy Anônimo;
  - Webmail;
  - Educacionais;
  - Saúde;
  - Notícias;
  - Compras;

- Governamentais;
- Mensagens instantâneas;
- Redes sociais;
- Chat;
- File sharing;
- Downloads;
- Streaming de mídia;
- Phishing;
- Atividades maliciosas (hacking);
- Pornografia;
- Racismo; e
- Pedofilia.

- Configuração de cota de tempo de utilização por categoria;
- Possuir base de dados contendo, no mínimo, 40 milhões de sítios web previamente registrados e classificados;
- Permitir a reclassificação de sítios web, tanto por URL quanto por endereço IP;
- Monitoração do tráfego internet sem bloqueio de acesso aos usuários;
- Prover Termo de Responsabilidade on-line para aceite pelo usuário, a ser apresentado toda vez que houver tentativa de acesso a determinado serviço permitido ou bloqueado;
- Exibir mensagem de bloqueio adaptável para resposta aos usuários na tentativa de acesso a recursos proibidos;
- Integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados;
- Prover funcionalidade de identificação transparente de usuários

cadastrados no Microsoft Active Directory;

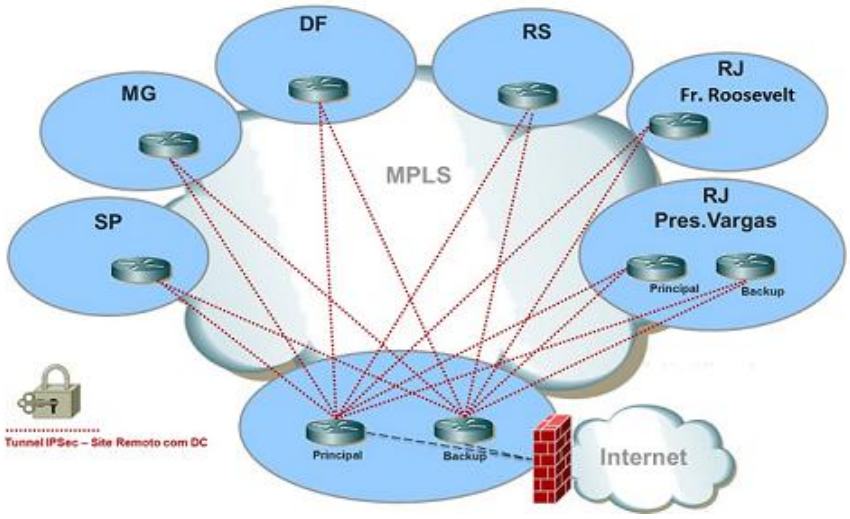
- Permitir a filtragem de todo o conteúdo de sítios conhecidos como fontes de material impróprio e/ou de códigos (programas/scripts) maliciosos através de base de URL própria atualizável;
- Permitir o bloqueio de páginas web através da construção de filtros específicos com mecanismo de busca textual;
- Permitir a criação de regras e categorias personalizadas de modo que haja flexibilidade na definição da política de acesso;
- Permitir o bloqueio de sítios cujo campo CN do certificado SSL não contenha um domínio válido;
- Filtro de conteúdo baseado em categorias em tempo real;
- Realizar atualizações regulares sem interromper a execução dos serviços de filtragem de conteúdo web;
- Permitir a criação de regras de acesso/bloqueio por grupo de usuários do serviço de diretório LDAP;
- Permitir a criação de regras para acesso/bloqueio por endereço IP de origem;
- Permitir a criação de regras para acesso/bloqueio por sub-rede de origem;
- Ser capaz de categorizar a página web tanto pela sua URL como pelo seu endereço IP;
- Permitir o bloqueio de redirecionamento HTTP;
- Permitir o bloqueio de páginas web por classificação como páginas que facilitam a busca de áudio, vídeo e URLs originadas de Spam;
- Deverá possuir as funcionalidade de proxy explícito e transparente.

B.12 Em relação à Segurança da Informação da Administração de Redes WAN, a PROPONENTE deverá observar o seguinte:

- O backbone deverá estabelecer isolamento de tráfego a partir da camada 3 ou inferior (modelo OSI) implementando o protocolo

TCP/IP sobre MPLS, que funcionalmente deverão comunicar-se entre si sob uma topologia *Any to Any* (*Full Mesh*).

- O tráfego de dados entre os pontos de acesso (Sede, Regionais e centro de dados da PROPONENTE) deverá ser criptografado fim-a-fim.
- Deverão ser utilizados algoritmos criptográficos de robustez reconhecida, tais como: algoritmo simétrico - AES de 256 bits; algoritmo assimétrico - RSA de 2048 bits; função hash – SHA-512.
- A CONTRATANTE poderá solicitar a substituição de qualquer algoritmo criptográfico implementado, caso haja indícios de fragilidades nos mesmos.
- A CONTRATANTE poderá autorizar o uso de outros algoritmos diferentes dos mencionados, por solicitação da PROPONENTE.
- Os procedimentos e equipamentos utilizados para o estabelecimento da criptografia deverão permitir que as chaves criptográficas permaneçam de posse ou conhecimento exclusivo da CONTRATANTE, de modo que nenhum terceiro, e nem mesmo a CONTRATADA, seja capaz de decifrar os dados em trânsito através da rede de longa distância.
- O equipamento utilizado para esta criptografia deverá estar disponível para acesso de leitura por parte da CONTRATANTE.



B.13 O máximo de latência admitido pela SUSEP no Serviço de comunicação de dados, fim-a-fim, entre a sede da Autarquia e o ambiente de hospedagem da CONTRATADA é de 300 ms (trezentos milissegundos). A latência será considerada como o tempo em que um pacote IP leva para ir de um ponto a outro da rede e retornar à origem.

- Coletar amostras de latência a intervalos máximos de 5 (cinco) minutos.
- Ao final de cada mês, a CONTRATADA deverá entregar o Relatório de Latência com as verificações do percentual de pacotes acima do limite de latência dentro do período de apuração.

B.14 O máximo de perda de pacotes admitido pela SUSEP para o Serviço de comunicação de dados, fim-a-fim, entre a Sede da Autarquia e o ambiente de hospedagem da CONTRATADA é de 1% (um por cento), índice que será aferido pela CONTRATADA da seguinte forma:

- A cada 5 (cinco) minutos deve ser medida a perda de pacotes.
- Ao final de cada mês, a CONTRATADA deverá entregar o Relatório de Perda de Pacotes com as verificações do percentual de pacotes perdidos dentro do período de apuração.

C) Do Nível Mínimo de Serviço dos Pontos de Acesso das Regionais da Susep (SP/RS/MG/DF/RJ2):

C.1 A PROPONENTE deverá prover disponibilidade dos pontos de acesso, entendida como tempo no qual os serviços permanecem aptos para utilização em condições normais de funcionamento, de 99,00%.
C.2 Haverá glosa de pagamento no caso de descumprimento da disponibilidade prevista no item anterior segundo a fórmula:

Desc = [1 – (Ia / Ic)] * Vs , onde :

Desc= valor do desconto
Ia= indicador aferido
Ic = indicador contratual
Vs= valor mensal pago relativo ao ponto de acesso

Excetua-se do cálculo previsto neste item a indisponibilidade:

- Para fins de manutenção preventiva, desde que previamente autorizada pela CONTRATANTE com, no mínimo, 48 (quarenta e oito) horas.
- Períodos de manutenção de interesse da CONTRATANTE.
- Motivos de calamidade pública e força maior conforme legislação em vigor.
- Incidentes que, após analisados, sejam descaracterizados como indisponibilidade do serviço, desde que comprovados e aceitos pela CONTRATANTE.

C.3 Percentuais de disponibilidade de qualquer dos pontos de acesso regionais inferiores a 90%, ensejarão a glosa de 50% do custo mensal do enlace correspondente.

C.4 Percentuais de disponibilidade de qualquer dos pontos de acesso regionais inferiores a 70%, ensejarão a glosa de 100% custo mensal do enlace correspondente.

D) Do Nível Mínimo de Serviço da comunicação com o Datacenter:

D.1 A PROPONENTE deverá prover disponibilidade da Rede WAN, entendida como tempo no qual o BACKBONE permanece em condições normais de funcionamento, de 99,00 %.

D.2 Haverá glosa de pagamento no caso de descumprimento da disponibilidade prevista no item anterior segundo a fórmula:

Desc = [1 – (Ia / Ic)] * Vs , onde :

Desc= valor do desconto
Ia= indicador aferido
Ic = indicador contratual
Vs= valor mensal pago relativo ao uso do BACKBONE.

Excetua-se do cálculo previsto neste item a indisponibilidade:

- Para fins de manutenção preventiva, desde que previamente autorizada pela CONTRATANTE com, no mínimo, 48 (quarenta e oito) horas;
- Períodos de manutenção de interesse da CONTRATANTE.
- Motivos de calamidade pública e força maior conforme legislação em vigor.
- Incidentes que, após analisados, sejam descaracterizados como indisponibilidade do serviço, desde que comprovados e aceitos pela CONTRATANTE.

D.3 Percentuais de disponibilidade do *backbone* inferiores a 90%, ensejarão a glosa de 50% do custo mensal dos serviços que forem indisponibilizados.

D.4 Percentuais de disponibilidade do *backbone* inferiores a 70%, ensejarão a

glosa de 100% do custo mensal dos serviços que forem indisponibilizados.

E) Do Nível Mínimo de Serviço do Ponto de Acesso da Sede (RJ):

E.1 A PROPONENTE deverá prover disponibilidade dos pontos de acesso, entendida como tempo no qual os serviços permanecem aptos para utilização em condições normais de funcionamento, de 99,70%.
E.2 Haverá glosa de pagamento no caso de descumprimento da disponibilidade prevista no item anterior segundo a fórmula:

Desc = [1 – (Ia / Ic)] * Vs , onde :

Desc= valor do desconto
Ia= indicador aferido
Ic = indicador contratual
Vs= valor mensal pago relativo ao ponto de acesso

Excetua-se do cálculo previsto neste item a indisponibilidade:

- Para fins de manutenção preventiva, desde que previamente autorizada pela CONTRATANTE com, no mínimo, 48 (quarenta e oito) horas.
- Períodos de manutenção de interesse da CONTRATANTE.
- Motivos de calamidade pública e força maior conforme legislação em vigor.
- Incidentes que, após analisados, sejam descaracterizados como indisponibilidade do serviço, desde que comprovados e aceitos pela CONTRATANTE.

E.3 Percentuais de disponibilidade do ponto de acesso da Sede inferiores a 90%, ensejarão a glosa de 50% do custo mensal do enlace correspondente.
E.4 Percentuais de disponibilidade do ponto de acesso da Sede inferiores a 70%, ensejarão a glosa de 100% custo mensal do enlace correspondente.

F) Do Nível Mínimo de Serviço Acesso à Internet:

F.1 A PROPONENTE deverá prover disponibilidade dos acesso à Internet, entendida como tempo no qual o serviço permanece apto para utilização em condições normais de funcionamento, de 98%.
F.2 Haverá glosa de pagamento no caso de descumprimento da disponibilidade prevista no item anterior segundo a fórmula:

Desc = [1 – (Ia / Ic)] * Vs , onde :

Desc= valor do desconto
Ia= indicador aferido
Ic = indicador contratual
Vs= valor mensal pago relativo ao ponto de acesso

Excetua-se do cálculo previsto neste item a indisponibilidade:

- Para fins de manutenção preventiva, desde que previamente autorizada pela CONTRATANTE com, no mínimo, 48 (quarenta e oito) horas;
- Períodos de manutenção de interesse da CONTRATANTE;
- Motivos de calamidade pública e força maior conforme legislação em vigor;
- Incidentes que, após analisados, sejam descaracterizados como indisponibilidade do serviço, desde que comprovados e aceitos pela CONTRATANTE.

F.3 Percentuais de disponibilidade do acesso à Internet inferiores a 90%, ensejarão a glosa de 50% do custo mensal do enlace correspondente.

F.4 Percentuais de disponibilidade do acesso à Internet inferiores a 70%, ensejarão a glosa de 100% custo mensal do enlace correspondente.

G) Da Velocidade Garantida dos Circuitos:

UF	***Tipo de Enlace (Link)***	***Endereço atual***	***Largura de banda em Mbps***
RJ	Link Principal	SEDE - Av. Presidente Vargas, 730 – Centro Rio de Janeiro - CEP: 20071-900.	100
RJ	Link Secundário(dupla abordagem)	SEDE - Av. Presidente Vargas, 730 – Centro Rio de Janeiro - CEP: 20071-900.	100
-	Link de acesso à Internet	Acessível a todas as localidades da Susep através da nuvem MPLS	30
SP	Link Único	Rua Formosa, 367 - 26º andar - Edifício CBI São Paulo - CEP: 01049-000.	4
RS	Link Único	Rua Coronel Genuíno, 421 - 11º andar Porto Alegre - CEP: 90010-350	4
MG	Link Único	Rua Piauí, 220 - 3º andar Santa Efigênia - Belo Horizonte - MG.	1
DF	Link Único	Setor Bancário Sul, Quadra 1 - BL. K - 13º andar - Ed. Seguradora CEP: 70093-900.	1
RJ	Link Único	Av. Franklin Roosevelt, n° 39. 2o andar Centro - Rio de Janeiro - CEP: 20021-120	1

G.1 Entende-se por banda garantida o valor efetivo de banda entregue à

CONTRATANTE, descontando-se eventuais perdas devidas a limitações de *trhoughput* de elementos de rede e equipamentos sob responsabilidade da PROPONENTE, admitindo-se uma *variação* de até 10%.

G.2 Os acessos considerados neste Termo de Referência são: acesso por fibra ótica, acesso por cabeamento metálico e acesso por enlaces rádio.

G.3 Em caso de necessidade, a CONTRATANTE poderá solicitar serviços de redundância de enlaces de dados nas suas regionais (dupla abordagem), mediante emissão de Ordem de Serviços. Neste caso, o valor a ser acrescido pelo pagamento do enlace redundante não poderá ultrapassar o custo contratado para o enlace original da localidade em questão.

G.4 Os endereços poderão ser alterados o longo do contrato. Tais alterações não ensejarão revisão nos valores pagos mensalmente, desde que ocorram dentro dos mesmos municípios.

I) Da prestação de contas

Deverão ser enviados relatórios periódicos que evidenciem o devido cumprimento das exigências do presente termo. Sem prejuízo de outros documentos que a CONTRATADA deseje gerar, esta deverá observar os relatórios e peridicidades mínimas listados abaixo:

I.1 Relatório de utilização de banda
Periodicidade: Mensal
Conteúdo mínimo: Gráfico de banda utilizada ao longo do período

I.2 Relatório de incidentes e solicitações
Periodicidade: Mensal
Conteúdo mínimo: Relação de solicitações e registros de incidentes, com o nome do responsável pela abertura, horário de registro, horário de encerramento, duração, e classificação e o número de identificação fornecido pela CONTRATANTE.

I.3 Relatório de incidente grave
Periodicidade: Em até 48 horas à conclusão de qualquer incidente que gere a indisponibilidade de um dos enlaces listados acima.
Conteúdo mínimo: Nome do responsável pela abertura, horário de registro, horário de encerramento, duração, e classificação e o número de identificação fornecido pela CONTRATANTE, soluções de contorno e solução definitiva adotadas ou previstas.

I.4 Relatório de desempenho de enlaces
Periodicidade: Mensal
Conteúdo mínimo: retardo, *jitter* e perda de pacotes

3	**Serviços de Administração de Correio Eletrônico e Ferramenta de Colaboração** Conjunto de atividades necessárias à administração, operação, disponibilidade e segurança dos serviços de correio eletrônico e agenda de compromissos, promovendo autenticação de usuários, armazenamento de caixas postais, acesso web e administração do banco de contas de correio eletrônico. **A) Funcionalidades Gerais do Serviço** A.1 Possibilidade de criação de endereços adicionais (apelidos) para um mesmo usuário. A.2 Redirecionamento temporário de mensagens de uma para outra(s) caixa(s) de correio. A.3 Integração com o serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, atualmente em uso na Susep, reconhecendo contas e usuários cadastrados, com possibilidade de autenticação única. A.4 Autenticação e acesso criptografados. A.5 Contemplar varredura de vírus, phishing e spam para todas as mensagens enviadas ou recebidas. A.6 Disponibilizar relatório de mensagens bloqueadas com a possibilidade de liberação de cada uma delas. A.7 Possibilitar criação de listas de distribuição. A.8 Calendários individuais com possibilidades de compartilhamento com outros usuários. A.9 Agenda, permitindo a delegação para outro(s) usuário(s) que não o titular da conta. A.10 Lista de contatos individual e de acesso compartilhado. A.11 Assistente de aviso de ausência temporária (férias, afastamentos). A.12 assistente para criação de regras personalizadas por usuário. A.13 Compartilhamento de caixas de correio que permita acesso simultâneo. A.14 Assinatura digital de mensagens.

	A.15 Redirecionamento temporário de mensagens de uma para outra(s) caixa(s) de correio. A.16 Possibilidade de armazenamento local de mensagens. configuração de assinatura personalizada. A.17 Possibilidade de criação de compromissos envolvendo grupos de usuários. A.18 Funcionalidade que permita a troca de mensagens instantâneas entre os usuários. A.19 Integração com smartphones nas plataformas Android e iOS (ex. ActiveSync). **B) Funcionalidade de Colaboração** O ambiente de colaboração deverá possuir as seguintes características mínimas: B.1 Ferramenta de mensageria, que permita a comunicação via chat entre os usuários internos e externos ao ambiente da Susep, integrada à ferramenta de correio eletrônico e permitindo a definição de status do usuário através de indicador de presença (ausente, disponível, ocupado, offline, entre outros). B.2 Os usuários habilitados poderão efetuar o agendamento de uma reunião com colaboração, integrado com as ferramentas de agenda, calendário, tarefas e contatos do correio eletrônico, bem como realizar uma reunião agendada ou emergencial a qualquer momento. B.3 Na mesma interface deverá ter as opções de mensagem instantânea, compartilhamento de aplicativos abertos na estação de trabalho, de toda área de trabalho e de arquivos da suite Microsoft Office, versão 2003 ou superior. B.4 Anotação nos documentos durante a apresentação tanto pelo palestrante quanto pelos participantes autorizados. B.5 Disponibilizar quadro branco para anotações compartilhadas. B.6 Permitir fixar os codecs de vídeo e de áudio, com compressões diferenciadas se dentro da mesma localidade como entre localidades. B.7 Opção de ceder a um determinado participante o direito de alterar o conteúdo do aplicativo compartilhado. B.8 Compatibilidade com os sistemas operacionais Windows XP, Windows 7 ou superior. Caso utilize interface WEB, deverá ser compatível com Internet Explorer

7 ou superior, Mozilla Firefox 32 ou superior e Google Chrome 39 ou superior.

C) Funcionalidade do Acesso via Interface Web

C.1 Compatível com Mozila Firefox e Internet Explorer.
C.2 Acesso a endereços e listas de correio eletrônico contidos em catálogo local ou corporativo.
C.3 Notificação de recebimento de mensagens e compromissos.
C.4 Configuração personalizada do bloco de endereços eletrônicos.
C.5 Recuperação de mensagens excluídas com limite de prazo.

D) Funcionalidades de Acesso via Programa Cliente

D.1 Opção de armazenamento local de mensagens.
D.2 Permitir acesso de representante (Proxy).
D.3 Configuração de assinatura personalizada.
D.4 Assistente de aviso de ausência temporária (férias, afastamentos).
D.5 Assistente para criação de regras personalizadas por usuário.
D.6 Acesso via protocolo IMAP ou HTTP, ambos com SSL.
D.7 Possibilitar acesso simultâneo a uma caixa postal compartilhada por mais de um usuário.
D.8 A solução deverá ser compatível com o cliente de e-mail Microsoft Office Outlook 2007, Service Pack 3, usando protocolo de comunicação MAPI. Esta é a configuração atualmente utilizada nos desktops de usuários da Susep.
D.9 Acesso às funcionalidades descritas nos itens A e B.

E) Dos Quantitativos Totais de Caixas de Correio Eletrônico a Serem Fornecidas

A PROPONENTE deverá oferecer perfis e quantidades diferenciadas de caixas (podendo variar conforme o interesse da CONTRATANTE):

	Quantitativo Mínimo	***Quantitativo Máximo***

Caixa Postal de 2 Gbytes	600	1000

F) Do Nível Mínimo de Serviço do Correio Eletrônico:

F.1 As solicitações de alterações, exclusões, inclusões e recuperações de caixas postais e listas de distribuição deverão ser avaliadas e efetivamente operacionalizadas pela PROPONENTE, em um prazo máximo de 24 (vinte e quatro) horas.
F.2 Será considerado como indisponibilidade todo o incidente que inviabilize a utilização das funcionalidades de que tratam os itens B ou C, e o tempo será contado a partir da abertura do chamado por parte da CONTRATANTE ou da detecção da falha pelo sistema de monitoramento, o que ocorrer primeiro.
Após a exclusão de uma caixa postal, ainda deverá ser possível recuperar seu conteúdo durante os 30 (trinta) dias subsequentes.
F.3 A PROPONENTE deverá prover disponibilidade do email corporativo, entendida como tempo no qual os serviços permanecem aptos para utilização em condições normais de funcionamento, de 98%.
F.4 Será calculado, mensalmente, o percentual de disponibilidade de acordo com a fórmula prevista no item anterior.
F.5 Percentuais de disponibilidade do ambiente do Centro de Dados inferiores a 90%, ensejarão a glosa de 50% do custo mensal dos serviços de correio eletrônico e ferramenta de colaboração.
F.6 Percentuais de disponibilidade do ambiente do Centro de Dados inferiores a 70%, ensejarão a glosa de 100% dos serviços de correio eletrônico e ferramenta de colaboração.
Excetua-se do cálculo previsto neste item a indisponibilidade:

- Para fins de manutenção preventiva, desde que previamente autorizada pela CONTRATANTE com, no mínimo, 48 (quarenta e oito) horas;
- Períodos de manutenção de interesse da SUSEP;
- Motivos de calamidade pública e força maior conforme legislação em vigor;
- Incidentes que, após analisados, sejam descaracterizados como indisponibilidade do serviço, desde que comprovados e aceitos pela CONTRATANTE;

G) Do Procedimento para Recebimento dos Serviços:

G.1 A proposta comercial deve informar o custo unitário das referidas caixas postais eletrônicas de acordo com os perfis.

G.2 A critério da CONTRATANTE, poderá haver acréscimos ou decréscimos das quantidades inicialmente previstas de caixas de correio eletrônico, em função do aumento ou diminuição do seu quadro de colaboradores.

G.3 O Serviço será remunerado pela quantidade de caixas de correio

	efetivamente habilitadas para uso, de acordo com a posição do último dia útil de cada mês (conforme definido neste TERMO DE REFERÊNCIA). G.4 O valor da parcela mensal a ser paga pelo serviço em questão poderá ser decrescido em razão do descumprimento do nível de serviço acordado. **H) Da prestação de contas** Deverão ser enviados relatórios periódicos que evidenciem o devido cumprimento das exigências do presente termo. Sem prejuízo de outros documentos que a CONTRATADA deseje gerar, esta deverá observar os relatórios e periodicidades mínimas listados abaixo: H.1 Relatório de caixas postais Periodicidade: Mensal Conteúdo mínimo: Relação das caixas postais existentes, criadas ou removidas durante o período e número de identificação de solicitação fornecido pela CONTRATANTE. H.2 Relatório de incidentes e solicitações Periodicidade: Mensal Conteúdo mínimo: Relação de solicitações e registros de incidentes, com o nome do responsável pela abertura, horário de registro, horário de encerramento, duração, e classificação e o número de identificação fornecido pela CONTRATANTE. H.3 Relatório de incidente grave Periodicidade: Em até 48 horas à conclusão de qualquer incidente que gere a indisponibilidade do serviço. Conteúdo mínimo: Nome do responsável pela abertura, horário de registro, horário de encerramento, duração, e classificação e o número de identificação fornecido pela CONTRATANTE, soluções de contorno e solução definitiva adotadas ou previstas. H.4 Relatório de filtro de mensagens Periodicidade: Mensal Conteúdo mínimo: Consolidado de mensagens bloqueadas com causas de bloqueio, principais causas, principais endereços IP originários de spam, principais endereços SMTP originários de spam, principais endereços IP originários de vírus, principais endereços SMTP originários de vírus
4	**A) Descrição da Migração de Dados** A criticidade das aplicações da CONTRATANTE, assim com seu caráter ininterrupto, requer um minucioso processo de migração de dados. Tal processo será composto das etapas:

I. Absorção de Conhecimentos por parte da PROPONENTE
II. Instalação de enlaces de Comunicação (Links)
III. Espelhamento do Ambiente Operacional da CONTRATANTE no Centro de Dados da PROPONENTE
IV. Homologação do Ambiente Operacional da CONTRATANTE na PROPONENTE, conforme descrito no item 1 - Serviço de Hospedagem de Sistemas e Gerenciamento do Centro de Dados.

A.1. A PROPONENTE deverá proceder à Migração de Dados atualmente utilizados pela SUSEP, os quais estão atualmente contratados com a empresa LEVEL3 COMUNICAÇÕES DO BRASIL e hospedados em centro de dados localizado no município de Cotia – SP. A empresa citada é atual fornecedora de serviço de *Data Center* e fora vencedora do pregão eletrônico 22/2012.

A.2 A Migração de Dados deverá ocorrer preferencialmente em finais de semana ou após o horário de expediente normal da CONTRATANTE visando a minimizar eventual impacto sobre a rotina dos usuários finais de sistemas informatizados.

A.3. A Migração total dos dados da CONTRATANTE deverá ser finalizada em até 90 (noventa) dias e será supervisionada a partir das dependências da SUSEP.

A.4 Durante a Migração de Dados propriamente dita, a PROPONENTE deverá realizar as seguintes atividades:

- Cópia de todos os dados do ambiente de Tecnologia da Informação e de todos os subsistemas de armazenamento de dados da SUSEP, estejam estes armazenados em ambiente próprio ou de terceiros, para o Centro de Dados da PROPONENTE.
- Verificação da consistência dos dados copiados com vistas a assegurar a preservação de sua integridade.
- Vemoção definitiva dos dados nos subsistemas de origem de forma a permitir que eles sejam desativados sem por em risco a confidencialidade dos dados.

A.5 Caberá à CONTRATANTE apoiar a configuração de servidores e da fitoteca da PROPONENTE, se necessário, com vistas a permitir a utilização dos dados copiados e a restauração dos mesmos.

A.7 Todas as despesas necessárias à prestação do serviço, inclusive com deslocamento de profissionais da PROPONENTE, horas-extras, entre outros encargos serão de exclusiva responsabilidade desta.

A.8 O volume total a ser copiado durante a Migração de Dados será de até 9TB (nove Terabytes), incluindo-se neste somatório: o total armazenado em banco de dados SQLSERVER, cópia dos arquivos de trabalho localizados na rede local da CONTRATANTE, intranet, página na internet e demais aplicativos.

A.10 O faturamento dos serviços contratados só terá início após a conclusão desta migração e aceite formal por parte da CONTRATANTE.

A.11 Caberá à Susep apoiar a configuração de servidores da CONTRATADA, se necessário, com vistas a permitir a utilização dos dados copiados e a restauração dos mesmos..

A.12 Caberá à CONTRATADA garantir que, ao fim da migração, todos os contatos, mensagens, itens de calendário e demais dados existentes no atual ambiente de correio eletrônico da Susep estejam disponíveis no centro de dados daquela.

.A.13 O faturamento dos serviços contratados só terá início após a conclusão desta migração e seu aceite formal por parte da Susep, mediante Termo de Recebimento Definitivo.

B) Do Cronograma de Migração para o Centro de Dados da Contratante

B.1 Para a migração em questão, a PROPONENTE deverá levar em consideração os prazos necessários para a conclusão dos eventuais processos de aquisição de hardware/software, bem como o fato de que os procedimentos de cópia de banco de dados da CONTRATANTE somente poderão ocorrer após o horário de expediente normal ou finais de semana. Ademais, a etapa denominada de "absorção de conhecimentos" ficará condicionada à disponibilidade de horário do corpo técnico da CONTRATANTE.

ETAPAS	***Prazos Previstos***	
D: dia da assinatura do contrato entre as partes.	***Início***	***Fim***
1 – 1ª. Etapa – Absorção de Conhecimentos e instalação de Link Principal conectando a Sede da Susep com o Data Center da Contratada.	D	D + 30
2 – 2ª. Etapa – Espelhamento do Ambiente Operacional da CONTRATANTE no Centro de Dados da CONTRATADA	D	D + 45

2.1 – Eventuais aquisições ou remanejamentos de hardware e softwares por parte da CONTRATADA	D	D + 30
2.2 - Instalações de Enlaces de Comunicação (*links*) e Configuração da Rede **M.P.L.S**. da Contratante.	D	D + 45
2.3 – Montagem, adaptação, testes de ambiente.	D+ 30	
2.4 – Definição dos eventos de monitoração do ambiente		
3 – 3ª. Etapa – Homologação do Ambiente Operacional da CONTRATANTE no Centro de Dados da CONTRATADA	D + 45	D + 90
3.1 Povoar o ambiente com réplica do Active Directory, cópia inicial de aplicativos, arquivos de trabalho/conteúdo e banco de dados da CONTRATANTE e mensagens de correio eletrônico.	D + 45	D + 60
3.2 Homologação do ambiente da CONTRATADA pela CONTRATANTE.	D + 60	D + 90
3.3 Povoar o ambiente com cópia definitiva de aplicativos, arquivos de trabalho/conteúdo e banco de dados da CONTRATANTE e mensagens de correio eletrônico.		

B.2 A cópia de dados para o ambiente da CONTRATADA poderá ser feita através dos enlaces de dados previstos neste edital, de outros enlaces de dados que venham a ser disponibilizados pela CONTRATADA, ou através de mídias de backup. Outros meios de transferência de dados estarão sujeitos à aprovação da Susep, durante a etapa 1 do cronograma acima.

C) Da vistoria facultativa

C.1 As empresas interessadas **poderão** realizar vistoria nas instalações da Susep, de forma a obter pleno conhecimento do ambiente operacional, bem como de todas as informações necessárias à formulação da sua proposta de preços.

C.2 A vistoria será agendada, com 2 (dois) dias úteis de antecedência mínima, por meio do telefone (21) 3233-4156.

C.3 Caso o licitante opte por realizar a vistoria, esta deverá ser efetuada com acompanhamento de um servidor da Susepde segunda a sexta-feira, no horário das 10h00min às 17h00min, com no mínimo 2 (dois) dias úteis de antecedência em relação à data fixada para abertura da sessão pública..

C.4 A realização da vistoria não se consubstancia em condição para participação na licitação, ficando, contudo, as licitantes cientes de que após a apresentação das propostas não serão admitidas, em hipótese alguma, alegações no sentido da inviabilidade de cumprir com as obrigações, devida ao desconhecimento dos serviços e de eventuais dificuldades técnicas não previstas.

4 – NÍVEIS DE SERVIÇO DA SOLUÇÃO DE TI E MULTAS

ITEM | **DESCRIÇÃO**

Haverá aferição de indicadores e métricas para a verificação do cumprimento do contrato. Como forma de tornar objetivos os critérios de avaliação e as sanções cabíveis, foi elaborado um sistema de pontuação no qual a ocorrência de cada falha prevista acarreta determinada pontuação, conforme tabela abaixo. A pontuação será totalizada mensalmente e haverá glosa de 1% (um por cento) sobre o valor da fatura para cada 15 pontos obtidos. Este sistema será aplicado sem prejuízo de nenhum outro tipo de multa ou sanção que a Lei preveja, tampouco das sanções previstas nos demais itens do presente termos, entre as quais se destacam as dos itens C, D, E e F do Serviço de Administração de Redes de Longa Distância.

Item	Descrição	Formas de verificação (*)	Pontos
Falha de antivírus	Detecção de que um servidor esteja sem antivírus, este último esteja inoperante, ou que o mesmo com as definições de vírus defasadas em mais de 2 (dois) dias.	Disponibilização por parte da PROPONENTE de relatório em tempo real da lista de servidores e datas das últimas definições.	10 pontos por ocorrência constatada
Incidente com vazamento de dados	Incidente em que, por falha comprovada da PROPONENTE, informações confidenciais da CONTRATANTE, venham a se tornar públicas ou do conhecimento de pessoas não autorizadas.	Verificação pontual caso surja o incidente ou haja suspeita de ocorrência.	100 pontos por ocorrência constatada
Incidente com perda de integridade de dados	Incidente em que, por falha comprovada da PROPONENTE, informações ou ativos pertencentes à CONTRATANTE, venham a sofrer danos ou alterações não autorizadas.	Verificação pontual caso surja o incidente ou haja suspeita de ocorrência.	100 pontos por ocorrência constatada

Deficiência em recuperação de falhas	Restauração de serviço em prazo superior ao RTO estipulado (4 horas) ou com dados mais defasados que o RPO estipulado (24 horas).	Disponibilização por parte da PROPONENTE de documento que relate relatório em tempo real da lista de servidores e datas das últimas definições.	15 pontos por ocorrência constatada	
Regras de firewall em desacordo com a política definida pela da CONTRATANTE	Verificação de que o equipamento de filtragem de pacotes possui regras, implícitas, ou não, de bloqueio ou liberação de serviços em desacordo com as solicitações previamente realizadas pela CONTRATANTE.	Acesso de leitura em tempo real às configurações do equipamento.	10 pontos por ocorrência constatada	
Regras de filtragem de conteúdo web em desacordo com a política definida pela da CONTRATANTE	Verificação de que o equipamento de filtragem de conteúdo possui regras, implícitas, ou não, de bloqueio ou liberação de serviços em desacordo com as solicitações previamente realizadas pela CONTRATANTE.	Acesso de leitura em tempo real às configurações do equipamento.	10 pontos por ocorrência constatada	
Regras de filtragem de correio eletrônico em desacordo com a política definida pela da CONTRATANTE	Verificação de que o equipamento de filtragem de correio eletrônico possui regras, implícitas, ou não, de bloqueio ou liberação de serviços em desacordo com as solicitações previamente realizadas pela CONTRATANTE.	Acesso de leitura em tempo real às configurações do equipamento.	10 pontos por ocorrência constatada	
Descumprimento do prazo definido para atendimento de solicitação de serviço	Falha em atender ao menos 80% das solicitações de serviços dentro dos prazos especificados no termo de referência, nos casos em que haja esta previsão, ou em prazo superior a 24 horas, nos demais casos. Entende-se por solicitação de serviço o pedido de ação, ou disponibilização de um novo recurso ou serviço, dentro do portfólio definido no contrato.	Acompanhamento da solicitação.	Entre 75% e 79,9%	15 pontos
			Abaixo de 75%	30 pontos

	Descumprimento do prazo definido para atendimento de chamados técnicos (**)	Falha em atender ao menos 80% dos chamados técnicos dentro dos prazos especificados no termo de referência, nos casos em que haja esta previsão, ou em prazo superior a 24 horas, nos demais casos. Entende-se por chamado técnico aquele que vise à correção de falha que esteja causando a indisponibilidade, ou funcionamento em desacordo com o previsto na documentação, de algum dos serviços previstos.	Acompanhamento das solicitações.	Entre 75% e 79,9%	15 pontos
				Abaixo de 75%	30 pontos
	Disponibilidade de servidor abaixo do mínimo determinado (exceto banco de dados)	Falha em atingir índice de disponibilidade de cada servidor (exceto banco de dados) em percentual maior ou igual a 98% no mês calendário.	Disponibilização por parte da PROPONENTE de ferramenta de monitoramento em tempo real que permita o acompanhamento da conectividade com o servidor e seus serviços essenciais.	Entre 97% e 97,9%	15 pontos
				Abaixo de 97% (***)	30 pontos
	Disponibilidade de servidor de banco de dados abaixo do mínimo determinado	Falha em atingir índice de disponibilidade do servidor de banco de dados em percentual maior ou igual a 98% no mês calendário.	Disponibilização por parte da PROPONENTE de ferramenta de monitoramento em tempo real que permita o acompanhamento da conectividade com o servidor e seus serviços essenciais.	Entre 98% e 98,9%	15 pontos
				Abaixo de 98% (***)	30 pontos
	Disponibilidade do Sítio da Susep na Internet abaixo do mínimo determinado	Falha em atingir índice de disponibilidade do serviço em percentual maior ou igual a 98% no mês calendário.	Disponibilização por parte da PROPONENTE de ferramenta de monitoramento em tempo real que permita o acompanhamento da conectividade com os servidores e seus serviços essenciais.	Entre 97% e 97,9%	15 pontos
				Abaixo de 97% (***)	30 pontos

Não execução do backup diário	Não realização da cópia de segurança incremental até as 12 horas do dia posterior.	Envio diário por parte da PROPONENTE de relatório em que constem as eventuais falhas.	5 pontos por ocorrência constatada	
Não execução do backup semanal	Não realização da cópia de segurança completa até as 12 horas do dia útil subsequente.	Envio semanal por parte da PROPONENTE de relatório em que constem as eventuais falhas.	10 pontos por ocorrência constatada	15 pontos por ocorrência constatada
Não execução do backup mensal	Não realização da cópia de segurança completa até as 12 horas do segundo dia útil subsequente.	Envio mensal por parte da PROPONENTE de relatório em que constem as eventuais falhas.	30 pontos por ocorrência constatada	
Não execução de restore de base de dados quando solicitado	Não execução de restore de base de dados em até 24 hs após solicitação da Susep	Verificação pontual caso surja a solicitação do serviço	10 pontos por ocorrência constatada	
Não emissão de alertas de monitoração das bases de dados	Não emissão de alertas de monitoração das bases de dados, via e-mail ou sms, no caso de ocorrência de eventos previamente definidos pela CONTRATANTE	Verificação pontual caso surja o incidente ou haja suspeita de ocorrência e/ou Envio mensal por parte da PROPONENTE de relatório em que constem as eventuais falhas.	5 pontos por ocorrência constatada	
Descumprimento da cláusula de armazenamento remoto de backups mensais e semanais	Incapacidade de comprovar a salvaguarda dos dados referentes às cópias de seguranças semanais e mensais em local alternativo, respeitando-se a distância mínima e os períodos de retenção definidos no termo de Referência.	Disponibilização por parte da PROPONENTE de documento comprobatório do transporte físico de mídias, OU de registro eletrônico de cópia para local previamente acordado entre as	60 pontos por dia de descumprimento	

		partes.		
Indisponibilidade de ferramenta que permita monitorar a disponibilidade dos servidores	Ocorrência de falha que impossibilite a verificação em tempo real da disponibilidade e de seus serviços, de acordo com o definido no termo de referência.	Verificação pontual caso surja o incidente.	10 pontos por ocorrência constatada	
Indisponibilidade de ferramenta que permita monitorar a utilização e disponibilidade dos enlaces.	Ocorrência de falha que impossibilite a verificação em tempo real da disponibilidade e do tráfego em cada um dos enlaces de dados.	Verificação pontual caso surja o incidente.	10 pontos por ocorrência constatada	
Falta de criptografia ou uso de algoritmo não aprovado em enlace de dados	Verificação de que os dados estejam trafegando nos enlaces em texto claro, ou criptografados com um padrão diferente dos previamente aceitos pela CONTRATANTE.	Verificação pontual caso surja o incidente ou haja suspeita de ocorrência.	10 pontos por dia de ocorrência constatada	
Indisponibilidade do serviço de filtragem de acesso à Internet	Falha em atingir índice de disponibilidade do serviço em percentual maior ou igual a 98% no mês calendário. Será considerada como indisponibilidade a possível verificação de que não haja bloqueio em mais de 20% das categorias de sítios da Internet previamente determinadas pela CONTRATANTE.	Verificação pontual caso surja o incidente ou haja suspeita de ocorrência.	Entre 97% e 97,9%	15 pontos
			Abaixo de 97%	30 pontos
Disponibilidade do correio eletrônico abaixo do mínimo determinado	Ocorrência de falha que impossibilite a utilização da ferramenta de correio eletrônico e colaboração por um período superior ao previsto no termo de referência.	Verificação pontual caso surja o incidente.	Entre 98% e 98,9%	15 pontos
			Abaixo de 98%	30 pontos
Indisponibilidade do acesso ao correio	Ocorrência de falha que impossibilite a utilização do	Verificação pontual caso surja o	Entre 97% e 97,9%	15 pontos

eletrônico via software cliente	correio eletrônico e colaboração através de ferramenta cliente por um período superior ao previsto no termo de referência.	incidente.	Abaixo de 97% (***)	30 pontos
Indisponibilidade do acesso ao correio eletrônico via webmail	Ocorrência de falha que impossibilite a utilização do correio eletrônico e ferramenta de colaboração através navegador Internet, via computador conectado à rede mundial de computadores, por um período superior ao previsto no termo de referência.	Verificação pontual caso surja o incidente.	Entre 97% e 97,9%	15 pontos
			Abaixo de 97%	30 pontos
Disponibilidade do SAR abaixo do mínimo determinado	Falha em atingir índice de disponibilidade do SAR em percentual maior ou igual a 99% no mês calendário.	Verificação pontual caso surja o incidente.	Entre 98% e 98,9%	15 pontos
			Abaixo de 98%	30 pontos
Indisponibilidade de acesso aos registros do SAR	Falha em atingir índice de disponibilidade do acesso ao registro de acessos ao SAR em percentual maior ou igual a 98% no mês calendário.	Verificação pontual caso surja o incidente.	Entre 97% e 97,9%	15 pontos
			Abaixo de 97%	30 pontos
Indisponibilidade de acesso aos registros de conexões no firewall	Falha em atingir índice de disponibilidade do monitoramento em tempo real das conexões que atravessaram ou foram bloqueadas pelo filtro de pacotes em percentual maior ou igual a 98% no mês calendário.	Verificação pontual caso surja o incidente.	Entre 97% e 97,9%	15 pontos
			Abaixo de 97%	30 pontos
Indisponibilidade de acesso aos registros do sistema de prevenção de intrusões (IPS)	Falha em atingir índice de disponibilidade da verificação em tempo real dos alertas e bloqueios realizados pelo Sistema de Prevenção à Intrusão em percentual maior ou igual a 98% no mês calendário.	Verificação pontual caso surja o incidente.	Entre 97% e 97,9%	15 pontos
			Abaixo de 97%	30 pontos

*** A CONTRATANTE se reserva o direito de auditar qualquer dos serviços prestados, a qualquer tempo. Nos casos em que a auditoria necessitar de ação ou concessão de acesso por parte da PROPONENTE, esta será comunicada com, no mínimo, 24 horas de antecedência.**

**** Chamados relativos a falhas que já tenham pontuação de glosa prevista estão excluídos.**

***** As pontuações da tabela acima não eliminam a aplicabilidade das cláusulas que especificam glosas nos serviços de Hospedagem de Sistemas e Gerenciamento do Centro de Dados; e do Serviço de Correio Eletrônico e Ferramenta de Colaboração do termo de referência.**

5 – ESPECIFICAÇÃO TÉCNICA (REQUISITOS DA SOLUÇÃO)

5.1 – CONSIDERAÇÕES GERAIS

O ambiente de Centro de Dados, Administração de Rede de Longa Distância e demais serviços associados são de missão crítica, complexos e com diversas peculiaridades técnicas.

5.2 – REQUISITOS INTERNOS

5.2.1 – Requisitos Internos Funcionais

Id	Requisito
1	Disponibilizar canais de contato para atendimento de problemas ou dúvidas por meio e-mail e/ou telefone, 24 (vinte e quatro horas) por dia e sete dias por semana.
2	A PROPONENTE deve fornecer relatórios mensais consolidados para acompanhamento dos serviços prestados.
3	Atendimento de Nível de Serviço mínimo para cada item da Contratação (Conforme especificado no presente termo de referência)
4	A PROPONENTE deverá inserir em seu planejamento de trabalho, a elaboração de um Catálogo de Serviços (CS) do Centro de Dados, contemplando: informações sobre os serviços e atividades correlatas, produtos gerados para um determinado serviço, procedimentos para solicitação do serviço; termos e condições de suporte; dentre outras informações que julgar convenientes. Este catálogo estará sujeita à aprovação da CONTRATANTE.

5.2.2 – Requisitos Internos Não funcionais

Id	Entrega	Prazo
1	Migração e configuração de todo o ambiente do Centro de Dados	Até 90 dias após a assinatura do contrato
2	Documentação dos serviços prestados	Até 90 dias após a assinatura do contrato
3	Obedecer aos métodos de trabalho, aos critérios e à metodologia estabelecida pela CONTRATANTE;	Durante toda a execução do contrato.
4	Notificar a CONTRATANTE quanto às paradas programadas que impactem na disponibilidade dos serviços prestados.	No mínimo, com 3 (três) dias de antecedência.
5	Plano para transferência de conhecimentos para a próxima empresa que vier a prestar serviços à CONTRATANTE ou para servidores integrantes do quadro funcional da mesma. Tal plano deverá conter a revisão de toda a documentação gerada relativas aos serviços prestados que sejam adequados ao correto entendimento do serviço executado.	Prazo máximo de 120 (cento e vinte) dias antes data de término do contrato vigente.
6	A PROPONENTE, por ocasião do término do contrato, deverá disponibilizar todos os	Prazo máximo de 5 (cinco) dias úteis a partir da solicitação da CONTRATANTE

	dados de propriedade da CONTRATANTE, de modo que possam ser transferidos para a mesma ou para qualquer terceiro por ela designado. Os meios de disponibilização deverão incluir, no mínimo, os enlaces de dados descritos no item 2 da solução de TI do presente documento e a gravação de todos os dados em mídias removíveis do mesmo tipo das utilizadas para as cópias de segurança sobre as quais versa o item 1, subitem K.	desde que haja menos de 120 (cento e vinte) dias para data de término do contrato vigente.
7	A PROPONENTE, por ocasião do término do contrato, deverá realizar o descarte seguro de todos os dados de propriedade da CONTRATANTE, utilizando-se de técnicas reconhecidamente eficazes, sujeitas à aprovação da CONTRATANTE, que se reserva o direito de acompanhar presencialmente tal procedimento.	Prazo máximo de 5 (cinco) dias úteis após a conclusão do item 6.

5.3 – REQUISITOS EXTERNOS

A Solução deve estar de acordo com as normas, padrões e políticas estabelecidas pelos respectivos fabricantes dos produtos de software e hardware componentes da solução. Obedecer ainda à legislação Federal em geral e da Susep em particular.

Id	Requisito
1	Atendimento às Normas Gerais de Segurança da Informação da CONTRATANTE (POSIC – Política de Segurança da Informação e Comunicações)
2	A PROPONENTE deverá comprovar aptidão para desempenho de atividade pertinente e compatível em características, quantidades e prazos com o objeto do presente Termo de Referência mediante apresentação de atestado fornecido por pessoas jurídicas de direito público ou privado.
3	A PROPONENTE não divulgará nenhuma Informação Confidencial da CONTRATANTE a nenhum terceiro, exceto para a finalidade do cumprimento deste Termo e com o consentimento prévio por escrito.

6 – MODELO DE PRESTAÇÃO DE SERVIÇO / FORNECIMENTO DE BENS

6.1 – JUSTIFICATIVA PARA PARCELAMENTO DO OBJETO

O parcelamento do objeto não é aplicável por se tratar de uma solução integrada de infraestrutura e operação, conforme melhor justificado no item 2.2.
Os pagamentos relativos aos demais serviços serão remunerados mensalmente.

6.2 – METODOLOGIA DE TRABALHO

Id Bem / Serviço	Forma de Execução / Fornecimento	Justificativa
Migração	Cópia de dados por parte da PROPONENTE, com o suporte operacional e acesso às	Requisitos de segurança da informação

	dependências da CONTRATANTE. Todo o transporte de dados, seja ele por enlace de dados, ou mídia física, deverá ser criptografado.	
Hospedagem de Sistemas e Gerenciamento do Centro de Dados	Hospedagem nas instalações da PROPONENTE com comunicação através dos enlaces de dados de que trata o presente documento.	N.A.
Fornecimento e Administração de Rede de Longa Distância	Disponibilização de conectividade entre a sede e as regionais da CONTRATANTE, bem como a centro de dados da PROPONENTE. O fornecimento de todos os roteadores e equipamentos necessários aos enlaces serão de responsabilidade da PROPONENTE.	N.A.
Serviço de Correio Eletrônico	Hospedagem no centro de dados da PROPONENTE com disponibilização de interface através de navegador (WWW) e cliente Outlook. Deverá ser possível o acesso tanto através dos enlaces de dados de que trata este documento, quanto através da Internet.	N.A.
Serviço de Acesso Remoto	Acesso aos serviços hospedados no centro de dados da PROPONENTE através de qualquer computador com acesso à Internet.	N.A.
6 – ELEMENTOS PARA GESTÃO DO CONTRATO		

6.1 – PAPÉIS E RESPONSABILIDADES				
Id	**Papel**	**Entidade**	**Id**	**Responsabilidade**
1	Gestor do Contrato		**1**	Elaboração do Plano de Inserção da PROPONENTE;
			2	Convocação e realização de reunião inicial;
			3	Encaminhamento formal de Ordem de Serviço;
			4	Encaminhamento das demandas de correção à PROPONENTE, quando houver;
			5	Encaminhamento de indicação de sanções à CGADM, quando houver;
			6	Analisar desvios de qualidade;
			7	Elaborar termo de recebimento definitivo;
			8	Autorizar a emissão de Notas Fiscais à PROPONENTE;
			9	Encaminhamento de pedidos de alteração contratual ao setor competente, quando os houver;
			10	Manutenção do Histórico de Gerenciamento do Contrato.
2	Fiscal Administrativo		**Id**	**Responsabilidade**
			1	Participar da elaboração do Plano de Inserção da PROPONENTE;
			2	Participar da reunião inicial;
			3	Verificar regularidades fiscal, trabalhista e previdenciária;
			4	Verificação da manutenção das condições classificatórias referentes à habilitação técnica;
3	Fiscal Técnico		**Id**	**Responsabilidade**
			1	Participar da elaboração do Plano de Inserção da PROPONENTE;
			2	Participar da reunião inicial;
			3	Receber o objeto do contrato e emitir termos de recebimento provisório e posteriormente, o definitivo;
			4	Avaliação da qualidade dos serviços realizados e das justificativas, quando as houver, de acordo com os Critérios de Aceitação definidos em contrato;
			5	Identificação de não conformidades com os termos contratuais;

			6	Verificação da manutenção das condições classificatórias referentes à habilitação técnica;
			7	Verificação da manutenção das condições elencadas no Plano de Sustentação;
			8	Verificação da aderência dos serviços prestados aos termos da contratação.
4	Representante da PROPONENTE	PROPONENTE	**Id**	**Responsabilidade**
			1	Participar da reunião inicial, entregando o termo de compromisso e o termo de ciência assinados, cf. IN04/2014 e prestando e recebendo esclarecimentos relativos a questões operacionais, administrativas e de gerenciamento do contrato.
			2	Garantir a aderência dos serviços prestados aos termos da contratação.

6.2 – DEVERES E RESPONSABILIDADES DA CONTRATANTE	
Id	**Dever / Responsabilidade**
1	Proporcionar todas as condições para que a PROPONENTE possa desempenhar seus serviços dentro das normas do contrato a ser celebrado.

6.3 – DEVERES E RESPONSABILIDADES DA PROPONENTE	
Id	**Dever / Responsabilidade**
1	Realizar os serviços para os quais foi CONTRATADA de acordo com o estabelecido no Caderno de Especificações dos Serviços ou documento similar por ela proposto, e em observância às recomendações aceitas pela boa técnica, normas e legislação;
2	Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas (sem quaisquer ônus para a SUSEP), no total ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados (art.69 da Lei nº 8.666/93);
3	Assumir todos os gastos e despesas que fizer, para o adimplemento das obrigações decorrentes do Contrato;
4	Manter, em compatibilidade com as obrigações por ela assumidas, todas as condições de habilitação e qualificação exigidas na licitação. Assim, durante a vigência do Contrato, a PROPONENTE ficará obrigada a renovar todos os documentos relativos à regularidade no SICAF - Sistema de Cadastramento Unificado de Fornecedores (art. 55, inciso XIII da Lei nº 8.666/93);
5	Guardar sigilo absoluto sobre as informações que vier a ter conhecimento por força da contratação, assinando o Termo de Compromisso correspondente quando da celebração do contrato e

	cobrando sua ciência e observância a todos os seus colaboradores envolvidos nos serviços prestados, mediante assinatura de Termo de Ciência. Ambos os documentos deverão estar em conformidade com o disposto na Instrução Normativa Nº04, de 2014, da SLTI;
6	Não transferir a terceiros o Contrato, por qualquer forma e nem mesmo parcialmente, bem como subcontratar qualquer das prestações a que está obrigada, sem prévio consentimento por escrito da SUSEP;
7	Manter os técnicos responsáveis pela prestação dos serviços devidamente identificados por crachás quando em trabalho nas instalações da SUSEP;
8	Assumir inteira responsabilidade civil, administrativa e penal por quaisquer danos e prejuízos, materiais e/ou pessoais, causados por seus empregados, à SUSEP ou a terceiros;
9	Assumir, também, a responsabilidade por todas as providências e obrigações estabelecidas na legislação específica em acidentes de trabalho, quando, em ocorrência da espécie, forem vítimas os seus empregados em serviço, ou em conexão com eles, ainda que acontecido nas dependências da SUSEP;
10	Arcar com as despesas decorrentes de qualquer infração seja qual for, desde que praticada por seus técnicos durante a execução dos serviços, ainda que no recinto da SUSEP;
11	Participar das reuniões convocadas pelos responsáveis pela fiscalização do contrato, sendo que, na primeira delas, deverá indicar o preposto e entregar, assinados, o Termo de Compromisso e o Termo de Ciência.
12	Providenciar por conta própria, o transporte e treinamento de seu pessoal;
13	Implantar, de forma adequada, a supervisão permanente dos serviços, de forma a obter uma operação correta e eficaz;
14	Indicar representante pertencente aos quadros da PROPONENTE para manter contato com a SUSEP para o esclarecimento de dúvidas, fornecendo nome, endereço eletrônico e telefone de contato;
15	Responder por eventuais problemas relacionados à execução dos serviços durante todo o período de garantia oferecido, solucionando-os consoante estabelecido no Termo de Referência.
16	Encaminhar à CONTRATANTE, previamente à emissão da fatura, relatórios demonstrativos dos serviços efetivamente prestados.

6.4 – FORMAS DE ACOMPANHAMENTO DO CONTRATO		
Id	**Evento**	**Forma de Acompanhamento**
1	Reunião Inicial	Presencial;
2	Encaminhamento de demandas	Retorno da PROPONENTE por telefone ou e-mail;
3	Reunião de acompanhamento	Presencial.

6.5 – METODOLOGIA DE AVALIAÇÃO DA QUALIDADE		
Id	**Etapa / Fase / Item**	**Método de Avaliação**
1	Relato de problemas de instalação ou uso	Disponibilidade e desempenho do Banco de Dados, dos Servidores de Aplicação e Web; bem como dos enlaces (links) de comunicação Wan;

6.6 – NÍVEIS DE SERVIÇO

Id	Etapa / Fase / Item	Valor Aceitável
Vide capítulos específicos deste documento.		

6.7 – ESTIMATIVA DE VOLUME DE BENS / SERVIÇOS

Id	Bem / Serviço	Estimativa	Forma de Estimativa
Vide capítulos específicos deste documento.			

6.8 – PRAZOS E CONDIÇÕES

Id	Etapa / Fase / Item	Prazo / Condição
Vide capítulos específicos deste documento.		

6.9 – ACEITE, ALTERAÇÃO E CANCELAMENTO

Id	Condição de Aceite
1	Aderência dos bens entregues e serviços prestados aos termos da contratação

Id	Condição de Alteração
1	N/A

Id	Condição de Cancelamento
1	Descumprimento do objeto do contrato
2	Inexecução total ou parcial de obrigações contratuais

6.10 – CONDIÇÕES DE PAGAMENTO

Id	Etapa / Fase / Item	Condição de Pagamento
1	Migração\Implantação dos Serviços	Durante o período de implantação do ambiente (montagem dos ambientes de produção, desenvolvimento e homologação no Centro de Dados, instalação de Links e migração de caixas postais), não será devido nenhum pagamento à CONTRATADA a esse título. Somente após o aceite definitivo da implantação, haverá pagamentos mensais regulares.
2	Serviço de Hospedagem, Fornecimento e Administração de Rede de Longa Distância, Serviço de Correio Eletrônico e Serviço de Acesso Remoto (VPN)	Pagamento mensal, condicionado às metas de NÍVEIS MÍNIMOS DE SERVIÇO, podendo haver glosa de pagamento.

6.11 – GARANTIA

Id	Garantia

1	Não se aplica.

6.12 – PROPRIEDADE, SIGILO E RESTRIÇÕES	
Id	**Direito de Propriedade**
1	Os produtos e marcas objeto do presente Termo de Referência permanecem sob a titularidade de seus fabricantes/distribuidores por toda a extensão do período de duração do contrato, nos termos da Lei Nº 9.610, de 19 de fevereiro de 1998.

Id	**Condição de Manutenção de Sigilo**
1	A SUSEP e a empresa PROPONENTE assumem mútuas obrigações de sigilo por intermédio do Termo de Compromisso estabelecido pela Instrução Normativa Nº 04, de 2014, da SLTI.

Id	**Restrição**
1	Sem restrições adicionais.

6.13– MECANISMOS FORMAIS DE COMUNICAÇÃO				
Função de Com. 1:	Quaisquer questões administrativas durante a execução do contrato, de cunho mais formal;			
Documento	**Emissor**	**Destinatário**	**Meio**	**Freqüência**
Ofício	Contratante / PROPONENTE	PROPONENTE / Contratante	Correio	Eventual
Função de Com. 2:	Questões administrativas cotidianas durante a execução do contrato;			
Documento	**Emissor**	**Destinatário**	**Meio**	**Freqüência**
Mensagem eletrônica (e-mail)	Contratante / PROPONENTE	PROPONENTE / Contratante	Internet	Eventual
Função de Com. 3:	Apresentação dos serviços prestados com vistas à sua avaliação.			
Documento	**Emissor**	**Destinatário**	**Meio**	**Freqüência**
Relatório de serviços prestados	PROPONENTE	Contratante	Correio / Internet	Mensal
Função de Com. 4:	Apresentação dos serviços prestados com vistas à sua quitação.			
Documento	**Emissor**	**Destinatário**	**Meio**	**Freqüência**
Nota Fiscal e Fatura ou Nota Fiscal e Boleta Bancária	PROPONENTE	Contratante	Correio / Internet	Mensal

7 – ESTIMATIVA DE PREÇO		
Id	**Serviços**	**Valores totais anualizados**
1	Serviço de Hospedagem *de Sistemas e Gerenciamento do Centro de Dados*	R$ 1.039.070,40
2	Serviço de Fornecimento e Administração de Rede de Longa Distância	R$ 442.368,00

3	*Serviço de Correio Eletrônico*	R$ 210.900,00
	Total anual:	R$ 1.692.338,40
	Total do contrato:	R$ 5.077.015,20

8 – ADEQUAÇÃO ORÇAMENTÁRIA		
8.1 – FONTE DE RECURSOS		
Id	**Valor**	**Fonte (Programa / Ação)**
1		**Programa 0779** - Desenvolvimento dos Mercados de Seguros, Previdência Complementar Aberta e Capitalização; **Ação 2216** - Sistema Informatizado da Superintendência de Seguros Privados.

9 – SANÇÕES APLICÁVEIS		
Id	**Ocorrência**	**Sanção**
a) Advertência; b) Multa de até 10% (dez por cento) sobre o valor da adjudicação; c) Impedimento de licitar e contratar com a União pelo prazo de até 5 (cinco) anos, sem prejuízo das demais sanções administrativas.		

10 – CRITÉRIOS DE SELEÇÃO DO FORNECEDOR			
10.1 – PROPOSTA TÉCNICA – (Não aplicável para a modalidade licitatória)			
10.1.1 – Organização			
Id	**Item**		**Descrição**
1	Conforme o objeto.		Conforme o objeto.
10.2 – QUALIFICAÇÃO TÉCNICA			
10.2.1 – Requisitos de Capacitação e Experiência			
Id	**Papel**	**Id**	**Requisitos**
1	N/A	**1**	Conforme o objeto.
10.3 – CRITÉRIOS DE SELEÇÃO			
Caracterização da Solução de Tecnologia da Informação			
Licitação			
Modalidade:	Pregão Eletrônico.	**Tipo:**	Menor Preço (Lote Único)
Justificativa:	A Lei n. 10.520/2002, art. 1º, parágrafo único, define bens e serviços comuns como aqueles cujos padrões de desempenho e qualidade possam ser objetivamente definidos pelo EDITAL, por meio de especificações usuais no mercado. O Decreto 7.174/2010 define em seu artigo 9º, § 2º que "será considerado comum o bem ou serviço cuja especificação estabelecer padrão objetivo de desempenho e qualidade e for capaz de ser atendido por vários fornecedores, ainda que		

	existam outras soluções disponíveis no mercado". Ademais, o Acórdão TCU nº 2.471/08-Plenário recomenda que a Administração Pública Direta, Autárquica e Fundacional utilizem o pregão para contratar bens e serviços de tecnologia da informação considerados comuns, haja vista que atendem a técnicas pré-estabelecidos e a padrões de desempenho e qualidade que podem ser objetivamente definidos por meio de especificações usuais no mercado. Assim sendo, adota-se a modalidade pregão, em sua forma eletrônica, para seleção da empresa a ser CONTRATADA.

Justificativa para Participação Exclusiva de ME ou EPP
Lei Complementar n° 123/06 e Lei n° 8.248/91

Lei Complementar n° 123/06.

Justificativa para Contratação Direta

N/A

Id	Critério de Habilitação	Justificativa
1	Solvência	A empresa cuja falência ou insolvência civil tenha sido decretada judicialmente ou que estejam em gozo de benefício da concordata ou que tenham requerido recuperação judicial, ainda não encerrada, nos termos do art. 63 da Lei nº 11.101, de 9.2.2005 não poderá ser CONTRATADA para as finalidades do presente Termo.
2	Idoneidade	A empresa que tenha sido declarada inidônea por qualquer órgão ou entidade das Administrações Públicas Federal, Estadual ou Municipal, bem como a empresa que estiver inscrita no Cadastro Nacional de Empresas Inidôneas e Suspensas – CEIS, conforme Portaria nº 516, de 15 de março de 2010, do Ministério do Controle e da Transparência, não poderá ser CONTRATADA para as finalidades do presente Termo.
3	Fé pública	A empresa que tenha prestado informações inverídicas em sua documentação para habilitação ou em sua proposta de preços não poderá ser CONTRATADA para as finalidades do presente Termo.
4	Singularidade	A empresa constituída em forma de consórcio não poderá ser CONTRATADA para as finalidades do presente Termo.
5	Nacionalidade	A empresa ou sociedade estrangeira não poderá ser CONTRATADA para as finalidades do presente Termo.
6	Isenção	A empresa da qual seja sócio, cooperado, dirigente ou responsável técnico qualquer servidor da SUSEP, não poderá ser CONTRATADA para as finalidades do presente Termo.

7	Regularidade legal	A empresa que esteja cumprindo a sanção de suspensão do direito de licitar não poderá ser CONTRATADA para as finalidades do presente Termo.
8	Imputabilidade	Cooperativas não poderão ser CONTRATADAs para as finalidades do presente Termo.

Id	**Critério Técnico Obrigatório**	**Justificativa**
1	Aptidão	A PROPONENTE deverá comprovar aptidão para desempenho de atividade pertinente e compatível em características, quantidades e prazos com o objeto do presente Termo de Referência mediante apresentação de atestado fornecida por pessoas jurídicas de direito público ou privado.

Id	**Critério de Aceitabilidade de Preços Unitários e Globais**	**Justificativa**
1	Compatibilidade com os preços praticados na Administração Pública.	Art. 15, Inciso V da Lei 8.666/93: As compras, sempre que possível, deverão balizar-se pelos preços praticados no âmbito dos órgãos e entidades da Administração Pública.

Id	**Critério de Julgamento**	**Justificativa**
1	Menor Preço Global	Atendimento ao princípio da Economicidade na Administração Pública.

CIÊNCIA DOS INTEGRANTES TÉCNICOS

Como parte da equipe de planejamento da contratação e conforme disposto no Art. 14 § 6º da IN SLTI/MPOG nº 04/2014, declaro ter pleno conhecimento das informações contidas no presente Termo de Referência.

Rio de Janeiro, ___ de _____ de _____.

_____

Cristiano Machado Cesário
Integrante Técnico
Matrícula SIAPE: 1742655

_____

Rodrigo Bomfim Rodrigues Pitta

Integrante Técnico
Matrícula SIAPE: 1818494

CIÊNCIA DO INTEGRANTE ADMINISTRATIVO

Como parte da equipe de planejamento da contratação e conforme disposto no Art. 14 § 6º da IN SLTI/MPOG nº 04/2014, declaro ter pleno conhecimento das informações contidas no presente Termo de Referência.

Rio de Janeiro, ___ de _____ de _____.

_____
Rafael Linhares de Alcântara
Integrante Administrativo
Matriícula SIAPE: 1480613

CIÊNCIA DO INTEGRANTE REQUISITANTE

Como parte da equipe de planejamento da contratação e conforme disposto no Art. 14 § 6º da IN SLTI/MPOG nº 04/2014, declaro ter pleno conhecimento das informações contidas no presente Termo de Referência.

Rio de Janeiro, ___ de _____ de _____.

_____
Sérgio Jorge Ramos de Oliveira
Integrante Requisitante
Matrícula 1894982