Anexo IX - REQUISITOS TÉCNICOS DA PRESTAÇÃO DOS SERVIÇOS

Sumário

1. Serviços

1.1. Serviço de Instalação e Configuração

1.1.1. Faz parte da prestação do serviço, além da porta de interconexão a Internet global de forma dedicada, o transporte do sinal da CONTRATADA até as instalações do Funasa, ou seja, com a instalação de cabos, *modems*, *switches*, *racks*, fibras óticas e/ou rádios necessários a prestação do serviço.

1.1.2. A instalação do ponto de acesso físico na Funasa é de responsabilidade exclusiva da CONTRATADA.

1.1.3. A CONTRATADA deverá fornecer toda a infraestrutura necessária para disponibilizar os serviços IP para acesso dedicado à Internet global, com os circuitos de acesso com a mesma capacidade de tráfego nos dois sentidos.

1.1.4. A CONTRATADA deverá fornecer toda a infraestrutura necessária para disponibilizar os serviços de Rede MPLS de forma dedicada e exclusiva, ou seja, não compartilhada. Os circuitos de acesso a esta Rede devem possuir a mesma capacidade de tráfego nos dois sentidos.

1.2. Serviço de Suporte Técnico

1.2.1. O serviço de suporte técnico consiste em manutenção preventiva e manutenção corretiva dos itens que compõem a solução contratada;

1.2.2. O período de suporte técnico, manutenção e garantia tem a vigência do contrato estabelecido para fornecimento do objeto do TR;

1.2.3. As atividades serão precedidas da abertura de um chamado técnico;

1.2.4. A CONTRATANTE poderá efetuar um número ilimitado de chamados durante a vigência do contrato;

1.2.5. A CONTRATADA deverá acordar com a Funasa as interrupções programadas com antecedência mínima de 7 (dias) dias úteis e deverão ser realizadas, de preferência, aos finais de semana ou feriados.

1.2.6. Nos casos em que a realização dos serviços de suporte técnico necessitarem de parada da solução, a CONTRATANTE deverá ser imediatamente notificada para que se proceda a autorização do suporte técnico, ou para que seja agendada nova data, a ser definida pela CONTRATANTE, para a realização do referido serviço de suporte;

1.2.7. O serviço de suporte técnico deverá ser realizado em regime de 24 (vinte e quatro) horas por 7 (sete) dias por semana, todos os dias do ano, no idioma português, devendo a empresa possuir uma central de atendimento sem custos para a CONTRATANTE e atender aos chamados da equipe técnica nos prazos estabelecidos no TR;

1.2.8. Durante o período de vigência do contrato e do suporte técnico e garantia, quando for o caso, todos os firmwares e softwares deverão ser atualizados a cada nova versão ou correção, sem nenhum custo adicional para a CONTRATANTE;

1.2.9. O serviço de suporte técnico poderá ser atendido através de contato telefônico, por e-mail ou presencial, sendo este critério decidido pela equipe técnica da CONTRATANTE;

1.2.10. Todos os prazos para atendimento dos chamados serão iniciados a partir da abertura do mesmo independentemente deste ter sido feito via telefone, e-mail ou website da CONTRATADA;

1.2.11. A CONTRATADA deverá disponibilizar um sistema de abertura de chamados para que a CONTRATANTE possa receber um identificador único para cada solicitação de atendimento e que tenha recursos (e-mail, página web, central telefônica ou etc.) que

possam manter a equipe técnica da CONTRATANTE informada sobre o andamento de cada chamado, esteja ele aberto, em andamento ou fechado;

1.2.12. Os serviços serão classificados pela Equipe Técnica da CONTRATANTE, quando da abertura dos chamados técnicos, segundo sua prioridade e obedecendo aos Níveis de Serviço;

1.2.13. A Funasa considerará efetivamente realizado o serviço quando houver confirmação por sua área técnica da conclusão satisfatória do atendimento;

1.2.14. Todos os chamados técnicos somente poderão ser encerrados com a anuência da CONTRATADA e da CONTRATANTE;

1.2.15. Qualquer chamado fechado, sem anuência da CONTRATANTE ou sem que o problema tenha sido de fato resolvido, será reaberto e os prazos serão contados a partir da abertura original do chamado;

1.2.16. A CONTRATADA manterá cadastro das pessoas indicadas pela CONTRATANTE que poderão efetuar abertura e fechamento de chamados;

1.2.17. A CONTRATADA deverá garantir, quando da execução dos serviços, o repasse dos conhecimentos teóricos e práticos que fundamentarem a solução dos problemas à equipe técnica da CONTRATANTE;

1.2.18. A CONTRATADA deverá dispor de equipe técnica capacitada para executar os serviços contratados de forma on-site, quando necessário;

1.2.19. Deverão ser emitidos, relatórios mensais referentes ao histórico dos incidentes, e atendimentos de suporte e manutenção independentemente de seu estado (abertos, fechado e em andamento).

1.3. Serviço de Gerenciamento da Rede

1.3.1. A CONTRATADA deverá prover um serviço de Gerenciamento da Rede que contemple as áreas funcionais de gestão de falhas, gestão de desempenho, gestão de configuração, gestão de segurança e de nível de serviço. O serviço deverá atender, no mínimo, às seguintes funcionalidades:

1.3.1.1. Abertura, acompanhamento e encerramento de chamados técnicos;

1.3.1.2. Geração e emissão de relatórios gerenciais que permitam o acompanhamento da qualidade dos serviços, dos níveis de serviço contratados e a validação das faturas.

1.3.2. O Serviço de Gerenciamento da Rede Contratada deverá abranger todos os equipamentos e enlaces, independentemente de suas tecnologias, necessários a prestação dos serviços contratados;

1.3.3. A CONTRATADA deverá disponibilizar uma Central de Atendimento Especializado em Rede e Segurança, com número telefônico único, não tarifado (0800), para registro dos chamados, operando 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, todos os dias do ano. Poderá ser disponibilizada pela CONTRATADA uma Central de Atendimento Especializada e exclusiva para a Gestão da Segurança (no que couber, ex: Anti DDoS).

1.3.4. A Funasa deverá ter acesso via rede mundial de computadores (internet) para acompanhamento dos chamados técnicos abertos, bem como dos relatórios de estatísticas e históricos dos chamados.

1.3.5. Os chamados abertos na Central de Atendimento Especializado poderão ser referentes a todas as atividades de responsabilidade da CONTRATADA considerando os serviços contratados, englobando, mas não se limitando a: instalação, configuração, recuperação, alteração e remoção de equipamentos, enlaces, roteamento, endereçamento IP entre outros.

1.3.6. Os chamados registrados pela gerência proativa ou pela Funasa deverão ser registrados no sistema de atendimento e disponibilizado de forma clara, compreensível e facilmente legível, devendo compreender as seguintes informações mínimas:
  1.3.6.1. Número do chamado registrado e nível de severidade, inclusive aqueles com reabertura;
  1.3.6.2. Data e hora de abertura do chamado técnico (horário de Brasília/DF);
  1.3.6.3. Identificação do link que apresenta a falha/interrupção;
  1.3.6.4. Identificação do funcionário da CONTRATANTE, responsável pela abertura do chamado;
  1.3.6.5. Identificação do técnico da CONTRATADA responsável pela execução do serviço de normalização do circuito ou equipamento;
  1.3.6.6. Descrição do problema apresentado;
  1.3.6.7. Descrição da solução;
  1.3.6.8. Status da solicitação (chamado em aberto, pendentes ou fechados);
  1.3.6.9. Data e hora da execução dos serviços necessários;
  1.3.6.10. Data e hora do encerramento do chamado.

1.3.7. A CONTRATADA emitirá relatórios sempre que solicitados pela CONTRATANTE, em papel e em arquivo eletrônico, preferencialmente nos formatos .DOC, .DOCX ou .PDF, com informações analíticas e sintéticas dos chamados abertos e fechados no período, total de chamados no mês e o total acumulado até a apresentação do relatório, com no mínimo as informações do item 1.3.6;

1.3.8. A CONTRATADA deverá armazenar todos os dados coletados nos elementos gerenciados e as informações geradas para confecção dos relatórios durante a vigência do contrato, devendo ao final do contrato disponibilizá-los para a Funasa em meio eletrônico, a ser acordado entre as partes posteriormente.

1.3.9. A CONTRATADA deverá disponibilizar, a qualquer tempo, sua base de dados de gerenciamento e de atendimentos prestados à Funasa, conjuntamente com o modelo de dados, para que Fundação possa gerar relatórios com a finalidade de acompanhamento, averiguação e auditoria.

1.3.10. A CONTRATADA deverá responsabilizar-se pela integridade e sigilo dos dados coletados armazenados em sua infraestrutura, relativos à gerência, aos chamados registrados e seus solicitantes.

1.3.11. A CONTRATADA deverá demonstrar ao quadro técnico da Funasa que os circuitos atendem as características especificadas no Termo de Referência, no ato da entrega do circuito ou a qualquer momento que a Fundação vier a solicitar.

1.3.12. A CONTRATADA deverá prestar um serviço de gerenciamento proativo que a capacite a detectar as falhas (fim a fim), incluindo todos os equipamentos que compõem a infraestrutura dos serviços contratados, gerar alarmes automáticos e dar início ao processo de recuperação dos serviços de forma autônoma em no máximo 10 (dez) minutos, sem a necessidade de reclamação técnica por parte da Funasa.

1.3.13. A ferramenta de gerenciamento a ser disponibilizada para acesso pela Funasa deverá gerar alarmes automáticos, relatórios e consultas para cada um dos links, informando sobre:
  1.3.13.1. Quedas de desempenho;
  1.3.13.2. Incremento de taxa de erros;
  1.3.13.3. Perda de pacotes;
  1.3.13.4. Aumento de latência.
  1.3.13.5. Relatório gerencial;

1.3.13.6. Relatório operacional;
1.3.13.7. Relatório consolidado;
1.3.13.8. Relatório detalhado;
1.3.13.9. Disponibilização de inventário: (informações sobre a localização física de ativos de rede como equipamentos CPE's, portas, placas e acessos);
1.3.13.10. Consulta de configuração corrente de equipamentos;
1.3.13.11. Consulta a inventário de equipamentos (modelos, fabricantes e interfaces);
1.3.13.12. Visão gráfica da rede com os respectivos alarmes;
1.3.13.13. Consulta de localidades (nomes, endereços);
1.3.13.14. Consulta de conexões (portas, sub-interfaces, velocidades, protocolos).

1.3.14. O sistema de gerenciamento proativo deverá funcionar 24 (vinte e quatro) horas por dia, todos os dias da semana.

1.3.15. A Funasa irá monitorar a rede contratada por meio de ferramenta, paralelamente ao sistema de gerenciamento fornecido pela CONTRATADA, devendo a CONTRATADA disponibilizar informações sobre os pontos de presença e de rede sempre que solicitado.

1.3.16. Deverá ser firmado um acordo operacional e de níveis de acesso aos equipamentos de rede, entre as partes contraentes, no qual deverão constar as informações necessárias ao processo operacional, como por exemplo: horário normal de funcionamento de cada link, desligamentos diários de equipamentos, contatos locais (nome, telefone, e-mail) e responsáveis por abertura de chamados, e outras informações que se fizerem necessárias à adequada operacionalização dos serviços.

1.3.17. A CONTRATADA deverá disponibilizar para a Funasa, um Relatório de Acompanhamento mensal, configurável e com filtros de fácil aplicação e remoção, de forma a permitir o acompanhamento da qualidade dos serviços prestados.

1.3.18. O relatório de acompanhamento mensal deve ser consolidado até o 5° (quinto) dia útil do mês subsequente para aferição dos serviços prestados no mês anterior, que deve ser entregue quando solicitado, e sempre em mídia digital;

1.3.19. Deverá ser firmado, entre as partes contraentes, um acordo de compartilhamento da operação e níveis de acesso à solução de segurança no qual deverão constar as informações necessárias ao processo operacional.

1.3.20. A gestão compartilhada inicia apenas após entrega dos equipamentos funcionando e com todas as regras iniciais implementadas e validadas pela CONTRATANTE.

1.3.21. Entende-se por gestão compartilhada, a atuação da CONTRATANTE e da CONTRATADA em configuração do equipamento do ponto de vista operacional, ou seja, configurações de regras.

1.3.22. O acordo operacional poderá ser flexibilizado, desde que acordado por ambas as partes.

1.3.23. Faz parte deste acordo o compartilhamento da operação dos equipamentos de segurança, níveis de acesso à solução de segurança no qual deverão constar: os equipamentos que fazem parte deste acordo, quais ações serão de responsabilidade da equipe da Funasa e demais informações necessárias ao processo operacional.

1.3.24. As falhas ou interrupções em decorrência da operação por parte da Funasa não acarretarão penalidades à CONTRATADA.

1.3.25. O relatório de acompanhamento mensal deve conter, no mínimo:
1.3.25.1. Informação da gerência de desempenho com volume total de tráfego do período de referência;

1.3.25.2. Informações relativas à instalação, desinstalação, alteração de política de acesso ou tecnologia de acesso e remanejamento de links;

1.3.25.3. Informações sobre todos os chamados recebidos no período de referência: quantidade total de chamados recebidos, quantidade total de chamados por link, a quantidade total de chamados por estado de solicitação e quantidade total de indisponibilidade por link;

1.3.25.4. Resumo dos chamados que geraram indisponibilidade no período de referência.

1.4. Serviço de Gerenciamento e Monitoramento de Segurança da Rede

1.4.1. A CONTRATADA deverá prover um serviço de Gerenciamento de Segurança da Rede que contemple as áreas funcionais de gestão de falhas, gestão de desempenho, gestão incidentes de segurança;

1.4.2. O Serviço de Gerenciamento proativo de Segurança da Rede deverá abranger todos os equipamentos de segurança contratados independentemente de suas tecnologias, necessários a prestação dos serviços, devendo funcionar 24 (vinte e quatro) horas por dia, todos os dias da semana;

1.4.3. Cabe à CONTRATADA acionar o suporte técnico de rede para correção de falhas na infraestrutura que esteja comprometendo o serviço de segurança;

1.4.4. Cabe à CONTRATADA acionar quando necessário o fabricante do equipamento que compõem a solução de segurança;

1.4.5. Cabe à CONTRATADA monitorar, diagnosticar e corrigir falhas que envolvam toda a infraestrutura e equipamentos de rede e de segurança entregues por ela, devendo, portanto, haver uma interação entre as equipes de suporte de rede e suporte de segurança, garantido uma completa integração entre todos os equipamentos e uma perfeita prestação do serviço contratado.

1.4.6. Cabe à CONTRATADA iniciar a recuperação dos serviços de forma autônoma em no máximo 15 (quinze) minutos, sem a necessidade de abertura de requisição técnica por parte da Funasa. Para efeito de contabilização do tempo de atendimento destes incidentes será considerado o tempo de identificação por parte da ferramenta de monitoramento da Contratada ou da abertura de chamado pela Funasa, o que ocorrer primeiro.

1.4.7. A CONTRATADA deverá disponibilizar uma Central de Atendimento Especializado em Segurança de Rede, com número telefônico único, não tarifado (0800), para registro dos chamados, operando 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, todos os dias do ano. Poderá ser disponibilizada pela CONTRATADA uma Central de Atendimento Especializada compartilhada com a gestão da Rede.

1.4.8. A Funasa deverá ter acesso via rede mundial de computadores (internet) para acompanhamento dos chamados técnicos abertos, bem como dos relatórios de estatísticas e históricos dos chamados.

1.4.9. Nos casos de incidentes ou problemas no ambiente gerenciado de segurança da Rede Funasa, as intervenções preventivas ou reativas serão identificadas, registradas e classificadas pela CONTRATADA ou, excepcionalmente, pelo CONTRATANTE, conforme sua severidade;

1.4.10. Para os chamados de suporte categorizado como Severidade Crítica ou Alta, o atendimento não pode ser interrompido até o completo restabelecimento de todas as funções do item gerenciado de segurança que esteja paralisado ou indisponível, mesmo

que para isso tenham que se estender por períodos noturnos e dias não úteis (sábados, domingos e feriados), de acordo com a disponibilidade da Funasa;

1.4.11. Cada requisição ou incidente identificado pela gerência proativa ou pela Funasa deverá ser registrado no sistema de atendimento e disponibilizado de forma clara, compreensível e facilmente legível, devendo compreender as seguintes informações mínimas:

1.4.11.1. Número do chamado registrado e nível de severidade ou prioridade, inclusive aqueles com reabertura;

1.4.11.2. Data e hora de abertura do chamado técnico (horário de Brasília/DF);

1.4.11.3. Identificação do ponto de presença que apresenta a falha/interrupção;

1.4.11.4. Identificação do funcionário do CONTRATANTE, responsável pela abertura do chamado;

1.4.11.5. Identificação do técnico da CONTRATADA responsável pela execução do serviço de normalização do circuito ou equipamento;

1.4.11.6. Descrição do problema apresentado;

1.4.11.7. Descrição da solução;

1.4.11.8. Status da solicitação (chamado em aberto, pendentes ou fechados);

1.4.11.9. Data e hora da execução dos serviços necessários;

1.4.11.10. Data e hora do encerramento do chamado.

1.4.12. A CONTRATADA emitirá relatórios sempre que solicitados pela CONTRATANTE, com informações analíticas e sintéticas dos chamados abertos e fechados no período, com no mínimo as informações coletadas no subitem 1.4.11;

1.4.13. A CONTRATADA deverá armazenar todos os dados coletados nos elementos gerenciados de segurança geradas para confecção dos relatórios durante a vigência do contrato, devendo ao final do contrato disponibilizá-los para a Funasa em meio eletrônico, a ser acordado entre as partes posteriormente;

1.4.14. A CONTRATADA deverá disponibilizar, a qualquer tempo, sua base de dados de gerenciamento e de atendimentos prestados para a Funasa, conjuntamente com o modelo de dados, para que a Fundação possa gerar relatórios com a finalidade de acompanhamento, averiguação e auditoria;

1.4.15. A CONTRATADA deverá responsabilizar-se pela integridade e sigilo dos dados coletados armazenados em sua infraestrutura, relativos à gerência, aos chamados registrados e seus solicitantes, atendendo ao que estabelece a LGPD;

1.4.16. A CONTRATADA deverá disponibilizar para a Funasa, Relatórios gerenciais mensais que permitam o acompanhamento da qualidade, disponibilidade e nível dos serviços prestados, com vistas a validação das faturas, devendo conter, no mínimo:

1.4.16.1. Informações relativas à reparos, manutenções e trocas de equipamentos;

1.4.16.2. Informações sobre todos os chamados relativos a incidentes e requisições recebidas no período de referência: quantidade total de chamados registrados, quantidade total de chamados por pontos de presença, a quantidade total de chamados por situação (status) das solicitações e quantidade total de indisponibilidade por pontos de presença;

1.4.16.3. Abertura, acompanhamento e encerramento de chamados técnicos;

1.4.16.4. Total de chamados no mês e o total acumulado até a apresentação do relatório.

1.4.17. O relatório de acompanhamento mensal deve ser consolidado até o 5° (quinto) dia útil do mês subsequente para aferição dos serviços prestados no mês anterior, sempre em mídia digital;

1.4.18. Deverá apresentar, quando solicitado, um relatório que demonstre o nível de segurança de seus equipamentos e as recomendações dos fabricantes quanto a melhoria em sistemas operacionais e configurações que compõem a solução contratada, visando detectar possíveis falhas no serviço e na segurança da rede.
1.4.19. Além destes indicadores de nível de serviço apresentados, outros podem ser definidos a qualquer tempo de comum acordo entre a Funasa e a CONTRATADA, permitindo desta forma, a melhoria continua a partir do próprio aprendizado que os atores forem adquirindo com a execução dos serviços.
1.4.20. A CONTRATADA deverá fazer constar no relatório de acompanhamento mensal a informação dos links que ficaram sem conectividade por mais de 5 (cinco) dias corridos.
1.4.21. A CONTRATADA deverá notificar sobre indisponibilidade de um link quando esse ficar indisponível por mais de 2(duas) horas;
1.4.22. Só poderão ser cobrados os serviços efetivamente ativados e em operação, ou seja, os serviços que foram aceitos pela Funasa.

1.5. Serviço de Proteção Contra Ataques "DDoS"

1.5.1. A CONTRATADA deverá disponibilizar em seu backbone proteção contra os ataques de negação de serviços DoS e DDoS, evitando assim a saturação da banda da Internet e a indisponibilidade dos serviços da Funasa;
1.5.2. O Serviço deverá ter pró-atividade na prevenção e tratamento de incidentes e ataques;
1.5.3. Deverá monitorar a disponibilidade e desempenho do link de dados do tipo C1 - Internet Corporativo contemplado no TR em regime 24x7, utilizando profissionais de forma dedicada;
1.5.4. Deverá tomar todas as providencias necessárias para recompor a disponibilidade do link em caso de incidentes de ataques de DDoS, recuperando seu pleno funcionamento;
1.5.5. Deverá possuir a capacidade de criar e analisar a reputação de endereços IP, possuindo base de informações próprias, gerada durante a filtragem de ataques, e interligada com os principais centros mundiais de avaliação de reputação de endereços IP;
1.5.6. Deverá suportar a mitigação automática de ataques, utilizando múltiplas técnicas como White Lists, Black Lists, limitação de taxa, técnicas desafio-resposta, descarte de pacotes mal-formados, técnicas de mitigação de ataques aos protocolos HTTP e DNS, bloqueio por localização geográfica de endereços IP, dentre outras;
1.5.7. Deverá implementar mecanismos capazes de detectar e mitigar todos e quaisquer ataques que façam o uso não autorizado de recursos de rede, incluindo, mas não se restringindo às seguintes categorias de ataques:
1.5.7.1. Ataques de inundação (Bandwidth Flood), incluindo Flood de UDP e ICMP;
1.5.7.2. Ataques a pilha TCP, incluindo mal uso das Flags TCP, ataques de RST e FIN, SYN Flood e TCP Idle Resets;
1.5.7.3. Ataques que utilizam fragmentação de pacotes, incluindo pacotes IP, TCP e UDP;
1.5.7.4. Ataques de Botnets, Worms e ataques que utilizam falsificação de endereços IP de origem (IP Spoofing);
1.5.7.5. Ataques a camada de aplicação, incluindo protocolos HTTP e DNS;
1.5.8. A solução deve manter uma lista dinâmica de endereços IP bloqueados, retirando dessa lista os endereços que não enviarem mais requisições maliciosas após um período considerado seguro pela CONTRATADA;

1.5.9. A CONTRATADA deve possuir centro de limpeza nacional e internacional com capacidade de mitigação; a
1.5.10. A CONTRATADA deve mitigar ataques enquanto o ataque não tiver sido cessado;
1.5.11. Caso o volume de tráfego do ataque ultrapasse as capacidades de mitigação especificadas ou sature as conexões do AS, devem ser tomadas contramedidas tais como aquelas que permitam o bloqueio seletivo por blocos de IP de origem no AS pelo qual o ataque esteja ocorrendo, utilizando técnicas como Remote Triggered Black Hole;
1.5.12. As soluções de detecção e mitigação devem possuir serviço de atualização de assinaturas de ataques;
1.5.13. A CONTRATADA deve disponibilizar um Centro de Operação de Segurança (SOC — Security Operations Center) no Brasil, com equipe especializada em monitoramento, detecção e mitigação de ataques, com opção de atendimento através de telefone 0800, correio eletrônico, em idioma português brasileiro, durante as 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, no período de vigência contratual.
1.5.14. A mitigação de ataques deve ser baseada em arquitetura na qual haja o desvio de trafego suspeito comandado pelo equipamento de monitoramento, por meio de alterações do plano de roteamento;
1.5.15. Em eventos de ataques DoS e DDoS, todo tráfego limpo deve ser reinjetado na infraestrutura da CONTRATANTE através de tuneis GRE (Generic Routing Encapsulation), configurado entre a plataforma de DoS e DDoS da CONTRATADA e o CPE do CONTRATANTE;
1.5.16. Para a mitigação dos ataques não será permitido o encaminhamento do tráfego para limpeza fora do território brasileiro;
1.5.17. As funcionalidades de monitoramento, detecção e mitigação de ataques devem ser mantidas em operação ininterrupta durante as 24(vinte e quatro) horas do dia, nos 7 (sete) dias da semana, no período de vigência contratual;
1.5.18. Em nenhum caso será aceito bloqueio de ataques de DoS e DDoS por ACLs em roteadores de bordas da CONTRATADA;
1.5.19. A CONTRATADA deve iniciar a mitigação de ataques de DDoS em no máximo 15 minutos;
1.5.20. A ferramenta de gerenciamento a ser disponibilizada para acesso pela Funasa deverá atender aos seguintes requisitos:
    1.5.20.1. Deverá atribuir a cada alerta um número de identificação que facilite sua consulta;
    1.5.20.2. Deverá registrar a data de início e fim do acompanhamento do alerta;
    1.5.20.3. Disponibilizar relatórios e consultas sobre o volume de ataques sumarizados por hora, dia, semana e mês;
    1.5.20.4. Relatório por tipos de ataques;
1.5.21. O Portal de monitoração da CONTRATADA devera possuir uma interface única para acesso as suas funcionalidades, independentemente dos equipamentos ou tecnologias empregadas para a prestação dos serviços;
1.5.22. O Portal de Gerência deverá permitir o acesso simultâneo a, pelo menos, dois administradores de rede da CONTRATANTE;

2. Características dos Equipamentos

2.1. Tipo-1 - CPE conectividade para os circuitos C1, C2 e C4

2.1.1. O roteador deverá ser dimensionado para atender o serviço na capacidade máxima especificada;
2.1.2. O roteador CPE deverá ser fornecido com todos os componentes, módulos e acessórios necessários ao seu perfeito funcionamento;
2.1.3. A configuração lógica do roteador CPE será definida pela CONTRATADA com a aprovação da Funasa.
2.1.4. Todos os roteadores suportarão, além dos protocolos básicos para operação em uma rede IP com compressão de dados e o protocolo de roteamento OSPF, com opção de security telnet e IPsecurity (IPSec);
2.1.5. Os roteadores terão facilidades de configuração e checagem por meio de porta serial e da console de monitoramento.
2.1.6. O roteador CPE deve ser modular;
2.1.7. Deverá ser instalado com no mínimo 2 interfaces 10GbE padrão SFP+, expansível a no mínimo 4 interfaces, quando necessário;
2.1.8. Deverá ser instalado com no mínimo 04 (quatro) interface LAN 100/1000BASE-T com slots RJ-45, expansível a no mínimo 8 interfaces;
2.1.9. Deve suportar fontes AC redundantes;
2.1.10. Deve possuir suporte a 4094 VLAN Tags 802.1q;
2.1.11. Deve possuir suporte a agregação de links 802.3ad e LACP;
2.1.12. Deve possuir suporte a Policy based routing ou policy based forwarding;
2.1.13. Deve possuir suporte a roteamento multicast (PIM-SM e PIM-DM);
2.1.14. Deve possuir suporte a DHCP Relay;
2.1.15. Deve possuir suporte a DHCP Server;
2.1.16. Deve suportar sFlow;
2.1.17. Deve possuir suporte a Jumbo Frames;
2.1.18. Deve suportar sub-interfaces ethernet lógicas;
2.1.19. Deve implementar o protocolo ECMP;
2.1.20. Deve permitir monitorar via SNMP;
2.1.21. Enviar log para sistemas de monitoração externos, simultaneamente;
2.1.22. Possuir a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;
2.1.23. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
2.1.24. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);
2.1.25. Suportar OSPF graceful restart;
2.1.26. Deve suportar o padrão de indústria 'syslog' protocol para armazenamento usando o formato Common Event Format (CEF);
2.1.27. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem;
2.1.28. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino;
2.1.29. Suportar a criação de políticas de QoS e Traffic Shaping por porta;
2.1.30. O QoS deve possibilitar a definição de tráfego com banda garantida;
2.1.31. O QoS deve possibilitar a definição de tráfego com banda máxima;
2.1.32. O QoS deve possibilitar a definição de fila de prioridade;
2.1.33. Suportar marcação de pacotes Diffserv, inclusive por aplicação;
2.1.34. Suportar modificação de valores DSCP para o Diffserv;
2.1.35. Suportar priorização de tráfego usando informação de Type of Service;
2.1.36. Deve suportar QOS (traffic-shapping), em interface agregadas ou redundantes;
2.1.37. Suportar IPSec VPN;
2.1.38. A VPN IPSEc deve suportar Autenticação MD5 e SHA-1;

2.1.39. A VPN IPSEc deve suportar Diffie-Hellman Groups;
2.1.40. A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1);
2.1.41. A VPN IPSEc deve suportar AES (Advanced Encryp on Standard);
2.1.42. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall, HPE/Aruba.

2.2. TIPO-2 - CPE equipamentos de conectividade para os circuitos C3.1 e C3.2

2.2.1. Os roteadores deverão ser dimensionados para atender o serviço na capacidade máxima especificada, sem a necessidade de troca de equipamento e devem possuir as seguintes características:
2.2.2. Throughput mínimo suficiente para suportar todo o tráfego de dados sem degradação;
2.2.3. Os equipamentos de conectividade de rede devem possuir suporte a Vlans;
2.2.4. Devem possuir suporte a agregação de links 802.3ad e LACP;
2.2.5. Devem possuir suporte a Policy based routing ou policy based forwarding;
2.2.6. Devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);
2.2.7. Devem suportar BGP, OSPF, RIP e roteamento estático;
2.2.8. Devem possuir suporte a DHCP Relay;
2.2.9. Devem possuir suporte a DHCP Server;
2.2.10. Devem possuir suporte a Jumbo Frames;
2.2.11. Devem suportar sub-interfaces ethernet logicas;
2.2.12. Devem suportar NAT dinâmico (Many-to-Many);
2.2.13. Devem suportar NAT estático (1-to-1);
2.2.14. Devem suportar NAT estático bidirecional 1-to-1;
2.2.15. Devem suportar Tradução de porta (PAT);
2.2.16. Devem suportar NAT de Origem;
2.2.17. Devem suportar NAT de Destino;
2.2.18. Devem suportar NAT de Origem e NAT de Destino simultaneamente;
2.2.19. Devem implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
2.2.20. Devem suportar NAT64 e NAT46;
2.2.21. Devem suportar roteamento estático e dinâmico (RIP, BGP e OSPF);
2.2.22. Devem permitir monitorar via SNMP, no mínimo, o uso de CPU, memória e interfaces;
2.2.23. Devem enviar log para sistemas de monitoração externo, inclusive via protocolo SSL;
2.2.24. Os equipamentos deverão possuir, no mínimo, 04 (quatro) interface LAN 100/1000BASE-T com slots RJ-45, com capacidade de expansão;