

# **Projeto Básico SUPSI 01078/2010**

## **Título**

### **Consulta Pública para Aquisição de Solução para implementar o Sistema SIMRAV**

#### **1ª Versão**

## **1.0 Objeto**

Aquisição de solução completa englobando Hardware, Software e Serviços, inclusive o gerenciamento, para implementar o Sistema SIMRAV.

## **2.0 Especificação do Objeto a ser Contratado**

I - A arquitetura da solução a ser adquirida é composta por:

### **2.1. Plataforma HLR (*Home Location Register*) - 02 HLRs em Cluster**

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

2.1.2. A plataforma ofertada 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 ofertada 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 falhas, garantindo assim o nível de disponibilidade Carrier Class de 99,999%.

2.1.4. A plataforma ofertada deve ser escalável para 100.000.000 de usuários cadastrados e 30.000.000 de usuários ativos.

2.1.5. A plataforma ofertada ofertado deverá estar preparado 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

2.1.5.5. Serviços suplementares e outras informações de usuários.

2.1.6. A plataforma ofertada deverá suportar as interfaces padrão através de suporte da sinalização MAP, de acordo com a especificação TS 29.002.

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

2.1.8. A plataforma ofertada 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 (ODBRCF)

#### 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. Authentication Failure Report
- 2.1.9.2.6. Subscriber Data Insertion
- 2.1.9.2.7. Subscriber Data Deletion
- 2.1.9.2.8. HLR Fault Recovery
- 2.1.9.2.9. VLR Fault Recovery
- 2.1.9.2.10. Send Routing Information
- 2.1.9.2.11. Provide Roaming Number

#### 2.1.9.3. Gerenciamento da Base de Dados de Usuários:

- 2.1.9.3.1. Subscriber Definition
- 2.1.9.3.2. Subscriber Deletion
- 2.1.9.3.3. IMSI Change
- 2.1.9.3.4. MSISDN Change
- 2.1.9.3.5. Subscriber Number Query
- 2.1.9.3.6. Dynamic Data Query
- 2.1.9.3.7. Operator Authority Management
- 2.1.9.3.8. Dynamic Subscriber Data Managent
- 2.1.9.3.9. Service Template Setting
- 2.1.9.3.10. Batch Operation
- 2.1.9.3.11. Operation Log Management
- 2.1.9.3.12. Subscriber Statistics

#### 2.1.9.4. Protocolo, Interfaces e padrões:

2.1.9.4.1. MAP Protocols – MAP Phase 1, MAP Phase 2 e MAP Phase 2+

2.1.9.4.2. BOSS Interface

2.1.9.4.3. Application/Data Layer Interface

2.1.9.4.4. M3UA / SIGTRAN

2.1.9.4.5. 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.

2.1.9.4.6. 3GPP, 3GPP TS 29.002.

#### 2.1.9.5. Funções de Operação e Manutenção:

2.1.9.5.1. Security Management

2.1.9.5.2. Performance Management

2.1.9.5.3. Fault Management

2.1.9.5.4. Configuration Management

2.1.9.5.5. Equipment Management

2.1.9.5.6. Interface Signaling Tracing

2.1.9.5.7. Subscriber Signaling Tracing

2.1.9.5.8. Equipment Archive Management

#### 2.1.9.6. Funções de Proteção e Confiabilidade:

2.1.9.6.1. Redundancy and Backup Design

2.1.9.6.2. Power Reliability

2.1.9.6.3. Distributed Boards

2.1.9.6.4. Dual-Plane Communications

2.1.9.6.5. Automatic Fault Detection and Self-Healing

2.1.9.6.6. Automatic/Manual Switchover

2.1.9.6.7. Automatic Multi-Level Backup and Recovery of Subscriber Data

2.1.9.6.8. Flow Control

2.1.9.6.9. Distributed Storage of Subscriber Data

2.1.9.6.10. Automatic Load Sharing Among Modules

#### 2.1.9.7. Serviços de Dados:

2.1.9.7.1. GPRS Services

#### 2.1.9.8. Redundância:

2.1.9.8.1. N+1 Compatibility Redundancy

2.1.9.8.2. Capacidade de implementar HLR lógico

#### 2.1.9.9. Serviços de Segurança:

##### 2.1.9.9.1. Cloned SIM Detection

#### 2.1.9.10. Políticas de Processos:

##### 2.1.9.10.1. MTP Policing

##### 2.1.9.10.2. SCCP Policing

##### 2.1.9.10.3. MAP Policing

#### 2.1.9.11. Funcionalidades de Autenticação:

##### 2.1.9.11.1. Registration, Call attempt,

##### 2.1.9.11.2. Call Delivery,

##### 2.1.9.11.3. Location Update,

##### 2.1.9.11.4. Supplementary service procedure,

##### 2.1.9.11.5. Short Message Service (SMS) transfer

##### 2.1.9.11.6. Location services.

##### 2.1.9.11.7. Algoritmos GSM A3/A8 conforme especificação 3GPP.

##### 2.1.9.11.8. COMP128-Versão 1 conforme especificação 3GPP.

##### 2.1.9.11.9. COMP128-Versão 2 conforme especificação 3GPP.

##### 2.1.9.11.10. COMP128-Versão 3 conforme especificação 3GPP.

##### 2.1.9.11.11. Millenage, conforme especificação 3GPP.

##### 2.1.9.11.12. Algoritmo GSM A4 em sua última versão.

##### 2.1.9.11.13. Autenticação Basic GSM Service

##### 2.1.9.11.14. Autenticação Alternative A4 algorithm

##### 2.1.9.11.15. Autenticação Basic Platform Feature Package

##### 2.1.9.11.16. Autenticação Basic WCDMA Service

2.1.9.11.17. A plataforma deve suportar todos os algoritmos de autenticação listados de forma simultânea.

#### 2.1.9.12. Funcionalidades de sinalização:

2.1.9.12.1. Permitir a redistribuição de carga automática nos links que estão disponíveis no linkset.

2.1.9.12.2. Suporte a link de sinalização de alta velocidade 2Mbit conforme ITU Q703.

2.1.9.12.3. Suporte a Load share em nível SCCP (combinação de routeset) e MTP.

2.1.9.12.4. Implementação de load share para todos destinos SCCP (Global Title) ou MTP3 (Point codes)

2.1.9.12.5. Suporte a Load share entre múltiplos STP usando GTT Alias point code para endereçamento do STP

#### 2.1.9.13. Suporte ao grupo SIGTRAN:

2.1.9.13.1. SCTP de acordo com RFC 2960

2.1.9.13.2. M3UA de acordo com RFC 3332

2.1.9.13.3. Suporte a Multi-signaling-point (Multi-SP)

#### 2.1.9.13.4 Suporte a 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 suportar 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. TIF-CSI (Translation Information Flag CAMEL Subscription Information)

2.1.11.5. U-CSI (USSD CAMEL Subscription Information)

2.1.11.6. UG-CSI (USSD General CAMEL Subscription Information)

2.1.11.7. GPRS-CSI (GPRS CAMEL Subscription Information)

2.1.11.8. SMS-CSI (Short Message Service CAMEL Subscription Information)

2.1.11.9. D-CSI (Dialed Service CAMEL Subscription Information)

2.1.11.10. M-CSI (Mobility Management event CAMEL Subscription Information)

2.1.11.11. VT-CSI (VMSC Terminating CAMEL Subscription Information).

2.1.12. A plataforma deve suportar 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 suportar filtro de endereços SMS.

2.1.15. A plataforma deve suportar a configuração de múltiplos HLRs virtuais no mesmo elemento físico

2.1.16. A plataforma deve suportar no mínimo 254 HLRs virtuais diferentes e independentes entre si.

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

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

2.1.19. A plataforma proposta deverá garantir que a chave de cada usuário será criptografada apenas através dos algoritmos padrão.

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

2.1.21. Arquitetura e Requisitos do Hardware:

2.1.21.1. A plataforma deve ser concebido 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 continua a funcionar normalmente sem grau reduzido de serviço ou a qualidade do serviço.

2.1.21.2. A Arquitetura deve obedecer o 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 ilustração abaixo:  
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 seguintes 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 a permita a replicação da mesma em locais geograficamente separados.

2.1.21.5. Para confiabilidade dos dados deve suportar:

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

2.1.21.5.4. Deve possuir arquitetura de Hardware arquitetura 100% (cem por cento) ATCA.

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 disponibilidade da plataforma ofertada deve ser superior a 99,999%.

2.1.21.5.7. A plataforma ofertada deverá ser hot-swap para todas as placas.

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

2.1.21.5.9. A plataforma ofertada 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 a disponibilidade mínima exigida.

2.1.22.3. A solução a ser ofertada pelo PROPONENTE 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. Suporte a provisionamento em batch em arquivos ASCII enviados via FTP

2.1.23.3. Capacidade de parar um provisionamento em batch por linha de comando

2.1.23.4. Suportar adição/deleção a uma taxa de 2000 comandos/seg

## 2.1.24. Características Construtivas

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

Item	Especificação
Taxa de reparo do sistema	? 0.3%
Disponibilidade	? 99.9999%
Taxa de detecção de falhas	> 95%
Mean time to repair (MTTR)	< 1 h
Tempo de interrupção do service para cada upgrade ou expansão.	< 30 segundos
Média de interrupção do s ervice em um ano.	< 5 minutos
Duração entre a inicialização do sistema e system pronto pra uso.	? 10 minutos
Taxa de sucesso do switchover entre os componentes redundantes.	> 95%
Tempo para realização do switchover entre placas OSTA 1.0	? 3 segundos
Tempo para realização do switchover entre placas OSTA 2.0	? 10 segundos

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

2.1.24.1.2. EN 55022 classe A

2.1.24.1.3. CISPR 22 classe A

2.1.24.1.4. ETSI EN 300 386

2.1.24.1.5. GB9254 classe A

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

2.1.24.1.7. GB 4798

2.1.24.1.8. ETS 300019

2.1.24.1.9. IEC 60721

## 2.1.25. Operação e Manutenção

2.1.25.1. O fornecedor 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 suportar os seguintes recursos de gerenciamento de dados de configuração:

2.1.25.1.1.1.1. Interface MML com função de texto preditivo entrada

2.1.25.1.1.1.2. Controle de autorização por usuário

2.1.25.1.1.1.3. Atribuição de tarefas razoável para fins de operações flexíveis

2.1.25.1.1.1.4. manutenção local, remota e centralizada

2.1.25.1.1.2. O HLR proposto deve suportar os seguintes ações gerenciamento de dados dos simcards:

2.1.25.1.1.2.1. Interface MML com função de texto preditivo entrada

2.1.25.1.1.2.2. Funções além de adição, modificação e exclusão.

2.1.25.1.1.2.3. Armazenamento de logs operacionais de todas ações executadas.

#### 2.1.25.2. Gerenciamento de Desempenho:

2.1.25.2.1. A plataforma proposta deve suportar 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 1 minuto 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 aberta, com função de impressão disponíveis.

2.1.25.2.1.5. Instrumentos de medição de desempenho dedicado 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 ofertada deve suportar as seguintes funcionalidades de gerenciamento de alarmes:

2.1.25.3.1.1. Coletar informações de alarme na ocorrência de algum alarme

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. Realizar tracing de mensagens sobre interfaces padrões do sistema

2.1.25.3.1.6. Manutenção remota da plataforma

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

2.1.25.3.1.8. Diagnóstico automático de falhas de hardware e software



2.1.25.3.1.9. Fornecer interface para informações de log detalhados com ajuda online

2.1.25.3.1.10. Filtros para aplicar nos logs facilitando debug de possíveis problemas

2.1.25.4. Gerenciamento de Sinalização (Tracing)

2.1.25.4.1. A plataforma proposta deverá entregar funções de tracing de sinalização sem qualquer dispositivo adicional de teste de sinalização.

2.1.25.4.2. Realizar o tracing de mensagens sobre interfaces padrão e armazenar as mensagens rastreadas, o armazenamento das mensagens rastreadas

2.1.25.4.3. Realizar o tracing de mensagens de IMSI / MSISDN assim como suportar a função multi-usuário.

2.1.25.4.4. Fornecer interface gráfica onde é possível realizar a gestão de rastreamento do HLR verificando os dados e eliminando as falhas de mensagens de sinalização.

2.1.25.4.5. gestão de rastreamento do HLR / AUC deve apoiar as funções como segue:

2.1.25.4.5.1. A plataforma ofertada deve possuir a funcionalidade de identificar um específico simcard (IMSI ou MSISDN) em um sistema centralizado de gerenciamento de tracing.

2.1.25.4.5.2. Possuir mensagens detalhadas e explicativas das mensagens de sinalização presentes no trace.

2.1.25.5. Gerenciamento de Segurança

2.1.25.5.1. A plataforma deve suportar gerenciamento de autoridade e gerenciamento de logs:

2.1.25.5.1.1. Gerenciamento de autoridade:

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

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

2.1.25.5.1.2. Gerenciamento de logs:

2.1.25.5.1.2.1. Deve ser possível habilitar o log de todas operações MML

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

2.2. SGW(Signaling gateway) - 02 Gateways em Cluster

2.2.1. Requisitos do Gateway de Sinalização

2.2.1.1. O SGW deve ser modular e escalável em sua arquitetura.

2.2.1.2. O SGW deve implementar Roteamento baseado em MSISDN/IMSI para um mínimo de 5.000.000 de acessos

2.2.1.3. O SGW deve implementar FNR (Flexible Number Routing) utilizando SRF de acordo com padrão 3GPP TS23.066

2.2.1.4. O SGW deve suportar SS7 FIREWALL

2.2.1.5. O SGW deve suportar Roteamento SMS

2.2.1.6. O SGW deve suportar Filtro SMS

2.2.1.7. O SGW deve suportar Conversão de protocolos ITU e ANSI

- 2.2.1.8. O SGW deve suportar Lista branca&negra
- 2.2.1.9. O SGW deve suportar Number transform
- 2.2.1.10. O SGW deve suportar Terminal Information Collector (TIC)
- 2.2.1.11. O SGW deve suportar Enhanced Routing Function
- 2.2.1.12. O SGW deve suportar IN voice call Bypass
- 2.2.1.13. O SGW deve suportar IN SMS Bypass
- 2.2.1.14. O SGW deve suportar International roaming and SIMM with IN
- 2.2.1.15. O SGW deve suportar Preferred network
- 2.2.1.16. O SGW deve suportar SUA function
- 2.2.1.17. O SGW deve suportar CDR function
- 2.2.1.18. O SGW deve suportar CFS function
- 2.2.1.19. O SGW deve suportar NTP function
- 2.2.1.20. O SGW deve suportar replicação de sinalização, ou seja, existir a possibilidade de quando houver um encaminhamento da mensagem de sinalização, o SGW pode copiá-la e encaminhá-la para um destino terceiro.
- 2.2.1.21. O SGW deve suportar o serviço de lista negra para 5.000.000 de entradas
- 2.2.1.22. A Base de dados com as entradas da lista negra deverá obrigatoriamente ser interna ao SGW.
- 2.2.1.23. O SGW deve possuir processamento dos links narrowband e boradband na mesma placa de processamento.
- 2.2.1.24. O SGW deve possuir disponibilidade de 99,999%.
- 2.2.1.25. O SGW deve obrigatoriamente ser carrier-class.
- 2.2.1.26. O SGW deve ter capacidade mínima de 2500 consultas por segundo a base de dados.
- 2.2.2. O SGW deverá possui 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 suportar SS7 Signalling Connection Control Part (SCCP,Global Title routing)
  - 2.2.3.1. SCCP é um protocolo de roteamento de camada 4 na pilha de protocolos SS7. O SCCP provê serviços orientados e não orientados a conexão sobre MTP de nível Enquanto no MTP nível 3 as mensagens são roteadas com base nos endereços "Point Code", o SCCP provê um sistema de numeração que permite que as mensagens sejam endereçadas para aplicações específicas ou subsistemas na rede de destino. O SCCP também permite que o STP possa realizar o procedimento de Global Title Translation, onde o ponto de destino (DPC) e o número do subsistema ( SSN ) é determinado por determinados dígitos presentes nas mensagens de sinalização.

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. Suportar 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

2.2.4.1.4 Controle de Congestionamento SCCP

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

2.2.4.1.6. Suportar as recomendações ITU-T Q.711 a Q.714

2.2.4.1.7. Offload de mensagens SMS sobre rede IP;

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

2.2.4.1.9. O SGW deverá suportar a funcionalidade SS7 TCAP, requerido para suportar 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 suportar 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 sub-dividida 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

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.

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/SUA acc. to IETF RFC 3868

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

2.2.9. O SGW deve suportar as capacidades mínimas abaixo:

Item	Valor
Número de links LSL (64-kbit/s)	>5000
Número de links HSL (2Mbit/s)	>600
Capacidade de GT	>180000
Número de DPCs suportados	>1800

2.2.9.1.O SGW deve suportar as performances mínimas abaixo:

Item	Index
Tráfego sobre links de 64-kbit/s	>0.85Erl
Tráfego sobre links de 2-Mbit/s	>0.85Erl
Tráfego sobre links de 1.544-Mbit/s	>0.80Erl
Atraso de transferência de mensagens	<15ms
Capacidade de processamento das mensagens	>3000000 MSU/s
Capacidade GTT para links de 64-kbit/s	>75GTT/s
Capacidade GTT para links de 2-Mbit/s	>2256GTT/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. Suportar comandos MML e interface GUI

#### 2.2.10.1.11. Implementar ferramenta que permita realizar o trace de sinalização devendo:

##### 2.2.10.1.11.1. Trace de sinalização online e em tempo real;

##### 2.2.10.1.11.2. Filtro de sinalização online e em tempo: Métodos de filtragem devem ser configuráveis através de: DPC, OPC, SI, NI, H0, H1, SLS, CIC e direção da mensagem;

- 2.2.10.1.11.3. Decodificação detalhada da sinalização: Detalhar a mensagem SS7 no nível de usuário: TUP/ISUP/MAP/INAP;
- 2.2.10.1.11.4. Armazenamento do histórico dos traces;
- 2.2.10.1.11.5. Capacidade de executar o trace em links parciais, linksets ou todos os links.
- 2.2.11. Backup das bases de dados aprovisionadas 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
    - 2.2.12.1.6. MTP Accounting incl. Postprocessing of MTP Accounting
    - 2.2.12.1.7. Incoming Linkset Screening
    - 2.2.12.1.8. OPC/DPC/SIO Screening
    - 2.2.12.1.9. MTP Gateway Screening
    - 2.2.12.1.10. MSU criteria for duplication
    - 2.2.12.1.11. Administration for M3UA
    - 2.2.12.1.12. 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 Accounting
    - 2.2.12.2.6. SCCP Measurements
    - 2.2.12.2.7. SCCP Gateway screening
    - 2.2.12.2.8. SCCP criteria for duplication
    - 2.2.12.2.9. Função de teste de GT
- 2.2.13. Padrões e Protocolos Suportados:
  - 2.2.13.1. ISUP Compliance
    - 2.2.13.1.1. Q.761 Functional Description of ISDN User Part
    - 2.2.13.1.2. Q.761 General Functions of Messages and Signals
    - 2.2.13.1.3. Q.763 Formats and Codes
    - 2.2.13.1.4. Q.764 Signalling Procedures

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

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

2.2.14.10. Q.710 Simplified MTP Version for Small Systems

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. ETSI CS1S2 compatible network specific INAP

2.2.17.2. CAP phase 1 -2

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. SCCP User Adaptation layer (SUA) according to RFC 3868 and ETSI TS 102 143.

2.2.18.4. 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 4129 – DPNSS e DASS2 Extensions to IUA Protocol
- 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;
- 2.2.19.8. Implementar a RFC 4166 – Telephony Signalling Transport over SCTP Applicability Statement
- 2.2.19.9. Implementar a RFC 3868 – Signalling Connection Control Part User Adaptation Layer (SUA)
- 2.2.19.10. 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 patch's 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. A PROPONENTE deve ofertar todas as funcionalidades especificadas para o Gateway de Sinalização em um equipamento dedicado (Stand Alone) para esta função.

### 2.3. SMSC (*Short Message System Center*)

- 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 de SMSC (Short Message Service Center) deve disponibilizar interface para a interconexão com as plataformas de Short Message de outras operadoras com tecnologia TDMA (IS-136), CDMA (IS-637), GSM (3GPP 23.040) e 3G através do protocolo SMPP.
- 2.3.4. A plataforma deve possibilitar interface WEB , envio de mensagens broadcast, envio de mensagens para códigos especiais, envio de notificação de chamada perdida.
- 2.3.5. A solução oferecida deve ser totalmente aderente às seguintes especificações, em suas últimas versões:
  - 2.3.5.1. TIA/EIA/ANSI-41-B/C/D, Cellular Radio telecommunications Intersystem



Operations.

2.3.5.2. TIA/EIA/IS-637-A, Short Message Service for Spread Spectrum Systems.

2.3.5.3. ANSI/TIA/EIA/664, Cellular Features Description.

2.3.5.4. TIA/EIA IS-725 Revision A, ANSI-41-D Enhancements for Over-The-Air Service Provisioning (OTASP) & Over-The-Air Parameter Administration (OTAPA).

2.3.5.5. TIA/EIA IS-683 Revision A, Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Systems.

2.3.5.6. SIP - Session Initiation Protocol

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

2.3.6.1. Especificações do 3GPP2 (TSG-A, TSG-C, TSG-P, TSG-R, TSG-S, TSG-N etc.);

2.3.6.2. Especificações do SMS Forum (SMPP).

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

2.3.6.3.1. Processamento de mensagens;

2.3.6.3.2. Sinalização ANSI-41

2.3.6.3.3. Sinalização SMPP (versão 3.4)

2.3.6.3.4. Partição de carga dos enlaces de sinalização;

2.3.6.3.5. Interface gráfica homem-máquina;

2.3.6.3.6. Padrão SNMP para sistema de gerencia

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

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

2.3.6.3.9. Centralização da base de dados;

2.3.6.3.10. Tolerância a falhas funcionando em cluster modo active-standby.

2.3.6.3.11. 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.

2.3.6.3.12. A plataforma deve suportar capacidade nominal de 250 MDAS (Message Delivery Attempt por segundo).

2.3.6.3.13. A plataforma deve suportar capacidade de 5.000.000 de assinantes.

2.3.6.3.14. A plataforma deve suportar capacidade de 2\*73Gb de banco de dados.

2.3.6.3.15. A plataforma deve suportar 25Mbit/s de enlaces de sinalização M3UA.

2.3.6.3.16. A plataforma deve suportar os padrões de interfaces SMPP e SMPP+ e TCP/IP

## 2.4. PLATAFORMA DE GERÊNCIA

### 2.4.1. Requerimentos Gerais

2.4.1.1. Essa especificação será para a plataforma de gerência da estrutura de Telecom de maior criticidade (HLR e SGW).

2.4.1.2. Deverá ser fornecido uma plataforma de gerencia centralizada, em modo cluster,

arquitetura cliente-servidor, com sistema operacional UNIX(Solaris) ou Linux OS.

2.4.1.3. Deve possuir arquitetura modular, onde os módulos de softwares são adicionados de acordo com o elemento a ser gerenciado

2.4.1.4. Deve possuir interfaces Lan redundantes para tolerância a falhas

2.4.1.5. Deve implementar NTP para sincronia de com um servidor NT

2.4.1.6. Todos os equipamentos devem ser gerenciados de forma centralizada (de uma localização única) e através de uma console remota.

2.4.1.7. O sistema de oferecer funcionalidades de tracing em nível de célula de acordo com o 3GPP TS32.421

2.4.1.8. A plataforma deve possuir disponibilidade de 99,9% MTBF mínimo de 25000 horas

2.4.1.9. Deve suportar interface WEB

2.4.2. Gerenciamento de falhas:

2.4.2.1. Todos alarmes gerados em algum elemento de rede devem ser visualizado na GUI da gerência em menos de 8 seg.

2.4.2.2. Mudanças de estados dos elementos de rede devem ser visualizadas através da GUI central (running/not running).

2.4.2.3. Deve ser capaz de gerar relatórios ao menos semanais com a lista de todos alarmes gerados com seu respectivo elemento de rede e/ou sub modulo.

2.4.2.4. Deve ser capaz de configurar indicadores de alarme que sirvam de parâmetros para sua geração.

2.4.2.5. Deve manter um histórico no banco de dados da plataforma de no mínimo 90 dias de todos os alarmes gerados.

2.4.2.6. A plataforma deve ser capaz de monitorar alarmes externos de racks, subracks e slots do elemento de rede monitorado.

2.4.2.7. Os alarmes devem ser classificados em níveis de severidade e deve conter uma descrição de cada tipo.

2.4.2.8. Os níveis de severidade dos alarmes devem ser:

2.4.2.8.1. Critical

2.4.2.8.2. Major

2.4.2.8.3. Minor

2.4.2.8.4. Warning

2.4.2.8.5. Cleared

2.4.2.9. Deve ser capaz de executar os comando de operações através da console GUI

2.4.2.10. Deve suportar correlacionamento de eventos através de regras de correlação

2.4.3. Gerenciamento de configuração:

2.4.3.1. Suportar a geração de arquivos em formatos XML que retrate toda configuração lógica dos elementos de redes incluindo informações das interfaces de cada um.

2.4.3.2. Suportar a geração de arquivos em formatos XML que retrate toda configuração física dos elementos de redes incluindo informações das interfaces de cada um.

2.4.3.3. Capacidade de armazenar os arquivos gerados em batches em repositório indicado pelo operador.

- 2.4.3.4. Capacidade de gerar tais arquivos XMLs e armazená-los em uma frequência diária.
- 2.4.3.5. Capacidade de manter armazenado pelo menos os arquivos gerados nos últimos 30 dias.
- 2.4.3.6. Suportar função de auto-discovery dos links entre os elementos de rede.
- 2.4.4. Gerenciamento de performance
  - 2.4.4.1. Suportar a geração de arquivos com o histórico de performance de cada elemento de rede
  - 2.4.4.2. Suportar o agendamento periódico da geração de tais arquivos de performance.
  - 2.4.4.3. Suportar indicadores de sistemas:
    - 2.4.4.3.1. Situação de cada serviço e processo
    - 2.4.4.3.2. Performance: memória física, uso de CPU, uso de memória
    - 2.4.4.3.3. Espaço disponível no banco de dados
    - 2.4.4.3.4. Informação das partições do disco rígido
    - 2.4.4.3.5. Análise de protocolos
    - 2.4.4.3.6. Indicadores de uso de redes virtuais (Alocação de VLAN, gerenciamento de troncos)
    - 2.4.4.3.7. Possuir ferramenta capaz de:
      - 2.4.4.3.7.1. Realizar traces de sinalização
      - 2.4.4.3.7.2. Determina a disponibilidade do elemento de rede
      - 2.4.4.3.7.3. Testar o QOS da rede
- 2.4.5. Gerenciamento de Segurança
  - 2.4.5.1. Todo acesso a plataforma deve ser identificado por usuário/senha
  - 2.4.5.2. Senha não deve ser visível no campo de formulário da GUI
  - 2.4.5.3. O equipamento deve estar com antivírus atualizado.
  - 2.4.5.4. Usuário deve ser bloqueado após sucessivas tentativas de login
  - 2.4.5.5. Deve suportar a criação de grupo de usuários
  - 2.4.5.6. Suportar regras de acesso para autorização tanto para usuários como para grupos
  - 2.4.5.7. Todas as conexões devem ser seguras utilizando SSL.
  - 2.4.5.8. Deve ser possível limitar o acesso do usuário a um período específico de tempo.
  - 2.4.5.9. Suportar no mínimo 30 conexões de clientes simultâneas
  - 2.4.5.10. Deve ser possível o bloqueio automático de usuários que tenham um período longo de inatividade
  - 2.4.5.11. Deve ser possível prevenir o acesso duplicado de um mesmo usuário
  - 2.4.5.12. Deve ser facultativo ao usuário trocar a própria senha
  - 2.4.5.14. A senha deve ter período validade configurável
  - 2.4.5.15. O usuário deve ser notificado dez dias antes da data de expiração da sua senha.
  - 2.4.5.16. A plataforma deve possuir log de auditoria que grave todas os acessos e

operações executadas na plataforma

2.4.5.17. O log de auditoria deve ser gerado com atributo “read-only”

#### 22.4.6. GERENCIAMENTO DE SOFTWARE:

2.4.6.1. Deve ser possível fazer upload remoto de todos Softwares que porventura devam ser instalados nos elementos de rede (versão, atualização e patches)

2.4.6.2. Deve ser possível realizar rollback de qualquer nova instalação feita em algum elemento de rede

2.4.6.3. Deve ser possível atualizar a plataforma de gerência sem que a mesma sofra de paralisação do serviço de gerenciamento

2.4.6.4. A plataforma deve prover controle de versão dos softwares instalados nos elementos de redes gerenciados

2.4.6.5. A plataforma deve prevenir que softwares incompatíveis sejam carregados nos elementos de redes gerenciados

2.4.6.6. Após uma atualização de software bem sucedida, a versão anterior deve permanecer armazenada no elemento de rede para que sirva como versão de fallback em caso de falhas futuras.

2.4.6.7. Após qualquer recuperação dos sistemas, todas as informações de alarmes e softwares devem ser automaticamente sincronizadas entre os elementos de rede e a plataforma de gerência

2.4.6.8. O gerenciamento de softwares da plataforma deve permitir:

2.4.6.8.1. Listar todos os arquivos de software presentes

2.4.6.8.2. Toda operação de carregamento de novos softwares devem ser armazenadas no log de operação

2.4.6.8.3. Interromper a qualquer momento alguma atualização de software

2.4.6.8.4. Atualização de softwares deve ser multi-sessão, ou seja, deve ser possível atualizar mais que um elemento de rede simultaneamente.

#### 2.4.7. REQUISITOS DE BACKUP E RECUPERAÇÃO:

2.4.7.1 Suportar backup de dados das seguintes situações:

2.4.7.1.1. Backup e recuperação da plataforma de gerência

2.4.7.1.2. Backup de dados e recuperação dos elementos de redes gerenciados

2.4.7.1.3. Cada elemento deve armazenar seu ultimo backup localmente

2.4.7.1.4. Suportar agendamento de backups

2.4.7.1.5. Suportar backups automáticos

2.4.7.1.6. Suportar Veritas net backup

2.4.7.1.8. Suportar online backups incrementais

2.4.7.1.9. Suportar retinas de backups centralizadas

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

2.4.7.1.11. Durante o backup não pode haver nenhum impacto ao tráfego de dados relativos as operações de gerenciamento

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

## 2.2.5. OTA (*Over-The-Air*)

### 2.5.1. Requerimentos Gerais

2.5.1.1. A solução OTA deve suportar no mínimo o volume transacional de 300 (trezentas) mensagens por segundo.

2.5.1.2. 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 3-DES.

2.5.1.3. Durante o aprovisionamento:

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

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

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

2.5.1.4. 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.

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

2.5.1.5.1 Esta funcionalidade deve permitir a gestão e constante atualização do conteúdo dos cartões SIM245, esta informação deve estar disponível na base de dados da Plataforma.

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

2.5.1.5.3. Os serviços que devem ser minimamente cobertos são:

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

2.5.1.5.3.2. Auditar o tamanho do arquivo: retorna o tamanho do arquivo.

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

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

2.5.1.5.3.5. Auditar presença de pacote Java: verifica a presença de pacote no cartão.

2.5.2. A solução OTA deve suportar 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:

2.5.2.1. Activate AND

2.5.2.2. Activate FD

2.5.2.3. Switch ADN/FDN

2.5.2.4. Update ACC

- 2.5.2.5. Update AND
- 2.5.2.6. Update BDN
- 2.5.2.7. Update CBMI
- 2.5.2.8. Update FDN
- 2.5.2.9. Update FPLMN
- 2.5.2.10. Update HPLMN
- 2.5.2.11. Update IMSI
- 2.5.2.12. Update LP
- 2.5.2.13. Update MSISDN
- 2.5.2.14. Update PLMN
- 2.5.2.15. Update SDN
- 2.5.2.16. Update SMSP
- 2.5.2.17. Update SPN
- 2.5.2.18. Update SST
- 2.5.2.19. Update PL
- 2.5.2.20. Update EST
- 2.5.2.21. Update UST
- 2.5.2.22. Generic Card Update
- 2.5.2.23. Update HPLMNwAct
- 2.5.2.24. Update PLMNwAct
- 2.5.2.25. Update OPLMNwAct

2.5.3. A solução OTA deve suportar 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:

- 2.5.3.1. Download applet
- 2.5.3.2. Delete applet
- 2.5.3.3. Lock applet
- 2.5.3.4. Unlock applet
- 2.5.3.5. Download package
- 2.5.3.6. Delete package
- 2.5.3.7. Install for load package
- 2.5.3.8. Load package
- 2.5.3.9. Extradite Executable Load File
- 2.5.3.10. Create applet instance
- 2.5.3.11. Delete applet instance

2.5.3.12. Make instance selectable

2.5.3.13. Extradite Application

2.5.3.14. Download applet to installed

2.5.3.15. Instantiate applet to installed

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

2.5.5. 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.

2.5.5.1. 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. Assim, não necessitando o processamento antes do envio de cada mensagem, otimizando a utilização do recurso das SMSCs.

2.5.6. A solução OTA deve permitir a descriptografia das chaves disponibilizadas pelo SERPRO, cifradas em padrão 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.

2.5.7. 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 suportar as funcionalidades de Remote File Management (RFM) e Remote Applet Management (RAM).

2.5.8. 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.

2.5.9. Integração e Interoperabilidade

2.5.9.1. 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.

2.5.9.2. 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 14 de abril de 2009, independente do fabricante deste cartão.

2.5.9.3. A solução OTA deve suportar 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 suportando minimamente os canais abaixo listados.

2.5.9.3.1. CMG de 3.1.0 até 4.6 (EMI UCP)

2.5.9.3.2. SMPP 3.3 e 3.4

2.5.9.3.3. Nokia SC 4 e SC 5 (CIMD2)

2.5.9.4. A solução OTA deve suportar a integração com os elementos de processamento e controle de dados proprietário do SERPRO, através de recebimento e envio de arquivos para provisionamento de cartões SIM245, com a utilização da ferramenta Q-Ware. O formato destes arquivos, bem como, o padrão de comunicação estão descritos no ANEXO

## XX – Manual SIMRAV.

2.5.9.5. A solução OTA deve suportar a integração com os elementos de processamento e controle de dados proprietário do SERPRO, através de recebimento e envio de requisições HTTP em formato XML para ativação, desativação e diagnósticos de cartões SIM245. O formato destas requisições, bem como, o padrão de comunicação estão descritos no ANEXO XX – Manual SIMRAV.

2.5.9.6. A solução OTA deve suportar 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 existente do SERPRO.

## 2.5.10. Requerimentos de Padrões

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

2.5.10.1.1 ANATEL – SMP – Resolução 477

2.5.10.1.2. 3GPP TS 31.102

2.5.10.1.3. 3GPP TS 31.10

2.5.10.1.4. 3GPP TS 11.11

2.5.10.1.5. 3GPP TS 51.011

2.5.10.1.6. 3GPP GSM TS 03.203

2.5.10.1.7. 3GPP GSM TS 23.003

2.5.10.1.8. ITU-T – E.164

2.5.10.1.9. ITU-T – G.703

2.5.10.1.10. ITU-T – G.704

2.5.10.1.11. IETF – RFC 2719

2.5.10.1.12. GSM 03.38

2.5.10.1.13. 3GPP 23.038

## 2.5.11. Requerimentos de Marketing

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

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

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

2.5.11.4. 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.

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

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

2.5.11.7. A solução deve dispor de logs de auditoria. Este 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.

## 2.6. Certificações

2.6.1. A plataforma ofertada deve obrigatoriamente estar certificada junto ao órgão regulador ANATEL.

## 3.0 Níveis de Serviço

### 3.1. Requerimentos Operacionais

#### 3.1.1. Relatórios e Estatísticas

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

3.1.1.2. A solução deve suportar as seguintes funcionalidades:

3.1.1.2.1 SNMP MIBs para alarmes de hardware

3.1.1.2.2. SNMP MIBs para alarmes da aplicação

3.1.1.2.3. SNMP traps

3.1.1.2.4. Interface gráfica para gestão dos alarmes

3.1.1.2.5. Interface gráfica para configuração

#### 3.1.2. Suporte e Manutenção

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

3.1.2.2. A CONTRATADA deve testar exaustivamente todos os corretivos antes de aplicá-los na solução.

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

3.1.2.4. A CONTRATADA deve prover e instalar todas as ações corretivas sem custos adicionais ao SERPRO.

3.1.2.5. A CONTRATADA deve manter uma imagem da solução no ambiente da CONTRATADA, visando a realização de testes e validações de corretivos a serem instalados no SERPRO.

3.1.2.6. A CONTRATADA deve dispor de interface web para gestão e abertura de chamados.

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

3.1.2.8. A CONTRATADA deve prover claramente o canal para solicitação de ajuste de prioridade de incidentes.

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

3.1.2.10. A CONTRATADA deve prover canal telefônico com disponibilidade 24x7 para abertura de chamados.

3.1.2.11. A CONTRATADA deve dispor de canal de relacionamento com o cliente,

realizando consultas periódicas ao SERPRO quanto a qualidade da solução e serviços ofertados.

3.1.2.12. A CONTRATADA deve realizar revisões presenciais, na solução, semestralmente.

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

3.1.2.14. A CONTRATADA deverá atender minimamente aos SLAs descritos na tabela abaixo:

Prioridade		Tempo de Resposta	Modelo de Serviço	Diagnóstico
1	Severo	15 minutos (Envio de primeiro diagnóstico do problema)	24 horas, 7 dias por semana, 365 dias por ano	A CONTRATADA deverá trabalhar continuamente até que o serviço seja restaurado completamente ou até que uma solução temporária seja adotada, restabelecendo o serviço.
2	Sério	2 horas (Envio de primeiro diagnóstico do problema)	24 horas, 7 dias por semana, 365 dias por ano	A CONTRATADA deverá trabalhar continuamente até que o serviço seja restaurado completamente ou até que uma solução temporária seja adotada, restabelecendo o serviço.
3	Baixo	1 dia comercial (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.

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

Nível de importância do Incidente	Descrição
Nível 1: Severo (Serviço de Criticidade igual a Crítica)	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 2 que impacte número significativo (30% do total) de usuários.
Nível 2: Sério (Serviço com Criticidade igual a Alta)	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.
Nível 3: Baixo	Problemas de baixa prioridade que não afetam o compromisso de SLA ofertado pela CONTRATADA.

3.1.2.16. A CONTRATADA deverá atender minimamente os tempos de restauração de serviço descritos abaixo, em caso de falha no sistema:

3.1.2.16.1. Aplicáveis as Plataformas HLR, SMSC e SGW

Prioridade		Tempo para Solução Paliativa	Tempo para Solução Definitiva (sem defeito de HW)	Tempo para Solução Definitiva (com defeito de HW)
1	Severo	8 horas	3 dias comerciais	30 dias comerciais
2	Sério	1 dia comercial	7 dias comerciais	45 dias comerciais
3	Baixo	3 dias comerciais	20 dias comerciais	90 dias comerciais

### 3.1.2.16.2. Aplicáveis a Plataforma OTA

Prioridade		Tempo para Solução Paliativa	Tempo para Solução Definitiva
1	Severo	8 horas	20 dias comerciais
2	Sério	1 dia comercial	60 dias comerciais
3	Baixo	3 dias comerciais	90 dias comerciais

## 4.0 Especificação de Valores

NÃO SE APLICA

## 5.0 Justificativa da Contratação

NÃO SE APLICA

## 6.0 Seleção do Contratado

NÃO SE APLICA

## 7.0 Justificativa para Aceitação de Preços

NÃO SE APLICA

## 8.0 Gerenciamento do Contrato

### 8.1. Requerimentos da solução

#### 8.1.1. Requerimentos Gerais:

8.1.1.1. A CONTRATADA deve incluir na proposta 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 existente do SERPRO.

8.1.1.2. A CONTRATADA deve incluir na proposta 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 provisionamento, ativação e desativação).

#### 8.1.2. Dimensionamento e Qualificação

8.1.2.1. A solução deve suportar no mínimo 6.000.000 (seis milhões) de novos cartões SIM245 cadastrados no sistema.

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

8.1.2.3. A CONTRATADA deve considerar todo o hardware requerido para a solução, com

margem de segurança de 20% (vinte por cento) no dimensionamento.

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

8.1.2.5. Deve ser apresentados atestados de capacidade de integração que atestem a existência de aplicações comerciais do fornecedor da plataforma HLR e do gateway de sinalização em ao menos uma operadora SMP envolvida no projeto DENATRAN SIMRAV.

### **8.1.3. Software e Licenças**

8.1.3.1. A CONTRATADA deve responsabilizar-se pela disponibilização e implantação de todas as atualizações de software, envolvidos na solução proposta. Estas atualizações incluem novas funcionalidades, serviços e pacotes corretivos, devendo estas atualizações serem aplicadas com o mínimo de interrupção do serviço.

8.1.3.2. A CONTRATADA deve listar todas as Licenças de Software envolvidas na solução.

### **8.1.4. Hardware**

8.1.4.1. A CONTRATADA deve informar todo hardware incluso na Proposta desta solução.

8.1.4.2. A CONTRATADA deve informar a capacidade de expansão de hardware da solução, e a metodologia utilizada para aplicação desta expansão, informando se a expansão é aplicada através de adição de componentes e servidores, ou na expansão dos componentes já existentes. A CONTRATADA deve informar a granularidade da solução.

8.1.4.3. A CONTRATADA deve prover todo material necessário para instalação da solução, tais como, cabeamento de rede, rack para instalação de servidores. Bem como, todo o serviço requerido para instalação destes materiais.

### **8.1.5. Disponibilidade**

8.1.5.1. 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.

8.1.5.2. A solução deve atender ao índice de 99,95% (noventa e nove vírgula noventa e cinco por cento) de disponibilidade.

8.1.5.3. A solução deve ser integralmente redundante, isto significa, que a solução deve dispor de hardware, software e informações duplicadas, atendendo aos requerimentos de disponibilidade do SERPRO. Estes elementos deverão estar separados geograficamente para proteger o sistema de falhas e indisponibilidades do site principal.

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

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

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

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

### **8.1.6. Segurança**

8.1.6.1. A CONTRATADA deve garantir que todos os elementos da solução devem ser

instalados com, e apenas com, os serviços requeridos para o perfeito funcionamento da solução. Todos os demais serviços devem ser desabilitados.

8.1.6.2. A CONTRATADA 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.

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

8.1.6.4. A CONTRATADA deve responsabilizar-se por qualquer intervenção que demande instalação de corretivos de segurança. Este item deve ser incluído no Contrato de Suporte.

8.1.6.5. A solução deve garantir que todos os elementos providos na solução utilizem protocolos de acesso remoto que permitam criptografia.

8.1.6.6. 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.

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

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

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

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

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

8.1.6.12. A CONTRATADA deve dispor de conexão remota ao SERPRO através de VPN via link internet, estando o mesmo disponível 24x7. Esta comunicação será utilizada para acesso tratamento de incidentes pela equipe de suporte da CONTRATADA.

## **8.2. Requerimentos Operacionais**

### **8.2.1. Relatórios e Estatísticas**

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

8.2.1.2. A solução deve suportar as seguintes funcionalidades:

8.2.1.2.1. SNMP MIBs para alarmes de hardware

8.2.1.2.2. SNMP MIBs para alarmes da aplicação

8.2.1.2.3. SNMP traps

8.2.1.2.4. Interface gráfica para gestão dos alarmes

8.2.1.2.5. Interface gráfica para configuração

### **8.2.2. Suporte e Manutenção**

8.2.2.1. A CONTRATADA 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.

8.2.2.2. A CONTRATADA deve testar exaustivamente todos os corretivos antes de aplicá-los na solução.

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

8.2.2.4. A CONTRATADA deve prover e instalar todas as ações corretivas sem custos adicionais ao SERPRO.

8.2.2.5. A CONTRATADA deve manter uma imagem da solução no ambiente da CONTRATADA, visando a realização de testes e validações de corretivos a serem instalados no SERPRO.

8.2.2.6. A CONTRATADA deve dispor de interface web para gestão e abertura de chamados.

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

8.2.2.8. A CONTRATADA deve prover claramente o canal para solicitação de ajuste de prioridade de incidentes.

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

8.2.2.10. A CONTRATADA deve prover canal telefônico com disponibilidade 24x7 para abertura de chamados.

8.2.2.11. A CONTRATADA deve dispor de canal de relacionamento com o cliente, realizando consultas periódicas ao SERPRO quanto a qualidade da solução e serviços ofertados.

8.2.2.12. A CONTRATADA deve realizar revisões presenciais na solução semestralmente.

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

### **8.3. Localização do Hardware**

8.3.1. As Plataformas de produção devem ser instaladas no site do SERPRO em Brasília, .

8.3.2. As Plataformas de contingência, que atuem como redundância geográfica do ambiente produtivo, devem ser instaladas no site do SERPRO em São Paulo.

### **8.4. Operação Assistida**

8.4.1. A CONTRATADA deve prover pelo período de 1 (um) ano o serviço de operação assistida para todos os elementos que compõem a solução ofertada.

8.4.2. A CONTRATADA deve prover o serviço de operação assistida localmente, na unidade de Brasília ou São Paulo do SERPRO.

8.4.3. O serviço de Operação Assistida deve ser provido em modelo 8x5 (horário comercial e dias úteis).

8.4.4. A CONTRATADA deverá prover relatório mensal ao SERPRO informando as ações tomadas durante este período.

8.4.5. O escopo do serviço de Operação Assistida consiste no suporte a equipe de

Operação e Manutenção do SERPRO, provendo a esta equipe sugestões de melhores práticas e configurações da solução.

## **8.5. Execução do Projeto**

### **8.5.1. Cronograma**

8.5.1.1. A CONTRATADA deve concluir este projeto em até 90 (noventa) dias, a partir da data da aquisição da solução pelo SERPRO. Onde, neste período, as atividades serão segmentadas da seguinte forma:

15 (quinze) dias para conclusão da implantação do ambiente principal.

90 (noventa) dias para conclusão da implantação do ambiente de contingência.

8.5.1.2. A CONTRATADA deve apresentar um cronograma detalhado de atividades no início do projeto.

8.5.1.3. Todos os equipamentos e suprimentos devem ser entregues nos locais estipulados pelo SERPRO ao menos 2 (dois) dias antes da instalação dos mesmos.

## **9.0 Considerações Gerais**

### **9.1. Equipes Especializadas**

9.1.1. A CONTRATADA deve prover de equipe local (Brasil) para cada integração requerida.

#### **9.1.2. Treinamento**

9.1.2.1. A CONTRATADA deve prover treinamento local referente a solução proposta, atendendo aos seguintes tópicos:

9.1.2.1.1. Funcionalidades e ferramentas da solução;

9.1.2.1.2. Arquitetura de Hardware e Software;

9.1.2.1.3. Protocolos e interfaces;

9.1.2.1.4. Dimensionamento do sistema;

9.1.2.1.5. Alarmes e Estatísticos;

9.1.2.1.6. Manutenção e operação do sistema;

9.1.2.1.7. Integração com demais sistemas;

9.1.2.2. O treinamento deve ser provido de acordo com a distribuição abaixo:

9.1.2.2.1 - **02** (duas) turmas de 40 horas em Brasília.

9.1.2.2.2 - **02** (duas) turmas de 40 horas em São Paulo.

9.1.2.2.3. O treinamento deve ser realizado em língua portuguesa.

9.1.2.2.4. Cada turma deste treinamento deverá ser dimensionada para até 10 (dez) participantes.

9.1.2.2.5. A CONTRATADA deve responsabilizar-se por toda a infraestrutura requerida para o treinamento.

### **9.2. Garantia**



9.2.1. O período de garantia tem início com a assinatura do Termo de Aceite Inicial ou com a operação comercial da solução.

9.2.2. A CONTRATADA de prover pelo período de 5 (cinco) anos a garantia de todos os hardwares e softwares.

9.2.3. O escopo desta garantia deve estar em conformidade com os requerimentos descritos no **item 8 – GERENCIAMENTO DO CONTRATO** deste documento.

Anexos

Nenhum Anexo encontrado.

## **Elaboração**

Data : 04/10/2010

EDUARDO LIMA - 12005240

SUPSI/SIGOC/SIGCO