

EDITAL DE CONVOCAÇÃO PARA CREDENCIAMENTO

CREDENCIAMENTO SUPGA/GABSA/GACOM Nº 019/2012	PROCESSO Nº 19863.000002/2012-19	SEDE
---	---	-------------

PREÂMBULO

O SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS (SERPRO), Empresa Pública Federal, regido pela Lei nº 5.615, de 13/10/70, com sede na SGAN Quadra 601, Módulo V, CEP 70836-900, Brasília-DF, inscrito no CNPJ/MF sob o nº 33.683.111/0001-07, torna público para ciência dos interessados que iniciará, a partir da publicação deste, o processo de CREDENCIAMENTO DE PESSOAS JURÍDICAS interessadas em ofertar insumo(s) para os serviços do Sistema Denatran de Telecomunicações, estes de responsabilidade desta Empresa Pública, mediante disponibilidade de infraestrutura por meio de contrato de prestação de serviço de *Colocation* e *Hosting* ofertado pelo SERPRO, com fundamento no Artigo 25 da Lei 8.666/93.

PERÍODO DE CREDENCIAMENTO: 06/01/2012 a 20/01/2012.

SEÇÃO I - DO OBJETO

1.1 O objeto do presente edital é promover o credenciamento de empresas interessadas em ofertar insumo(s) para os serviços do Sistema Denatran de Telecomunicações, estes de responsabilidade desta Empresa Pública, mediante disponibilidade de infraestrutura por meio de contrato de prestação de serviço de *Colocation* e *Hosting* ofertado pelo SERPRO, doravante denominado “CONTRATADO”, nos termos das condições descritas nesse edital e anexos. As empresas credenciadas serão doravante denominadas “CONTRATANTES” ou “CONTRATANTE”, conforme o caso, e seus contratantes ou usuários finais serão designados “CLIENTES”

SEÇÃO II - DAS CONDIÇÕES PARA PARTICIPAÇÃO

2.1 Poderão participar do presente procedimento as pessoas jurídicas que atenderem todas as condições e exigências, inclusive quanto à documentação, conforme consta da Seção IV deste Edital.

2.2 Não serão admitidos à participação:

- a) Os interessados que por qualquer motivo estejam regularmente declarados como inidôneos ou punidos com suspensão do direito de contratar com a Administração Pública;
- b) Empresas que tenham sócio gerente ou acionista majoritário, ou ainda, como titular de empresa individual empregado ou dirigente do SERPRO.
- c) As Empresas prestadoras do Serviço de Telefonia Móvel Pessoal – SMP, conforme estabelecido no contrato RG 47796 (Ctr 1/2011) firmado entre o SERPRO e o Denatran, com o objetivo de evitar a venda casada de serviços, com fundamento no Art. 39, Inc. I do Código do Consumidor (Lei n. 8.078/90).

SEÇÃO III – DAS PREMISSAS PARA O CREDENCIAMENTO

3.1 As disposições do presente edital e todas as regras correlatas à prestação dos serviços, bem como os termos dos contratos que regem a relação entre o CONTRATANTE e o CONTRATADO, guardam absoluta conformidade com o disposto na Deliberação nº. 121, de 22/12/2011, do CONTRAN e com o disposto na Portaria nº. 902, de 8 de novembro de 2011, do DENATRAN, e em seus respectivos anexos, cujas disposições prevalecerão sobre qualquer eventual disposição deste Edital que as contrarie.

3.2 Os requisitos ora estabelecidos serão averiguados no período havido entre a instalação dos equipamentos da CONTRATANTE e o termo final de 60 (sessenta) dias, ao cabo dos quais, inexistindo providências da CONTRATANTE, no sentido de garantir seu atendimento, o contrato correspondente será denunciado, devendo a CONTRATANTE recolher seu equipamento mediante pagamento dos encargos correspondentes ao número de dias em que houver a permanência do equipamento.

3.3 O atendimento aos requisitos do presente Edital e a celebração do contrato correspondente à prestação dos serviços à CONTRATANTE se dá sem exclusividade, razão pela qual inexistente qualquer preferência ou direcionamento da concessão dos serviços de *hostage* e gerenciamento, sendo, referidos serviços, prestados a qualquer pessoa jurídica que atenda aos requisitos de ordem técnica ora exigidos.

SEÇÃO IV – DA DOCUMENTAÇÃO EXIGIDA PARA CREDENCIAMENTO

4.1 No período definido no preâmbulo deste Edital, poderão se credenciar as empresas interessadas em ofertar insumo(s) para os serviços do Sistema Denatran de Telecomunicações, estes de responsabilidade desta Empresa Pública, mediante disponibilidade de infraestrutura por meio de contrato de prestação de serviço de *Colocation* e *Hosting* ofertado pelo SERPRO, não vedadas pelas disposições do item anterior, que apresentarem a seguinte documentação, original ou em cópia autenticada por cartório competente, frente e verso, quando necessário:

4.1.1 Relativos à Habilitação Jurídica:

- a) registro comercial, no caso de empresário;
- b) ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado, em se tratando de sociedades comerciais, e, no caso de sociedades por ações, acompanhado de documento de eleição de seus administradores;
- b.1) os documentos de que trata a alínea anterior, deverão estar acompanhados de todas as alterações ou da consolidação respectiva;
- c) decreto de autorização, em se tratando de empresa ou sociedade estrangeira em funcionamento no País, e ato de registro ou autorização, para funcionamento expedido por órgão competente, quando a atividade assim o exigir; e
- d) inscrição do ato constitutivo, no caso de sociedades civis, acompanhada de prova

de diretoria em exercício.

4.1.2 Relativos à Regularidade Fiscal:

- a) prova de inscrição no Cadastro Nacional de Pessoas Jurídicas - CNPJ;
- b) prova de regularidade com a Fazenda Federal (Certidão Negativa de Débitos de Tributos e Contribuições Federais, emitida pela Secretaria da Receita Federal – SRF e Certidão quanto à Dívida Ativa da União emitida pela Procuradoria-Geral da Fazenda Nacional – PGFN), e com a Fazenda Estadual e a Municipal, do domicílio ou sede da interessada, na forma da lei; e,
- c) prova de regularidade perante a Seguridade Social (INSS) e perante o Fundo de Garantia por Tempo de Serviço (FGTS) demonstrando situação regular no cumprimento dos encargos sociais instituídos por lei.

4.1.3 Relativos à Qualificação Econômico - Financeira:

- a) certidão negativa de feitos sobre falência, recuperação judicial ou recuperação extrajudicial, expedida pelo distribuidor da sede da licitante;
- a.1) a certidão, referida na alínea anterior, que não estiver mencionando explicitamente o prazo de validade, somente será aceita com o prazo máximo de 90 (noventa) dias, contados da data de sua emissão.

4.1.4 Outras declarações

- a) declaração de que cumpre o inc. XXXIII do art. 7º da Constituição da República, que se refere à proibição de trabalho noturno, perigoso ou insalubre a menor de dezoito anos e de qualquer trabalho a menor de dezesseis.

4.2 A interessada já regularmente cadastrada e habilitada no Sistema de Cadastramento Unificado de Fornecedores – SICAF, ficará dispensada de apresentar os documentos relacionados nos subitens 4.1.1 e 4.1.2.

4.3 Na assinatura do Contrato, será exigida a comprovação das condições exigidas para o credenciamento, consignadas neste Edital, as quais deverão ser mantidas pela CONTRATANTE durante a vigência do contrato.

4.4 Toda a documentação para o credenciamento deverá ser entregue no SERPRO SEDE, localizado no seguinte endereço:

SERPRO SEDE – Divisão de Compras
SGAN Quadra 601 Módulo V, Asa Norte, CEP 70836-900, Brasília-DF

SEÇÃO V - DA PROPOSTA DE CONTRATAÇÃO DE SERVIÇOS

5.1 A interessada deverá apresentar a proposta de contratação de serviços, conforme modelo do Anexo II.

5.2 A proposta deverá conter o detalhamento técnico de todos os equipamentos que serão disponibilizados para a instalação no SERPRO, conforme exigências mínimas descritas no Anexo I.

5.3 O SERPRO fará a avaliação da documentação apresentada em até 10 (dez) dias úteis contados do recebimento da mesma.

5.4 O SERPRO poderá solicitar esclarecimentos quanto à documentação apresentada, o que suspenderá o prazo previsto no item anterior, até que a interessada responda aos questionamentos.

5.5 Caso a documentação não seja aceita, a recusa será devidamente fundamentada e informada a interessada.

5.6 Caso a documentação seja totalmente aceita, a interessada será convocada para a assinatura do Contrato, conforme modelo do Anexo III.

SEÇÃO VI – DO CONTRATO DE PRESTAÇÃO DE SERVIÇOS

6.1 Após o comunicado do SERPRO quanto à completa aprovação da documentação apresentada, a credenciada será convocada para a assinatura do contrato de prestação de serviços, conforme modelo do Anexo III em até 05 (cinco) dias.

6.1.1 O prazo previsto no subitem anterior poderá ser prorrogado, por igual período, por solicitação justificada da credenciada e aceita pelo SERPRO;

6.1.2 Para assinatura do Contrato, será exigida a apresentação de instrumento público de procuração ou de instrumento particular com firma reconhecida do representante que irá assiná-lo, onde comprove a outorga de poderes, na forma da lei. Em sendo sócio, proprietário, dirigente ou assemelhado da empresa, deverá apresentar cópia do respectivo estatuto ou contrato social, no qual estejam expressos seus poderes para exercer direitos e assumir obrigações em decorrência de tal investidura.

6.2 Se a credenciada recusar-se a assinar o Contrato no prazo estipulado, o SERPRO reserva o direito de cancelar o pedido de Credenciamento.

SEÇÃO VII - DA IMPUGNAÇÃO DO INSTRUMENTO CONVOCATÓRIO

7.1 Qualquer pessoa poderá impugnar o Edital, na forma eletrônica, devendo encaminhá-lo para o endereço compras.gabsa@serpro.gov.br, ou protocolá-lo no horário entre às 08:00Hs as 17:30Hs no SERPRO - Sede, localizado no(a) SGAN Quadra 601 Módulo

V – Divisão de Compras – Asa Norte – Brasília/DF - CEP: 70836-900. Caso a impugnação seja encaminhada fora do horário indicado, será considerado o seu recebimento no próximo dia útil.

7.1.1 Não será considerada e/ou recebida impugnação sem as devidas qualificações do interessado, como Razão Social ou nome, número do CNPJ/MF ou CPF/MF, endereço eletrônico, logradouro, nome completo do representante legal quando for o caso, telefone e fac-símile, data e assinatura, não sendo o SERPRO obrigado a respondê-la;

7.1.2 Caberá ao SERPRO decidir sobre a petição no prazo de 05 (cinco) dias;

7.1.3 Acolhida a petição contra o ato convocatório, será publicado nova versão do edital.

SEÇÃO VIII - DOS PEDIDOS DE ESCLARECIMENTOS

8.1 Qualquer pedido de esclarecimento em relação a eventuais dúvidas na interpretação do presente Edital e seus Anexos, deverá ser encaminhado, exclusivamente por meio eletrônico, através do e-mail: compras.gabsa@serpro.gov.br. Caso o pedido de esclarecimento seja encaminhado fora do horário comercial, será considerado o seu recebimento no próximo dia útil.

8.1.1 As respostas aos pedidos de esclarecimentos, bem como demais informações relevantes, serão divulgadas mediante publicações de notas na página web do SERPRO, no endereço www.serpro.gov.br, ficando as empresas interessadas em participar do presente credenciamento obrigadas a acessá-las para a obtenção das informações prestadas.

SEÇÃO IX - DAS DISPOSIÇÕES GERAIS

9.1 Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça o funcionamento do SERPRO, as datas previstas serão automaticamente transferidas para o primeiro dia útil subsequente, no mesmo horário anteriormente estabelecido, desde que não haja comunicação do SERPRO em contrário.

9.2 Todos os horários estabelecidos neste Edital observarão o horário de Brasília – DF

9.3 As normas que disciplinam este Edital serão sempre interpretadas de forma a evitar exclusividade de fornecimento, sem preferências ou direcionamento da concessão dos serviços entre os interessados.

9.4 O desatendimento de exigências formais não essenciais não importará no afastamento do interessado, desde que seja possível a aferição da sua qualificação e a exata compreensão da sua proposta, durante o processo de credenciamento.

9.5 Os interessados proponentes são responsáveis pela fidelidade e legitimidade das informações e dos documentos apresentados em qualquer fase deste processo.

9.6 Na contagem dos prazos estabelecidos neste Edital e seus Anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento. Só se iniciam e vencem os prazos em dias de expediente no **SERPRO**.

9.7 A autoridade competente poderá revogar o presente credenciamento por razões de interesse público decorrentes de fato superveniente devidamente comprovado, pertinente e suficiente para justificar tal conduta, devendo anulá-lo por ilegalidade, de ofício ou por provocação de terceiros, mediante parecer escrito e devidamente fundamentado.

9.8 Será comunicado em tempo hábil, por escrito, às empresas que retirarem o Edital mediante acesso do arquivo pela Internet, qualquer alteração que venha a ocorrer nele ou em seus Anexos. Para que a empresa interessada receba tais alterações, quando da retirada do edital na Internet é imprescindível o cadastramento correto dos dados de sua empresa no site do SERPRO.

9.8.1 Qualquer erro no cadastramento dos dados da empresa interessada em participar desta licitação será de responsabilidade da mesma.

9.9 Os Anexos deste Edital constituem o rol das obrigações decorrentes do presente credenciamento, dele fazendo parte, obrigando as partes ao inteiro teor de suas disposições.

9.10 Os documentos emitidos pela interessada deverão conter sua logomarca, sendo expressamente proibida a inclusão/uso da marca SERPRO.

9.11 Os casos não previstos neste Edital serão resolvidos pelo SERPRO, no SERPRO/ Sede, sito na SGAN Quadra 601 Módulo V – Divisão de Compras – Asa Norte – Brasília/DF - CEP: 70836-900, ou por intermédio do telefone (61) 2021-8422, fax (61) 2021-8195, no horário de 08h00 h às 12h00 e de 14h00 h às 18h00 de segundas às sextas-feiras.

SEÇÃO X - DOS ANEXOS

10.1 Constituem anexos do presente Edital, dele fazendo parte integrante:

Anexo I – Termo de Referência – Características da contratação;
Anexo II – Modelo de proposta a ser emitida pela interessada;
Anexo III – Minuta de Contrato.

Brasília, 05 de Janeiro de 2012.

Roni R. S. Cantuária Alves
Serviço Federal de Processamento de Dados

ANEXO I – TERMO DE REFERÊNCIA

CREDENCIAMENTO SUPGA/GABSA/GACOM Nº 019/2012	PROCESSO Nº 19863.000002/2012-19	SEDE
---	---	-------------

CARACTERÍSTICAS DA CONTRATAÇÃO

1.0 Objeto

1.1 O serviço de *Credenciamento* do SERPRO, foi planejado com vistas ao fornecimento, ao usuário final, de um alto nível de infraestrutura e gerenciamento de ambiente de TIC, visando atender aos requerimentos do cliente, sendo constituído de hospedagem de Hardware, Software e Serviços para implementar o Sistema Denatran de Telecomunicações (subsistema do SIMRAV).

1.2 Detalhamento do serviço

1.2.1 O *Credenciamento* faculta ao CONTRATANTE a disponibilidade de hospedagem, necessária à instalação de servidores/equipamentos do CONTRATANTE e compreende, além de espaço físico, o fornecimento de energia elétrica, de infraestrutura para conectividade com a internet, climatização do ambiente, a rede lógica, o serviço de monitoramento ininterrupto desta infraestrutura e recursos de segurança física de acesso, além da operação e gerenciamento desse conjunto de soluções para atingimento dos fins a que a solução se destina, no relacionamento entre o CONTRATANTE e seus clientes (usuário final).

1.3 Elementos que compõem o serviço

- Edificação especializada para a solução;
- Energia elétrica estabilizada garantida por *nobreaks*;
- Grupos geradores garantindo a qualidade e a continuidade do fornecimento de energia elétrica independente do fornecedor local;
- Sistema de climatização especializado para equipamentos de processamento de dados;
- Sistema de controle de segurança e acesso às instalações, e de climatização;
- Circuito Fechado de Televisão (CFTV);
- Infraestrutura necessária à conectividade do cliente ao ambiente DENATRAN SIMRAV;
- Equipe técnica especializada de atendimento, suporte e operação.

1.4 Do prazo

1.4.1 O CONTRATANTE deverá respeitar o prazo mínimo de 60 (sessenta) meses para hospedagem de sua estrutura dedicada ao projeto DENATRAN SIMRAV sob a garantia de manutenção do serviço durante o mesmo período.

1.5 Valor do serviço

1.5.1 O valor a ser pago pelo CONTRATANTE para hospedagem de sua solução será

proporcional ao espaço físico ocupado nas dependências da CONTRATADA, sendo a unidade padrão de referência estabelecida como múltiplos de rack em bastidor padrão 19 ou 21 Polegadas.

1.5.2 O preço estabelecido será de R\$ 50.000,00 (cinquenta mil) reais/mensal por rack hospedado, incluindo o espaço necessário para a instalação de fontes de alimentação, retificadores, etc. As condições para pagamento e correção dos valores citados, constam da minuta de Contrato, conforme Anexo III.

2.0 Especificação do Objeto

A arquitetura completa da solução a ser hospedada é composta por:

2.1 Plataforma HLR (Home Location Register) – No mínimo 01 (um) HLRs em alta disponibilidade

2.1.1 A plataforma em referência deve atuar como banco de dados central da rede GSM/3G que contém os detalhes de cada perfil de cliente autorizado a utilizar os serviços da plataforma.

2.1.2 A plataforma em referência deve também possuir a função de autenticar todo SIM/USIM card que fizer a tentativa de conexão ao core da rede GSM/3G.

2.1.3 A plataforma em referência deverá possuir redundância de processamento, redundância de placas controladoras e redundância de fontes de alimentação para permitir que o tráfego possa fluir mesmo em casos de falha, garantindo assim o nível de disponibilidade Carrier Class de 99,999%.

2.1.4 A plataforma em referência deverá ter capacidade para 7.200.000 usuários e ser escalável para 100.000.000 de usuários.

2.1.5 A plataforma em referência deverá estar preparada para gerenciar as seguintes ações:

2.1.5.1 Validação

2.1.5.2 Perfil

2.1.5.3 Localização

2.1.5.4 Estado

2.1.6 A plataforma em referência deverá implementar as interfaces padrão através de implemento da sinalização MAP, de acordo com a especificação TS 29.002.

2.1.7 A plataforma em referência deverá possuir mecanismos de controle automático de sobrecarga dos sistemas de processamento, armazenamento e sinalização.

2.1.8 A plataforma em referência deverá possuir contingenciamento transparente em caso de falhas.

2.1.9 Funcionalidades

2.1.9.1 Serviços Básicos:

2.1.9.1.1 Telefonia;

2.1.9.1.2 Short message MT/PP;

2.1.9.1.3 Short message MO/PP;

- 2.1.9.1.4 Bloqueios Determinados pelo Operador;
- 2.1.9.1.5 Barring of Outgoing Calls (ODB-BAOC);
- 2.1.9.1.6 Barring of Outgoing International Calls (ODB-BOIC);
- 2.1.9.1.7 Barring of All Incoming Calls (ODB-BAIC);
- 2.1.9.1.8 Barring of Registration of Forwarded-to Number (ODBRFC).
- 2.1.9.2 Serviços de Mobilidade:
- 2.1.9.2.1 Location Update;
- 2.1.9.2.2 Location Cancellation;
- 2.1.9.2.3 MS Purge;
- 2.1.9.2.4 Authentication Information Provision;
- 2.1.9.2.5 Subscriber Data Insertion;
- 2.1.9.2.6 Subscriber Data Deletion;
- 2.1.9.2.7 HLR Fault Recovery;
- 2.1.9.2.8 VLR Fault Recovery;
- 2.1.9.2.9 Send Routing Information;
- 2.1.9.2.10 Provide Roaming Number.
- 2.1.9.2.11 Gerenciamento da Base de Dados de Usuários:
- 2.1.9.2.12 Subscriber Definition;
- 2.1.9.2.13 Subscriber Deletion;
- 2.1.9.2.14 IMSI Change;
- 2.1.9.2.15 MSISDN Change;
- 2.1.9.2.16 Subscriber Number Query;
- 2.1.9.2.17 Dynamic Data Query;
- 2.1.9.2.18 Operator Authority Management;
- 2.1.9.2.19 Dynamic Subscriber Data Managent;
- 2.1.9.2.20 Service Template Setting;
- 2.1.9.2.21 Batch Operation;
- 2.1.9.2.22 Operation Log Management;
- 2.1.9.2.23 Subscriber Statistics;
- 2.1.9.3. Protocolo, Interfaces e padrões:
- 2.1.9.3.1. MAP Protocols – MAP Phase 1, MAP Phase 2 e MAP Phase 2+;
- 2.1.9.3.2. BOSS Interface;
- 2.1.9.3.3. Application/Data Layer Interface;
- 2.1.9.3.4. M3UA / SIGTRAN;
- 2.1.9.3.5. IETF RFC 4666, IETF RFC 4166, IETF RFC 4165, ITU-T Q.701-Q709, ITU-T Q.711-Q719, ITU-T Q.770-Q779, MAP 1, 2, 3 – 3GPP 23.002 e 29.002, GSMA IR22, IR3 e IR 35;
- 2.1.9.3.6. 3GPP, 3GPP TS 29.002.
- 2.1.9.4. Funções de Operação e Manutenção:
- 2.1.9.4.1. Security Management;
- 2.1.9.4.2. Performance Management;
- 2.1.9.4.3. Fault Management;
- 2.1.9.4.4. Configuration Management;
- 2.1.9.4.5. Equipment Management;
- 2.1.9.4.6. Equipment Archive Management.
- 2.1.9.5. Funções de Proteção e Confiabilidade:
- 2.1.9.5.1. Redundancy and Backup Design;
- 2.1.9.5.2. Power Reliability;
- 2.1.9.5.3. Distributed Boards;
- 2.1.9.5.4. Dual-Plane Communications;
- 2.1.9.5.5. Automatic Fault Detection and Self-Healing;
- 2.1.9.5.6. Automatic/Manual Switchover;
- 2.1.9.5.7. Automatic Multi-Level Backup and Recovery of Subscriber Data;
- 2.1.9.5.8. Flow Control;

- 2.1.9.5.9. Distributed Storage of Subscriber Data;
 - 2.1.9.5.10. Automatic Load Sharing Among Modules;
 - 2.1.9.6. Serviços de Dados:
 - 2.1.9.6.1. GPRS Services.
 - 2.1.9.7. Redundância:
 - 2.1.9.7.1. N+1 Compatibility Redundancy;
 - 2.1.9.7.2. Capacidade de implementar HLR lógico com base de dados centralizada.
 - 2.1.9.8. Políticas de Processos:
 - 2.1.9.8.1. MTP Policing;
 - 2.1.9.8.2. SCCP Policing;
 - 2.1.9.8.3. MAP Policing.
 - 2.1.9.9. Funcionalidades de Autenticação:
 - 2.1.9.9.1. Registration, Call attempt;
 - 2.1.9.9.2. Call Delivery;
 - 2.1.9.9.3. Location Update;
 - 2.1.9.9.4. Supplementary service procedure;
 - 2.1.9.9.5. Short Message Service (SMS) transfer;
 - 2.1.9.9.6. Location services;
 - 2.1.9.9.7. Algoritmos GSM A3/A8, conforme especificação 3GPP;
 - 2.1.9.9.8. COMP128-Versão 1, conforme especificação 3GPP;
 - 2.1.9.9.9. COMP128-Versão 2, conforme especificação 3GPP;
 - 2.1.9.9.10. COMP128-Versão 3, conforme especificação 3GPP;
 - 2.1.9.9.11. Millenage, conforme especificação 3GPP;
 - 2.1.9.9.12. Algoritmo GSM A4 em sua última versão;
 - 2.1.9.9.13. Autenticação Basic GSM Service;
 - 2.1.9.9.14. Autenticação Alternative A4 algorithm;
 - 2.1.9.9.15. Autenticação Basic Platform Feature Package;
 - 2.1.9.9.16. Autenticação Basic WCDMA Service;
 - 2.1.9.9.17. A plataforma deve implementar todos os algoritmos de autenticação listados de forma simultânea.
 - 2.1.9.10. Funcionalidades de sinalização:
 - 2.1.9.10.1. Permitir a redistribuição de carga automática nos links que estão disponíveis no linkset;
 - 2.1.9.10.2. Suporte a link de sinalização de alta velocidade 2Mbit conforme ITU Q703;
 - 2.1.9.10.3. Implementar Load share em nível SCCP (combinação de routeset) e MTP;
 - 2.1.9.10.4. Implementação de load share para todos destinos SCCP (Global Title) ou MTP3 (Point codes);
 - 2.1.9.10.5. Implementar Load share entre múltiplos STP usando GTT Alias point code para endereçamento do STP.
 - 2.1.9.11. Implementar grupo SIGTRAN:
 - 2.1.9.11.1. SCTP de acordo com RFC 2960;
 - 2.1.9.11.2. M3UA de acordo com RFC 3332;
 - 2.1.9.11.3. Implementar Multi-signaling-point (Multi-SP);
 - 2.1.9.11.4. Implementar SCTP multi-homing;
- 2.1.10. A plataforma proposta deverá ser implementada com o algoritmo DES para as chaves de encriptação.
- 2.1.11. A plataforma deve implementar serviços CAMEL 3, fornecendo:
- 2.1.11.1. O-CSI (Originating CAMEL Subscription Information);
 - 2.1.11.2. T-CSI (Terminating CAMEL Subscription Information);
 - 2.1.11.3. SS-CSI (Supplementary Service Invocation Notification CAMEL Subscription Information);
 - 2.1.11.4. SMS-CSI (Short Message Service CAMEL Subscription Information);

- 2.1.11.5. D - CSI (Dialed Service CAMEL Subscription Information);
- 2.1.11.6. M - CSI (Mobility Management event CAMEL Subscription Information);
- 2.1.11.7. VT - CSI (VMSC Terminating CAMEL Subscription Information).

2.1.12. A plataforma deve implementar ATI (any time interrogation) para operações iniciadas por um SCP (service control point). Através dessa operação deve ser possível obter o status e localização de um sim card;

2.1.13. A plataforma deve suportar ARD (Access Restriction Data) para controle do comportamento dos simcards 2G e/ou 3G;

2.1.14. A plataforma deve implementar a configuração de HLR lógico no mesmo elemento físico de forma a garantir operações de áreas numéricas diferentes;

2.1.15. A plataforma deve suportar no mínimo 128 áreas de numeração diferentes;

2.1.16. A plataforma proposta deverá implementar proteções de todos os dados sensíveis e contra manipulação de algoritmos não-autorizados, manipulação e mau uso dos métodos de criptografia e segurança física;

2.1.17. A plataforma proposta deverá associar apenas uma chave para cada usuário armazenado;

2.1.18. A plataforma proposta deverá garantir que a chave de cada usuário será criptografada apenas por intermédio do uso de algoritmos padrão;

2.1.19. A plataforma proposta deverá garantir que cada chave associada a cada usuário seja descriptografada apenas durante o tempo de geração do vetor de autenticação e que os valores gerados serão destruídos em seguida.

2.1.20. A plataforma em referência deve permitir recuperação total e 100% automática (sem necessidade de nenhuma intervenção humana), depois de falha e recuperação de energia.

2.1.21. Arquitetura e Requisitos do Hardware:

2.1.21.1. A plataforma deve ser concebida de tal forma que as falhas individuais no software não devem causar uma falha no sistema ou serviço de interrupção ou degradação do desempenho do sistema. Sob condições de falha, o sistema deve poder dispor continuidade e deve seguir funcionando normalmente sem grau reduzido de serviço ou com prejuízo para a qualidade do mesmo;

2.1.21.2. A arquitetura deve obedecer ao conceito de ngHLR para garantir a confiabilidade e nível de serviço da plataforma;

2.1.21.3. A arquitetura deve ser composta pelos elementos lógicos de processamento e banco de dados – Front End (FE) e Back End (BE), conforme Arquitetura ngHLR.

2.1.21.4. O Back End BE deve implementar as seguintes funções:

2.1.21.4.1. Adição, deleção, atualização e busca do banco de dados de acordo com o serviço requisitado pelo bloco funcional FE;

2.1.21.4.2. O Front end FE deve implementar as funções de processamento de sinalização e mensagens. Não deve armazenar nenhum dado de simcard;

2.1.21.4.3. Todo o hardware deve possuir o seu backup em site local (arquitetura 1+1);

2.1.21.4.4. A plataforma deve ser concebida de tal forma que permita a replicação da mesma em locais geograficamente separados.

2.1.21.5. Para confiabilidade dos dados, a plataforma deve implementar:

2.1.21.5.1. backup de dados entre placas diferentes;

2.1.21.5.2. backup de dados para disco rígido local;

2.1.21.5.3. backup de dados para DiskArray externo à solução da CONTRATANTE;

2.1.21.5.4. Capacidade de efetuar backup para sistema de armazenamento externo à solução fornecida;

2.1.21.5.5. Deve possuir arquitetura modular com design distribuído podendo ser expandido com adição de frames e racks cascadeados;

- 2.1.21.5.6. A plataforma em referência deverá ser hot-swap para todas as placas;
2.1.21.5.7. A plataforma deverá permitir ampliação de hardware sem paralisação do hardware já instalado;

2.1.22 Arquitetura e Requisitos do Software

- 2.1.22.1 A plataforma deve permitir upgrade das licenças software sem perda de conectividade, de registros dos usuários, de sessões ativas, etc;
2.1.22.2. A plataforma deve ser capaz de aplicar Hot Patches sem a paralisação do serviço de forma a atender à disponibilidade mínima exigida;
2.1.22.3. A solução apresentada pela CONTRATANTE deverá considerar correções de Software com o sistema em operação (soft software upgrade).

2.1.23 Interface de provisionamento

- 2.1.23.1. As interfaces de provisionamento devem ser redundantes para garantir a ausência de pontos únicos de falha;
2.1.23.2. Implementar o provisionamento em batch em arquivos ASCII enviados via FTP;
2.1.23.3. Suportar adição/deleção a uma taxa de 1000 comandos/seg .

2.1.24. Características Construtivas

2.1.24.1. A plataforma em referência deverá ser aderente aos requisitos abaixo com relação ao seu Hardware:

- Taxa de reparo do sistema < 0.3%
- Disponibilidade > 99.999%
- Taxa de detecção de falhas > 95%
- Mean time to repair (MTTR) < 1 h
- Tempo de interrupção do serviço para cada upgrade ou expansão < 30 segundos
- Média de interrupção do serviço em um ano < 5 minutos
- Duração entre a inicialização do sistema e pronto para uso < 10 minutos
- Taxa de sucesso do switchover entre os componentes redundantes > 95%

2.1.24.1.1. Com relação a interferências eletromagnéticas – EMC, a plataforma deve ser aderente aos padrões abaixo listados:

2.1.24.1.1.1. EN 55022 classe A

2.1.24.1.1.2. CISPR 22 classe A

2.1.24.1.1.3. ETSI EN 300 386

2.1.24.1.1.4. GB9254 classe A

2.1.24.1.2. Com relação aos requisitos do ambiente de instalação, a plataforma deve ser aderente aos padrões abaixo listados:

2.1.24.1.2.1. GB 4798

2.1.24.1.2.2. ETS 300019

2.1.24.1.2.3. IEC 60721

2.1.25. Operação e Manutenção

2.1.25.1. O CONTRATANTE deve fornecer Operação e Manutenção do sistema para HLR/AUC com interface homem-máquina personalizado para oferecer gerenciamento de falhas, gerenciamento de configuração, gerenciamento de alarmes, medição de desempenho e gerenciamento de segurança.

2.1.25.1.1. Gerenciamento da Configuração

2.1.25.1.1.1. O HLR proposto deve implementar os seguintes recursos de gerenciamento de dados de configuração:

2.1.25.1.1.1.1. Controle de autorização por usuário;

- 2.1.25.1.1.1.2. Atribuição de tarefas razoável para fins de operações flexíveis;
- 2.1.25.1.1.1.3. Manutenção local, remota e centralizada.
- 2.1.25.1.1.2. O HLR proposto deve implementar as seguintes ações de gerenciamento de dados dos simcards:
- 2.1.25.1.1.2.1. Funções além de adição, modificação e exclusão;
- 2.1.25.1.1.2.2. Armazenamento de logs operacionais de todas ações executadas.

2.1.25.2. Gerenciamento de Desempenho

- 2.1.25.2.1. A plataforma proposta deve implementar as seguintes funções de medição de desempenho:
- 2.1.25.2.1.1. Relatórios de medição personalizados e entidade de medição personalizados;
- 2.1.25.2.1.2. Três segmentos de medição de tempo por dia com o dia de medida designada por mês ou por semana, e ciclo de medição de 5 minutos a 24 horas;
- 2.1.25.2.1.3. As chamadas de tráfego podem ser digitalizadas e medidas com base em tempo real;
- 2.1.25.2.1.4. Padrão e formato de saída abertos, com função de impressão disponível;
- 2.1.25.2.1.5. Instrumentos de medição de desempenho dedicados para análise de taxa de conclusão de chamada, congestionamentos, quedas de chamadas, handoffs e densidade de tráfego.

2.1.25.3. Gerenciamento de Alarmes e Manutenção

- 2.1.25.3.1. A plataforma em referência deve implementar as seguintes funcionalidades de gerenciamento de alarmes:
- 2.1.25.3.1.1. Coletar informações de alarme na hipótese de acionamento;
- 2.1.25.3.1.2. Classificar os alarmes de acordo com seu nível de criticidade;
- 2.1.25.3.1.3. Mostrar descrição detalhada do alarme, assim como, sugestões para resolução do mesmo;
- 2.1.25.3.1.4. Monitoramento do status de links, timeslots e placas de uma unidade funcional;
- 2.1.25.3.1.5. **Manutenção remota da plataforma**
- 2.1.25.3.1.6. Fornecer interface de teste para conexão sem afetar o funcionamento normal da plataforma;
- 2.1.25.3.1.7. Possuir diagnóstico automático de falhas de hardware e software;
- 2.1.25.3.1.8. Fornecer interface para informações de log detalhados com ajuda online;
- 2.1.25.3.1.9. Possuir filtros para aplicar nos logs facilitando debug de possíveis problemas.

2.1.25.4. Gerenciamento de Segurança

- 2.1.25.4.1. A plataforma deve implementar gerenciamento de autoridade e gerenciamento de logs.
- 2.1.25.4.1.1. **Gerenciamento de autoridade:**
- 2.1.25.4.1.1.1. A autoridade de operadores e estações deve estar submetida a regras de hierarquia;
- 2.1.25.4.1.1.2. A execução de qualquer comando MMI deve estar condicionada à autoridade do operador ou da estação de trabalho. O comando não pode ser executado caso não esteja sob alguma dessas condições.
- 2.1.25.4.1.2. **Gerenciamento de logs:**
- 2.1.25.4.1.2.1. Deve ser possível habilitar o log de todas as operações MML;
- 2.1.25.4.1.2.2. Deve ser possível realizar buscas online e offline aos logs referentes a realização de qualquer comando MML;

2.1.26. Dimensionamento do HLR

Name	3G(R4/R5)
Basic Parameters	
Number of SMS/BH/SUB(MO)	0,2
Number of SMS/BH/SUB(MT)	0,3
Location update/BH/SUB	1,5
Location update/BH/SUB(To HLR)	0,2
Send authentication to AuC/BH/SUB	0,8
IMSI Detach (BH/SUB)	0,15
SendRoutingInfo to HLR/BH/SUB	0,6
GPRS Location update/BH/SUB	0,25
InsertSubscriberData/BH/SUB	0,1
DeleteSubscriberData/BH/SUB	0,1
CancelLocation/BH/SUB	0,7
Send authentication to AuC/BH/SUB(PS)	0,6
Proportion of Direct delivery SMS (%)	0,6
SendRoutingInfoForSMS to HLR/BH/SUB	0,7
note: BH=BusyHour, SUB=Subscriber, Auc=Auth center	

2.2. SGW (Signaling Gateway) No mínimo 01 (um) Gateways em alta disponibilidade

2.2.1. Requisitos do Gateway de Sinalização

- 2.2.1.1. O SGW deve suportar Number transform;
- 2.2.1.2. O SGW deve suportar Terminal Information Collector (TIC);
- 2.2.1.3. O SGW deve suportar Enhanced Routing Function;
- 2.2.1.4. O SGW deve suportar IN voice call Bypass;
- 2.2.1.5. O SGW deve suportar International roaming and SIMM with IN;
- 2.2.1.6. O SGW deve suportar Preferred network;
- 2.2.1.7. O SGW deve suportar CDR function;
- 2.2.1.8. O SGW deve suportar NTP function;
- 2.2.1.9. O SGW deve possuir processamento dos links narrowband e broadband na mesma placa de processamento;
- 2.2.1.10. O SGW deve possuir disponibilidade de 99,999%;
- 2.2.1.11. O SGW deve obrigatoriamente ser carrier-class;
- 2.2.1.12. O SGW deve ter capacidade mínima de 2500 consultas por segundo à base de dados.

2.2.2. O SGW deverá possuir as seguintes funcionalidades para o MTP:

- 2.2.2.1. MTP loadsharing;
- 2.2.2.2. MTP estatísticas;
- 2.2.2.3. MTP estatísticas de tráfego;
- 2.2.2.4. MTP Gerenciamento da Rede e Restart.

2.2.3. O SGW ofertado deverá implementar SS7 Signalling Connection Control Part (SCCP,Global Title routing);

2.2.4. O sistema proposto deverá permitir as seguintes funcionalidades para o SCCP

2.2.4.1. SCCP Loadsharing:

2.2.4.1.1. Implementar SCCP LoadSharing ou Active / Standby entre 16 DPCs/DPC_SSNs;

2.2.4.1.2. Utilização de múltiplos PC dentro da mesma rede SS7;

2.2.4.1.3. Gerenciamento do subsistema SCCP;

2.2.4.1.5. Serviços Orientados e Não-Orientados a Conexão SCCP over IP, SUA;

2.2.4.1.6. Implementar as recomendações ITU-T Q.711 a Q.714;

2.2.4.1.7. Offload de mensagens SMS sobre rede IP (SIGTRAN) ;

2.2.4.1.8. O SGW ofertado deverá implementar SS7 Transaction Capabilities Application Part(TCAP);

2.2.4.1.9. O SGW deverá implementar a funcionalidade SS7 TCAP, requerido para implementar os protocolos MAP, INAP e CAP - Phase1,2,3;

2.2.4.1.10. Implementar as Recomendações do ITU – T – Q.771- Q.774;

2.2.5. O SGW ofertado deverá implementar as funções adicionais de Sinalização SS7.

2.2.5.1. Funcionalidades Adicionais:

2.2.5.1.1. Múltiplas Redes SS7 - Implementar a funcionalidade de Múltiplas Redes SS7, onde uma Rede SS7 pode ser subdividida em vários nós lógicos ou redes virtuais, possibilitando a associação de um OPC exclusivo para cada Rede Virtual;

2.2.5.1.2. Múltiplos Point Codes - Permitir a criação e administração de Múltiplos OPC's para uma mesma rede;

2.2.5.1.3. High-speed Signalling Links - Permitir a implementação de Links de Sinalização de Alta Velocidade, conforme ITU Q.703, Anexo A;

2.2.5.1.4. SS7 Screening - Implementar a função de Screening para as mensagens SS7 relativas aos protocolos MTP, SCCP e MAP. A função de Screening SS7 permite ao operador examinar detalhadamente as mensagens SS7 que circulam pela sua rede. Com base neste exame, o SGW pode ser configurado para rejeitar ou permitir o tráfego entre determinadas Redes, e também, para alterar o destino ou campos da mensagem, conforme sua conveniência e necessidade.

2.2.6. Métodos para MTP Screening:

2.2.6.1. OPC/DPC/SIO screening;

2.2.6.2. Incoming linkset / DPC screening;

2.2.6.3. Message length (LI) screening;

2.2.6.4. Network indicator (NI) screening;

2.2.6.5. MTP Gateway Screening ("Bellcore" Screening);

2.2.6.6. SCCP and User context Screening, tal como Screening baseado no tipo de mensagem;

2.2.6.7. Subsystem screening;

2.2.6.8. Protocol-class screening.

2.2.7. **Monitoração Flexível** - O SGW deverá permitir a monitoração do tráfego de mensagens SS7, através da configuração de parâmetros e critérios que permitam a obtenção de informações específicas de determinado tipo de tráfego.

2.2.7.1. Os dados a serem analisados são armazenados na memória do sistema e em seguida são aplicados filtros para obtenção de informações relativas ao tipo de tráfego observado. Caso o SGW fornecido não possua essas funções, poderá ser adicionado dispositivo externo como probe ou similar.

2.2.8. O SGW deverá suportar os seguintes tipos de interfaces externas:

2.2.8.1. Circuit interface: E1 interface (2.048 Mbit/s), T1 interface (1.544 Mbit/s);

2.2.8.2. Clock interface: 2.084 Mbit/s, 2.048 MHz and 8 kHz clock signal interfaces;

2.2.8.3. FE interface: 10BaseT/Fx and 100BaseT/Fx;

2.2.8.4. Standard NM interface: SNMP interface;

- 2.2.8.4.1. Other: supporting MML;
- 2.2.8.5. SS7 over TDM with narrowband signalling links with 56 (PCM24) and 64 (PCM30) kbit/s (G.703/MTP1/MTP2/MTP3);
- 2.2.8.6. SS7 over TDM with High-speed Signalling Links with 1.5 / 2 Mbit/s G.703 Annex A;
- 2.2.8.7. SS7 over IP with 10/100 bT/Ethernet/IP/SCTP/M3UA acc. to IETF RFC 4666;
- 2.2.8.8. SS7 over IP with 10/100 bT/Ethernet/IP/SCTP/M2PA acc. to IETF RFC 4165;
- 2.2.8.9. SS7 over IP with 10/100 bT/Ethernet/IP/SCTP/M3UA acc. to IETF RFC 2960 & 4666.

2.2.9. O SGW deve implementar as capacidades mínimas abaixo:

Item	Valor
Número de links LSL (64-kbit/s)	>384
Número de links HSL (2-Mbit/s)	>24
Capacidade de GT	>18000
Número de DPCs suportados	>900

2.2.9.1.O SGW deve implementar as performances mínimas abaixo:

Item	Index
Tráfego sobre links de 64-kbit/s	>0.80Erl
Tráfego sobre links de 2-Mbit/s	>0.80Erl
Tráfego sobre links de 1.544-Mbit/s	>0.80Erl
Atraso de transferência de mensagens	<15ms
Capacidade de processamento das mensagens	>60480 MSU/s
Capacidade GTT	>60480 GTT/s

2.2.10. Gerenciamento do SGW

- 2.2.10.1. Gerência e Manutenção:
 - 2.2.10.1.1. Status da Rede através de Geração de Relatórios;
 - 2.2.10.1.2. Automation of everyday tasks;
 - 2.2.10.1.3. Session Control;
 - 2.2.10.1.4. Alarm browser for QoS Alarms (SSNC);
 - 2.2.10.1.5. Alarmes de Performance Real Time through Threshold Supervision and forwarding to SNMP server;
 - 2.2.10.1.6. Alarm Threshold Administration;
 - 2.2.10.1.7. Monitoração de Alarme da Rede SS7;
 - 2.2.10.1.8. Logging and browsing de alarmes de performance;
 - 2.2.10.1.9. Flexibilidade e facilidade de geração de relatórios para auxiliar nos processos de investigação de falhas na rede de sinalização;
 - 2.2.10.1.10. Implementar comandos MML e interface GUI;
 - 2.2.10.1.11. Implementar ferramenta que permita realizar o trace de sinalização, conforme descrito a seguir:
 - 2.2.10.1.11.1. Armazenamento do histórico dos traces. Caso o SGW fornecido não execute essa função, será permitido uso de dispositivo externo como probe ou equivalente;
 - 2.2.10.1.11.2. Capacidade de executar o trace em links parciais, linksets ou todos os links. Caso o SGW fornecido não execute essa função, será permitido uso de dispositivo externo como probe ou equivalente;

2.2.11. Backup das bases de dados provisionadas no SGW;

2.2.11.1. Mecanismos para verificação de integridade e correção das bases de dados no SGW;

2.2.12. Gerenciamento de SS7:

2.2.12.1. MTP:

2.2.12.1.1. Signalling Points;

2.2.12.1.2. Signalling Links and Linksets;

2.2.12.1.3. Signalling Routes and Destinations;

2.2.12.1.4. Combined Linksets;

2.2.12.1.5. Protocol Profiles tal como Configuração MTP

2.2.12.1.6. Incoming Linkset Screening;

2.2.12.1.7. OPC/DPC/SIO Screening;

2.2.12.1.8. MTP Gateway Screening;

2.2.12.1.9. MSU criteria for duplication tal como MTP multiplas rotas;

2.2.12.1.10. Administration for M3UA;

2.2.12.1.11. MTP Measurement Configuration.

2.2.12.2. SCCP:

2.2.12.2.1. SCCP Routing;

2.2.12.2.2. SCCP Global Title Translators and Rules;

2.2.12.2.3. Local SCCP user Calling Party addresses;

2.2.12.2.4. SCCP Analysis criteria for Traffic Partitioning;

2.2.12.2.5. SCCP Measurements;

2.2.12.2.6. SCCP Gateway screening;

2.2.12.2.7. SCCP criteria for duplication tal como SSN backup

2.2.12.2.8. Função de teste de GT para evitar GT loop.

2.2.13. Padrões e Protocolos Suportados

2.2.13.1. ISUP Compliance

2.2.13.1.1. Suportar Q.761 Functional Description of ISDN User Part

2.2.13.1.2. Suportar Q.761 General Functions of Messages and Signals

2.2.13.1.3. Suportar Q.763 Formats and Codes

2.2.13.1.4. Suportar Q.764 Signalling Procedures

2.2.13.1.5. Suportar Q.767 Application of the ISDN User Part for International ISDN Interconnections

2.2.13.2. Suportar, descritos de 2.2.13.1.1 até 2.2.13.1.5, significa funcionalidade realizada pela plataforma, mas não necessariamente fornecida, podendo ser implementada no futuro com a adição de módulos e/ou licenças de software.

2.2.14. MTP Compliance:

2.2.14.1. Q.701 Functional Description of the Message Transfer Part;

2.2.14.2. Q.702 Signalling Data Link;

2.2.14.3. Q.703 Signalling Link;

2.2.14.4. Q.704 Signalling Network Functions and Messages;

2.2.14.5. Q.705 Signalling Network Structure;

2.2.14.6. Q.706 Message Transfer Part Signalling Performance;

2.2.14.7. Q.707 Testing and Maintenance;

2.2.14.8. Q.708 Number of International Signalling Point Codes;

2.2.14.9. Q.709 Hypothetical Signalling Reference Connection;

2.2.15. SCCP Compliance:

2.2.15.1. Q.711 Functional Description os Signalling Conection Control Part;

2.2.15.2. Q.712 Definition and Function of SCCP Messages;

2.2.15.3. Q.713 SCCP Formats and Codes;

- 2.2.15.4. Q.714 SCCP Procedures;
- 2.2.15.5. Q.715 SCCP User Guide;
- 2.2.15.6. Q.716 SCCP Performance.

2.2.16. TCAP Compliance:

- 2.2.16.1. Q.771 Functional Description of Transaction Capabilities;
- 2.2.16.2. Q.772 TCAP Information Element Definitions;
- 2.2.16.3. Q.773 TCAP Formats and Encoding;
- 2.2.16.4. Q.774 TCAP Procedures;
- 2.2.16.5. Q.775 Guidelines for Using TCAP;
- 2.2.16.6. ETSI 300 008-1 latest edition;
- 2.2.16.7. Q.2110, Q.2140, Q.2210 for E1/T1 High-speed Signalling Links acc. to Bellcore;
- 2.2.16.8. ETSI 300 009-1 latest edition

2.2.17. INAP versions:

- 2.2.17.1. Suportar ETSI, CS1S2 ou CS1+ compatible network
- 2.2.17.2. Suportar CAP phase 1 -2;
- 2.2.17.3. Suportar, descritos em 2.2.17.1 até 2.2.17.2, significa funcionalidade realizada pela plataforma, mas não necessariamente fornecida, podendo ser implementada no futuro com a adição de módulos e/ou licenças de software.

2.2.18. SS7 Over IP:

- 2.2.18.1. MTP3 User Adaptation layer (M3UA) according to RFC 4666 and ETSI TS 102 142;
- 2.2.18.2. MTP2 Peer to Peer Adaptation layer (M2PA) according to RFC 4165;
- 2.2.18.3. Internet Protocol according to RFC 791.

2.2.19. O SGW ofertado deverá implementar o protocolo SIGTRAN, conforme suas variantes:

- 2.2.19.1 Implementar a RFC 2719 – Framework Architecture for Signaling Transport.
- 2.2.19.2. Implementar a RFC 4233 – ISDN Q.921 User Adaptation Layer;
- 2.2.19.3. Implementar a RFC 4165 – SS7 MTP2 User Peer-to-Peer Adaptation Layer (M2PA);
- 2.2.19.4. Implementar a RFC 4666 – SS7 MTP3 – User Adaptation Layer (M3UA);
- 2.2.19.5. Implementar a RFC 3257 – Stream Control Transmission Protocol Applicability Statement;
- 2.2.19.6. Implementar a RFC 3873 – SCTP Management Information Base (MIB);
- 2.2.19.7. Implementar a RFC 3788 – Security Considerações para o SIGTRAN;

2.2.20. O sistema ofertado deverá disponibilizar interfaces independentes para separar o tipo de tráfego – gerência e sinalização.

- 2.2.20.1. As interfaces deverão ser Gigabit Ethernet IEEE 802.3z;
- 2.2.20.2. Arquitetura de software, Backup e Recuperação;
- 2.2.20.3. A solução ofertada deverá possuir arquitetura de software que permita sua atualização sem a necessidade do sistema ser paralisado;
- 2.2.20.4. Deve permitir a inserção e retirada de patches de correção de programa sem a necessidade de paralisação do sistema;
- 2.2.20.5. O SGW deverá permitir o reinício manual mediante comando homem-máquina ou agendamento prévio através da Plataforma de Gerência;
- 2.2.20.6. O SGW deve permitir o armazenamento do seu backup e possibilitar a transferência do seu conteúdo para outras mídias através do protocolo FTP;
- 2.2.20.7. Devem ofertar todas as funcionalidades especificadas para o Gateway de Sinalização em um equipamento dedicado (Stand Alone) para esta função;

2.2.21. Interfaces físicas do SGW: SGW = 4+4 interfaces GbE (Gigabit Ethernet) 1000Base T, interfaces RJ45 (15 links lógicos - SIGTRAN), cada equipamento.

2.2.22. O SGW deve ser dimensionado considerando as capacidades especificadas para o HLR e o SMSC.

2.3. SMSC (Short Message System Center) – No mínimo 01 (um) SMSC em alta disponibilidade

2.3.1. A plataforma deverá ser centralizada e deve ser provida de interfaces de sinalização Sigtran - M3UA.

2.3.2. A conexão entre a plataforma SMSC e os elementos de rede HLR(s) será feita através de STPs/SGW (Signaling Transfer Points), garantindo o funcionamento em caso de falha na rede de sinalização.

2.3.3. A plataforma deve possibilitar interface WEB, envio de mensagens broadcast, envio de mensagens para códigos Especiais. Caso a SMSC fornecida não execute esta função, será permitido uso de dispositivo ou ferramenta externa.

2.3.4. A solução oferecida deve ser totalmente aderente às seguintes especificações, em suas últimas versões:

2.3.4.1. SIP - Session Initiation Protocol

2.3.5. Outras especificações de regulamentação e padronização a serem seguidas e atendidas pelo CONTRATANTE:

2.3.5.1. Especificações do 3GPP para SMS;

2.3.5.2. Especificações do SMS Forum (SMPP).

2.3.5.3. O SMSC ofertado deverá implementar, no mínimo, as seguintes funções:

2.3.5.3.1. Processamento de mensagens;

2.3.5.3.2. Sinalização SMPP (versão 3.4);

2.3.5.3.3. Partição de carga dos enlaces de sinalização;

2.3.5.3.4. Interface gráfica homem-máquina;

2.3.5.3.5. Padrão SNMP para sistema de gerência;

2.3.5.3.6. Conter dispositivos de segurança multi-nível para acessos ao sistema;

2.3.5.3.7. APIs para a customização com sistemas de Customer Care, Billing e provisionamento remoto;

2.3.5.3.8. Tolerância a falhas funcionando em cluster modo active-standby;

2.3.5.3.9. A plataforma deve possuir a tecnologia de Banco de Dados Baseados em Memória, ou seja, a capacidade de o processamento de uma transação ocorrer dentro da memória, aperfeiçoando a eficiência;

2.3.5.3.10. A plataforma deve implementar capacidade nominal de 250 MDAS (Message Delivery Attempt por segundo);

2.3.5.3.11. A plataforma deve implementar capacidade de 7.200.000 de assinantes;

2.3.5.3.12. A plataforma deve implementar capacidade mínima de 600Gb de banco de dados;

2.3.5.3.13. A plataforma deve implementar 25Mbit/s de enlaces de sinalização M3UA;

2.3.5.3.14. A plataforma deve implementar os padrões de interfaces SMPP ou SMPP+ e TCP/IP;

2.3.5.3.15. A plataforma deve implementar relatório de entrega de mensagens (SMS Delivery Reports);

2.3.5.3.16. A plataforma deve implementar reenvio imediato após uma tentativa mal-sucedida (SMS Retry);

2.3.5.3.17. A plataforma deve implementar armazenamento da mensagem para envio posterior, configurado pelo operador (SMS Store and Forward);

2.4. OTA (Over-The-Air) – No mínimo 01 (um) OTA em alta disponibilidade

2.4.1. Requerimentos Gerais

2.4.1.1. A solução OTA deve implementar no mínimo o volume transacional de 30 (trinta) mensagens por segundo;

2.4.1.2. A solução OTA deve, antes de aprovisionar os dados relativos aos cartões SIM245, criptografar as chaves utilizando a chave de transporte selecionada, através do método DES e 3-DES.

2.4.1.3. Durante o aprovisionamento:

2.4.1.3.1. As chaves devem ser descriptografadas com a correspondente chave de transporte;

2.4.1.3.2. As chaves devem ser criptografadas utilizando a chave mestre do sistema;

2.4.1.3.3. Só então, as chaves devem ser armazenadas no repositório do sistema;

2.4.1.4. A solução OTA deve dispor de funcionalidade de agrupamento de registros de cartões SIM245 na Plataforma. Esta funcionalidade deve permitir a execução simplificada de Campanhas de gestão dos cartões SIM245;

2.4.1.5. A solução OTA deve dispor de funcionalidade de Application Repository Manager, permitindo a auditoria do conteúdo dos cartões SIM245;

2.4.1.5.1 Esta funcionalidade deve permitir a gestão e constante atualização do conteúdo dos cartões SIM245; tal informação deve estar disponível na base de dados da Plataforma;

2.4.1.5.2 Esta funcionalidade deve estar disponível para os canais SMS e BIP CAT-TP.

2.4.1.5.3. Os serviços que devem ser minimamente cobertos são os seguintes:

2.4.1.5.3.1. Auditar o conteúdo dos registros: retornar o conteúdo de um registro, contido em um arquivo;

2.4.1.5.3.2. Auditar o tamanho do arquivo: retorna o tamanho do arquivo;

2.4.1.5.3.3. Auditar o tamanho da memória livre: retorna o tamanho da memória livre no cartão SIM245;

2.4.1.5.3.4. Auditar a presença de instância Java: verifica a presença de um applet no cartão;

2.4.1.5.3.5. Auditar presença de pacote Java: verifica a presença de pacote no cartão;

2.4.2. A solução OTA deve implementar a funcionalidade de Remote File Management (RFM) para os cartões SIM245, em conformidade com os padrões 3GPP TS 51.011, 3GPP TS 31.102 e 3GPP TS 11.11, para cartões de tecnologia 2G e 3G, atendendo minimamente as funções descritas abaixo:

2.4.2.1. Activate ADN

2.4.2.2. Activate FDN

2.4.2.3. Switch ADN/FDN

2.4.2.4. Update ACC

2.4.2.5. Update AND

2.4.2.6. Update BDN

2.4.2.7. Update CBMI

2.4.2.8. Update FDN

2.4.2.9. Update FPLMN

2.4.2.10. Update HPLMN

2.4.2.11. Update IMSI

2.4.2.12. Update LP

2.4.2.13. Update MSISDN

2.4.2.14. Update PLMN

2.4.2.15. Update SDN

2.4.2.16. Update SMSP

2.4.2.17. Update SPN

2.4.2.18. Update SST

2.4.2.19. Update PL

- 2.4.2.20. Update EST
- 2.4.2.21. Update UST
- 2.4.2.22. Generic Card Update
- 2.4.2.23. Update HPLMNwAct
- 2.4.2.24. Update PLMNwAct
- 2.4.2.25. Update OPLMNwAct

2.4.3. A solução OTA deve implementar a funcionalidade de Remote Applet Management (RAM) para os cartões SIM245, em conformidade com os padrões 3GPP TS 51.011, 3GPP TS 31.102 e 3GPP TS 11.11, para cartões de tecnologia 2G e 3G, atendendo minimamente as funções descritas abaixo:

- 2.4.3.1. Download applet
- 2.4.3.2. Delete applet
- 2.4.3.3. Lock applet
- 2.4.3.4. Unlock applet
- 2.4.3.5. Download package
- 2.4.3.6. Delete package
- 2.4.3.7. Install for load package
- 2.4.3.8. Load package
- 2.4.3.9. Extradite Executable Load File
- 2.4.3.10. Create applet instance
- 2.4.3.11. Delete applet instance
- 2.4.3.12. Make instance selectable
- 2.4.3.13. Extradite Application
- 2.4.3.14. Download applet to installed
- 2.4.3.15. Instantiate applet to installed

2.4.4. A solução OTA deve implementar Proof of Receipt (PoR), em conformidade com o padrão 3GPP TS 23.048 V5.9.0, e SMSs de texto e binários;

2.4.5. A solução OTA deve dispor de Módulo de Campanha que permita a execução de atualização de arquivo SIM, download de applets Java e atualizações de menu IOD;

2.4.5.1. Este Módulo de Campanha deve permitir a execução de campanhas em batch único, realizando o pré-processamento de todo o pacote antes da entrega do mesmo, fazendo desnecessário o processamento antes do envio de cada mensagem e otimizando a utilização do recurso das SMSCs;

2.4.6. A solução OTA deve permitir a descritografia das chaves-mestre disponibilizadas pelo Serpro, cifradas em padrão DES e 3-DES, utilizando a chave de transporte correspondente. Posteriormente, deverá realizar a criptografia utilizando chave mestre do sistema, para só então serem armazenadas no repositório do sistema;

2.4.7. A solução OTA deve dispor de módulo de campanha, com gestão via interface gráfica, que permita atualizações Over-The-Air para cartões SIM245 por MSISDN, IMSI e ICCID. O módulo de campanha deve implementar as funcionalidades de Remote File Management (RFM) e Remote Applet Management (RAM);

2.4.8. A solução OTA deve dispor de ferramenta de gestão de roaming, através da gestão Over-The-Air dos arquivos PLMN e FPLMN 2G e 3G;

2.4.9. Integração e Interoperabilidade

2.4.9.1. A solução OTA deve estar integralmente em conformidade com o processo estabelecido pelos grupos de trabalho do Projeto Denatran SIMRAV, que estabelece que a OTA deve ser capaz de gerir requisições encaminhadas da rede de uma Operadora de

Telefonia, recebendo a resposta desta requisição através da rede de outra Operadora de Telefonia, no momento da troca de operadora nos cartões SIM245. Garantindo assim, a gestão segura destes cartões;

2.4.9.2. A solução OTA deve ser interoperável, suportando todos os cartões SIM245 que estejam em conformidade com o padrão descrito na “Especificação Técnica Aplicativo SIM 245 v1.2.0” de 24 de abril de 2009, independente do fabricante deste cartão;

2.4.9.3. A solução OTA deve implementar a integração com as Plataformas SMSC das Operadoras de Telefonia do Serviço Móvel Pessoal (SMP) envolvidas no Projeto Denatran SIMRAV, utilizando a infraestrutura de rede existente do SERPRO, e implementando minimamente os canais abaixo listados:

2.4.9.3.1. CMG de 3.1.0 até 4.6 (EMI UCP)

2.4.9.3.2. SMPP 3.3 e 3.4

2.4.9.3.3. Nokia SC 4 e SC 5 (CIMG2)

2.4.9.4. A solução OTA deverá realizar integração de comunicação com o Mediador item 2.7.

2.4.9.5. A solução OTA deve implementar integração com a rede IP das Operadoras de Telefonia do Serviço Móvel Pessoal (SMP) envolvidas no Projeto Denatran SIMRAV via BIP (Bearer Independent Protocol) CAT-TP, utilizando a infraestrutura de rede do SERPRO para uso futuro e em concordância com futuras especificações técnicas do aplicativo SIM245 que venham a utilizar este canal de comunicação.

2.4.10. Requerimentos de Padrões

2.4.10.1. A solução OTA deve estar em conformidade com os padrões abaixo listados:

2.4.10.1.1 ANATEL – SMP – Resolução 477

2.4.10.1.2. 3GPP TS 23.040

2.4.10.1.3. 3GPP TS 23.048

2.4.10.1.4. 3GPP TS 31.102

2.4.10.1.5. 3GPP TS 31.10

2.4.10.1.6. 3GPP TS 11.11

2.4.10.1.7. 3GPP TS 51.011

2.4.10.1.8. 3GPP GSM TS 03.203

2.4.10.1.9. 3GPP GSM TS 23.003

2.4.10.1.10. ITU-T – E.164

2.4.10.1.11. GSM 03.38

2.4.10.1.12. 3GPP 23.038

2.4.10.1.13. ETSI TS 102 226

2.4.10.1.14. ETSI TS 102 227

2.4.11. Requerimentos de Marketing

2.4.11.1. A solução deve dispor de interface web para visualização e obtenção de estatísticas e relatórios em tempo real;

2.4.11.2. A ferramenta de estatística e relatórios deve permitir a geração de relatórios sob demanda, através da interface web;

2.4.11.3. A ferramenta de estatística e relatórios deve permitir a geração de relatórios automáticos, com seu agendamento definido pelo SERPRO;

2.4.11.4. A ferramenta de estatística e relatórios deve dispor de mecanismo de exportação de relatórios para diferentes formatos, tais como, Excel, Word, TXT, PDF, HTML and XML;

2.4.11.5. Os dados expressos pelas estatísticas e relatórios da solução devem permanecer acessíveis por no mínimo 30 (trinta) dias após sua geração;

2.4.11.6. Os relatórios devem ser flexíveis por período (data inicial e data final);

2.4.11.7. A solução deve dispor de logs de auditoria. Estes logs de auditoria devem ser gerados para todos os perfis de usuários definidos na solução, para os casos de: criação, modificação, consulta e uso da solução.

2.4.12. Dimensionamento da solução OTA:

Para cada SIM245 ativado, poderá ser executada uma transação de desativação, caso aplicável, sem que a mesma gere custo adicional de licenciamento. As plataformas OTA e Mediador deverão garantir o pleno funcionamento do sistema, mesmo que o pacote de licenças contratado seja esgotado durante o período contratado, garantindo a disponibilidade de serviço para o usuário final.

2.5. PLATAFORMA DE GERÊNCIA – No mínimo 01 (uma) plataforma de gerência.

2.5.1. Requerimentos Gerais

2.5.1.1. Essa especificação aplica-se a todas as plataformas alocadas para o atendimento da infraestrutura de telecomunicações que visa a atender atendimento ao projeto SIMRAV, alocada na estrutura do SERPRO.

2.5.1.2. Todas as plataformas pertencentes ao Sistema Denatran de Telecomunicações (HLR, SGW, SMSC e OTA) para o projeto SIMRAV, deverão ser integradas a uma plataforma de gerência centralizada em modo cluster, arquitetura cliente-servidor.

2.5.1.3. A plataforma de gerência centralizada deverá ser única para todos os sistemas de telecomunicações implantados para o projeto SIMRAV e deverá ser fornecida pela aderente a qual ficará responsável pelo gerenciamento da mesma.

2.5.1.4. A plataforma de gerência centralizada deverá possuir interfaces Lan redundantes para tolerância a falhas e em número suficiente para a interligação de todos os dispositivos a serem gerenciados;

2.5.1.5. Deve implementar NTP para sincronia com um servidor NT;

2.5.1.6. A plataforma deve possuir disponibilidade de 99,999% MTBF mínimo de 25000 horas;

2.5.1.7. Deve implementar interface WEB.

2.5.2 Requisitos de Backup e Recuperação

2.5.2.1 Implementar backup de dados das seguintes situações:

2.5.2.1.1. Backup e recuperação da plataforma de gerência;

2.5.2.1.2. Backup de dados e recuperação dos elementos de redes gerenciados;

2.5.2.1.3. Cada elemento deve armazenar seu último backup localmente;

2.5.2.1.4. Implementar agendamento de backups;

2.5.2.1.5. Implementar backups automáticos;

2.5.2.1.6. Implementar Veritas net backup;

2.5.2.1.7. Implementar online backups incrementais;

2.5.2.1.8. Implementar rotinas de backups centralizadas;

2.5.2.1.9. O tempo para realização de uma rotina de backup não deve ser superior a 20 horas;

2.5.2.1.10. Durante o backup não pode haver nenhum impacto ao tráfego de dados relativos às operações de gerenciamento;

2.5.2.1.11. Deve ser possível fazer um snapshot backup de um determinado momento da situação da rede para que seja utilizado em procedimentos de fallback.

2.6. Certificações

As plataformas ofertadas devem, obrigatoriamente, estar certificadas junto ao órgão regulador ANATEL.

2.7. Plataforma do Mediador – No mínimo 01 (um) conjunto de Mediador em alta disponibilidade

2.7.1. Características da Plataforma de Mediação

2.7.1.1. A Plataforma mediadora para SIMRAV é uma plataforma única que deverá prover

serviços por meio de integração com os sistemas SIMRAV, HLR e OTA, realizando operações de Aprovisionamento e Portabilidade.

Toda a infraestrutura de telecomunicações a ser implantada no SERPRO para atendimento ao projeto SIMRAV deverá ser integrada à plataforma de mediação.

2.7.1.2. A Plataforma Mediador deve possuir módulos para Gestão de Log e Eventos;

2.7.1.3. A Plataforma Mediador deve possuir Interface WEB para Aplicações de Monitoramento de Log e Eventos;

2.7.1.4. A Plataforma Mediador deve possuir Componentes de Detecção, Roteamento e Adaptação de Conteúdo de Mensageria XML e Arquivos XML e Transferência com conectividade para HLR e OTA via MML, SMPP ou SOAP;

2.7.1.4.1 JAVA padrão J2EE, sob Jboss versão 5.1. As licenças de Jboss, JAVA e HornetQ, são open source. A licença da ferramenta Q-Ware deverá ser fornecida pelo SERPRO;

2.7.1.5. A Plataforma Mediador deve suportar no mínimo o volume transacional de 30 (trinta) mensagens por segundo, para provisionamento e portabilidade;

2.7.1.6. A Solução deve Integrar com arquitetura composta pelos elementos lógicos de processamento e banco de dados – Front End (FE) e Back End (BE);

2.7.1.7. A Solução deve Integrar com OTA.

2.7.1.8. A plataforma de mediador da CONTRATANTE deve prover uma ferramenta de verificação de consistência de dados nos HLRs redundantes. A funcionalidade de verificação de consistência procurará e mostrará quaisquer inconsistências de dados existentes entre os HLRs.

2.7.1.9. A plataforma de mediação fornecida pela CONTRATANTE deverá possuir registros dos provisionamentos. A solução deverá prover uma base de dados detalhada de logs com ferramenta de procura e análise estatística (data mining) configurada pelo operador.

2.7.1.10. A solução deverá suportar alta disponibilidade com 99,99%.

2.7.1.11. A plataforma de provisionamento deverá ser hot stand-by entre os servidores principal e de backup, em caso de falha da unidade principal o sistema de backup entrará em operação sem intervenção humana.

2.7.2. Serviço de Adaptação e Customização da Plataforma Mediadora

2.7.2.1. A Plataforma Mediadora será objeto de customização, adequação e geração de interfaces para integração com sistemas SIMRAV com o Mediador e o HLR e OTA.

2.7.2.1.1 - O fornecedor é obrigado a realizar a integração da plataforma do Serpro, mediante serviços de customização das interfaces utilizadas no SIMRAV, integrando os protocolos advindos do Qware para interfaces padrões 3GPP que são utilizadas nas plataformas de provisionamento do HLR e OTA.

2.7.2.2. Este serviço consistirá na adaptação da plataforma mediadora ao ambiente computacional e às necessidades negociais do Serpro.

2.7.2.3. Os artefatos disponibilizados pela CONTRATANTE na implementação da solicitação de Adaptação serão:

2.7.2.3.1. Validados pela equipe de Testes, Qualidade de Software e representantes das áreas gestoras da Solução, visando à verificação da conformidade com respectivos Padrões Tecnológicos SERPRO e requisitos de negócios;

2.7.2.3.2. Encaminhados para o Ambiente de Homologação de Processos;

2.7.2.3.3. Disponibilizados para produção ao final dos testes, após o aceite do artefato pelo SERPRO.

2.7.2.4. Os custos para a prestação dos serviços de Adaptação e Customização são de responsabilidade exclusiva da CONTRATANTE.

2.7.2.5. A adaptação e Customização da Solução observarão o descrito neste Termo de Referência.

2.7.3. Integração da Solução Ofertada com o SIMRAV

A plataforma de mediação única, deverá ser capaz de integrar todos os Sistemas Denatran de Telecomunicações ao sistema SIMRAV.

2.7.3.1. A Solução deverá ser integrada com o Sistema SIMRAV através de XML/Webservices.

2.7.3.2. A integração com o Sistema SIMRAV dar-se-á por filas padrão processando mensagens no formato XML - Extensible Markup Language, como meio padrão para troca de informações.

2.7.3.3. A integração com os Sites SIMRAV WEB do SERPRO dependerá do tipo de solução ofertada para Detecção, Roteamento e Adaptação de Conteúdo e Apresentação.

2.7.3.3.1. Os Sites referidos acima estão baseados na plataforma CISC/Linux em linguagem Java/HTML.

2.7.3.4. A Solução de mediação aos elementos ofertados com o objetivo de ativação, deve poder ser integrada tendo a capacidade de administração de sessões e conexões flexíveis para suprir os volumes de mensagens necessários assim como a topologia ofertada.

2.7.3.5. É necessário que a solução tenha um único ponto de aprovisionamento para toda a solução ofertada e que a mesma possua capacidades tais como:

2.7.3.5.1. Capacidade de executar comandos relacionados a grupos de assinantes, os quais serão provisionados pelos mesmos. O sistema tem que executar de forma agendada e com respostas dedicadas um grande número de subscrições no qual se deseja o aprovisionamento em grupo.

2.7.3.5.2. O sistema deve poder agendar comandos para serem executados nos sistemas provisionados. Este agendamento deve ser assíncrono e diferenciado quanto ao usuário e tempo.

2.7.3.5.3. Deve haver a possibilidade de se realizar uma verificação de consistência nas bases de dados a partir do elemento mediador. O mesmo deve fornecer flexibilidade, usabilidade, qualidade dos dados, extensibilidade, escalabilidade e capacidade de integração a outros sistemas.

2.7.3.5.4. Em caso necessitando de sistemas redundantes para as bases de dados, o mediador deve ter capacidade de provisionar mantendo a manipulação da redundância existente. No caso de os elementos provisionados oferecerem a mesma base de dados de subscrições, o mediador terá de provisionar ambas e ainda assim coordenando a base ativa e secundária. Terá de ser transparente para o SIMRAV o envio dos comandos de provisionamento mesmo sem ter conhecimento de qual elemento provisionado está ativo ou em stand-by

2.7.4. Padrões Tecnológicos SERPRO

2.7.4.1. A Plataforma Mediadora para Serviços SIMRAV deverá ser adaptada aos padrões tecnológicos do SERPRO, ambiente de homologação e produção, conectividade, de desenvolvimento e manutenção de sistemas.

2.7.4.2. Padrão de Construção de Aplicação e Ambiente Computacional.

2.7.4.3. As implementações realizadas pela empresa CONTRATANTE nos processos de adaptação, integração e modelagem de dados da Solução deverão obedecer às definições de três camadas básicas de arquitetura a seguir:

2.7.4.4. **Camada de Dados** – Sistema Gerenciador de Banco de Dados:

2.7.4.4.1. É responsável pelo acesso e armazenamento de dados garantindo integridade, disponibilidade, confidencialidade, manutenção e documentação;

2.7.4.4.2. As regras de negócio não deverão ser desenvolvidas em componentes do SGBD como TRIGGERS ou STORED PROCEDURES.

2.7.5. **Camada de Aplicação** (Fluxo de Processo e Regras de Negócio):

2.7.5.1. Essa camada é constituída de um conjunto de componentes que agrupam regras de negócio (Camada de Regras de Negócio) e definições de fluxo de processo dos sistemas que compõem a solução (Camada de Fluxo de Processo);

2.7.5.2. Uma regra de negócio define critérios - condições e/ou transformações que devem ser obedecidos dentro de um contexto do negócio;

2.7.5.3. As regras de negócio devem estar contidas na camada de aplicação e somente esta poderá acessar a camada de dados;

2.7.5.4. A camada de aplicação deve utilizar a linguagem Java;

2.7.6. **Camada de Apresentação:** A camada de apresentação formata as informações e dados oferecidos pelo sistema para que sejam adequadamente apresentados no acesso WEB utilizado pelo usuário de gerenciamento;

2.7.6.1. A camada de apresentação deve residir em servidor Web, sendo que neste último caso deve ser mantida a compatibilidade com o padrão W3C;

2.7.6.2. A Camada de Apresentação deverá suportar Browsers e utilizar linguagens Java, HTML e XML.

2.8. Conectividade

2.8.1. Será permitida à CONTRATANTE a conexão ao ambiente de Desenvolvimento do SERPRO que processará o sistema Denatran de Telecomunicações na cidade de Brasília/DF, mediante atendimento aos requisitos de segurança no processamento e no acesso correlato.

2.8.2. A forma de Conectividade atenderá obrigatoriamente aos requisitos de segurança disponíveis nas diversas formas de interligação definidas no portfólio de conexão com empresas externas, conforme regulamentação do SERPRO:

2.8.2.1. O acesso será feito pela Extranet do SERPRO e da CONTRATANTE, com todos os recursos tecnológicos inerentes a esse tipo de ambiente;

2.8.2.2. Após a autenticação na Extranet do SERPRO, a empresa terá acesso aos sistemas de acordo com a necessidade dos serviços;

2.8.3. A conectividade descrita neste item será utilizada pela empresa CONTRATANTE para transmitir ao SERPRO os códigos fonte das Adaptações, Desenvolvimento e Manutenções efetuadas, nas customizações realizadas; também será utilizado software de controle de versões do SERPRO, para submeter os códigos transmitidos aos processos de Compilação, Testes, Homologação e Produção;

2.8.4. As despesas de conexão – linha de comunicação - de acesso ao ambiente do SERPRO serão custeadas pela CONTRATANTE.

2.9. Da Operacionalização dos Serviços

2.9.1. O SERPRO e a CONTRATANTE, sempre que necessário, agendarão reuniões periódicas de caráter gerencial e/ou técnico para avaliar os trabalhos, adotar resoluções e obter esclarecimento de pendências durante toda a vigência do contrato.

2.10. Relação de hardware, software e serviços mínimos para implantação do Sistema Denatran de Telecomunicações:

Item	Quantidade
HLR (Home Location Register)	01
SGW (Signaling Gateway)	01
SMSC (Short Message System Center)	01
OTA (Over-The-Air)	01
Plataforma Mediador	01
Plataforma de Gerência	01
Serviços de Suporte e Manutenção	01
Serviços de Operação Assistida	01

2.11. Repasse de conhecimento

2.11.1. A Contratante deverá prover repasse de conhecimento técnico aos profissionais do Serpro para configuração e operação dos equipamentos e softwares.

2.11.2. O repasse de conhecimento deverá ocorrer sem ônus adicional para o Serpro, incluindo todo o material didático necessário. O material de aula deverá abordar conteúdo teórico e prático, e deverá ser submetido ao Serpro para aprovação antes da realização da capacitação.

2.11.3. O repasse de conhecimento deverá ser ofertada através de profissionais certificados e credenciados pelo fabricante ou empresa credenciada para tal finalidade.

2.11.4. A Contratante deve prover O repasse de conhecimento referente a solução proposta, sem ônus para o Serpro, atendendo aos seguintes tópicos:

2.11.4.1. Funcionalidades e ferramentas da solução;

2.11.4.2. Arquitetura de Hardware e Software;

2.11.4.3. Protocolos e interfaces;

2.11.4.4. Dimensionamento do sistema;

2.11.4.5. Alarmes e Estatísticas;

2.11.4.6. Manutenção e operação do sistema;

2.11.4.7. Integração com demais sistemas;

2.11.5. O repasse de conhecimento deve ser provido de acordo com a distribuição abaixo:

2.11.5.1. Para a Solução instalada em São Paulo, 02 (duas) turmas de 10 (dez) participantes cada com 160 (cento e sessenta) horas cada em São Paulo ou em local no Brasil indicado pelo licitante, desde que acordado pelo Serpro. O ônus do deslocamento dos empregados do Serpro, com hospedagem correrá por conta do Serpro;

2.11.5.2. Para o Mediador, instalado em São Paulo, 02 (duas) turmas de 10 (dez) participantes cada com 40 (quarenta) horas cada, em São Paulo ou em local no Brasil indicado pelo licitante no caso de impossibilidade da capacitação do treinamento em São Paulo, desde que acordado pelo Serpro. O ônus do deslocamento dos empregados do Serpro, com hospedagem correrá por conta do Serpro;

2.11.5.3. O repasse de conhecimento deve ser realizada em língua portuguesa.

2.11.5.4. Cada turma desta capacitação deverá ser dimensionada para até 10 (dez) participantes.

2.11.5.5. A Contratante deve responsabilizar-se por toda a infraestrutura requerida para o treinamento.

2.11.5.6. A contratante deve fornecer treinamentos práticos em equipamentos com a mesma versão de SW ofertado.

2.11.6. O repasse de conhecimento deverá ser iniciada no prazo máximo de 60 (sessenta) dias corridos após a assinatura do contrato.

3.0 Níveis de Serviço

3.1. A CONTRATANTE deverá dispor de todos os requisitos que assegurem o cumprimento de todos os Níveis de Serviços, abaixo identificados, para atendimento nos locais de instalação e funcionamento dos hardwares, softwares e serviços.

3.1.1. Os chamados poderão ser efetuados por intermédio de telefone 0800 (ligação gratuita), acesso Web ou e-mail, e serão registrados. Estes registros deverão estar disponíveis por meio de relatórios encaminhados mensalmente, para acompanhamento da equipe do SERPRO, atendendo aos seguintes tópicos:

3.1.1.1. Chamados Abertos no Período: Relatório com todas as ocorrências abertas no mês e o status;

- 3.1.1.2. Chamados em Andamento: Relatório onde constam as ocorrências que estão sendo tratadas e qual o status;
- 3.1.1.3. Chamados Fechados no Período: Relatório com todos os chamados que foram fechados no mês;
- 3.1.1.4. Histórico de Chamados em 12 Meses: Relatório com o histórico de chamados que foram abertos no período de 12 meses;
- 3.1.1.5. Controle de Troca de Equipamentos: Relatório com todos os chamados de troca de equipamentos que foram abertos no período.

3.1.2. Os relatórios deverão estar disponíveis via WEB (em formato HTML) para a Gerência de Qualidade e Recuperação da Superintendência de Redes do SERPRO, em Salvador-BA (Divisão de Gerenciamento de Incidentes - SUPOP/OPGPS/OPPBA - Serpro/Regional Salvador - Av. Luiz Vianna Filho, 2.355, Salvador - BA). Os dados necessários para viabilização do acesso serão informados após a instalação do primeiro equipamento fornecido.

3.1.3. Deve ser feita uma notificação de conclusão do atendimento no momento do fechamento de cada chamado.

3.2. Requerimentos Operacionais

3.2.1. Relatórios e Estatísticas

3.2.1.1. A solução deve dispor de histórico de eventos que permitam a investigação de qualquer tipo de falha.

3.2.1.2. A solução deve suportar as seguintes funcionalidades:

3.2.1.2.1. SNMP MIBs para alarmes de hardware

3.2.1.2.2. SNMP MIBs para alarmes da aplicação

3.2.1.2.3. SNMP traps

3.2.1.2.4. Interface gráfica para gestão dos alarmes

3.2.1.2.5. Interface gráfica para configuração

3.2.2. Suporte e Manutenção

3.2.2.1. A CONTRATANTE deve ofertar serviço de suporte, manutenção e monitoramento através de equipes baseadas em território nacional e capazes de comunicar-se em língua portuguesa, a fim de facilitar e agilizar possíveis interações com as equipes do SERPRO.

3.2.2.2. A CONTRATANTE deve testar exaustivamente todos os corretivos antes de aplicá-los na solução.

3.2.2.3. A CONTRATANTE deve notificar o SERPRO de qualquer nova atualização disponível para a solução, sendo responsabilidade da CONTRATANTE a instalação da mesma.

3.2.2.4. A CONTRATANTE deve prover e instalar todos as ações corretivas sem custos adicionais ao SERPRO.

3.2.2.5. A CONTRATANTE deve manter uma imagem da solução no ambiente da CONTRATADA , visando a realização de testes e validações de corretivos a serem instalados no Serpro;

3.2.2.6. A CONTRATANTE deve dispor de interface web para gestão e abertura de chamados.

3.2.2.7. A CONTRATANTE deve manter toda a documentação relativa a solução atualizada, estando a mesma em conformidade com os corretivos aplicados na solução.

3.2.2.8. A CONTRATANTE deve prover claramente o canal para solicitação de ajuste de severidade de incidentes.

3.2.2.9. A CONTRATANTE deve prover serviço de manutenção preventiva, com entrega de relatórios periódicos indicando possíveis impactos na solução.

3.2.2.10. A CONTRATANTE deve prover canal telefônico com disponibilidade 24x7 para abertura de chamados.

3.2.2.11. A CONTRATANTE deve dispor de canal de relacionamento com o cliente, realizando consultas periódicas ao Serpro quanto à qualidade da solução e serviços ofertados.

3.2.2.12. A CONTRATANTE deverá atender minimamente aos SLAs descritos na tabela abaixo:

Severidade	Tempo de Resposta	Disponibilidade de Atendimento	Diagnóstico
Alta	30 minutos	24 horas, 7 dias por semana, 365 dias por ano	A Contratante deverá trabalhar continuamente até que o serviço seja restaurado completamente ou até que uma solução temporária seja adotada, restabelecendo o serviço.
Média	2 horas	24 horas, 7 dias por semana, 365 dias por ano	A Contratante deverá trabalhar continuamente até que o serviço seja restaurado completamente ou até que uma solução temporária seja adotada, restabelecendo o serviço.
Baixa	1 dia	8 horas, 5 dias por semana, em horário comercial	A Contratante deverá despender todo o esforço razoável para solucionar o chamado, sem compromisso em tempo de solução.

3.2.2.13. Os níveis de chamados classificam-se de acordo com a tabela abaixo:

Nível Identificação da Severidade	Descrição	Características
Alta	Serviço de Alta Criticidade	<ul style="list-style-type: none"> O usuário não consegue utilizar o serviço, por indisponibilidade do mesmo. Qualquer suspeita de falha na política de segurança, ameaçando a confidencialidade e integridade dos dados, a disponibilidade dos serviços, que ocasione impacto significativo na aplicação. Qualquer incidente que ocasione impacto à imagem do Serpro. Um incidente de severidade de nível 2 que impacte número significativo (30% do total) de usuários.
Média	Serviço de Média Criticidade	<ul style="list-style-type: none"> Sérios problemas com um impacto importante em toda, ou parte da, operação do Serviço provido. O serviço está parcialmente interrompido ou severamente degradado, porém sem Impacto no negócio
Baixa	Serviço de Baixa Criticidade	<ul style="list-style-type: none"> Problemas de baixa severidade que não afetam o compromisso de SLA ofertado pela Contratante .

3.2.2.14. A CONTRATANTE deverá atender minimamente aos tempos de restauração de serviço descritos na tabela abaixo, em caso de falha no sistema:

Severidade	Tempo para Solução Contorno	Tempo para Solução Definitiva (sem defeito de HW)	Tempo para Solução Definitiva (com defeito de HW)
Alta	4 horas	3 dias úteis	30 dias úteis

Média	1 dia	7 dias úteis	60 dias úteis
Baixa	3 dias corridos	20 dias úteis	90 dias úteis

3.2.2.14.1. A tabela acima é aplicável a todo o Sistema Denatran de Telecomunicações (HLR, SMSC, SGW, OTA e Mediador) referente ao atendimento ao projeto SIMRAV.

3.2.2.15. A critério do SERPRO, os chamados poderão ter seu grau de severidade revisado (Escalação da Severidade) após o atendimento inicial pela CONTRATANTE.

3.2.2.15.1. Os chamados classificados com severidade 2 e 3, sem correção definitiva ou solução de contorno nos prazos

acordados, serão automaticamente escalados para o nível de severidade imediatamente superior, ou seja, um chamado de severidade 2, enquadrado nesta situação será automaticamente escalado para severidade 1;

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

3.2.2.16. O tempo de atendimento começa a contar a partir do acionamento inicial realizado junto ao Service Desk da CONTRATANTE.

3.2.2.17. A CONTRATANTE deverá trabalhar, ininterruptamente, na solução dos problemas críticos até que o equipamento contratado esteja novamente operando em regime normal de produção. Caso a solução do problema reportado exija a presença de analista(s) da CONTRATANTE no local de instalação do equipamento, mesmo fora do horário comercial, este(s) deverá(ão) ficar dedicado(s) à resolução do problema até que este esteja resolvido.

3.2.2.18. Os chamados considerados como de Severidade 1 e 2 deverão ser encaminhados diretamente para o segundo nível de atendimento pela CONTRATANTE.

3.2.2.19. O suporte técnico para chamados de Severidade 1 e 2 não pode ser interrompido até o completo restabelecimento de todas as funções do sistema paralisado (indisponível), mesmo que para isso tenha que se estender por períodos noturnos e/ou dias não úteis (sábados, domingos e feriados).

3.2.2.20. A CONTRATANTE deverá garantir os serviços de suporte a customização, parametrização e configuração voltadas à utilização de funcionalidades disponibilizadas na versão corrente do software ou em novas versões lançadas durante a vigência da garantia para todos os produtos feitos disponíveis no ambiente de produção, com prazo máximo de atendimento de 72 horas após a abertura do chamado.

3.2.2.21. Considera-se um problema plenamente solucionado quando os sistemas e serviços forem restabelecidos sem restrições e de forma definitiva, ou seja, quando não se tratar de uma resolução paliativa.

4.1. Das obrigações da CONTRATANTE

4.1.1. Entregar equipamentos NOVOS, SEM USO. Todas as especificações devem estar plenamente disponíveis nos produtos entregues, como por exemplo: novas versões de softwares, dispositivos complementares, chaves e/ou licenças.

4.1.2. Garantir o pleno funcionamento da solução responsabilizando-se por fornecer quaisquer componentes adicionais que sejam necessários ao funcionamento dos equipamentos na configuração especificada, e dentro das condições estabelecidas neste documento, inclusive partes elétricas e mecânicas, ferragens, cabos e conectores. Todos os equipamentos devem ser

entregues e instalados em racks padrão 19", com rodas para movimentação e fechados com portas removíveis, em quantidades suficientes para acomodação de toda a solução.

4.1.3. Promover a instalação e configuração de todos os componentes e placas dos equipamentos, inclusive a conexão física e lógica, que abrange a conexão dos cabos do meio de transmissão de dados disponibilizado pelo SERPRO e dos cabos de conexão aos demais equipamentos já instalados naquele nó de comunicações, deixando-os em

perfeitas condições de uso.

4.1.4. Providenciar a correção em até 5 (cinco) dias corridos, contados a partir da notificação da ocorrência por parte do SERPRO, de quaisquer defeitos de operação, constatados durante a instalação do equipamento. Caso não seja possível a correção, fica a CONTRATANTE obrigada a substituir o dispositivo.

4.1.5. Responsabilizar-se por toda e qualquer despesa, independente da sua natureza, decorrente das instalações supra mencionadas.

4.1.6. Durante a o período de funcionamento do sistema, a CONTRATANTE, deverá prover os serviços de escalonamento dos chamados abertos seguindo a estrutura abaixo:

A) SERVICE DESK

- Abertura da ocorrência (através do contato telefônico, e-mail ou web);
- Coleta das informações referente à ocorrência, possibilitando sua abertura;
- Fornecimento do número da ocorrência ao SERPRO;
- Escalonamento gerencial da ocorrência, conforme tempo de retorno definido com o SERPRO;
- Verificação das respostas de pesquisas de satisfação com o SERPRO.

B) PRIMEIRO NÍVEL

- Acesso à base de dados de Conhecimento (Problemas Característicos), detalhando ações tomadas, descrição do problema, códigos de erro;
- Definição do nível de prioridade junto com o SERPRO;
- Troubleshooting simples;
- Localização da falha e respectivo equipamento;
- Aplicação de soluções documentadas e utilizadas em outros eventos;
- Escalonamento da ocorrência para o segundo nível.

C) SEGUNDO NÍVEL

- Avaliação das ações tomadas pelo primeiro nível de suporte;
- Troubleshooting avançado, técnicas de resolução de problemas e coleta de informações mais detalhadas;
- Suporte às soluções de negócios do SERPRO;
- Desenvolvimento e implementação de soluções provisórias (Workaround);
- Escalonamento do problema para o terceiro nível;
- Acompanhamento, análise e implementação da solução dada pelo terceiro nível.

D) TERCEIRO NÍVEL

- Serviços executados pelo fabricante, por profissionais certificados no produto ofertado. Os chamados abertos com o nível de prioridade "ALTA" deverão sempre ser tratados nesse nível.

4.2. Requerimentos da solução

4.2.1. Requerimentos Gerais:

4.2.1.1. A CONTRATANTE deverá ser responsável por todos itens requeridos para a integração entre os elementos que compõem a solução por ela proposta e os elementos de rede das Operadoras de Telefonia do Serviço Móvel Pessoal (SMP) envolvidas no Projeto Denatran SIMRAV, utilizando a infraestrutura de rede do SERPRO.

4.2.1.2. A CONTRATANTE deverá disponibilizar todos os itens requeridos para a integração entre os elementos que compõem a solução por ela proposta e os elementos de processamento e controle de dados proprietário do SERPRO (ambiente gerado das requisições de aprovisionamento, ativação e desativação).

4.2.2. Dimensionamento e Qualificação

4.2.2.1. A solução deve implementar no mínimo 7.200.000 (sete milhões e duzentos mil)

novos cartões SIM245 cadastrados no sistema.

4.2.2.2. A solução deve ser escalável para 100.000.000 (cem milhões) de cartões SIM245 cadastrados no sistema.

4.2.2.3. A solução ofertada pela CONTRATANTE deve garantir a interoperabilidade dos serviços específicos relativos ao projeto SIMRAV.

4.2.3. Disponibilidade

4.2.3.1. A solução deve gerenciar falhas em componentes individuais de hardware e software, falhas de componentes de alimentação de energia ou outros tipos de desastres inesperados, atendendo aos requerimentos exigidos.

4.2.3.2. A solução deve atender ao índice de 99,999% (noventa e nove vírgula novecientos e noventa e nove por cento) de disponibilidade.

4.2.3.3. A CONTRATANTE deve utilizar uma solução de Alta Disponibilidade que garanta, através de elementos redundantes, a correta continuidade dos processos na presença de falhas.

4.2.3.4. A solução deve dispor de funcionalidade de recuperação automática do sistema em caso de falhas.

4.2.3.5. A solução deve permitir intervenção manual em caso de falhas, quando um dos elementos da mesma não for recuperado automaticamente.

4.2.3.6. A CONTRATANTE deve prover a solução completa de backup & restore (HW e SW).

4.2.4. Segurança

4.2.4.1. A CONTRATANTE deve garantir que todos os elementos da solução sejam instalados com, e apenas com, os serviços requeridos para o perfeito funcionamento da solução.

4.2.4.2. A CONTRATANTE deve ajustar o nível de segurança do Sistema Operacional e das aplicações de todos os elementos da solução proposta, mantendo-os em conformidades com os padrões estabelecidos pelo SERPRO. Todos os corretivos de segurança devem ser instalados.

4.2.4.3. O SERPRO terá o direito de realizar auditorias periódicas na solução, visando certificar o nível de segurança de todos os elementos.

4.2.4.4. A CONTRATANTE deve responsabilizar-se por qualquer intervenção que demande instalação de corretivos de segurança.

4.2.4.5. Todos os elementos providos na solução devem permitir o armazenamento do histórico, em logs, de todas as tentativas de acesso finalizadas em falha ou sucesso.

4.2.4.6. A solução deve implementar comunicação criptografada entre cliente/servidor, bem como, implementar o armazenamento criptografado dos dados críticos do sistema.

4.2.4.7. A solução não deve permitir acesso simultâneo do mesmo usuário no sistema.

4.2.4.8. A solução deve identificar, de forma única, cada sessão de usuário que acesse o sistema.

4.2.4.9. A informação da identificação da sessão deve ser expirada após o primeiro uso, sendo renovada a cada novo acesso do usuário no sistema.

4.2.4.10 A solução deve dispor de configuração de tempo máximo de inatividade da sessão, expirando a mesma após atingir o intervalo configurado.

4.2.4.11. A CONTRATANTE deve dispor de conexão remota ao SERPRO por intermédio de VP; via link internet, estando o mesmo disponível 24x7. Essa comunicação será utilizada para acesso tratamento de incidentes pela equipe de suporte da CONTRATANTE.

4.2.4.12. A CONTRATANTE será responsável por todo o gerenciamento de peças de reposição (Gerenciamento de Sobressalentes), garantindo a rápida disponibilidade de peças sobressalentes e organizando a substituição e recuperação da parte com defeito. A CONTRATANTE deve atender ao prazo de próximo dia útil para reposição do hardware com 95% de precisão.

4.3. Requerimentos Operacionais

4.3.1. Relatórios e Estatísticas

4.3.1.1. A solução deve dispor de histórico de eventos que permitam a investigação de

qualquer tipo de falha.

4.3.1.2. A solução deve implementar as seguintes funcionalidades:

4.3.1.2.1. SNMP MIBs para alarmes de hardware

4.3.1.2.2. SNMP MIBs para alarmes da aplicação

4.3.1.2.3. SNMP traps

4.3.1.2.4. Interface gráfica para gestão dos alarmes

4.3.1.2.5. Interface gráfica para configuração

4.3.2. Suporte e Manutenção

4.3.2.1. A CONTRATANTE deve ofertar serviço de suporte, manutenção e monitoramento por meio de equipes baseadas em território nacional e capazes de comunicar-se em língua portuguesa, a fim de facilitar e agilizar possíveis interações com as equipes do SERPRO.

4.3.2.2. A CONTRATANTE deve testar exaustivamente todos os corretivos antes de aplicá-los na solução.

4.3.2.3. A CONTRATANTE deve prover e instalar todos as ações corretivas sem custos adicionais para o SERPRO.

4.3.2.4. A CONTRATANTE deve dispor de interface web para gestão e abertura de chamados.

4.3.2.5. A CONTRATANTE deve prover claramente o canal para solicitação de ajuste de prioridade de incidentes.

4.3.2.6. A CONTRATANTE deve prover serviço de manutenção preventiva, com entrega de relatórios periódicos indicando possíveis impactos na solução.

4.3.2.7. A CONTRATANTE deve prover canal telefônico com disponibilidade 24x7 para abertura de chamados.

4.3.2.8. A CONTRATANTE deve dispor de canal de relacionamento com o cliente, realizando consultas periódicas ao SERPRO quanto à qualidade da solução e serviços ofertados.

4.3.2.9. A CONTRATANTE deve realizar revisões presenciais na solução semestralmente.

4.3.2.10. A CONTRATANTE deve prover relatórios mensais informando todos os incidentes abertos no período, bem como, o status e ações da resolução dos mesmos.

4.4. Localização do Hardware/Software

4.4.1. As Plataformas de produção, Gerenciamento e Mediação podem ser instaladas preferencialmente nas localidades do SERPRO em Brasília e São Paulo.

4.4.2 Os serviços objeto do presente Contrato serão realizado(s) no(s) estabelecimento(s) do SERPRO, localizado(s) no(s) seguinte(s) endereço(s):

REGIONAL BRASÍLIA/DF

CNPJ: 33.683.111/0002-80

ENDEREÇO: SGAN Av. L2 Norte, Quadra 601 – Módulo “G”

CEP: 70830-900

REGIONAL BELÉM/PA

CNPJ: 33.683.111/0003-60

ENDEREÇO: Av. Perimetral da Ciência, nº 2010

CEP: 66077-530

REGIONAL FORTALEZA/CE

CNPJ: 33.683.111/0004-41

ENDEREÇO: Av. Pontes Vieira, nº 832, São João do Tatuapé

CEP: 60130-240

REGIONAL RECIFE/PE

CNPJ: 33.683.111/0005-22

ENDEREÇO: Av. Parnamirim, nº 295, Bairro Parnamirim

CEP: 52060-000

REGIONAL SALVADOR/BA

CNPJ: 33.683.111/0006-03

ENDEREÇO: Av. Luiz Viana Filho, nº 2355, Bairro Paralela

CEP: 41130-530

REGIONAL BELO HORIZONTE/MG

CNPJ: 33.683.111/0007-94

ENDEREÇO: Av. José Cândido da Silveira, nº 1200, Cidade Nova

CEP: 31170-000

REGIONAL RIO DE JANEIRO/HORTO

CNPJ: 33.683.111/0008-75

ENDEREÇO: Rua Pacheco Leão, nº 1235, Fundos – Jardim Botânico

CEP: 22460-030

REGIONAL SÃO PAULO/SP

CNPJ: 33.683.111/0009-56

ENDEREÇO: R. Olívia Guedes Penteado, nº 941, Capela do Socorro

CEP: 04766-900

REGIONAL CURITIBA/PR

CNPJ: 33.683.111/0010-90

ENDEREÇO: Rua Carlos Pioli, nº 133, Bairro Centro Cívico

CEP: 80520-170

REGIONAL PORTO ALEGRE/RS

CNPJ: 33.683.111/0011-70

ENDEREÇO: Av. Augusto de Carvalho, nº 1133, Bairro Centro

CEP: 90010-390

4.5. Serviço de Operação da plataforma de Telecomunicações para atendimento ao projeto SIMRAV

4.5.1. A CONTRATANTE deverá prover toda a operação do sistema durante todo o período de funcionamento do mesmo.

4.5.2. O serviço de Operação deve ser provido em modelo 8x5 (horário comercial e dias úteis). Com a presença física de no mínimo um técnico no local de instalação da plataforma de gerência.

4.5.3. A CONTRATANTE deverá prover relatório mensal ao SERPRO informando as ações tomadas durante este período.

4.6. Documentação técnica

4.6.1. Os CD/DVD-ROM de instalação e toda a documentação dos produtos deverão ser entregues em até 10 (dez) dias corridos, após a assinatura do contrato pela empresa vencedora.

4.7. O processo será acompanhado pelos empregados relacionados abaixo:

4.7.1. Eduardo Lima, matrícula nº. 1200524-0, telefone: 61-2021-8431, endereço eletrônico: eduardo.lima@serpro.gov.br;

4.7.2. Nauro Luiz Scheufler, matrícula nº. 1201056-1, telefone: 61-2021-8216, endereço eletrônico: nauro.scheufler@serpro.gov.br;

4.7.3. Carlos Henrique Bacellar Bon, matrícula nº. 0106554-8, telefone: 61-2021-8747, endereço eletrônico: carlos.bon@serpro.gov.br;

4.7.4. Paulo Cesar Caldera Brantes, matrícula nº. 1101425-3, telefone: 61-2021-8147, endereço eletrônico: jose-edson.sousa@serpro.gov.br.

5. Responsabilidades

5.1 Do SERPRO

- Hospedagem dos equipamentos da solução, 24 horas por dia, 7 dias na semana, 365 dias por ano, envolvendo a segurança física e lógica;
- Contato operacional continuado e escala de acionamento segundo acordo de nível de serviço (SLA) definido com o cliente;
- Monitorar a conexão da rede;
- Configurar e administrar os ativos de rede;
- Zelar pela segurança física dos equipamentos e por suas condições de funcionamento;
- Resolver quaisquer problemas referentes a conexão com a rede Denatran que independam das operadoras de telecomunicações.

5.1.1. Recursos de infraestrutura disponibilizados pelo SERPRO

5.1.1.1. Ambiente físico (instalações prediais)

Os equipamentos da Contratante serão instalados nos Centros de Dados do SERPRO conforme item 4.4. Estes Centros de Dados possuem alta disponibilidade de energia e refrigeração, além de controle de acesso, detecção e combate a incêndio, monitoração por Circuito Fechado de TV - CFTV e Supervisão e controle dos ativos dessa infraestrutura.

5.1.1.2. Energia elétrica

O sistema de alimentação elétrica do Centro de Dados é redundante, composto por duas linhas independentes, Dual01 e Dual02, de 700kVA cada uma, estabilizadas por no-breaks modulares com autonomia de no mínimo 15 minutos em plena carga e contingenciadas por grupos motor-geradores de 900kVA, um para cada linha. Os equipamentos com fonte dupla (dual) são alimentados por circuitos distintos provenientes de cada uma dessas linhas. Para os equipamentos de fonte singela (single) existe um terceiro circuito, Single, proveniente de uma chave estática que comuta entre os dois circuitos (Dual01 e Dual2) e garante a alimentação elétrica mesmo em caso de pane em uma dessas duas linhas.

5.1.1.3. Sistema de refrigeração

O Sistema de refrigeração é composto por equipamentos de precisão que controlam temperatura e umidade. Em cada compartimentação do ambiente, do Centro de Dados, rede de longa distância ou rede local, existem equipamentos em número suficiente para o dimensionamento da carga térmica e mais um equipamento de reserva (backup) para contingenciar qualquer indisponibilidade que possa existir.

5.1.1.4. Controle de acesso

Existem quatro níveis de acesso no Centro de Dados controlados por um sistema que utiliza cartões de proximidade mesclados com uso de senha ou biometria. O nível 01 é a recepção do Centro de Dados onde se encontra vigilantes em turno de 24 horas treinados para cadastrar os funcionários ou visitantes para acesso as demais áreas. O Acesso para esse nível se dá por uma porta eclusa. O nível 02 são áreas de uso comum e salas de apoio. O acesso é por cartões de proximidade. O nível 03 são áreas de monitoração acessadas por cartões de proximidade e senha pessoal. O nível 04 são os ambientes de

produção, onde estão os ativos de TI. O acesso a essas áreas somente é possível com cartões de proximidade e biometria (impressão digital).

5.1.1.5. Detecção e combate a incêndio

O Ambiente do Centro de Dados é dotado de um sistema misto de detecção de incêndio e combate por gás inerte. É composto por detectores convencionais (velocimétricos) que detectam fumaça e/ou calor e por um sistema de análise laser (VESDA) que detecta o princípio de incêndio antes mesmo da formação de fumaça ou elevação de temperatura. O combate a incêndio é feito por um gás inerte, FE- 25, atóxico e não sufocante, permitindo que pessoas possam estar no ambiente no momento do disparo do gás sem que sofram qualquer consequência. Para evitar que o gás seja acionado acidentalmente, os sistemas convencionais e VESDA foram interligados, sendo assim, o sistema VESDA irá emitir um pré-alarme caso haja um princípio de incêndio, mas só irá disparar o gás quando cruzar com o sinal do detector velocimétrico, quando evidenciar realmente um incêndio. Cabe ressaltar ainda que em todo ambiente existem extintores portáteis que permitem o combate manual no princípio de incêndio.

5.1.1.6. Monitoração por CFTV

O Circuito Fechado de TV (CFTV) do Centro de Dados é composto por 92 câmeras dispostas pelos principais acessos e ambientes do Centro de Dados. A monitoração é feita por vigilantes em turno de 24 horas 7 dias por semana. As imagens são gravadas em média por 2 meses.

5.1.1.7. Supervisão e controle dos ativos de infraestrutura

Além da monitoração do CFTV, os equipamentos como no-break, geradores, climatizadores e sistema de detecção e combate a incêndio, bem como grandezas como tensão, carga (potência) e temperatura, são monitorados continuamente.

5.1.2 Níveis de Serviço ofertados pelo SERPRO

Energia e Refrigeração	99,6%	
Conjunto	% Disponibilidade	Tipo
Conjunto Energia Novo CPD	100,0%	P
CEB	99,9%	
Grupo Gerador (GMG) 1	99,9%	
Grupo Gerador (GMG) 2	99,9%	
Conjunto Quadro de Transferência CEB / GMG Novo CPD	99,8%	S
Disjuntor 1	99,9%	
Disjuntor 2	99,9%	
Conjunto No Break Novo CPD	100,0%	P

NB 1	99,9%	
NB 2	99,9%	
Conjunto Ar Condicionado Novo CPD	100,0%	P
AC 1	99,8%	
AC 2	99,8%	
Conjunto Energia Sala Cofre	100,0%	P
CEB	99,9%	
Grupo Gerador (GMG) 1	99,9%	
Grupo Gerador (GMG) 2	99,9%	
Conjunto Quadro de Transferência CEB / GMG Sala Cofre	99,8%	S
Disjuntor 1	99,9%	
Disjuntor 2	99,9%	
Conjunto No Break Sala Cofre	100,0%	P
NB 1	99,9%	
NB 2	99,9%	
Conjunto Ar Condicionado Sala Cofre	100,0%	P
AC 1	99,8%	
AC 2	99,8%	

P – Recurso em Paralelo

S – Recurso em Série

5.2. Do CONTRATANTE

- Indicar o contato administrativo e o contato técnico responsáveis pelos equipamentos e sistemas hospedados no SERPRO, com respectivos telefones fixos e celulares, e-mails e endereços;
- Atender prontamente aos comunicados, questionamentos e chamados do SERPRO incluindo chamados fora do horário de expediente normal, de 8h às 18h, finais de semana e feriados;

- Administrar o sistema operacional dos equipamentos e os softwares neles instalados;
- Fornecer todos os hardwares e softwares necessários e respectivas licenças;
- Responsabilizar-se por quaisquer problemas técnicos ou operacionais, de hardware ou software, nos equipamentos;

6. Procedimento para revisão/atualização das condições técnicas para credenciamento

6.1 O SERPRO poderá, a qualquer tempo, e a seu critério, rever e/ou atualizar os procedimentos operacionais, o regulamento de utilização do seu ambiente de hospedagem e/ou os presentes requisitos de forma a aperfeiçoar a prestação do serviço.

6.2 O SERPRO informará por intermédio de e-mail enviado ao responsável administrativo e ao responsável técnico da CONTRATANTE sobre qualquer alteração nos referidos documentos, com 15 (quinze) dias de antecedência.

7. Considerações gerais

7.1. Alimentação Elétrica

O SERPRO disponibilizará alimentação elétrica em 110 ou 220 Volts, monofásica ou trifásica, caso sejam necessárias fontes de alimentação ou retificadores para alimentação em corrente contínua (DC), estes deverão ser fornecidos pela CONTRATANTE e estes serão considerados para efeito do cálculo do preço do serviço conforme especificado no item 1.5.

7.2. Sanções

7.2.1 O não cumprimento de quaisquer cláusulas bem como o dos níveis de serviço implicará na aplicação de multas.

7.2.2 O não atendimento as cláusulas contratuais implicará no descredenciamento da CONTRATANTE.

7.3. Prazo para disponibilização da Infraestrutura pela CONTRATANTE

O prazo para disponibilização da infraestrutura pela CONTRATANTE será de até 60 (sessenta dias) após a assinatura do contrato.

7.4. Remuneração da CONTRATANTE

A Remuneração da CONTRATANTE será efetuada de acordo com o previsto na Portaria 902/2011 do Denatran e será de responsabilidade da CONTRATANTE mediante relacionamento comercial que mantenha com os fabricantes de módulos antifurto e empresas de Tecnologia de Informação Veicular – TIVs, em para o registro do SIMRAV-ID gerado pelo SERPRO e Ativação/Desativação dos serviços e rastreamento e bloqueio dos veículos.

ANEXO II – PROPOSTA DE CONTRATAÇÃO DE SERVIÇOS

CREDENCIAMENTO SUPGA/GABSA/GACOM Nº 019/2012	PROCESSO Nº 19863.000002/2012-19	SEDE
---	---	-------------

Ao

SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS (SERPRO)

A presente proposta é baseada nas especificações, condições e prazos estabelecidos no **Edital de Credenciamento nº 019/2012**.

Vimos, por meio desta, solicitar o credenciamento para ofertar insumo(s) para os serviços do Sistema Denatran de Telecomunicações, estes de responsabilidade dessa Empresa Pública, mediante disponibilidade de infraestrutura por meio de contrato de prestação de serviço de *Colocation* e *Hosting* ofertado pelo SERPRO.

Declaramos que esta proposta tem validade pelo prazo mínimo de 60 (sessenta) dias, contados da data de sua assinatura, e que atendemos e concordamos com todas as condições estabelecidas no **Edital de Credenciamento nº 019/2012** e respectivos Anexos.

O detalhamento da solução ofertada consta Anexo a esta proposta.

(ANEXAR DOCUMENTAÇÃO TÉCNICA)

DADOS DA EMPRESA: *(Informar dados da Matriz e/ou Filial, constando os dados para o faturamento decorrente do contrato a ser firmado)*

Nome: _____
 Endereço: _____ CEP: _____
 Telefone: _____ e-mail: _____
 Fac-Símile: _____ CNPJ: _____

Dados da Autoridade Competente que irá assinar o contrato:

Nome:

Cargo:

Documento de Identidade: RG nº Órgão Expedidor: UF:

CPF nº

Residente e domiciliado em:

(local e data)

(assinatura, devidamente identificada)

ANEXO III- MINUTA DE CONTRATO		
CREDENCIAMENTO SUPGA/GABSA/GACOM Nº 019/2012	PROCESSO Nº 19863.000002/2012-19	SEDE

**CONTRATO DE PRESTAÇÃO DE SERVIÇO
ESPECIALIZADO DE PROCESSAMENTO DE DADOS QUE
ENTRE SI CELEBRAM A XXXXXXXXXXXX, E O SERVIÇO
FEDERAL DE PROCESSAMENTO DE DADOS (SERPRO)
NA FORMA ABAIXO:**

A XXXXXXXXXXXXXXXXXXXX, adiante denominada CONTRATANTE, inscrita no CNPJ/MF sob o nº xx.xxx.xxx/xxxx-xx com sede no endereço x, representada por x, portador da carteira de identidade nº xxxxxxxx, expedida pelo xxxxx e do CPF/MF nº xxx.xxx.xxx-xx, e do outro lado, o SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS (SERPRO), adiante denominado CONTRATADO, Empresa Pública criada pela Lei Federal nº 5615/70, inscrita no CNPJ/MF sob o nº 33.683.111/0001-07, estabelecida na cidade de Brasília-DF, no Setor de Grandes Áreas Norte, Quadra 601, Módulo V, neste ato representada pelo SR. XXXXXXXXXXXXXXXXXXXX, brasileiro, portador da Carteira de Identidade nº xxxxxxxxx, emitida pelo xxxxxxxx, CPF, xxx.xxx.xxx-xx, com amparo no art. 25, *caput*, da Lei n. 8.666/93, o qual ensejou o presente credenciamento, e fundamento no Art. 594 do Código Civil e demais legislações aplicáveis à matéria, resolvem celebrar o presente contrato regido pelas seguintes cláusulas e condições:

CLÁUSULA PRIMEIRA – DO OBJETO

O presente contrato tem por objeto a prestação de serviço de *Colocation e Hosting* ofertado pelo CONTRATADO nos termos e condições descritas nesse contrato, sendo constituído de hospedagem de Hardware, Software e Serviços para implementar o Sistema Denatran de Telecomunicações (subsistema do SIMRAV), consoante Edital de Convocação Para Credenciamento SUPGA/GABSA/GACOM nº 019/2012, e seus Anexos e Proposta de Contratação de Serviços nº _____, de ____/____/2012, constantes do Processo **19863.000002/2012-19**, às folhas __ à __, respectivamente, parte integrante deste contrato independentemente de transcrição.

1.1. DETALHAMENTO DOS SERVIÇOS

O *Serviço* faculta ao CONTRATANTE a disponibilidade de hospedagem, necessária à instalação de servidores/equipamentos do CONTRATANTE e compreende, além de espaço físico, o fornecimento de energia elétrica, de infraestrutura para conectividade com a internet, climatização do ambiente, a rede lógica, o serviço de monitoramento ininterrupto desta infraestrutura e recursos de segurança física de acesso, além da operação e gerenciamento desse conjunto de soluções para atingimento dos fins a que a solução se destina, no relacionamento entre o CONTRATANTE e seus clientes (usuário final).

1.2. ELEMENTOS QUE COMPÕEM O SERVIÇO

- Edificação especializada para a solução;
- Energia elétrica estabilizada garantida por *nobreaks*;
- Grupos geradores garantindo a qualidade e a continuidade do fornecimento de energia elétrica independente do fornecedor local;
- Sistema de climatização especializado para equipamentos de processamento de dados;
- Sistema de controle de segurança e acesso às instalações, e de climatização;
- Circuito Fechado de Televisão (CFTV);
- Infraestrutura necessária à conectividade do cliente ao ambiente DENATRAN SIMRAV;
- Equipe técnica especializada de atendimento, suporte e operação.

CLÁUSULA SEGUNDA – DA DESCRIÇÃO DOS SERVIÇOS

A arquitetura completa da solução a ser hospedada é composta por:

2.1. Plataforma HLR (Home Location Register) – No mínimo 01 (um) HLRs em alta disponibilidade

2.1.1. A plataforma em referência deve atuar como banco de dados central da rede GSM/3G que contém os detalhes de cada perfil de cliente autorizado a utilizar os serviços da plataforma.

2.1.2. A plataforma em referência deve também possuir a função de autenticar todo SIM/USIM card que fizer a tentativa de conexão ao core da rede GSM/3G.

2.1.3. A plataforma em referência deverá possuir redundância de processamento, redundância de placas controladoras e redundância de fontes de alimentação para permitir que o tráfego possa fluir mesmo em casos de falha, garantindo assim o nível de disponibilidade Carrier Class de 99,999%.

2.1.4. A plataforma em referência deverá ter capacidade para 7.200.000 usuários e ser escalável para 100.000.000 de usuários.

2.1.5. A plataforma em referência deverá estar preparada para gerenciar as seguintes ações:

2.1.5.1. Validação;

2.1.5.2. Perfil;

2.1.5.3. Localização;

2.1.5.4. Estado;

2.1.6. A plataforma em referência deverá implementar as interfaces padrão através de implemento da sinalização MAP, de acordo com a especificação TS 29.002.

2.1.7. A plataforma em referência deverá possuir mecanismos de controle automático de sobrecarga dos sistemas de processamento, armazenamento e sinalização.

2.1.8. A plataforma em referência deverá possuir contingenciamento transparente em caso de falhas.

2.1.9. Funcionalidades

2.1.9.1. Serviços Básicos:

2.1.9.1.1. Telefonia;

2.1.9.1.2. Short message MT/PP;

2.1.9.1.3. Short message MO/PP;

2.1.9.1.4. Bloqueios Determinados pelo Operador;

2.1.9.1.5. Barring of Outgoing Calls (ODB-BAOC);

2.1.9.1.6. Barring of Outgoing International Calls (ODB-BOIC);

2.1.9.1.7. Barring of All Incoming Calls (ODB-BAIC);

2.1.9.1.8. Barring of Registration of Forwarded-to Number (ODBRFCF).

2.1.9.2. Serviços de Mobilidade:

2.1.9.2.1. Location Update;

2.1.9.2.2. Location Cancellation;

2.1.9.2.3. MS Purge;

2.1.9.2.4. Authentication Information Provision;

- 2.1.9.2.5. Subscriber Data Insertion;
- 2.1.9.2.6. Subscriber Data Deletion;
- 2.1.9.2.7. HLR Fault Recovery;
- 2.1.9.2.8. VLR Fault Recovery;
- 2.1.9.2.9. Send Routing Information;
- 2.1.9.2.10. Provide Roaming Number.
- 2.1.9.2.11. Gerenciamento da Base de Dados de Usuários;
- 2.1.9.2.12. Subscriber Definition;
- 2.1.9.2.13. Subscriber Deletion;
- 2.1.9.2.14. IMSI Change;
- 2.1.9.2.15. MSISDN Change;
- 2.1.9.2.16. Subscriber Number Query;
- 2.1.9.2.17. Dynamic Data Query;
- 2.1.9.2.18. Operator Authority Management;
- 2.1.9.2.19. Dynamic Subscriber Data Managent;
- 2.1.9.2.20. Service Template Setting;
- 2.1.9.2.21. Batch Operation;
- 2.1.9.2.22. Operation Log Management;
- 2.1.9.2.23. Subscriber Statistics;
- 2.1.9.3. Protocolo, Interfaces e padrões:
- 2.1.9.3.1. MAP Protocols – MAP Phase 2. MAP Phase 2 e MAP Phase 2+;
- 2.1.9.3.2. BOSS Interface;
- 2.1.9.3.3. Application/Data Layer Interface;
- 2.1.9.3.4. M3UA / SIGTRAN;
- 2.1.9.3.5. IETF RFC 4666, IETF RFC 4166, IETF RFC 4165, ITU-T Q.701-Q709, ITU-T Q.711-Q719, ITU-T Q.770-Q779, MAP 1, 2 e 3 – 3GPP 23.002 e 29.002, GSMA IR22, IR3 e IR 35;
- 2.1.9.3.6. 3GPP, 3GPP TS 29.002.
- 2.1.9.4. Funções de Operação e Manutenção:
- 2.1.9.4.1. Security Management;
- 2.1.9.4.2. Performance Management;
- 2.1.9.4.3. Fault Management;
- 2.1.9.4.4. Configuration Management;
- 2.1.9.4.5. Equipment Management;
- 2.1.9.4.6. Equipment Archive Management.
- 2.1.9.5. Funções de Proteção e Confiabilidade:
- 2.1.9.5.1. Redundancy and Backup Design;
- 2.1.9.5.2. Power Reliability;
- 2.1.9.5.3. Distributed Boards;
- 2.1.9.5.4. Dual-Plane Communications;
- 2.1.9.5.5. Automatic Fault Detection and Self-Healing;
- 2.1.9.5.6. Automatic/Manual Switchover;
- 2.1.9.5.7. Automatic Multi-Level Backup and Recovery of Subscriber Data;
- 2.1.9.5.8. Flow Control;
- 2.1.9.5.9. Distributed Storage of Subscriber Data;
- 2.1.9.5.10. Automatic Load Sharing Among Modules;
- 2.1.9.6. Serviços de Dados:
- 2.1.9.6.1. GPRS Services.
- 2.1.9.7. Redundância:
- 2.1.9.7.1. N+1 Compatibility Redundancy;
- 2.1.9.7.2. Capacidade de implementar HLR lógico com base de dados centralizada.
- 2.1.9.8. Políticas de Processos:
- 2.1.9.8.1. MTP Policing;
- 2.1.9.8.2. SCCP Policing;

- 2.1.9.8.3. MAP Policing.
- 2.1.9.9. Funcionalidades de Autenticação:
 - 2.1.9.9.1. Registration, Call attempt;
 - 2.1.9.9.2. Call Delivery;
 - 2.1.9.9.3. Location Update;
 - 2.1.9.9.4. Supplementary service procedure;
 - 2.1.9.9.5. Short Message Service (SMS) transfer;
 - 2.1.9.9.6. Location services;
 - 2.1.9.9.7. Algoritmos GSM A3/A8, conforme especificação 3GPP;
 - 2.1.9.9.8. COMP128-Versão 1, conforme especificação 3GPP;
 - 2.1.9.9.9. COMP128-Versão 2, conforme especificação 3GPP;
 - 2.1.9.9.10. COMP128-Versão 3, conforme especificação 3GPP;
 - 2.1.9.9.11. Millenage, conforme especificação 3GPP;
 - 2.1.9.9.12. Algoritmo GSM A4 em sua última versão;
 - 2.1.9.9.13. Autenticação Basic GSM Service;
 - 2.1.9.9.14. Autenticação Alternative A4 algorithm;
 - 2.1.9.9.15. Autenticação Basic Platform Feature Package;
 - 2.1.9.9.16. Autenticação Basic WCDMA Service;
 - 2.1.9.9.17. A plataforma deve implementar todos os algoritmos de autenticação listados de forma simultânea.
- 2.1.9.10. Funcionalidades de sinalização:
 - 2.1.9.10.1. Permitir a redistribuição de carga automática nos links que estão disponíveis no linkset;
 - 2.1.9.10.2. Suporte a link de sinalização de alta velocidade 2Mbit conforme ITU Q703;
 - 2.1.9.10.3. Implementar Load share em nível SCCP (combinação de routeset) e MTP;
 - 2.1.9.10.4. Implementação de load share para todos destinos SCCP (Global Title) ou MTP3 (Point codes);
 - 2.1.9.10.5. Implementar Load share entre múltiplos STP usando GTT Alias point code para endereçamento do STP.
- 2.1.9.11. Implementar grupo SIGTRAN:
 - 2.1.9.11.1. SCTP de acordo com RFC 2960;
 - 2.1.9.11.2. M3UA de acordo com RFC 3332;
 - 2.1.9.11.3. Implementar Multi-signaling-point (Multi-SP);
 - 2.1.9.11.4. Implementar SCTP multi-homing;
- 2.1.10. A plataforma proposta deverá ser implementada com o algoritmo DES para as chaves de encriptação.
- 2.1.11. A plataforma deve implementar serviços CAMEL 3, fornecendo:
 - 2.1.11.1. O-CSI (Originating CAMEL Subscription Information);
 - 2.1.11.2. T-CSI (Terminating CAMEL Subscription Information);
 - 2.1.11.3. SS-CSI (Supplementary Service Invocation Notification CAMEL Subscription Information);
 - 2.1.11.4. SMS-CSI (Short Message Service CAMEL Subscription Information);
 - 2.1.11.5. D - CSI (Dialed Service CAMEL Subscription Information);
 - 2.1.11.6. M - CSI (Mobility Management event CAMEL Subscription Information);
 - 2.1.11.7. VT - CSI (VMSC Terminating CAMEL Subscription Information).
- 2.1.12. A plataforma deve implementar ATI (any time interrogation) para operações iniciadas por um SCP (service control point). Através dessa operação deve ser possível obter o status e localização de um sim card;
- 2.1.13. A plataforma deve suportar ARD (Access Restriction Data) para controle do comportamento dos simcards 2G e/ou 3G;
- 2.1.14. A plataforma deve implementar a configuração de HLR lógico no mesmo elemento físico de forma a garantir operações de áreas numéricas diferentes;
- 2.1.15. A plataforma deve suportar no mínimo 128 áreas de numeração diferentes;
- 2.1.16. A plataforma proposta deverá implementar proteções de todos os dados sensíveis

e contra manipulação de algoritmos não-autorizados, manipulação e mau uso dos métodos de criptografia e segurança física;

2.1.17. A plataforma proposta deverá associar apenas uma chave para cada usuário armazenado;

2.1.18. A plataforma proposta deverá garantir que a chave de cada usuário será criptografada apenas por intermédio do uso de algoritmos padrão;

2.1.19. A plataforma proposta deverá garantir que cada chave associada a cada usuário seja descriptografada apenas durante o tempo de geração do vetor de autenticação e que os valores gerados serão destruídos em seguida.

2.1.20. Arquitetura e Requisitos do Hardware:

2.1.20.1. A plataforma deve ser concebida de tal forma que as falhas individuais no software não devem causar uma falha no sistema ou serviço de interrupção ou degradação do desempenho do sistema. Sob condições de falha, o sistema deve poder dispor continuidade e deve seguir funcionando normalmente sem grau reduzido de serviço ou com prejuízo para a qualidade do mesmo;

2.1.20.2. A arquitetura deve obedecer ao conceito de ngHLR para garantir a confiabilidade e nível de serviço da plataforma;

2.1.20.3. A arquitetura deve ser composta pelos elementos lógicos de processamento e banco de dados – Front End (FE) e Back End (BE).

2.1.20.4. O Back End BE deve implementar as seguintes funções:

2.1.20.4.1. Adição, deleção, atualização e busca do banco de dados de acordo com o serviço requisitado pelo bloco funcional FE;

2.1.20.4.2. O Front end FE deve implementar as funções de processamento de sinalização e mensagens. Não deve armazenar nenhum dado de simcard;

2.1.20.4.3. Todo o hardware deve possuir o seu backup em site local (arquitetura 1+1);

2.1.20.4.4. A plataforma deve ser concebida de tal forma que permita a replicação da mesma em locais geograficamente separados.

2.1.20.5. Para confiabilidade dos dados, a plataforma deve implementar:

2.1.20.5.1. backup de dados entre placas diferentes;

2.1.20.5.2. backup de dados para disco rígido local;

2.1.20.5.3. backup de dados para DiskArray externo à solução da CONTRATANTE;

2.1.20.5.4. Capacidade de efetuar backup para sistema de armazenamento externo à solução fornecida;

2.1.20.5.5. Deve possuir arquitetura modular com design distribuído podendo ser expandido com adição de frames e racks cascadeados;

2.1.20.5.6. A plataforma em referência deverá ser hot-swap para todas as placas;

2.1.20.5.7. A plataforma deverá permitir ampliação de hardware sem paralisação do hardware já instalado;

2.1.21. A plataforma em referência deve permitir recuperação total e 100% automática (sem necessidade de nenhuma intervenção humana), depois de falha e recuperação de energia.

2.1.22. Arquitetura e Requisitos do Software

2.1.22.1. A plataforma deve permitir upgrade das licenças software sem perda de conectividade, de registros dos usuários, de sessões ativas, etc;

2.1.22.2. A plataforma deve ser capaz de aplicar Hot Patches sem a paralisação do serviço de forma a atender à disponibilidade mínima exigida;

2.1.22.3. A solução apresentada pela CONTRATANTE deverá considerar correções de Software com o sistema em operação (soft software upgrade).

2.1.23. Interface de provisionamento

2.1.23.1. As interfaces de provisionamento devem ser redundantes para garantir a ausência de pontos únicos de falha;

2.1.23.2. Implementar o provisionamento em batch em arquivos ASCII enviados via FTP;

2.1.23.4. Suportar adição/deleção a uma taxa de 1000 comandos/seg .

2.1.24. Características Construtivas

2.1.24.1. A plataforma em referência deverá ser aderente aos requisitos abaixo com relação ao seu Hardware:

- Taxa de reparo do sistema < 0.3%
- Disponibilidade > 99.999%
- Taxa de detecção de falhas > 95%
- Mean time to repair (MTTR) < 1 h
- Tempo de interrupção do serviço para cada upgrade ou expansão < 30 segundos
- Média de interrupção do serviço em um ano < 5 minutos
- Duração entre a inicialização do sistema e pronto para uso < 10 minutos
- Taxa de sucesso do switchover entre os componentes redundantes > 95%

2.1.24.1.1. Com relação a interferências eletromagnéticas – EMC, a plataforma deve ser aderente aos padrões abaixo listados:

2.1.24.1.1.1. EN 55022 classe A

2.1.24.1.1.2. CISPR 22 classe A

2.1.24.1.1.3. ETSI EN 300 386

2.1.24.1.1.4. GB9254 classe A

2.1.24.1.2. Com relação aos requisitos do ambiente de instalação, a plataforma deve ser aderente aos padrões abaixo listados:

2.1.24.1.2.1. GB 4798

2.1.24.1.2.2. ETS 300019

2.1.24.1.2.3. IEC 60721

2.1.25. Operação e Manutenção

2.1.25.1. O CONTRATANTE deve fornecer Operação e Manutenção do sistema para HLR/AUC com interface homem-máquina personalizado para oferecer gerenciamento de falhas, gerenciamento de configuração, gerenciamento de alarmes, medição de desempenho e gerenciamento de segurança.

2.1.25.1.1. **Gerenciamento da Configuração**

2.1.25.1.1.1. O HLR proposto deve implementar os seguintes recursos de gerenciamento de dados de configuração:

2.1.25.1.1.1.1. Controle de autorização por usuário;

2.1.25.1.1.1.2. Atribuição de tarefas razoáveis para fins de operações flexíveis;

2.1.25.1.1.1.3. Manutenção local, remota e centralizada.

2.1.25.1.1.2. O HLR proposto deve implementar as seguintes ações de gerenciamento de dados dos simcards:

2.1.25.1.1.2.1. Funções além de adição, modificação e exclusão;

2.1.25.1.1.2.2. Armazenamento de logs operacionais de todas ações executadas.

2.1.25.2. **Gerenciamento de Desempenho**

2.1.25.2.1. A plataforma proposta deve implementar as seguintes funções de medição de desempenho:

2.1.25.2.1.1. Relatórios de medição personalizados e entidade de medição personalizados;

2.1.25.2.1.2. Três segmentos de medição de tempo por dia com o dia de medida designada por mês ou por semana, e ciclo

de medição de 5 minutos a 24 horas;

2.1.25.2.1.3. As chamadas de tráfego podem ser digitalizadas e medidas com base em tempo real;

2.1.25.2.1.4. Padrão e formato de saída abertos, com função de impressão disponível;

2.1.25.2.1.5. Instrumentos de medição de desempenho dedicados para análise de taxa de conclusão de chamada, congestionamentos, quedas de chamadas, handoffs e densidade de tráfego.

2.1.25.3. Gerenciamento de Alarmes e Manutenção

2.1.25.3.1. A plataforma em referência deve implementar as seguintes funcionalidades de gerenciamento de alarmes:

2.1.25.3.1.1. Coletar informações de alarme na hipótese de acionamento;

2.1.25.3.1.2. Classificar os alarmes de acordo com seu nível de criticidade;

2.1.25.3.1.3. Mostrar descrição detalhada do alarme, assim como, sugestões para resolução do mesmo;

2.1.25.3.1.4. Monitoramento do status de links, timeslots e placas de uma unidade funcional;

2.1.25.3.1.5. **Manutenção remota da plataforma**

2.1.25.3.1.6. Fornecer interface de teste para conexão sem afetar o funcionamento normal da plataforma;

2.1.25.3.1.7. Possuir diagnóstico automático de falhas de hardware e software;

2.1.25.3.1.8. Fornecer interface para informações de log detalhados com ajuda online;

2.1.25.3.1.9. Possuir filtros para aplicar nos logs facilitando debug de possíveis problemas.

2.1.25.4. Gerenciamento de Segurança

2.1.25.4.1. A plataforma deve implementar gerenciamento de autoridade e gerenciamento de logs.

2.1.25.4.1.1. **Gerenciamento de autoridade:**

2.1.25.4.1.1.1. A autoridade de operadores e estações deve estar submetida a regras de hierarquia;

2.1.25.4.1.1.2. A execução de qualquer comando MMI deve estar condicionada à autoridade do operador ou da estação de trabalho. O comando não pode ser executado caso não esteja sob alguma dessas condições.

2.1.25.4.1.2. **Gerenciamento de logs:**

2.1.25.4.1.2.1. Deve ser possível habilitar o log de todas as operações MML;

2.1.25.4.1.2.2. Deve ser possível realizar buscas online e offline aos logs referentes a realização de qualquer comando MML;

2.1.26. Dimensionamento do HLR

Name	3G(R4/R5)
Basic Parameters	
Number of SMS/BH/SUB(MO)	0,2
Number of SMS/BH/SUB(MT)	0,3
Location update/BH/SUB	1,5
Location update/BH/SUB(To HLR)	0,2
Send authentication to AuC/BH/SUB	0,8
IMSI Detach (BH/SUB)	0,15
SendRoutingInfo to HLR/BH/SUB	0,6
GPRS Location update/BH/SUB	0,25
InsertSubscriberData/BH/SUB	0,1
DeleteSubscriberData/BH/SUB	0,1
CancelLocation/BH/SUB	0,7
Send authentication to AuC/BH/SUB(PS)	0,6
Proportion of Direct delivery SMS (%)	0,6
SendRoutingInfoForSMS to HLR/BH/SUB	0,7
note: BH=BusyHour, SUB=Subscriber, Auc=Auth center	

2.2. SGW (Signaling Gateway) No mínimo 01 (um) Gateways em alta disponibilidade

2.2.1. Requisitos do Gateway de Sinalização

- 2.2.1.1. O SGW deve suportar Number transform;
- 2.2.1.2. O SGW deve suportar Terminal Information Collector (TIC);
- 2.2.1.3. O SGW deve suportar Enhanced Routing Function;
- 2.2.1.4. O SGW deve suportar IN voice call Bypass;
- 2.2.1.5. O SGW deve suportar International roaming and SIMM with IN;
- 2.2.1.6. O SGW deve suportar Preferred network;
- 2.2.1.7. O SGW deve suportar CDR function;
- 2.2.1.8. O SGW deve suportar NTP function;
- 2.2.1.9. O SGW deve possuir processamento dos links narrowband e broadband na mesma placa de processamento;
- 2.2.1.10. O SGW deve possuir disponibilidade de 99,999%;
- 2.2.1.11. O SGW deve obrigatoriamente ser carrier-class;
- 2.2.1.12. O SGW deve ter capacidade mínima de 2500 consultas por segundo à base de dados.

2.2.2. O SGW deverá possuir as seguintes funcionalidades para o MTP:

- 2.2.2.1. MTP loadsharing;
- 2.2.2.2. MTP estatísticas;
- 2.2.2.3. MTP estatísticas de tráfego;
- 2.2.2.4. MTP Gerenciamento da Rede e Restart.
- 2.2.3. O SGW ofertado deverá implementar SS7 Signalling Connection Control Part (SCCP, Global Title routing);

2.2.4. O sistema proposto deverá permitir as seguintes funcionalidades para o SCCP:

- 2.2.4.1. SCCP Loadsharing:
 - 2.2.4.1.1. Implementar SCCP LoadSharing ou Active / Standby entre 16 DPCs/DPC SSNs;
 - 2.2.4.1.2. Utilização de múltiplos PC dentro da mesma rede SS7;
 - 2.2.4.1.3. Gerenciamento do subsistema SCCP;
 - 2.2.4.1.5. Serviços Orientados e Não-Orientados a Conexão SCCP over IP, SUA;
 - 2.2.4.1.6. Implementar as recomendações ITU-T Q.711 a Q.714;
 - 2.2.4.1.7. Offload de mensagens SMS sobre rede IP (SIGTRAN) ;
 - 2.2.4.1.8. O SGW ofertado deverá implementar SS7 Transaction Capabilities Application Part (TCAP);
 - 2.2.4.1.9. O SGW deverá implementar a funcionalidade SS7 TCAP, requerido para implementar os protocolos MAP, INAP e CAP - Phase1,2,3;
 - 2.2.4.1.10. Implementar as Recomendações do ITU – T – Q.771- Q.774;
- 2.2.5. O SGW ofertado deverá implementar as funções adicionais de Sinalização SS7.

2.2.5.1. Funcionalidades Adicionais:

- 2.2.5.1.1. Múltiplas Redes SS7 - Implementar a funcionalidade de Múltiplas Redes SS7, onde uma Rede SS7 pode ser subdividida em vários nós lógicos ou redes virtuais, possibilitando a associação de um OPC exclusivo para cada Rede Virtual;
- 2.2.5.1.2. Múltiplos Point Codes - Permitir a criação e administração de Múltiplos OPC's para uma mesma rede;
- 2.2.5.1.3. High-speed Signalling Links - Permitir a implementação de Links de Sinalização de Alta Velocidade, conforme **ITU Q.703, Anexo A**;
- 2.2.5.1.4. SS7 Screening - Implementar a função de Screening para as mensagens SS7 relativas aos protocolos MTP, SCCP e MAP. A função de Screening SS7 permite ao operador examinar detalhadamente as mensagens SS7 que circulam pela sua rede. Com base neste exame, o SGW pode ser configurado para rejeitar ou permitir o tráfego entre determinadas Redes, e também, para alterar o destino ou campos da mensagem, conforme sua conveniência e

necessidade.

2.2.6. Métodos para MTP Screening:

2.2.6.1. OPC/DPC/SIO screening;

2.2.6.2. Incoming linkset / DPC screening;

2.2.6.3. Message length (LI) screening;

2.2.6.4. Network indicator (NI) screening;

2.2.6.5. MTP Gateway Screening ("Bellcore" Screening);

2.2.6.6. SCCP and User context Screening, tal como Screening baseado no tipo de mensagem;

2.2.6.7. Subsystem screening;

2.2.6.8. Protocol-class screening.

2.2.7. **Monitoração Flexível** - O SGW deverá permitir a monitoração do tráfego de mensagens SS7, através da configuração de parâmetros e critérios que permitam a obtenção de informações específicas de determinado tipo de tráfego.

2.2.7.1. Os dados a serem analisados são armazenados na memória do sistema e em seguida são aplicados filtros para obtenção de informações relativas ao tipo de tráfego observado. Caso o SGW fornecido não possua essas funções, poderá ser adicionado dispositivo externo como probe ou similar.

2.2.8. O SGW deverá suportar os seguintes tipos de interfaces externas:

2.2.8.1. Circuit interface: E1 interface (2.048 Mbit/s), T1 interface (1.544 Mbit/s) suportar, não precisa ser fornecido nesta aquisição;

2.2.8.2. Clock interface: 2.084 Mbit/s, 2.048 MHz and 8 kHz clock signal interfaces;

2.2.8.3. FE interface: 10BaseT/Fx and 100BaseT/Fx;

2.2.8.4. Standard NM interface: SNMP interface;

2.2.8.4.1. Other: supporting MML;

2.2.8.5. SS7 over TDM with narrowband signalling links with 56 (PCM24) and 64 (PCM30) kbit/s (G.703/MTP1/MTP2/MTP3);

2.2.8.6. SS7 over TDM with High-speed Signalling Links with 1.5 / 2 Mbit/s G.703 Annex A;

2.2.8.7. SS7 over IP with 10/100 bT/Ethernet/IP/SCTP/M3UA acc. to IETF RFC 4666;

2.2.8.8. SS7 over IP with 10/100 bT/Ethernet/IP/SCTP/M2PA acc. to IETF RFC 4165;

2.2.8.9. SS7 over IP with 10/100 bT/Ethernet/IP/SCTP/M3UA acc. to IETF RFC 2960 & 4666.

2.2.9. O SGW deve implementar as capacidades mínimas abaixo:

Item	Valor
Número de links LSL (64-kbit/s)	>384
Número de links HSL (2-Mbit/s)	>24
Capacidade de GT	>18000
Número de DPCs suportados	>900

2.2.9.1. O SGW deve implementar as performances mínimas abaixo:

Item	Index
Tráfego sobre links de 64-kbit/s	>0.80Erl
Tráfego sobre links de 2-Mbit/s	>0.80Erl
Tráfego sobre links de 1.544-Mbit/s	>0.80Erl
Atraso de transferência de mensagens	<15ms
Capacidade de processamento das mensagens	>60480 MSU/s
Capacidade GTT	>60480 GTT/s

2.2.10. Gerenciamento do SGW

2.2.10.1. Gerência e Manutenção:

2.2.10.1.1. Status da Rede através de Geração de Relatórios;

2.2.10.1.2. Automation of everyday tasks;

2.2.10.1.3. Session Control;

2.2.10.1.4. Alarm browser for QoS Alarms (SSNC);

2.2.10.1.5. Alarmes de Performance Real Time through Threshold Supervision and forwarding to SNMP server;

2.2.10.1.6. Alarm Threshold Administration;

2.2.10.1.7 Monitoração de Alarme da Rede SS7;

2.2.10.1.8. Logging and browsing de alarmes de performance;

2.2.10.1.9. Flexibilidade e facilidade de geração de relatórios para auxiliar nos processos de investigação de falhas na rede de sinalização;

2.2.10.1.10. Implementar comandos MML e interface GUI;

2.2.10.1.11. Implementar ferramenta que permita realizar o trace de sinalização, conforme descrito a seguir:

2.2.10.1.11.1. Armazenamento do histórico dos traces. Caso o SGW fornecido não execute essa função, será permitido uso de dispositivo externo como probe ou equivalente;

2.2.10.1.11.2. Capacidade de executar o trace em links parciais, linksets ou todos os links. Caso o SGW fornecido não execute essa função, será permitido uso de dispositivo externo como probe ou equivalente;

2.2.11. Backup das bases de dados provisionadas no SGW;

2.2.11.1. Mecanismos para verificação de integridade e correção das bases de dados no SGW;

2.2.12. Gerenciamento de SS7:

2.2.12.1. MTP:

2.2.12.1.1. Signalling Points;

2.2.12.1.2. Signalling Links and Linksets;

2.2.12.1.3. Signalling Routes and Destinations;

2.2.12.1.4. Combined Linksets;

2.2.12.1.5. Protocol Profiles tal como Configuração MTP

2.2.12.1.6. Incoming Linkset Screening;

2.2.12.1.7. OPC/DPC/SIO Screening;

2.2.12.1.8. MTP Gateway Screening;

2.2.12.1.9. MSU criteria for duplication tal como MTP multiplas rotas;

2.2.12.1.10. Administration for M3UA;

2.2.12.1.11. MTP Measurement Configuration.

2.2.12.2. SCCP:

2.2.12.2.1. SCCP Routing;

2.2.12.2.2. SCCP Global Title Translators and Rules;

2.2.12.2.3. Local SCCP user Calling Party addresses;

2.2.12.2.4. SCCP Analysis criteria for Traffic Partitioning;

2.2.12.2.6. SCCP Measurements;

2.2.12.2.7. SCCP Gateway screening;

2.2.12.2.8. SCCP criteria for duplication tal como SSN backup

2.2.12.2.9. Função de teste de GT para evitar GT loop.

2.2.13. Padrões e Protocolos Suportados

2.2.13.1. ISUP Compliance

2.2.13.1.1. Suportar Q.761 Functional Description of ISDN User Part

2.2.13.1.2. Suportar Q.761 General Functions of Messages and Signals

2.2.13.1.3. Suportar Q.763 Formats and Codes

2.2.13.1.4. Suportar Q.764 Signalling Procedures

2.2.13.1.5. Suportar Q.767 Application of the ISDN User Part for International ISDN Interconnections

2.2.13.2. Suportar, descritos de 2.2.13.1.1 até 2.2.13.1.5, significa funcionalidade realizada pela plataforma, mas não necessariamente fornecida, podendo ser implementada no futuro com a adição de módulos e/ou licenças de software.

2.2.14. MTP Compliance:

2.2.14.1. Q.701 Functional Description of the Message Transfer Part;

2.2.14.2. Q.702 Signalling Data Link;

2.2.14.3. Q.703 Signalling Link;

2.2.14.4. Q.704 Signalling Network Functions and Messages;

2.2.14.5. Q.705 Signalling Network Structure;

2.2.14.6. Q.706 Message Transfer Part Signalling Performance;

2.2.14.7. Q.707 Testing and Maintenance;

2.2.14.8. Q.708 Number of International Signalling Point Codes;

2.2.14.9. Q.709 Hypothetical Signalling Reference Connection;

2.2.15. SCCP Compliance:

2.2.15.1. Q.711 Functional Description of Signalling Connection Control Part;

2.2.15.2. Q.712 Definition and Function of SCCP Messages;

2.2.15.3. Q.713 SCCP Formats and Codes;

2.2.15.4. Q.714 SCCP Procedures;

2.2.15.5. Q.715 SCCP User Guide;

2.2.15.6. Q.716 SCCP Performance.

2.2.16. TCAP Compliance:

2.2.16.1. Q.771 Functional Description of Transaction Capabilities;

2.2.16.2. Q.772 TCAP Information Element Definitions;

2.2.16.3. Q.773 TCAP Formats and Encoding;

2.2.16.4. Q.774 TCAP Procedures;

2.2.16.5. Q.775 Guidelines for Using TCAP;

2.2.16.6. ETSI 300 008-1 latest edition;

2.2.16.7. Q.2110, Q.2140, Q.2210 for E1/T1 High-speed Signalling Links acc. to Bellcore;

2.2.16.8. ETSI 300 009-1 latest edition

2.2.17. INAP versions:

2.2.17.1. Suportar ETSI, CS1S2 ou CS1+ compatible network

2.2.17.2. Suportar CAP phase 1 -2;

2.2.17.3. Suportar, descritos em 2.2.17.1 até 2.2.17.2, significa funcionalidade realizada pela plataforma, mas não necessariamente fornecida, podendo ser implementada no futuro com a adição de módulos e/ou licenças de software.

2.2.18. SS7 Over IP:

2.2.18.1. MTP3 User Adaptation layer (M3UA) according to RFC 4666 and ETSI TS 102 142;

2.2.18.2. MTP2 Peer to Peer Adaptation layer (M2PA) according to RFC 4165;

2.2.18.3. Internet Protocol according to RFC 791.

2.2.19. O SGW ofertado deverá implementar o protocolo SIGTRAN, conforme suas variantes:

2.2.19.1. Implementar a RFC 4233 – ISDN Q.921 User Adaptation Layer;

2.2.19.2. Implementar a RFC 4165 – SS7 MTP2 User Peer-to-Peer Adaptation Layer (M2PA);

2.2.19.3. Implementar a RFC 4666 – SS7 MTP3 – User Adaptation Layer (M3UA);

2.2.19.4. Implementar a RFC 3257 – Stream Control Transmission Protocol Applicability Statement;

2.2.19.5. Implementar a RFC 3873 – SCTP Management Information Base (MIB);

2.2.19.6. Implementar a RFC 3788 – Security Considerações para o SIGTRAN;

2.2.19.7. Implementar a RFC 2719 – Framework Architecture for Signaling Transport.

2.2.20. O sistema ofertado deverá disponibilizar interfaces independentes para separar o tipo de tráfego – gerência e sinalização.

2.2.20.1. As interfaces deverão ser Gigabit Ethernet IEEE 802.3z;

2.2.20.2. Arquitetura de software, Backup e Recuperação;

2.2.20.3. A solução ofertada deverá possuir arquitetura de software que permita sua

atualização sem a necessidade do sistema ser paralisado;

2.2.20.4. Deve permitir a inserção e retirada de patches de correção de programa sem a necessidade de paralisação do sistema;

2.2.20.5. O SGW deverá permitir o reinício manual mediante comando homem-máquina ou agendamento prévio através da Plataforma de Gerência;

2.2.20.6. O SGW deve permitir o armazenamento do seu backup e possibilitar a transferência do seu conteúdo para outras mídias através do protocolo FTP;

2.2.20.7. Devem ofertar todas as funcionalidades especificadas para o Gateway de Sinalização em um equipamento dedicado (Stand Alone) para esta função;

2.2.21. Interfaces físicas do SGW: SGW = 4+4 interfaces GbE (Gigabit Ethernet) 1000Base T, interfaces RJ45 (15 links lógicos - SIGTRAN), cada equipamento.

2.2.22. O SGW deve ser dimensionado considerando as capacidades especificadas para o HLR e o SMSC.

2.3. SMSC (Short Message System Center) – No mínimo 01 (um) SMSC em alta disponibilidade

2.3.1. A plataforma deverá ser centralizada e deve ser provida de interfaces de sinalização Sigtran - M3UA.

2.3.2. A conexão entre a plataforma SMSC e os elementos de rede HLR(s) será feita através de STPs/SGW (Signaling Transfer Points), garantindo o funcionamento em caso de falha na rede de sinalização.

2.3.4. A plataforma deve possibilitar interface WEB, envio de mensagens broadcast, envio de mensagens para códigos Especiais. Caso a SMSC fornecida não execute esta função, será permitido uso de dispositivo ou ferramenta externa.

2.3.5. A solução oferecida deve ser totalmente aderente às seguintes especificações, em suas últimas versões:

2.3.5.1. SIP - Session Initiation Protocol

2.3.6. Outras especificações de regulamentação e padronização a serem seguidas e atendidas pelo CONTRATANTE:

2.3.6.1. Especificações do 3GPP para SMS;

2.3.6.2. Especificações do SMS Forum (SMPP).

2.3.6.3. O SMSC ofertado deverá implementar, no mínimo, as seguintes funções:

2.3.6.3.1. Processamento de mensagens;

2.3.6.3.2. Sinalização SMPP (versão 3.4);

2.3.6.3.3. Partição de carga dos enlaces de sinalização;

2.3.6.3.4. Interface gráfica homem-máquina;

2.3.6.3.5. Padrão SNMP para sistema de gerência;

2.3.6.3.6. Conter dispositivos de segurança multi-nível para acessos ao sistema;

2.3.6.3.7. APIs para a customização com sistemas de Customer Care, Billing e provisionamento remoto;

2.3.6.3.8. Tolerância a falhas funcionando em cluster modo active-standby;

2.3.6.3.9. A plataforma deve possuir a tecnologia de Banco de Dados Baseados em Memória, ou seja, a capacidade de o processamento de uma transação ocorrer dentro da memória, aperfeiçoando a eficiência;

2.3.6.3.10. A plataforma deve implementar capacidade nominal de 250 MDAS (Message Delivery Attempt por segundo);

2.3.6.3.11. A plataforma deve implementar capacidade de 7.200.000 de assinantes;

2.3.6.3.12. A plataforma deve implementar capacidade mínima de 600Gb de banco de dados;

2.3.6.3.13. A plataforma deve implementar 25Mbit/s de enlaces de sinalização M3UA;

2.3.6.3.14. A plataforma deve implementar os padrões de interfaces SMPP ou SMPP+ e TCP/IP;

2.3.6.3.15. A plataforma deve implementar relatório de entrega de mensagens (SMS Delivery Reports);

- 2.3.6.3.16. A plataforma deve implementar reenvio imediato após uma tentativa mal-sucedida (SMS Retry);
- 2.3.6.3.17. A plataforma deve implementar armazenamento da mensagem para envio posterior, configurado pelo operador (SMS Store and Forward);
- 2.4. OTA (Over-The-Air) – No mínimo 01 (um) OTA em alta disponibilidade
- 2.4.1. Requerimentos Gerais
- 2.4.1.1. A solução OTA deve implementar no mínimo o volume transacional de 30 (trinta) mensagens por segundo;
- 2.4.1.2. A solução OTA deve, antes de aprovisionar os dados relativos aos cartões SIM245, criptografar as chaves utilizando a chave de transporte selecionada, através do método DES e 3-DES.
- 2.4.1.3. Durante o aprovisionamento:
- 2.4.1.3.1. As chaves devem ser descriptografadas com a correspondente chave de transporte;
- 2.4.1.3.2. As chaves devem ser criptografadas utilizando a chave mestre do sistema;
- 2.4.1.3.3. Só então, as chaves devem ser armazenadas no repositório do sistema;
- 2.4.1.4. A solução OTA deve dispor de funcionalidade de agrupamento de registros de cartões SIM245 na Plataforma. Esta funcionalidade deve permitir a execução simplificada de Campanhas de gestão dos cartões SIM245;
- 2.4.1.5. A solução OTA deve dispor de funcionalidade de Application Repository Manager, permitindo a auditoria do conteúdo dos cartões SIM245;
- 2.4.1.5.1 Esta funcionalidade deve permitir a gestão e constante atualização do conteúdo dos cartões SIM245; tal informação deve estar disponível na base de dados da Plataforma;
- 2.4.1.5.2 Esta funcionalidade deve estar disponível para os canais SMS e BIP CAT-TP.
- 2.4.1.5.3. Os serviços que devem ser minimamente cobertos são os seguintes:
- 2.4.1.5.3.1. Auditar o conteúdo dos registros: retornar o conteúdo de um registro, contido em um arquivo;
- 2.4.1.5.3.2. Auditar o tamanho do arquivo: retorna o tamanho do arquivo;
- 2.4.1.5.3.3. Auditar o tamanho da memória livre: retorna o tamanho da memória livre no cartão SIM245;
- 2.4.1.5.3.4. Auditar a presença de instância Java: verifica a presença de um applet no cartão;
- 2.4.1.5.3.5. Auditar presença de pacote Java: verifica a presença de pacote no cartão;
- 2.4.2. A solução OTA deve implementar a funcionalidade de Remote File Management (RFM) para os cartões SIM245, em conformidade com os padrões 3GPP TS 51.011, 3GPP TS 31.102 e 3GPP TS 11.11, para cartões de tecnologia 2G e 3G, atendendo minimamente as funções descritas abaixo:
- 2.4.2.1. Activate ADN
- 2.4.2.2. Activate FDN
- 2.4.2.3. Switch ADN/FDN
- 2.4.2.4. Update ACC
- 2.4.2.5. Update AND
- 2.4.2.6. Update BDN
- 2.4.2.7. Update CBMI
- 2.4.2.8. Update FDN
- 2.4.2.9. Update FPLMN
- 2.4.2.10. Update HPLMN
- 2.4.2.11. Update IMSI
- 2.4.2.12. Update LP
- 2.4.2.13. Update MSISDN
- 2.4.2.14. Update PLMN
- 2.4.2.15. Update SDN
- 2.4.2.16. Update SMSP
- 2.4.2.17. Update SPN

- 2.4.2.18. Update SST
- 2.4.2.19. Update PL
- 2.4.2.20. Update EST
- 2.4.2.21. Update UST
- 2.4.2.22. Generic Card Update
- 2.4.2.23. Update HPLMNwAct
- 2.4.2.24. Update PLMNwAct
- 2.4.2.25. Update OPLMNwAct
- 2.4.3. A solução OTA deve implementar a funcionalidade de Remote Applet Management (RAM) para os cartões SIM245, em conformidade com os padrões 3GPP TS 51.011, 3GPP TS 31.102 e 3GPP TS 11.11, para cartões de tecnologia 2G e 3G, atendendo minimamente as funções descritas abaixo:
 - 2.4.3.1. Download applet
 - 2.4.3.2. Delete applet
 - 2.4.3.3. Lock applet
 - 2.4.3.4. Unlock applet
 - 2.4.3.5. Download package
 - 2.4.3.6. Delete package
 - 2.4.3.7. Install for load package
 - 2.4.3.8. Load package
 - 2.4.3.9. Extradite Executable Load File
 - 2.4.3.10. Create applet instance
 - 2.4.3.11. Delete applet instance
 - 2.4.3.12. Make instance selectable
 - 2.4.3.13. Extradite Application
 - 2.4.3.14. Download applet to installed
 - 2.4.3.15. Instantiate applet to installed
- 2.4.4. A solução OTA deve implementar Proof of Receipt (PoR), em conformidade com o padrão 3GPP TS 23.048 V5.9.0, e SMSs de texto e binários;
- 2.4.5. A solução OTA deve dispor de Módulo de Campanha que permita a execução de atualização de arquivo SIM, download de applets Java e atualizações de menu IOD;
 - 2.4.5.1. Este Módulo de Campanha deve permitir a execução de campanhas em batch único, realizando o pré-processamento de todo o pacote antes da entrega do mesmo, fazendo desnecessário o processamento antes do envio de cada mensagem e otimizando a utilização do recurso das SMSCs;
- 2.4.6. A solução OTA deve permitir a descritografia das chaves-mestre disponibilizadas pelo Serpro, cifradas em padrão DES e 3-DES, utilizando a chave de transporte correspondente. Posteriormente, deverá realizar a criptografia utilizando chave mestre do sistema, para só então serem armazenadas no repositório do sistema;
- 2.4.7. A solução OTA deve dispor de módulo de campanha, com gestão via interface gráfica, que permita atualizações Over-The-Air para cartões SIM245 por MSISDN, IMSI e ICCID. O módulo de campanha deve implementar as funcionalidades de Remote File Management (RFM) e Remote Applet Management (RAM);
- 2.4.8. A solução OTA deve dispor de ferramenta de gestão de roaming, através da gestão Over-The-Air dos arquivos PLMN e FPLMN 2G e 3G;

2.4.9. Integração e Interoperabilidade

- 2.4.9.1. A solução OTA deve estar integralmente em conformidade com o processo estabelecido pelos grupos de trabalho do Projeto Denatran SIMRAV, que estabelece que a OTA deve ser capaz de gerir requisições encaminhadas da rede de uma Operadora de Telefonia, recebendo a resposta desta requisição através da rede de outra Operadora de Telefonia, no momento da troca de operadora nos cartões SIM245. Garantindo assim, a gestão segura destes cartões;
- 2.4.9.2. A solução OTA deve ser interoperável, suportando todos os cartões SIM245 que

estejam em conformidade com o padrão descrito na “Especificação Técnica Aplicativo SIM 245 v1.2.0” de 24 de abril de 2009, independente do fabricante deste cartão;

2.4.9.3. A solução OTA deve implementar a integração com as Plataformas SMSC das Operadoras de Telefonia do Serviço Móvel Pessoal (SMP) envolvidas no Projeto Denatran SIMRAV, utilizando a infraestrutura de rede existente do SERPRO, e implementando minimamente os canais abaixo listados:

2.4.9.3.1. CMG de 3.1.0 até 4.6 (EMI UCP)

2.4.9.3.2. SMPP 3.3 e 3.4

2.4.9.3.3. Nokia SC 4 e SC 5 (CIMD2)

2.4.9.4. A solução OTA deverá realizar integração de comunicação com o Mediador item 2.6.

2.4.9.5. A solução OTA deve implementar integração com a rede IP das Operadoras de Telefonia do Serviço Móvel Pessoal (SMP) envolvidas no Projeto Denatran SIMRAV via BIP (Bearer Independent Protocol) CAT-TP, utilizando a infraestrutura de rede do SERPRO para uso futuro e em concordância com futuras especificações técnicas do aplicativo SIM245 que venham a utilizar este canal de comunicação.

2.4.10. Requerimentos de Padrões

2.4.10.1. A solução OTA deve estar em conformidade com os padrões abaixo listados:

2.4.10.1.1 ANATEL – SMP – Resolução 477

2.4.10.1.2. 3GPP TS 23.040

2.4.10.1.3. 3GPP TS 23.048

2.4.10.1.4. 3GPP TS 31.102

2.4.10.1.5. 3GPP TS 31.10

2.4.10.1.6. 3GPP TS 11.11

2.4.10.1.7. 3GPP TS 51.011

2.4.10.1.8. 3GPP GSM TS 03.203

2.4.10.1.9. 3GPP GSM TS 23.003

2.4.10.1.10. ITU-T – E.164

2.4.10.1.11. GSM 03.38

2.4.10.1.12. 3GPP 23.038

2.4.10.1.13. ETSI TS 102 226

2.4.10.1.14. ETSI TS 102 227

2.4.11. Requerimentos de Marketing

2.4.11.1. A solução deve dispor de interface web para visualização e obtenção de estatísticas e relatórios em tempo real;

2.4.11.2. A ferramenta de estatística e relatórios deve permitir a geração de relatórios sob demanda, através da interface web;

2.4.11.3. A ferramenta de estatística e relatórios deve permitir a geração de relatórios automáticos, com seu agendamento definido pelo SERPRO;

2.4.11.4. A ferramenta de estatística e relatórios deve dispor de mecanismo de exportação de relatórios para diferentes formatos, tais como, Excel, Word, TXT, PDF, HTML and XML;

2.4.11.5. Os dados expressos pelas estatísticas e relatórios da solução devem permanecer acessíveis por no mínimo 30 (trinta) dias após sua geração;

2.4.11.6. Os relatórios devem ser flexíveis por período (data inicial e data final);

2.4.11.7. A solução deve dispor de logs de auditoria. Estes logs de auditoria devem ser gerados para todos os perfis de usuários definidos na solução, para os casos de: criação, modificação, consulta e uso da solução.

2.4.12. Dimensionamento da solução OTA:

Para cada SIM245 ativado, poderá ser executada uma transação de desativação, caso aplicável, sem que a mesma gere custo adicional de licenciamento. As plataformas OTA e Mediador deverão garantir o pleno funcionamento do sistema, mesmo que o pacote de

licenças contratado seja esgotado durante o período contratado, garantindo a disponibilidade de serviço para o usuário final.

2.5. PLATAFORMA DE GERÊNCIA – No mínimo 01 (uma) plataforma de gerência.

2.5.1. Requerimentos Gerais

2.5.1.1. Essa especificação aplica-se a todas as plataformas alocadas para o atendimento da infraestrutura de telecomunicações que visa a atender atendimento ao projeto SIMRAV, alocada na estrutura do SERPRO.

2.5.1.2. Todas as plataformas pertencentes ao Sistema Denatran de Telecomunicações (HLR, SGW, SMSC e OTA) para o projeto SIMRAV, deverão ser integradas a uma plataforma de gerência centralizada em modo cluster, arquitetura cliente-servidor.

2.5.1.3. A plataforma de gerência centralizada deverá ser única para todos os sistemas de telecomunicações implantados para o projeto SIMRAV e deverá ser fornecida pela aderente a qual ficará responsável pelo gerenciamento da mesma.

2.5.1.4. A plataforma de gerência centralizada deverá possuir interfaces Lan redundantes para tolerância a falhas e em número suficiente para a interligação de todos os dispositivos a serem gerenciados;

2.5.1.5. Deve implementar NTP para sincronia com um servidor NT;

2.5.1.6. A plataforma deve possuir disponibilidade de 99,999% MTBF mínimo de 25000 horas;

2.5.1.7. Deve implementar interface WEB.

2.5.2. Requisitos de Backup e Recuperação

2.5.2.1 Implementar backup de dados das seguintes situações:

2.5.2.1.1. Backup e recuperação da plataforma de gerência;

2.5.2.1.2. Backup de dados e recuperação dos elementos de redes gerenciados;

2.5.2.1.3. Cada elemento deve armazenar seu último backup localmente;

2.5.2.1.4. Implementar agendamento de backups;

2.5.2.1.5. Implementar backups automáticos;

2.5.2.1.6. Implementar Veritas net backup;

2.5.2.1.7. Implementar online backups incrementais;

2.5.2.1.8. Implementar rotinas de backups centralizadas;

2.5.2.1.9. O tempo para realização de uma rotina de backup não deve ser superior a 20 horas;

2.5.2.1.10. Durante o backup não pode haver nenhum impacto ao tráfego de dados relativos às operações de gerenciamento;

2.5.2.1.11. Deve ser possível fazer um snapshot backup de um determinado momento da situação da rede para que seja utilizado em procedimentos de fallback.

2.6. Certificações

As plataformas ofertadas devem, obrigatoriamente, estar certificadas junto ao órgão regulador ANATEL.

2.7. Plataforma do Mediador – No mínimo 01 (um) conjunto de Mediador em alta disponibilidade

2.7.1. Características da Plataforma de Mediação

2.7.1.1. A Plataforma mediadora para SIMRAV é uma plataforma única que deverá prover serviços por meio de integração com os sistemas SIMRAV, HLR e OTA, realizando operações de Aprovisionamento e Portabilidade.

Toda a infraestrutura de telecomunicações a ser implantada no SERPRO para atendimento ao projeto SIMRAV deverá ser integrada à plataforma de mediação.

2.7.1.2. A Plataforma Mediador deve possuir módulos para Gestão de Log e Eventos;

2.7.1.3. A Plataforma Mediador deve possuir Interface WEB para Aplicações de Monitoramento de Log e Eventos;

2.7.1.4. A Plataforma Mediador deve possuir Componentes de Detecção, Roteamento e Adaptação de Conteúdo de Mensageria XML e Arquivos XML e Transferência com

conectividade para HLR e OTA via MML, SMPP ou SOAP;

2.7.1.4.1 JAVA padrão J2EE, sob Jboss versão 5.1. As licenças de Jboss, JAVA e HornetQ, são open source. A licença da ferramenta Q-Ware deverá ser fornecida pelo SERPRO;

2.7.1.5. A Plataforma Mediador deve suportar no mínimo o volume transactional de 30 (trinta) mensagens por segundo, para provisionamento e portabilidade;

2.7.1.6. A Solução deve Integrar com arquitetura composta pelos elementos lógicos de processamento e banco de dados – Front End (FE) e Back End (BE);

2.7.1.7. A Solução deve Integrar com OTA.

2.7.1.8. A plataforma de mediador da CONTRATANTE deve prover uma ferramenta de verificação de consistência de dados nos HLRs redundantes. A funcionalidade de verificação de consistência procurará e mostrará qualquer inconsistências de dados existentes entre os HLRs.

2.7.1.9. A plataforma de mediação fornecida pela CONTRATANTE deverá possuir registros dos provisionamentos. A solução deverá prover uma base de dados detalhada de logs com ferramenta de procura e análise estatística (data mining) configurada pelo operador.

2.7.1.10. A solução deverá suportar alta disponibilidade com 99,99%.

2.7.1.11. A plataforma de provisionamento deverá ser hot stand-by entre os servidores principal e de backup, em caso de falha da unidade principal o sistema de backup entrará em operação sem intervenção humana.

2.7.2. Serviço de Adaptação e Customização da Plataforma Mediadora

2.7.2.1. A Plataforma Mediadora será objeto de customização, adequação e geração de interfaces para integração com sistemas SIMRAV com o Mediador e o HLR e OTA.

2.7.2.1.1 - O fornecedor é obrigado a realizar a integração da plataforma do Serpro, mediante serviços de customização das interfaces utilizadas no SIMRAV, integrando os protocolos advindos do Qware para interfaces padrões 3GPP que são utilizadas nas plataformas de provisionamento do HLR e OTA.

2.7.2.2. Este serviço consistirá na adaptação da plataforma mediadora ao ambiente computacional e às necessidades negociais do Serpro.

2.7.2.3. Os artefatos disponibilizados pela CONTRATANTE na implementação da solicitação de Adaptação serão:

2.7.2.3.1. Validados pela equipe de Testes, Qualidade de Software e representantes das áreas gestoras da Solução, visando à verificação da conformidade com respectivos Padrões Tecnológicos SERPRO e requisitos de negócios;

2.7.2.3.2. Encaminhados para o Ambiente de Homologação de Processos;

2.7.2.3.3. Disponibilizados para produção ao final dos testes, após o aceite do artefato pelo SERPRO.

2.7.2.4. Os custos para a prestação dos serviços de Adaptação e Customização são de responsabilidade exclusiva da CONTRATANTE.

2.7.2.5. A adaptação e Customização da Solução observarão o descrito neste Termo de Referência.

2.7.3. Integração da Solução Ofertada com o SIMRAV

2.7.3.0 A plataforma de mediação única, deverá ser capaz de integrar todos os Sistemas Denatran de Telecomunicações ao sistema SIMRAV.

2.7.3.1. A Solução deverá ser integrada com o Sistema SIMRAV através de XML/WebServices.

2.7.3.2. A integração com o Sistema SIMRAV dar-se-á por filas padrão processando mensagens no formato XML - Extensible Markup Language, como meio padrão para troca de informações.

2.7.3.3. A integração com os Sites SIMRAV WEB do SERPRO dependerá do tipo de solução ofertada para Detecção, Roteamento e Adaptação de Conteúdo e Apresentação.

2.7.3.3.1. Os Sites referidos acima estão baseados na plataforma CISC/Linux em linguagem Java/HTML.

2.7.3.4. A Solução de mediação aos elementos ofertados com o objetivo de ativação, deve

poder ser integrada tendo a capacidade de administração de sessões e conexões flexíveis para suprir os volumes de mensagens necessários assim como a topologia ofertada.

2.7.3.5. É necessário que a solução tenha um único ponto de provisionamento para toda a solução ofertada e que a mesma possua capacidades tais como:

2.7.3.5.1. Capacidade de executar comandos relacionados a grupos de assinantes, os quais serão provisionados pelos mesmos. O sistema tem que executar de forma agendada e com respostas dedicadas um grande número de subscrições no qual se deseja o provisionamento em grupo.

2.7.3.5.2. O sistema deve poder agendar comandos para serem executados nos sistemas provisionados. Este agendamento deve ser assíncrono e diferenciado quanto ao usuário e tempo.

2.7.3.5.3. Deve haver a possibilidade de se realizar uma verificação de consistência nas bases de dados a partir do elemento mediador. O mesmo deve fornecer flexibilidade, usabilidade, qualidade dos dados, extensibilidade, escalabilidade e capacidade de integração a outros sistemas.

2.7.3.5.4. Em caso necessitando de sistemas redundantes para as bases de dados, o mediador deve ter capacidade de provisionar mantendo a manipulação da redundância existente. No caso de os elementos provisionados oferecerem a mesma base de dados de subscrições, o mediador terá de provisionar ambas e ainda assim coordenando a base ativa e secundária. Terá de ser transparente para o SIMRAV o envio dos comandos de provisionamento mesmo sem ter conhecimento de qual elemento provisionado está ativo ou em stand-by

2.7.4. Padrões Tecnológicos SERPRO

2.7.4.1. A Plataforma Mediadora para Serviços SIMRAV deverá ser adaptada aos padrões tecnológicos do SERPRO, ambiente de homologação e produção, conectividade, de desenvolvimento e manutenção de sistemas.

2.7.4.2. Padrão de Construção de Aplicação e Ambiente Computacional.

2.7.4.3. As implementações realizadas pela empresa CONTRATANTE nos processos de adaptação, integração e modelagem de dados da Solução deverão obedecer às definições de três camadas básicas de arquitetura a seguir:

2.7.4.4. **Camada de Dados** – Sistema Gerenciador de Banco de Dados:

2.7.4.4.1. É responsável pelo acesso e armazenamento de dados garantindo integridade, disponibilidade, confidencialidade, manutenção e documentação;

2.7.4.4.2. As regras de negócio não deverão ser desenvolvidas em componentes do SGBD como TRIGGERS ou STORED PROCEDURES.

2.7.5. **Camada de Aplicação** (Fluxo de Processo e Regras de Negócio):

2.7.5.1. Essa camada é constituída de um conjunto de componentes que agrupam regras de negócio (Camada de Regras de Negócio) e definições de fluxo de processo dos sistemas que compõem a solução (Camada de Fluxo de Processo);

2.7.5.2. Uma regra de negócio define critérios - condições e/ou transformações que devem ser obedecidos dentro de um contexto do negócio;

2.7.5.3. As regras de negócio devem estar contidas na camada de aplicação e somente esta poderá acessar a camada de dados;

2.7.5.4. A camada de aplicação deve utilizar a linguagem Java;

2.7.6. **Camada de Apresentação:** A camada de apresentação formata as informações e dados oferecidos pelo sistema para que sejam adequadamente apresentados no acesso WEB utilizado pelo usuário de gerenciamento;

2.7.6.1. A camada de apresentação deve residir em servidor Web, sendo que neste último caso deve ser mantida a compatibilidade com o padrão W3C;

2.7.6.2. A Camada de Apresentação deverá suportar Browsers e utilizar linguagens Java, HTML e XML.

2.8. Conectividade

2.8.1. Será permitida à CONTRATANTE a conexão ao ambiente de Desenvolvimento do SERPRO que processará o sistema Denatran de Telecomunicações na

cidade de Brasília/DF, mediante atendimento aos requisitos de segurança no processamento e no acesso correlatos.

2.8.2. A forma de Conectividade atenderá obrigatoriamente aos requisitos de segurança disponíveis nas diversas formas de interligação definidas no portfólio de conexão com empresas externas, conforme regulamentação do SERPRO:

2.8.2.1. O acesso será feito pela Extranet do SERPRO e da CONTRATANTE, com todos os recursos tecnológicos inerentes a esse tipo de ambiente;

2.8.2.2. Após a autenticação na Extranet do SERPRO, a empresa terá acesso aos sistemas de acordo com a necessidade dos serviços;

2.8.3. A conectividade descrita neste item será utilizada pela empresa CONTRATANTE para transmitir ao SERPRO os códigos fonte das Adaptações, Desenvolvimento e Manutenções efetuadas, nas customizações realizadas; também será utilizado software de controle de versões do SERPRO, para submeter os códigos transmitidos aos processos de Compilação, Testes, Homologação e Produção;

2.8.4. As despesas de conexão – linha de comunicação - de acesso ao ambiente do SERPRO serão custeadas pela CONTRATANTE.

2.9. Da Operacionalização dos Serviços

2.9.1. O SERPRO e a CONTRATANTE, sempre que necessário, agendarão reuniões periódicas de caráter gerencial e/ou técnico para avaliar os trabalhos, adotar resoluções e obter esclarecimento de pendências durante toda a vigência do contrato.

2.10. Relação de hardware, software e serviços mínimos para implantação do Sistema Denatran de Telecomunicações:

ITEM QTDE

HLR (Home Location Register) 01

SGW (Signaling Gateway) 01

SMSC (Short Message System Center) 01

OTA (Over-The-Air) 01

Plataforma Mediador 01

Plataforma de Gerência 01

Serviços de Suporte e Manutenção 01

Serviços de Operação Assistida 01

2.11. Repasse de conhecimento

2.11.1. A Contratante deverá prover repasse de conhecimento técnico aos profissionais do Serpro para configuração e operação dos equipamentos e softwares.

2.11.2. O repasse de conhecimento deverá ocorrer sem ônus adicional para o Serpro, incluindo todo o material didático necessário. O material de aula deverá abordar conteúdo teórico e prático, e deverá ser submetido ao Serpro para aprovação antes da realização da capacitação.

2.11.3. O repasse de conhecimento deverá ser ofertada através de profissionais certificados e credenciados pelo fabricante ou empresa credenciada para tal finalidade.

2.11.4. A Contratante deve prover O repasse de conhecimento referente a solução proposta, sem ônus para o Serpro, atendendo aos seguintes tópicos:

2.11.4.1. Funcionalidades e ferramentas da solução;

2.11.4.2. Arquitetura de Hardware e Software;

2.11.4.3. Protocolos e interfaces;

2.11.4.4. Dimensionamento do sistema;

2.11.4.5. Alarmes e Estatísticas;

2.11.4.6. Manutenção e operação do sistema;

2.11.4.7. Integração com demais sistemas;

2.11.5. O repasse de conhecimento deve ser provido de acordo com a distribuição abaixo:

2.11.5.1. Para a Solução instalada em São Paulo, 02 (duas) turmas de 10 (dez) participantes cada com 160 (cento e sessenta) horas cada em São Paulo ou em local no

Brasil indicado pelo licitante, desde que acordado pelo Serpro. O ônus do deslocamento dos empregados do Serpro, com hospedagem correrá por conta do Serpro;

2.11.5.2. Para o Mediador, instalado em São Paulo, 02 (duas) turmas de 10 (dez) participantes cada com 40 (quarenta) horas cada, em São Paulo ou em local no Brasil indicado pelo licitante no caso de impossibilidade da capacitação do treinamento em São Paulo, desde que acordado pelo Serpro. O ônus do deslocamento dos empregados do Serpro, com hospedagem correrá por conta do Serpro;

2.11.5.3. O repasse de conhecimento deve ser realizada em língua portuguesa.

2.11.5.4. Cada turma desta capacitação deverá ser dimensionada para até 10 (dez) participantes.

2.11.5.5. A Contratante deve responsabilizar-se por toda a infraestrutura requerida para o treinamento.

2.11.5.6. A contratante deve fornecer treinamentos práticos em equipamentos com a mesma versão de SW ofertado.

2.11.6. O repasse de conhecimento deverá ser iniciada no prazo máximo de 60 (sessenta) dias corridos após a assinatura do contrato.

CLÁUSULA TERCEIRA – DA ABRANGÊNCIA DOS SERVIÇOS

3.1 As Plataformas de produção, Gerenciamento e Mediação podem ser instaladas preferencialmente nas localidades do SERPRO em Brasília e São Paulo.

3.2 Os serviços objeto do presente Contrato serão realizado(s) no(s) estabelecimento(s) do SERPRO, localizado(s) no(s) seguinte(s) endereço(s):

REGIONAL BRASÍLIA/DF

CNPJ: 33.683.111/0002-80

ENDEREÇO: SGAN Av. L2 Norte, Quadra 601 – Módulo “G”

CEP: 70830-900

REGIONAL BELÉM/PA

CNPJ: 33.683.111/0003-60

ENDEREÇO: Av. Perimetral da Ciência, nº 2010

CEP: 66077-530

REGIONAL FORTALEZA/CE

CNPJ: 33.683.111/0004-41

ENDEREÇO: Av. Pontes Vieira, nº 832, São João do Tatuapé

CEP: 60130-240

REGIONAL RECIFE/PE

CNPJ: 33.683.111/0005-22

ENDEREÇO: Av. Parnamirim, nº 295, Bairro Parnamirim

CEP: 52060-000

REGIONAL SALVADOR/BA

CNPJ: 33.683.111/0006-03

ENDEREÇO: Av. Luiz Viana Filho, nº 2355, Bairro Paralela

CEP: 41130-530

REGIONAL BELO HORIZONTE/MG

CNPJ: 33.683.111/0007-94

ENDEREÇO: Av. José Cândido da Silveira, nº 1200, Cidade Nova

CEP: 31170-000

REGIONAL RIO DE JANEIRO/HORTO

CNPJ: 33.683.111/0008-75

ENDEREÇO: Rua Pacheco Leão, nº 1235, Fundos – Jardim Botânico

CEP: 22460-030

REGIONAL SÃO PAULO/SP

CNPJ: 33.683.111/0009-56

ENDEREÇO: R. Olívia Guedes Penteado, nº 941, Capela do Socorro

CEP: 04766-900

REGIONAL CURITIBA/PR

CNPJ: 33.683.111/0010-90

ENDEREÇO: Rua Carlos Pioli, nº 133, Bairro Centro Cívico

CEP: 80520-170

REGIONAL PORTO ALEGRE/RS

CNPJ: 33.683.111/0011-70

ENDEREÇO: Av. Augusto de Carvalho, nº 1133, Bairro Centro

CEP: 90010-390

CLÁUSULA QUARTA – DAS OBRIGAÇÕES DAS PARTES

4.1. DO CONTRATADO

- Hospedagem dos equipamentos da solução, 24 horas por dia, 7 dias na semana, 365 dias por ano, envolvendo a segurança física e lógica;
- Contato operacional continuado e escala de acionamento segundo acordo de nível de serviço (SLA) definido com o cliente;
- Monitorar a conexão da rede;
- Configurar e administrar os ativos de rede;
- Zelar pela segurança física dos equipamentos e por suas condições de funcionamento;
- Resolver quaisquer problemas referentes a conexão com a rede Denatran que independam das operadoras de telecomunicações.

4.1.1. Recursos de infraestrutura disponibilizados pelo SERPRO

4.1.1.1. Ambiente físico (instalações prediais)

Os equipamentos da Contratante serão instalados nos Centros de Dados do SERPRO conforme item 4.4. Estes Centros de Dados possuem alta disponibilidade de energia e refrigeração, além de controle de acesso, detecção e combate a incêndio, monitoração por Circuito Fechado de TV - CFTV e Supervisão e controle dos ativos dessas infraestrutura.

4.1.1.2. Energia elétrica

O sistema de alimentação elétrica do Centro de Dados é redundante, composto por duas linhas independentes, Dual01 e Dual02, de 700kVA cada uma, estabilizadas por no-breaks modulares com autonomia de no mínimo 15 minutos em plena carga e contingenciadas por grupos motor-geradores de 900kVA, um para cada linha. Os equipamentos com fonte dupla (dual) são alimentados por circuitos distintos provenientes de cada uma dessas

linhas. Para os equipamentos de fonte singela (single) existe um terceiro circuito, Single, proveniente de uma chave estática que comuta entre os dois circuitos (Dual01 e Dual2) e garante a alimentação elétrica mesmo em caso de pane em uma dessas duas linhas.

4.1.1.3. Sistema de refrigeração

O Sistema de refrigeração é composto por equipamentos de precisão que controlam temperatura e umidade. Em cada compartimentação do ambiente, do Centro de Dados, rede de longa distância ou rede local, existem equipamentos em número suficiente para o dimensionamento da carga térmica e mais um equipamento de reserva (backup) para contingenciar qualquer indisponibilidade que possa existir.

4.1.1.4. Controle de acesso

Existem quatro níveis de acesso no Centro de Dados controlados por um sistema que utiliza cartões de proximidade mesclados com uso de senha ou biometria. O nível 01 é a recepção do Centro de Dados onde se encontra vigilantes em turno de 24 horas treinados para cadastrar os funcionários ou visitantes para acesso as demais áreas. O Acesso para esse nível se dá por uma porta eclusa. O nível 02 são áreas de uso comum e salas de apoio. O acesso é por cartões de proximidade. O nível 03 são áreas de monitoração acessadas por cartões de proximidade e senha pessoal. O nível 04 são os ambientes de produção, onde estão os ativos de TI. O acesso a essas áreas somente é possível com cartões de proximidade e biometria (impressão digital).

4.1.1.5. Detecção e combate a incêndio

O Ambiente do Centro de Dados é dotado de um sistema misto de detecção de incêndio e combate por gás inerte. É composto por detectores convencionais (velocimétricos) que detectam fumaça e/ou calor e por um sistema de análise laser (VESDA) que detecta o princípio de incêndio antes mesmo da formação de fumaça ou elevação de temperatura. O combate a incêndio é feito por um gás inerte, FE- 25, atóxico e não sufocante, permitindo que pessoas possam estar no ambiente no momento do disparo do gás sem que sofram qualquer consequência. Para evitar que o gás seja acionado acidentalmente, os sistemas convencionais e VESDA foram interligados, sendo assim, o sistema VESDA irá emitir um pré-alarme caso haja um princípio de incêndio, mas só irá disparar o gás quando cruzar com o sinal do detector velocimétrico, quando evidenciar realmente um incêndio. Cabe ressaltar ainda que em todo ambiente existem extintores portáteis que permitem o combate manual no princípio de incêndio.

4.1.1.6. Monitoração por CFTV

O Circuito Fechado de TV (CFTV) do Centro de Dados é composto por 92 câmeras dispostas pelos principais acessos e ambientes do Centro de Dados. A monitoração é feita por vigilantes em turno de 24 horas 7 dias por semana. As imagens são gravadas em média por 2 meses.

4.1.1.7. Supervisão e controle dos ativos de infraestrutura

Além da monitoração do CFTV, os equipamentos como no-break, geradores, climatizadores e sistema de detecção e combate a incêndio, bem como grandezas como tensão, carga (potência) e temperatura, são monitorados continuamente.

4.1.2. Níveis de Serviço ofertados pelo SERPRO

Energia e Refrigeração	99,6%	
Conjunto	% Disponibilidade	Tipo
Conjunto Energia Novo CPD	100,0%	P
CEB	99,9%	
Grupo Gerador (GMG) 1	99,9%	
Grupo Gerador (GMG) 2	99,9%	
Conjunto Quadro de Transferência CEB / GMG Novo CPD	99,8%	S
Disjuntor 1	99,9%	
Disjuntor 2	99,9%	
Conjunto No Break Novo CPD	100,0%	P
NB 1	99,9%	
NB 2	99,9%	
Conjunto Ar Condicionado Novo CPD	100,0%	P
AC 1	99,8%	
AC 2	99,8%	
Conjunto Energia Sala Cofre	100,0%	P
CEB	99,9%	
Grupo Gerador (GMG) 1	99,9%	
Grupo Gerador (GMG) 2	99,9%	
Conjunto Quadro de Transferência CEB / GMG Sala Cofre	99,8%	S
Disjuntor 1	99,9%	

Disjuntor 2	99,9%	
Conjunto No Break Sala Cofre	100,0%	P
NB 1	99,9%	
NB 2	99,9%	
Conjunto Ar Condicionado Sala Cofre	100,0%	P
AC 1	99,8%	
AC 2	99,8%	

P – Recurso em Paralelo
S – Recurso em Série

4.1.3. Alimentação Elétrica

O SERPRO disponibilizará alimentação elétrica em 110 ou 220 Volts, monofásica ou trifásica, caso sejam necessárias fontes de alimentação ou retificadores para alimentação em corrente contínua (DC), estes deverão ser fornecidos pela CONTRATANTE e estes serão considerados para efeito do cálculo do preço do serviço conforme especificado na Cláusula 7.

4.2. DA CONTRATANTE

- Indicar o contato administrativo e o contato técnico responsáveis pelos equipamentos e sistemas hospedados no SERPRO, com respectivos telefones fixos e celulares, e-mails e endereços;
- Atender prontamente aos comunicados, questionamentos e chamados do SERPRO incluindo chamados fora do horário de expediente normal, de 8h às 18h, finais de semana e feriados;
- Administrar o sistema operacional dos equipamentos e os softwares neles instalados;
- Fornecer todos os hardwares e softwares necessários e respectivas licenças;
- Responsabilizar-se por quaisquer problemas técnicos ou operacionais, de hardware ou software, nos equipamentos;

4.3. Níveis de Serviço

4.3.1. A CONTRATANTE deverá dispor de todos os requisitos que assegurem o cumprimento de todos os Níveis de Serviços, abaixo identificados, para atendimento nos locais de instalação e funcionamento dos hardwares, softwares e serviços.

4.3.1.1. Os chamados poderão ser efetuados por intermédio de telefone 0800 (ligação gratuita), acesso Web ou e-mail, e serão registrados. Estes registros deverão estar disponíveis por meio de relatórios encaminhados mensalmente, para acompanhamento da equipe do SERPRO, atendendo aos seguintes tópicos:

4.3.1.1.1. Chamados Abertos no Período: Relatório com todas as ocorrências abertas no mês e o status;

4.3.1.1.2. Chamados em Andamento: Relatório onde constam as ocorrências que estão sendo tratadas e qual o status;

4.3.1.1.3. Chamados Fechados no Período: Relatório com todos os chamados que foram

fechados no mês;

4.3.1.1.4. Histórico de Chamados em 12 Meses: Relatório com o histórico de chamados que foram abertos no período de 12 meses;

4.3.1.1.5. Controle de Troca de Equipamentos: Relatório com todos os chamados de troca de equipamentos que foram abertos no período.

4.3.1.2. Os relatórios deverão estar disponíveis via WEB (em formato HTML) para a Gerência de Qualidade e Recuperação da Superintendência de Redes do SERPRO, em Salvador-BA (Divisão de Gerenciamento de Incidentes - SUPOP/OPGPS/OPPBA - Serpro/Regional Salvador - Av. Luiz Vianna Filho, 2.355, Salvador - BA). Os dados necessários para viabilização do acesso serão informados após a instalação do primeiro equipamento fornecido.

4.3.1.3. Deve ser feita uma notificação de conclusão do atendimento no momento do fechamento de cada chamado.

4.3.2. Requerimentos Operacionais

4.3.2.1. Relatórios e Estatísticas

4.3.2.1.1. A solução deve dispor de histórico de eventos que permitam a investigação de qualquer tipo de falha.

4.3.2.1.2. A solução deve suportar as seguintes funcionalidades:

4.3.2.1.2.1. SNMP MIBs para alarmes de hardware

4.3.2.1.2.2. SNMP MIBs para alarmes da aplicação

4.3.2.1.2.3. SNMP traps

4.3.2.1.2.4. Interface gráfica para gestão dos alarmes

4.3.2.1.2.5. Interface gráfica para configuração

4.3.2.2. Suporte e Manutenção

4.3.2.2.1. A CONTRATANTE deve ofertar serviço de suporte, manutenção e monitoramento através de equipes baseadas em território nacional e capazes de comunicar-se em língua portuguesa, a fim de facilitar e agilizar possíveis interações com as equipes do SERPRO.

4.3.2.2.2. A CONTRATANTE deve testar exaustivamente todos os corretivos antes de aplicá-los na solução.

4.3.2.2.3. A CONTRATANTE deve notificar o SERPRO de qualquer nova atualização disponível para a solução, sendo responsabilidade da CONTRATANTE a instalação da mesma.

4.3.2.2.4. A CONTRATANTE deve prover e instalar todos as ações corretivas sem custos adicionais ao SERPRO.

4.3.2.2.5. A CONTRATANTE deve manter uma imagem da solução no ambiente da CONTRATADA, visando a realização de testes e validações de corretivos a serem instalados no Serpro;

4.3.2.2.6. A CONTRATANTE deve dispor de interface web para gestão e abertura de chamados.

4.3.2.2.7. A CONTRATANTE deve manter toda a documentação relativa a solução atualizada, estando a mesma em conformidade com os corretivos aplicados na solução.

4.3.2.2.8. A CONTRATANTE deve prover claramente o canal para solicitação de ajuste de severidade de incidentes.

4.3.2.2.9. A CONTRATANTE deve prover serviço de manutenção preventiva, com entrega de relatórios periódicos indicando possíveis impactos na solução.

4.3.2.2.10. A CONTRATANTE deve prover canal telefônico com disponibilidade 24x7 para abertura de chamados.

4.3.2.2.11. A CONTRATANTE deve dispor de canal de relacionamento com o cliente, realizando consultas periódicas ao Serpro quanto à qualidade da solução e serviços ofertados.

4.3.2.2.12. A CONTRATANTE deverá atender minimamente aos SLAs descritos na tabela abaixo:

Severidade		Tempo de Resposta	Disponibilidade e de Atendimento	Diagnóstico
1	Alta	30 minutos (Envio de primeiro diagnóstico do problema)	24 horas, 7 dias por semana, 365 dias por ano	A Contratada deverá trabalhar continuamente e até que o serviço seja restaurado completamente ou até que uma solução temporária seja adotada, restabelecendo o o serviço.
2	Média	2 horas (Envio de primeiro diagnóstico do problema)	24 horas, 7 dias por semana, 365 dias por ano	A Contratada deverá trabalhar continuamente e até que o serviço seja restaurado completamente ou até que uma solução temporária seja adotada, restabelecendo o o serviço.
3	Baixa	1 dia (Envio de primeiro diagnóstico do problema)	8 horas, 5 dias por semana, em horário comercial	A Contratada deverá despender todo o esforço razoável para solucionar o chamado, sem compromisso em tempo de solução.

4.3.2.2.13. Os níveis de chamados classificam-se de acordo com a tabela abaixo:

Nível	Identificação	da	Descrição
-------	---------------	----	-----------

	Severidade	
1	Alta = Serviço de Alta Criticidade igual a Crítica	<p>O usuário não consegue utilizar o serviço, por indisponibilidade do mesmo.</p> <p>Qualquer suspeita de falha na política de segurança, ameaçando a confidencialidade e integridade dos dados, a disponibilidade dos serviços, que ocasione impacto significativo na aplicação.</p> <p>Qualquer incidente que ocasione impacto à imagem do Serpro.</p> <p>Um incidente de severidade de nível 2 que impacte número significativo (30% do total) de usuários.</p>
2	Média = Serviço de Média Criticidade	<p>Sérios problemas com um impacto importante em toda, ou parte da, operação do Serviço provido.</p> <p>O serviço está parcialmente interrompido ou severamente degradado, porém sem impacto no negócio.</p>
3	Baixa = Serviço de Baixa Criticidade	<p>Problemas de baixa severidade que não afetam o compromisso de SLA ofertado pela Contratada .</p>

4.3.2.2.14. A CONTRATANTE deverá atender minimamente aos tempos de restauração de serviço descritos na tabela abaixo, em caso de falha no sistema:

Severidade	Tempo para Solução Contorno	Tempo para Solução Definitiva (sem defeito de HW)	Tempo para Solução Definitiva (com defeito de HW)
1	Alta	4 horas	3 dias úteis
2	Média	1 dia	7 dias úteis
3	Baixa	3 dias	20 dias úteis

		corridos		
--	--	----------	--	--

4.3.2.2.14.1. A tabela acima é aplicável a todo o Sistema Denatran de Telecomunicações (HLR, SMSC, SGW, OTA e Mediador) referente ao atendimento ao projeto SIMRAV.

4.3.2.2.15. A critério do SERPRO, os chamados poderão ter seu grau de severidade revisado (Escalação da Severidade) após o atendimento inicial pela CONTRATANTE.

4.3.2.2.15.1. Os chamados classificados com severidade 2 e 3, sem correção definitiva ou solução de contorno nos prazos acordados, serão automaticamente escalados para o nível de severidade imediatamente superior, ou seja, um chamado de severidade 2, enquadrado nesta situação será automaticamente escalado para severidade 1;

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

4.3.2.2.16. O tempo de atendimento começa a contar a partir do acionamento inicial realizado junto ao Service Desk da CONTRATANTE.

4.3.2.2.17. A CONTRATANTE deverá trabalhar, ininterruptamente, na solução dos problemas críticos até que o equipamento contratado esteja novamente operando em regime normal de produção. Caso a solução do problema reportado exija a presença de analista(s) da CONTRATANTE no local de instalação do equipamento, mesmo fora do horário comercial, este(s) deverá(ão) ficar dedicado(s) à resolução do problema até que este esteja resolvido.

4.3.2.2.18. Os chamados considerados como de Severidade 1 e 2 deverão ser encaminhados diretamente para o segundo nível de atendimento pela CONTRATANTE.

4.3.2.2.19. O suporte técnico para chamados de Severidade 1 e 2 não pode ser interrompido até o completo restabelecimento de todas as funções do sistema paralisado (indisponível), mesmo que para isso tenha que se estender por períodos noturnos e/ou dias não úteis (sábados, domingos e feriados).

4.3.2.2.20. A CONTRATANTE deverá garantir os serviços de suporte a customização, parametrização e configuração voltadas à utilização de funcionalidades disponibilizadas na versão corrente do software ou em novas versões lançadas durante a vigência da garantia para todos os produtos feitos disponíveis no ambiente de produção, com prazo máximo de atendimento de 72 horas após a abertura do chamado.

4.3.2.2.21. Considera-se um problema plenamente solucionado quando os sistemas e serviços forem restabelecidos sem restrições e de forma definitiva, ou seja, quando não se tratar de uma resolução paliativa.

4.4. Gerenciamento do Contrato

4.4.1. Das obrigações da CONTRATANTE

4.4.1.1. Entregar equipamentos NOVOS, SEM USO. Todas as especificações devem estar plenamente disponíveis nos produtos entregues, como por exemplo: novas versões de softwares, dispositivos complementares, chaves e/ou licenças.

4.4.1.2. Garantir o pleno funcionamento da solução responsabilizando-se por fornecer quaisquer componentes adicionais que sejam necessários ao funcionamento dos equipamentos na configuração especificada, e dentro das condições estabelecidas neste documento, inclusive partes elétricas e mecânicas, ferragens, cabos e conectores. Todos os equipamentos devem ser

entregues e instalados em racks padrão 19", com rodas para movimentação e fechados com portas removíveis, em quantidades suficientes para acomodação de toda a solução.

4.4.1.3. Promover a instalação e configuração de todos os componentes e placas dos equipamentos, inclusive a conexão física e lógica, que abrange a conexão dos cabos do meio de transmissão de dados disponibilizado pelo SERPRO e dos cabos de conexão aos demais equipamentos já instalados naquele nó de comunicações, deixando-os em perfeitas condições de uso.

4.4.1.4. Providenciar a correção em até 5 (cinco) dias corridos, contados a partir da

notificação da ocorrência por parte do SERPRO, de quaisquer defeitos de operação, constatados durante a instalação do equipamento. Caso não seja possível a correção, fica a CONTRATANTE obrigada a substituir o dispositivo.

4.4.1.5. Responsabilizar-se por toda e qualquer despesa, independente da sua natureza, decorrente das instalações supra mencionadas.

4.4.1.6. Durante a o período de funcionamento do sistema, a CONTRATANTE, deverá prover os serviços de escalonamento dos chamados abertos seguindo a estrutura abaixo:

A) SERVICE DESK

- Abertura da ocorrência (através do contato telefônico, e-mail ou web);
- Coleta das informações referente à ocorrência, possibilitando sua abertura;
- Fornecimento do número da ocorrência ao SERPRO;
- Escalonamento gerencial da ocorrência, conforme tempo de retorno definido com o SERPRO;
- Verificação das respostas de pesquisas de satisfação com o SERPRO.

B) PRIMEIRO NÍVEL

- Acesso à base de dados de Conhecimento (Problemas Característicos), detalhando ações tomadas, descrição do problema, códigos de erro;
- Definição do nível de prioridade junto com o SERPRO;
- Troubleshooting simples;
- Localização da falha e respectivo equipamento;
- Aplicação de soluções documentadas e utilizadas em outros eventos;
- Escalonamento da ocorrência para o segundo nível.

C) SEGUNDO NÍVEL

- Avaliação das ações tomadas pelo primeiro nível de suporte;
- Troubleshooting avançado, técnicas de resolução de problemas e coleta de informações mais detalhadas;
- Suporte às soluções de negócios do SERPRO;
- Desenvolvimento e implementação de soluções provisórias (Workaround);
- Escalonamento do problema para o terceiro nível;
- Acompanhamento, análise e implementação da solução dada pelo terceiro nível.

D) TERCEIRO NÍVEL

- Serviços executados pelo fabricante, por profissionais certificados no produto ofertado. Os chamados abertos com o nível de prioridade "ALTA" deverão sempre ser tratados nesse nível.

4.4.2. Requerimentos da solução

4.4.2.1. Requerimentos Gerais:

4.4.2.1.1. A CONTRATANTE deverá ser responsável por todos itens requeridos para a integração entre os elementos que compõem a solução por ela proposta e os elementos de rede das Operadoras de Telefonia do Serviço Móvel Pessoal (SMP) envolvidas no Projeto Denatran SIMRAV, utilizando a infraestrutura de rede do SERPRO.

4.4.2.1.2. A CONTRATANTE deverá disponibilizar todos os itens requeridos para a integração entre os elementos que compõem a solução por ela proposta e os elementos de processamento e controle de dados proprietário do SERPRO (ambiente gerado das requisições de aprovisionamento, ativação e desativação).

4.4.2.2. Dimensionamento e Qualificação

4.4.2.2.1. A solução deve implementar no mínimo 7.200.000 (sete milhões e duzentos mil) novos cartões SIM245 cadastrados no sistema.

4.4.2.2.2. A solução deve ser escalável para 100.000.000 (cem milhões) de cartões SIM245 cadastrados no sistema.

4.4.2.2.3. A solução ofertada pela CONTRATANTE deve garantir a interoperabilidade dos serviços específicos relativos ao projeto SIMRAV.

4.4.2.3. Disponibilidade

4.4.2.3.1. A solução deve gerenciar falhas em componentes individuais de hardware e

software, falhas de componentes de alimentação de energia ou outros tipos de desastres inesperados, atendendo aos requerimentos exigidos.

4.4.2.3.2. A solução deve atender ao índice de 99,999% (noventa e nove vírgula novecentos e noventa e nove por cento) de disponibilidade.

4.4.2.3.3. A CONTRATANTE deve utilizar uma solução de Alta Disponibilidade que garanta, através de elementos redundantes, a correta continuidade dos processos na presença de falhas.

4.4.2.3.4. A solução deve dispor de funcionalidade de recuperação automática do sistema em caso de falhas.

4.4.2.3.5. A solução deve permitir intervenção manual em caso de falhas, quando um dos elementos da mesma não for recuperado automaticamente.

4.4.2.3.6. A CONTRATANTE deve prover a solução completa de backup & restore (HW e SW).

4.4.2.4. Segurança

4.4.2.4.1. A CONTRATANTE deve garantir que todos os elementos da solução sejam instalados com, e apenas com, os serviços requeridos para o perfeito funcionamento da solução.

4.4.2.4.2. A CONTRATANTE deve ajustar o nível de segurança do Sistema Operacional e das aplicações de todos os elementos da solução proposta, mantendo-os em conformidades com os padrões estabelecidos pelo SERPRO. Todos os corretivos de segurança devem ser instalados.

4.4.2.4.3. O SERPRO terá o direito de realizar auditorias periódicas na solução, visando certificar o nível de segurança de todos os elementos.

4.4.2.4.4. A CONTRATANTE deve responsabilizar-se por qualquer intervenção que demande instalação de corretivos de segurança.

4.4.2.4.5. Todos os elementos providos na solução devem permitir o armazenamento do histórico, em logs, de todas as tentativas de acesso finalizadas em falha ou sucesso.

4.4.2.4.6. A solução deve implementar comunicação criptografada entre cliente/servidor, bem como, implementar o armazenamento criptografado dos dados críticos do sistema.

4.4.2.4.7. A solução não deve permitir acesso simultâneo do mesmo usuário no sistema.

4.4.2.4.8. A solução deve identificar, de forma única, cada sessão de usuário que acesse o sistema.

4.4.2.4.9. A informação da identificação da sessão deve ser expirada após o primeiro uso, sendo renovada a cada novo acesso do usuário no sistema.

4.4.2.4.10. A solução deve dispor de configuração de tempo máximo de inatividade da sessão, expirando a mesma após atingir o intervalo configurado.

4.4.2.4.11. A CONTRATANTE deve dispor de conexão remota ao SERPRO por intermédio de VP; via link internet, estando o mesmo disponível 24x7. Essa comunicação será utilizada para acesso tratamento de incidentes pela equipe de suporte da CONTRATANTE.

4.4.2.4.12. A CONTRATANTE será responsável por todo o gerenciamento de peças de reposição (Gerenciamento de Sobressalentes), garantindo a rápida disponibilidade de peças sobressalentes e organizando a substituição e recuperação da parte com defeito. A CONTRATANTE deve atender ao prazo de próximo dia útil para reposição do hardware com 95% de precisão.

4.4.3. Requerimentos Operacionais

4.4.3.1. Relatórios e Estatísticas

4.4.3.1.1. A solução deve dispor de histórico de eventos que permitam a investigação de qualquer tipo de falha.

4.4.3.1.2. A solução deve implementar as seguintes funcionalidades:

4.4.3.1.2.1. SNMP MIBs para alarmes de hardware

4.4.3.1.2.2. SNMP MIBs para alarmes da aplicação

4.4.3.1.2.3. SNMP traps

4.4.3.1.2.4. Interface gráfica para gestão dos alarmes

4.4.3.1.2.5. Interface gráfica para configuração

4.4.3.2. Suporte e Manutenção

4.4.3.2.1. A CONTRATANTE deve ofertar serviço de suporte, manutenção e monitoramento por meio de equipes baseadas em território nacional e capazes de comunicar-se em língua portuguesa, a fim de facilitar e agilizar possíveis interações com as equipes do SERPRO.

4.4.3.2.2. A CONTRATANTE deve testar exaustivamente todos os corretivos antes de aplicá-los na solução.

4.4.3.2.3. A CONTRATANTE deve prover e instalar todos as ações corretivas sem custos adicionais para o SERPRO.

4.4.3.2.4. A CONTRATANTE deve dispor de interface web para gestão e abertura de chamados.

4.4.3.2.5. A CONTRATANTE deve prover claramente o canal para solicitação de ajuste de prioridade de incidentes.

4.4.3.2.6. A CONTRATANTE deve prover serviço de manutenção preventiva, com entrega de relatórios periódicos indicando possíveis impactos na solução.

4.4.3.2.7. A CONTRATANTE deve prover canal telefônico com disponibilidade 24x7 para abertura de chamados.

4.4.3.2.8. A CONTRATANTE deve dispor de canal de relacionamento com o cliente, realizando consultas periódicas ao SERPRO quanto à qualidade da solução e serviços ofertados.

4.4.3.2.9. A CONTRATANTE deve realizar revisões presenciais na solução semestralmente.

4.4.3.2.10. A CONTRATANTE deve prover relatórios mensais informando todos os incidentes abertos no período, bem como, o status e ações da resolução dos mesmos.

4.5. Serviço de Operação da plataforma de Telecomunicações para atendimento ao projeto SIMRAV

4.5.1. A CONTRATANTE deverá prover toda a operação do sistema durante todo o período de funcionamento do mesmo.

4.5.2. O serviço de Operação deve ser provido em modelo 8x5 (horário comercial e dias úteis). Com a presença física de no mínimo um técnico no local de instalação da plataforma de gerência.

4.5.3. A CONTRATANTE deverá prover relatório mensal ao SERPRO informando as ações tomadas durante este período.

4.6. Prazo para disponibilização da Infraestrutura pela CONTRATANTE

4.6.1 O prazo para disponibilização da infraestrutura pela CONTRATANTE será de até 60 (sessenta dias) após a assinatura do contrato.

CLÁUSULA QUINTA – DO REPRESENTANTE DA ADMINISTRAÇÃO

Ficam desde já designados como Representantes da Administração pela CONTRATANTE o Sr(a) xxxxxxxxxxxxxxxxxxxxxx e pela CONTRATADA o Sr(a) xxxxxxxxxxxxxxxxxxxxxx, para acompanharem, fiscalizarem e para atestarem a prestação dos serviços e obrigações decorrentes deste Contrato e na sua falta o seu substituto formal.

CLÁUSULA SEXTA – DO REGIME DE EXECUÇÃO

A execução deste Contrato ocorrerá sob a modalidade de empreitada por preço global.

CLÁUSULA SÉTIMA – DA EXECUÇÃO E DO VALOR

7.1. O valor dos serviços, objeto do presente Contrato, ficam estabelecidos na forma desta

Cláusula:

7.1.1. VALOR TOTAL DO CONTRATO

Para a prestação dos serviços de *Colocation e Hosting*, objeto deste contrato o valor importa em R\$ xxxxxxxx (xxxxxxxxxx) mensais, referentes a alocação de xx racks, a serem pagos contra a apresentação de faturas. Considerando o período de vigência, o valor total do contrato é de R\$ XXXXXX (XXXXXX).

7.1.2. CONDIÇÕES DE PAGAMENTO

O pagamento deverá ser efetuado pela CONTRATANTE ao CONTRATADO, mensalmente com base nos serviços efetivamente executados e consoante a respectiva comprovação dos serviços discriminados nas Notas Fiscais atestadas pela CONTRATANTE e executada pelo CONTRATADO.

7.1.2.1 Para fins de pagamento, considerar-se-á efetivamente executado pela CONTRATADA, o serviço objeto do presente contrato, a partir do início da prestação dos serviços especializados de Tecnologia da Informação para Produção do Sistema Integrado de Monitoramento e Registro Automático de Veículos (SIMRAV), previsto no Contrato RG 47796 (Ctr 1/2011), firmado entre o SERPRO e o Denatran.

7.1.3. COMPOSIÇÃO DO PREÇO GLOBAL POR SERVIÇOS

O valor a ser pago pelo CONTRATANTE para hospedagem de sua solução será proporcional ao espaço físico ocupado nas dependências da CONTRATADA, sendo a unidade padrão de referência estabelecida como múltiplos de rack em bastidor padrão 19 ou 21 polegadas.

O preço estabelecido será de R\$ 50.000,00 reais/mensal por rack hospedado, incluindo o espaço necessário para a instalação de fontes de alimentação, retificadores etc.

CLÁUSULA OITAVA – DEMAIS CONDIÇÕES DE PAGAMENTO

8.1. Toda fatura emitida pelo CONTRATADO, deverá ser atestada pela CONTRATANTE no prazo máximo de 5 (cinco) dias de sua apresentação, ou recusada, caso haja discordância. No caso de discordância pela CONTRATANTE, esta deverá devolvê-la ao emitente, com as justificativas, por escrito, no prazo máximo de 24 (vinte e quatro) horas;

8.2. Toda fatura emitida pelo CONTRATADO será paga no prazo de 15 (quinze) dias, contados a partir da data de sua recepção, pelo CONTRATANTE;

8.3. Caso o CONTRATANTE, no local da prestação do serviço e/ou do pagamento, for responsável legal, pela retenção e recolhimento do Imposto Sobre, Serviços de Qualquer Natureza – ISSQN na fonte deverá encaminhar, no prazo estabelecido, o correspondente documento de Declaração de Retenção e Recolhimento do Imposto (ISSQN) para a Regional Brasília, situada na SGAN Quadra 601, Módulo “G”, estabelecimento do CONTRATADO;

8.4. O CONTRATANTE efetuará a liquidação dos valores devidos, através de GRU – Guia de Recolhimento da União, que seguirá juntamente com a Fatura e Nota Fiscal de Serviços, emitida.

8.5. Caso a fatura não seja paga em até 30 (trinta) dias, contados a partir da data da sua apresentação, o valor da fatura será atualizado pela aplicação pró-rata temporis do INPC-

IBGE, do mês ou meses que contemplem os dias em atraso.

CLÁUSULA NONA – DAS PENALIDADES

9.1. Pela não observância ou descumprimento das cláusulas pactuadas nesse Contrato, fica a parte infringente, sujeita às seguintes penalidades:

- a) advertência;
- b) aplicação de 2% (dois por cento) de multa sobre o valor do serviço não prestado, pelo não cumprimento, mesmo que parcial, do objeto e prazos estipulados neste Contrato.

Subcláusula Primeira – As sanções previstas nos itens “a” e “b” acima poderão ser aplicadas desde que facultada a defesa prévia do interessado, no respectivo processo, no prazo de 5 (cinco) dias úteis.

CLÁUSULA DÉCIMA – DO ATRASO DO PAGAMENTO

10.1 Não ocorrendo o pagamento pela CONTRATANTE dentro do prazo estipulado neste Contrato, fica a CONTRATANTE sujeita às penalidades abaixo relacionadas:

- a) o valor devido será acrescido de multa de 2% (dois por cento) e juros de mora de 1% (um por cento) ao mês, *pró rata die* correspondente aos dias em atraso;
- b) suspensão dos serviços prestados pelo CONTRATADO até a devida quitação dos valores devidos e em atraso; e
- c) declaração de sua inidoneidade no Cadastro de Inadimplentes do Governo Federal (CADIN).

CLÁUSULA DÉCIMA PRIMEIRA – DE REAJUSTAMENTO

11.1. Mediante acordo entre as partes, os preços definidos serão reajustados após um ano de vigência do Contrato, visando manter sua compatibilidade com a Política de Preços adotada pelo SERPRO, com base na variação percentual do IGPM ou outro índice que venha substituí-lo.

CLÁUSULA DÉCIMA SEGUNDA – DA VIGÊNCIA

12.1. O prazo de vigência do presente Contrato será de 60 (sessenta) meses e entrará em vigor a partir da data de sua assinatura.

CLÁUSULA DÉCIMA TERCEIRA – DO ADITAMENTO E ALTERAÇÕES

13.1. O presente Contrato poderá ser aditado ou alterado no todo ou em qualquer de suas cláusulas, dentro do prazo de vigência, por meio de Termo Aditivo, numerado em ordem crescente e publicado no Diário Oficial.

CLÁUSULA DÉCIMA QUARTA – DAS DISPOSIÇÕES GERAIS

14.1. Todas e quaisquer alterações que venha a ocorrer nas relações comerciais entre o CONTRATADO e a CONTRATANTE, deverão imediatamente ser formalizadas por instrumento de Termo Aditivo a este Contrato, e que fará parte integrante deste.

14.2 Da Confidencialidade

14.2.1 – A CONTRATANTE obrigará-se a manter a mais absoluta confidencialidade, mesmo após a eventual rescisão do contrato, sobre todas as informações relativas à:

a) Política de segurança adotada pelo SERPRO e configurações de hardware e software decorrente;

b) Processo de instalação e configuração de produtos, ferramentas e equipamentos, em atendimento aos itens de segurança, constantes da proposta;

c) Quaisquer dados que a CONTRATANTE venha a ter conhecimento em decorrência da presente contratação, pertinentes a hardware, software, serviços e sistemas aplicativos ao SERPRO, cujo conhecimento por terceiros exponha o ambiente a riscos de invasão ou resulte na vulnerabilidade do mesmo.

d) Processo de implementação no ambiente do SERPRO de mecanismos de criptografia e autenticação adotados na solução;

14.2.2 – Ficará a CONTRATANTE terminantemente proibida de fazer uso ou revelação, sob qualquer justificativa, a respeito de quaisquer informações, dados, processo, fórmulas, códigos, cadastro, fluxogramas, diagramas lógicos, dispositivos, modelos ou outros materiais de propriedade do SERPRO aos quais tiver acesso em decorrência da presente contratação.

14.2.3 – As questões pertinentes aos negócios do SERPRO, tais como propriedade e conhecimentos tecnológicos e segredos industriais/comerciais que eventualmente passarem pela apreciação dos profissionais da CONTRATANTE, deverão ser tratadas da mesma forma com que são tratados os dados econômicos e financeiros dos quais tomarem conhecimento nas demais áreas de atuação, dentro do mais absoluto sigilo profissional.

14.2.4 - Os empregados da CONTRATANTE deverão obedecer as normas sobre confidencialidade e segurança, internas e externas, adotadas pelo SERPRO, além das cláusulas específicas constantes deste instrumento.

14.2.5 – A violação desta cláusula ensejará a rescisão do contrato vigente, sem prejuízo das demais penalidades cabíveis, previstas em Lei.

14.2.6 – Por descumprimento das obrigações relacionadas com a confidencialidade e segurança dos dados, de informações e sistemas, mediante ações ou omissões, intencionais ou acidentais que impliquem em perda, destruição, inserção, cópia, acesso ou alterações indevidas, independentemente do meio no qual estejam armazenados, em que trafeguem ou do ambiente em que estejam sendo processados, a CONTRATANTE determinará a responsabilização, na forma da Lei, de seus dirigentes e funcionários envolvidos.

CLÁUSULA DÉCIMA QUINTA – DA MODIFICAÇÃO E DA RESCISÃO

15.1. São causas que podem determinar a rescisão do instrumento contratual:

a) o não cumprimento ou cumprimento irregular de quaisquer das obrigações contratuais;

b) a lentidão no seu cumprimento, levando a parte lesada a presumir a não conclusão das obrigações assumidas;

c) o atraso injustificado, superior a 30 (trinta) dias na execução dos serviços, sem que caiba direito algum ao contratado mesmo que a obrigação tenha sido parcialmente

cumprida;

d) paralisação dos serviços sem justa causa e prévia comunicação ao CONTRATANTE;

e) o cometimento reiterado de faltas na execução dos serviços;

f) o presente contrato poderá ser rescindido, na forma e na ocorrência de qualquer das hipóteses previstas no art.77 a 80 da Lei 8.666/93.

15.2. A rescisão do instrumento contratual poderá ser:

a) por acordo entre as partes;

b) judicial, nos termos da legislação pertinente.

15.3. Na hipótese de rescisão a que se refere a alínea “d” do item 15.1 será o CONTRATADO ressarcido dos prejuízos, regularmente comprovados, que houver sofrido, tendo ainda, direito aos pagamentos devidos pela execução do contrato até a data da rescisão.

CLÁUSULA DÉCIMA SEXTA – DA PUBLICAÇÃO

16.1 A publicação do presente Contrato no Diário Oficial da União, deverá ser feita pela CONTRATADA, no prazo de até o 5o. (quinto) dia do mês subsequente à data de sua assinatura.

CLÁUSULA DÉCIMA SÉTIMA – DO FORO

17.1 Fica eleito o foro de Brasília, Distrito Federal como competente para dirimir quaisquer questões oriundas do presente contrato, com exclusão de qualquer outro, por mais privilegiado que seja.

E assim por estarem justas e contratadas, assinam o presente Termo, em 3 (três) vias de igual teor e forma, para os mesmos fins e efeitos de direito, na presença das testemunhas infraqualificadas.

Brasília, ____ de _____ de 2012

PELA CONTRATANTE:

NOME:

ASSINATURA : _____

PELO SERPRO:

NOME:

ASSINATURA: _____

TESTEMUNHAS:

NOME: _____ NOME: _____

CPF: _____ CPF: _____

ASSINATURA: _____ ASSINATURA: _____