ANEXO X

REQUISITOS DE GERENCIAMENTO DOS SERVIÇOS

O presente Anexo tem como finalidade disponibilizar uma solução de Gerência de Rede e Serviços abrangendo todo o serviço prestado e contemplando as áreas funcionais de gerência de Disponibilidade, Falhas, Desempenho, Configuração, Segurança da Informação e de Nível de Serviço.

A Gerência de Rede e Serviços da CONTRATADA deverá atuar de forma proativa, conforme definido no **Anexo XIII – Requisitos de Assistência e Suporte Técnico**, antecipando-se aos problemas na rede e garantindo a qualidade do serviço conforme estabelecida no **Anexo XI - Acordos de Níveis de Serviços**, realizando abertura, acompanhamento e fechamento de chamados relacionados com indisponibilidade e desempenho nos serviços de rede e gerenciamento de rede, operando em regime 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano. Deverão ser disponibilizadas as informações dos chamados relativos à rede do Banco.

Todos os requisitos apresentados devem ser integralmente atendidos pela CONTRATADA. O não atendimento a qualquer dos requisitos apresentados, no todo ou em parte, sujeitará o licitante à desclassificação do processo de licitação, às sanções previstas em contrato, e às eventuais medidas legais cabíveis.

Todos os requisitos objeto deste Anexo deverão ser plenamente atendidos sem nenhum custo adicional para o Banco.

1 CARACTERÍSTICAS GERAIS DOS SERVIÇOS

1.1. Interligação com o CAPGV: Site Primário e Site Secundário

Todos os circuitos de acesso à rede da operadora para concentração dos circuitos no Site Primário e Site Secundário deverão ser atendidos de acordo com o **Anexo VII - Requisitos dos Serviços Integrados de Comunicação.**

1.2. Relatórios e Configurações

Na necessidade de ajustes em relatórios e configurações, seja por solicitação do Banco ou por sugestão da CONTRATADA, esta última será a responsável por tais alterações, as quais deverão ser implementadas dentro do prazo estipulado no **Anexo XI - Acordos de Níveis de Serviços**.

1.3 Serviços de NOC/SOC e Alocação de Técnicos Residentes

A CONTRATADA deverá alocar técnicos residentes para operar as funcionalidades do Sistema de Gerenciamento observando as exigências constantes do subitem **- (NOC/SOC).** A princípio, os técnicos ficarão lotados no Site Primário do Banco.

Fica facultado a CONTRATADA a disponibilização de equipe remota, sem custo adicional ao BANCO, para apoiar a equipe residente dedicada no BANCO.

1.4 Fornecimento de Sistema de Gerenciamento

O Gerenciamento das soluções ofertadas deve abranger gerenciamento de falhas, configuração, contabilização, desempenho e segurança.

1.5 Monitoração e Gerenciamento da Interconexão das Redes das Operadoras

O Serviço de NOC/SOC da CONTRATADA deverá monitorar e gerenciar todos os componentes da solução de **SDWAN,** além de também monitorar os componentes da Solução de SSE e dos componentes da solução WAN e as interfaces dos comutadores de rede providos pelo Banco

para a interconexão das redes d, devendo fornecer ao Banco uma visão única de falhas, performance, configuração, tráfego e disponibilidade de todo o ambiente das redes. Banco disponibilizará acesso de leitura a esses equipamentos, da mesma forma que o exigido para as demais CONTRATADA **no Anexo VII – Requisitos dos Serviços Integrados de Comunicação**. Quaisquer mudanças de configurações desses equipamentos deverão ser solicitadas ao Banco, que as implementará após análise e aprovação formal.

Para a plataforma de segurança (SSE), o gerenciamento do ambiente ficará à cargo da equipe técnica do Ambiente de Segurança Corporativa do BANCO. À CONTRATADA caberá monitorar o ambiente, avaliar continuamente as configurações com base nas melhores práticas de segurança e nas recomendações do fabricante da solução ofertada e propor melhorias no ambiente, além de prover suporte técnico para sanar dúvidas e resolver incidentes relacionados à plataforma. A CONTRATADA não poderá realizar quaisquer configurações na plataforma de segurança SSE sem o acompanhamento e o consentimento da equipe técnica do BANCO responsável pelo gerenciamento das políticas de acesso.

Caso os IPs utilizados pelo fabricante da solução SSE para acesso à internet sejam bloqueados por qualquer provedor ou parceiro do BANCO, caberá à equipe técnica da CONTRATADA a resolução definitiva, seja contornando o incidente com a alteração do IP de saída para a Internet ou entrando diretamente em contato com empresas e órgãos públicos que eventualmente bloqueiem os IPs de saída para a Internet utilizados pelo BANCO. Os tempos de atendimento e solução para esses atendimentos está descrito no ANEXO XI - ACORDO DE NÍVEIS DE SERVIÇO - REDE WAN e SASE.

O monitoramento dos componentes ofertados deverá conter, no mínimo, o monitoramento de disponibilidade (UP/DOWN) dos componentes físicos e túneis/VPN; performance (CPU, Memória, tráfego, degradação)

2 *NETWORK OPERATIONS CENTER/ SECURITY OPERATIONS CENTER (NOC/SOC)*

Para operar os serviços do NOC/SOC, a contratada deverá fornecer equipe residente dedicada no CAPGV de acordo com as características, perfis e responsabilidades descritas logo abaixo.

A CONTRATADA deverá disponibilizar uma equipe especializada para a gestão da Segurança dos equipamentos das soluções ofertadas.

Cabe às CONTRATADA monitorar, diagnosticar e corrigir falhas que envolvam toda a infraestrutura e equipamentos de rede e de segurança entregues por elas, devendo, portanto, haver uma interação entre as equipes de suporte de rede e suporte de segurança das CONTRATADA com a equipe do Banco de forma a garantir uma completa integração entre todos os equipamentos e uma perfeita prestação do serviço contratado. Se necessário contactar o Fabricante das soluções ofertadas, a CONTRATADA se responsabilizará pelo acionamento, sem custos adicionais ao Banco.

2.1 Perfil

Para operar os serviços do NOC/SOC, a CONTRATADA deverá fornecer equipes residentes de acordo com as características/requisitos, perfis e responsabilidades abaixo:

PERFIL
2.1.1 serviços de gerenciamento de relatórios e dashboards: 1) Formação: Curso superior na área de Informática, acrescido de certificação em nível A*ssociate level* de Redes de Computadores fornecida pelo fabricante dos equipamentos da Rede do Banco utilizados na interconexão das redes das operadoras (Cisco), acrescido de Treinamento Técnico Específico nas áreas das soluções propostas. 2) Experiência mínima de 24 (meses) meses na implementação e suporte de ferramentas de monitoramento e extração de relatórios de comunicação de dados.

2.1.2 serviços de coordenação de NOC/SOC:

1) Formação: Curso superior na área de informática ou gestão, acrescido de certificação dos fabricantes de SD-WAN e SSE propostos e certificação em

2) Experiência mínima de 24 (meses) meses em atividades relacionadas à coordenação de NOC/SOC.

2.1.3 serviços de especialista de tráfego de rede SD-WAN (Sênior):

1) Formação: Curso superior na área de Informática, acrescido de certificação em nível professional *level* na área de Redes de Computadores fornecida pelo fabricante dos equipamentos da Rede do Banco utilizados na interconexão das redes das operadoras (Cisco CCNP ou superior) e certificação em nível *Professional level* do fabricante de SD-WAN e certificação na solução SSE), acrescido de certificação *ITILv3 ou superior;*

2) Experiência mínima de 36 (meses) meses na implementação, gerenciamento e suporte de redes SD-WAN.

2.1.4 serviços de especialista de tráfego de rede WAN (Pleno):

1) Formação: Curso superior, acrescido de certificação em associate level na área de Redes de Computadores fornecida pelo fabricante dos equipamentos da Rede do Banco utilizados na interconexão das redes das operadoras (Cisco CCNA ou superior) e certificação do fabricante de SD-WAN, acrescido de certificação ITILv3 ou superior;

2) Experiência mínima de 24 (meses) meses no suporte de solução de redes SD-WAN.

2.1.5 serviços de especialista de Segurança (Sênior):

1) Formação Acadêmica: Curso Superior completo em Tecnologia da Informação, Sistemas da Informação, Segurança da Informação ou correlatos, ou Curso Superior completo em qualquer área de formação acrescido de pós-graduação na área de informática e seus correlatos;

2) Deve possuir experiência profissional comprovada de 5 (cinco) anos na área de Tecnologia da Informação e 02 (dois) anos de atuação na identificação e análise de problemas, bem como administração, gerenciamento, monitoramento, instalação e configuração de soluções de Segurança da Informação de mercado;

3) Deve possuir, pelo menos, uma das certificações a seguir:
- Information Security Management Expert baseada na ISO/IEC 27001
- Certified Information Systems Auditor (CISA)
- ISC² Certified Information System Security Professional – CISSP
- GIAC Information Security Professional Certification (GISP);

4) Deve possuir certificação técnica em nível *Engineer* ou *Professional*, para a plataforma **SSE** ofertada;

2.1.6 serviços de operação/monitoração:

1) Formação: Curso técnico de nível médio na área de Telecomunicações e/ou Redes de Computadores, concluído em Escolas Técnicas Federais ou Institutos Federais; Nível superior completo na área de informática ou cursando, acrescido de treinamento na área de Redes de Computadores reconhecido pelo fabricante dos equipamentos da Rede do Banco utilizados na interconexão das redes das operadoras (Cisco);
2) Treinamento Técnico Específico na Solução ofertada.

Em todos os casos os técnicos deverão possuir treinamento específico para operar os equipamentos e a solução ofertada para o Sistema de Gerenciamento de cada CONTRATADA.

2.2 Local e Horário de Atuação

A CONTRATADA disponibilizará técnicos residentes dos **serviços de operação/monitoração** (item 2.1.6) de segunda a sexta-feira, no CAPGV, iniciando a prestação dos serviços a partir das 06h (horário de Brasília), com encerramento previsto para 0h (horário de Brasília). Entre 0h (horário de Brasília) e 06h (horário de Brasília) de segunda a sexta-feira e de 0h até 24hs nos finais de semana, será aceito que os **serviços de operação/monitoração** sejam realizados fora do CAPGV. Para o caso de serviços de operação/monitoração fora do CAPGV, a CONTRATADA poderá acessar a ferramenta de gerenciamento/monitoramento instalada nas dependências do Banco do Nordeste através de conexão VPN via Internet, sem custo adicional para o BANCO.

A CONTRATADA garantirá, ainda, a alocação de técnicos residentes nos finais de semana, desde que constatada a necessidade por parte do BANCO. Na ocorrência de algum incidente grave, nos horários em que os técnicos residentes não estejam nas dependências do BANCO, este poderá solicitar que os serviços de diagnóstico e solução do problema sejam realizados localmente nas dependências do BANCO, no CAPGV. Nos casos de feriado no Estado do Ceará ou Município de Fortaleza, deverá ser assegurada a alocação de técnicos residentes com a carga horária, início e término de suas atividades, nos moldes já estabelecidos para a jornada diária. No caso de feriado nacional será aceito que os **serviços de operação** sejam garantidos fora do CAPGV, a CONTRATADA garantirá a alocação de técnicos residentes, desde que constatada a necessidade por parte do BANCO. Os serviços prestados pelos técnicos residentes em horários extraordinários (sábados, domingos, feriados nacionais e de 0h as 06h, nos dias úteis da semana) não terão custo adicional para o BANCO. Fica a critério do BANCO, desde que constatada a necessidade, que os técnicos utilizarão as dependências do Site Secundário para execução de suas atividades.

A CONTRTADA disponibilizará para os serviços de **gerenciamento de relatórios / dashboards** (perfil 2.1.1) e **serviços de especialista de tráfego de rede SDWAN (Sênior)** (perfil 2.1.3), **serviços de especialista de Segurança** (perfil 2.1.5), técnicos residentes alocados em regime 8x5, em dias úteis, no CAPGV, sem prejuízo das necessidades de alocação em horários extraordinários, conforme acima previsto. Os **serviços de especialista de tráfego de rede WAN (Pleno)** (perfil 2.1.4) deverão cobrir os horários entre 7h e 0h, em dias úteis, no CAPGV, sem prejuízo das necessidades de alocação em horários extraordinários, conforme acima previsto. Os **serviços de coordenação de NOC/SOC** deverão estar disponíveis 24x7x365, devendo ser 08h às 17h presencial, nos dias úteis, no CAPGV.

Não será permitido o acúmulo de funções entre os perfis de serviços aqui especificados, com exceção dos perfis **2.1.1 e 2.1.2**, sem prejuízo para a regime de atuação.

2.3 Organização das especialidades em turnos

É responsabilidade da CONTRATADA o dimensionamento de todos os recursos necessários (principalmente da equipe de monitoração) para atender ao serviço contratado nos níveis de qualidade definidos neste anexo e demais anexos deste edital. A CONTRATADA deverá realizar a alocação da equipe do NOC/SOC, em turnos/jornada, de forma que os serviços sejam prestados conforme **Anexo XIII – Requisitos de Assistência e Suporte Técnico**.

Para alocação, segue tabela orientativa com cobertura mínima de serviços, agrupada por dia e turnos de trabalho (visão por perfil).

	Dias úteis				Sábado			Domingo			
Serviços (por perfil)	00h00 às 08h00 (terça a sábado)	07h00 às 16h00	08h00 às 17h00	15h15 às 00h00	07h00 às 16h00	08h00 às 17h00	15h15 às 00h00	00h00 às 08h00	08h00 às 17h00	15h15 às 00h00	00h00 às 08h00 (segunda)
serviços de gerenciamento de			X								

relatórios e dashboards											
serviços de especialista de tráfego de rede SDWAN (Sênior)		X									
serviços de especialista de Segurança (Sênior)		X									
serviços de especialista de tráfego de rede WAN (Pleno)		X		X							
serviços de operação/monitoração	X	X	X	X	X		X	X	X	X	X
serviços de coordenação de NOC/SOC *			X								

* O serviço de Coordenação de NOC/SOC deverá cobrir o regime 24x7x365, devendo ser 08h às 17h presencial no CAPGV e o restante do tempo poderá ser de forma remota.

Eventuais substituições dos técnicos residentes deverão ocorrer de modo que não prejudique o BANCO, ou seja, sem interrupção do acompanhamento do sistema por técnico qualificado.

2.4 Serviços Gerenciados

Os serviços gerenciados pelo NOC/SOC da CONTRATADA contemplam todos os componentes utilizados na interconexão das soluções ofertadas para o CAPGV, Unidades Distribuídas, Parceiros e Postos.

Entre as atividades previstas para serem realizadas pela equipe técnica do NOC/SOC, as principais são:

1) Realizar testes de funcionalidades dos serviços, incluindo testes de ativação e desativação de contingência;
2) Definição, implantação, acompanhamento e monitoramento do balanceamento do tráfego pelos circuitos de acesso contratados, assim como das funcionalidades/políticas de segurança da informação;
3) Atender e acompanhar chamados técnicos, realizados pelas Unidades Distribuídas, Postos e Parceiros do Banco, que estejam relacionados aos serviços fornecidos neste Edital;
4) Realizar e acompanhar a abertura de chamados de suporte e assistência técnica junto ao NOC/SOC dos serviços WAN que, por sua vez, deverá fornecer número de contato 0800 e WhatsApp disponíveis 24 horas por dia, 7 dias por semana, 365 dias por ano, bem como lista de contatos de recorrência para a realização e acompanhamento de chamados abertos pelo BANCO e pelos Técnicos Residentes, conforme **item 2.3 do Anexo XIII - Requisitos de Assistência e Suporte Técnico** deste Instrumento;
5) Realizar e acompanhar a abertura de chamados de suporte e assistência técnica na ferramenta de Help Desk do Banco, para fim de acompanhamento do Banco;
6) Realizar procedimento de identificação e solução de problemas relacionados aos serviços prestados;
7) Realizar procedimento de identificação e solução de problemas relacionados aos serviços prestados pelas operadoras, intervindo fisicamente nos componentes fornecidos pela CONTRATADA, caso necessário;
8) Monitorar os componentes da solução WAN. A CONTRATADA deverá utilizar suas próprias ferramentas;
9) Gerenciar os componentes da solução **SASE** (appliances, servidores, comutadores, configurações, aplicação de políticas, componentes lógicos, etc.);
10) Criar e manter atualizada documentação sobre topologia e componentes fornecidos no escopo dos serviços prestados, bem como sobre sua relação com outros componentes;

11) Realizar o backup da configuração lógica dos roteadores, *firewalls* e demais *appliances* fornecidos;
12) Sugerir adequações em relatórios e demais documentos utilizados pela equipe de comunicação, implementando-as quando aprovadas pelo Banco;
13) Analisar e sugerir novos formatos para documentos com base nas experiências do dia-a-dia, implementando-os quando aprovados pelo Banco;
14) Reportar falhas e sugestões de melhorias relacionadas às atividades desenvolvidas;
15) Configurar todas as funcionalidades do sistema de gerenciamento e utilizá-las para informar as equipes do Banco a respeito da ocorrência de falhas e anomalias nos serviços;
16) Contatar o Banco quando da sua entrada em contingência, informando os procedimentos que devem ser adotados em relação ao uso da rede, assim como informar acerca das ações que estão sendo adotadas para solução do problema;
17) Acompanhar os alertas gerados pelo Sistema de Gerenciamento e atuar pró e reativamente na identificação e correção de anomalias no tráfego;
18) Realizar batimento do SLA previsto no **Anexo XI - Acordo de Níveis de Serviços** deste Instrumento, confrontando os relatórios gerados pela solução de gerenciamento com os fornecidos pelas operadoras prestadoras dos serviços de comunicação. O batimento deverá constar as discrepâncias encontradas entre os relatórios apresentados pelas operadoras e os gerados com base nas informações obtidas pela rede. Além de informar mensalmente as eventuais multas inerentes ao descumprimento do SLA (ver o exemplo de relatório de disponibilidade e de faturamento).
19) Acompanhar a adequação das políticas vigentes de QoS à evolução das necessidades de negócios do Banco. Analisando se as políticas de QoS informadas pelo Banco estão sendo aplicadas, sugerindo e implementando as melhorias e alertando em caso de anomalias.
20) Acompanhar a adequação às políticas vigentes de Segurança da Informação ativas no Banco. Realizando configurações nos componentes fornecidos, realizando os devidos ajustes de configurações, análise de relatórios, sugerindo melhorias e alertando em caso de anomalias.
21) Manter documentação de controle sobre indisponibilidade e performance dos serviços, incluindo:

    - Data e hora de início;
    - Data e hora de fim;
    - Tempo total de indisponibilidade;
    - Taxas de erro;
    - Perdas de pacote;
    - Variações de Jitter;
    - Problemas de rotas BGP;
    - Sobrecarga dos circuitos de acesso;
    - Se existe imputabilidade; se não for imputável, registrar o motivo;
    - Se a contingência e/ou o acesso secundário funcionou; se não funcionou, registrar o motivo;
    - Forma de cálculo e valor apurado da multa ou desconto, quando aplicável.

3 SISTEMA DE GERENCIAMENTO

Fornecimento, instalação, configuração, operação, assistência técnica e suporte técnico de um sistema de gerenciamento para os serviços de comunicação de dados, capaz de monitorar todos os níveis de atendimento e desempenho exigidos no Edital. A manutenção preventiva e corretiva do sistema de gerenciamento (hardware e software) será de responsabilidade e expensas da CONTRATADA.

A gestão dos CPEs será realizada pela contratada destes itens. Entretanto, a responsabilidade de monitoração desses equipamentos será compartilhada com a CONTRATADA do SD-WAN + SSE, a medida que os equipamentos CPEs estarão equipados com recursos que permitirão a exportação de informações para outras ferramentas de monitoramento indicadas pelo Banco, por exemplo as ferramentas da contratada.

O monitoramento sobre as soluções ofertadas deverá possibilitar criação de alertas também para alteração de status de protocolos usados como BGP e VRRP por exemplo, evidenciando e alarmando falhas de intermitência.

3.1 Local de instalação e operação

A solução do Sistema de Gerenciamento (*hardware* e *software* com as respectivas licenças de uso, sob a responsabilidade da **CONTRATADA** poderá ser instalada nas dependências do Banco no CAPGV, no bloco B1 Térreo, assim como a solução de contingência no Site Secundário. Caso esta opte por instalar a solução do Sistema de Gerenciamento fora das dependências do Banco, a mesma obriga-se a manter comunicação de dados para tráfego das informações de gerência entre a rede do Banco e a sua solução seguindo os seguintes critérios:

- Utilização de comunicação de acesso redundante, com pelo menos 01 (um) acesso no Site Primário e 01 (um) no Secundário;
- Os acessos deverão ser totalmente independentes, tanto em última milha como em subestação e backbone;
- A largura de banda mínima individual dos acessos deverá ser sempre superior em 60% da média de picos mensais obtidos em horários comerciais. Isto é, caso a média mensal acima seja de 600Kbps, cada acesso fornecido deverá ter capacidade de 960Kbpps de *upload* e *download*. Devendo a CONTRATADA estar sempre realizando os ajustes baseado no mês anterior;
- A tecnologia permitida será MPLS ou Internet VPN, com enlaces terrestres;
- Não haverá prejuízo no cálculo de SLA de disponibilidade e desempenho caso a CONTRATADA do opte por esta alternativa.

3.2 Funcionalidades

O **Sistema de Gerenciamento** da CONTRATADA deverá permitir a visualização das atualizações realizadas a cada 5 (cinco) minutos de cada um dos parâmetros listados abaixo, através de mensagem (com ícones e dados) e/ou sinalização com alarme visual ou sonoro na console de gerenciamento, no alcance de limites máximos ou mínimos de valores definidos no **Anexo XI – Acordo de Níveis de Serviços:**

- Utilização acima de determinado percentual da capacidade de banda disponível para cada classe e da capacidade total do circuito por períodos superiores a 10 minutos;
- Utilização da capacidade total da banda disponível para cada classe e da capacidade total do circuito;
- Percentual de pacotes recebidos ou transmitidos com erro, quando aplicável;
- Percentual de pacotes recebidos e transmitidos com indicadores de congestionamento no circuito, quando aplicável;
- Sejam gerados alertas quando a capacidade de um recurso exceder um valor definido (*threshold);*

O **Sistema de Gerenciamento** deverá permitir a visualização, das atualizações realizadas a cada 5 (cinco) minutos em qualquer das extremidades e sem a interrupção dos serviços de comunicação de dados, dos seguintes indicadores quantitativos de cada circuito:

- Velocidade de transmissão e recepção;
- Sinais elétricos das interfaces dos roteadores das unidades;
- Taxas de pacotes recebidos e transmitidos com indicadores de congestionamento no circuito, quando aplicável.

Especificamente para a **CONTRATADA**, de forma a que sua solução de gerência tenha uma visão unificada da rede WAN do Banco e que possa atuar na detecção de problemas que eventualmente tenham origem potencial na rede das operadoras, a solução de gerência utilizada deverá garantir que:

- A gerência de SLA seja realizada preferencialmente, de forma automática conforme previsto no **Anexo XI – Acordo de Níveis de Serviço**, em tempo real, devendo os

SLAs serem monitorados e acompanhados a qualquer tempo durante todo o contrato e não somente no final de cada mês, através de um portal disponibilizado pela solução;

- Todo o trabalho de descoberta e monitoramento dos dispositivos da rede deverá ser feito sem a necessidade de instalação de agentes, bastando apenas que os dispositivos de rede possuam o protocolo SNMP v2 ou superior e tenham MIBs publicadas;

- Realizar descoberta e gerenciamento de redes MPLS VPN;

- Realizar descobrimento automático da topologia de nível 2 e nível 3 da rede para apresentação do mapa de conectividade e de informações de configurações dos elementos;

- A ferramenta deverá prover mecanismos para correlação dos eventos e geração de alarmes das falhas de forma nativa. Os seguintes mecanismos de correlação de eventos devem ser suportados:

  a) Pares de Eventos: Há eventos onde se espera que ocorram em pares. Se o segundo evento não ocorrer, pode indicar uma falha na infraestrutura. A regra de Pares de Eventos gerará um alarme quando um evento ocorrer sem o seu respectivo par. Deverá ser possível que eventos de outra natureza ocorram entre os eventos especificados sem afetar a regra de Pares de Eventos;

  b) Sequência de Eventos: Deve permitir identificar uma sequência específica de eventos que podem ter significância na infraestrutura. Esta sequência pode incluir qualquer quantidade e tipo de eventos. Quando a sequência for detectada num dado período de tempo, um alarme deverá ser gerado. Deverá ser possível que eventos de outra natureza ocorram entre os eventos especificados na sequência sem alterar a regra de Sequência de Eventos;

  c) Combinação de Eventos: Deverá ser possível especificar uma combinação de eventos que podem ocorrer em qualquer ordem. A combinação pode incluir qualquer quantidade e tipo de eventos. Quando a combinação for detectada num dado período de tempo, um alarme deverá ser gerado. Deverá ser possível que eventos de outra natureza ocorram entre os eventos especificados na combinação sem alterar a regra de Combinação de Eventos;

  d) Taxa de Eventos: Deverá ser gerado um alarme quando uma quantidade um mesmo evento ocorrer na infraestrutura num dado período;

  e) Condicional: Deverá ser possível gerar um alarme quando uma condição específica for satisfeita. A regra deverá aceitar como entrada uma lista de condições e eventos associados. Cada condição deverá ser avaliada e um alarme gerado quando uma condição for satisfeita;

- Realizar Isolamento de falhas para um dado segmento da topologia, indicando a causa raiz de forma automática e suprimindo eventos de dispositivos dependentes resultantes da falha principal;

- A análise de causa raiz por isolamento de falhas deverá ser compatível com recebimento de alertas e suporte a no mínimo as seguintes tecnologias: VLan, Multicast, MPLS, SNMP, Syslog, VPN, Ethernet e Aplicações;

- A análise de causa raiz por isolamento de falhas deverá ocorrer com base na topologia de nível 2 e 3, sem a necessidade de cadastramento e manutenção de tabelas de relacionamento entre dispositivos pais e filhos;

- Nas condições de alarme, mensagens por e-mail deverão ser encaminhadas para responsáveis, designados pelo BANCO, para conhecimento e providências;

- A plataforma deverá permitir o agrupamento de um ou mais dispositivos por unidades, departamentos, processos de negócios ou serviços, configurados de acordo com a melhor conveniência da contratante;

- Disponibilizar ferramentas para apresentar a topologia da rede em múltiplos níveis hierárquicos;

- Quando houver conectividade entre dois dispositivos posicionados em níveis hierárquicos diferentes na topologia, a ferramenta deverá representar no nível inferior, a conexão com o dispositivo no nível superior;

- A topologia montada deverá ser consistente com os protocolos de nível 2 e 3 da rede gerenciada.

- Suportar protocolo de coleta de informações de fluxos que circulam pelo equipamento a cada instante, contemplando no mínimo as seguintes informações: IP origem/destino; Protocol type; Porta TCP/UDP, Interface de entrada e saída; Bytes e pacotes transmitidos.

3.3 Dashboard

As soluções de gerenciamento fornecidas pela CONTRATADA deverão dispor das informações gerenciais em formato de *dashboard*. Onde será possível ao Banco encontrar, de forma sumarizada, as principais informações de utilização das redes existentes, bem como de disponibilidade e performance.

Deverá capaz de fornecer dados trafegados por cada link em tempo real (para troubleshoot) e também via portal de relatórios (gerenciamento) após no máximo 5 minutos do tráfego em questão.

Deverá ser capaz de fornecer portal personalizado para gerenciamento de todos os dispositivos dos Postos de Crédito e Unidades Distribuídas, Access Points, políticas e objetos, junto com painéis, relatórios e visualizações personalizadas para atualizações de segurança abrangentes, análises em tempo real e respostas exclusivas às suas necessidades.

3.4 Integração com a plataforma de gerenciamento do Banco

O **Sistema de Gerenciamento/Monitoramento** para os serviços de comunicação de dados provido pela CONTRATADA deverá suportar a integração com a solução de gerenciamento de serviços de TI – CA Service Management - Service Desk Manager, versão 17.3, ou a outra que o Banco vier a contratar – de forma que:

- Seja aberto um *ticket* de incidente registrando a indisponibilidade, parcial ou total, de qualquer componente da solução (incluindo enlaces físicos, túneis, interfaces, roteadores, comutadores, access-points, appliances, concentradores, repetidores, recursos alocados na rede da operadora e demais itens necessários ao perfeito funcionamento da solução);

- Sejam abertos *tickets* de incidente quando a capacidade de um recurso exceder um valor definido (*threshold);*

- Seja finalizado um *ticket*, atualizando o *status do incidente e* informando o momento em que o componente retornou aos níveis definidos para o perfeito funcionamento da solução;

A solução de gerenciamento do Banco deverá receber essa informação através de um dos seguintes mecanismos:

- Linha de comando;
- E-mail;
- *Web Service;*
- *API*.

Ao verificar o início de um incidente, a ferramenta da CONTRATADA deverá registrá-lo na solução de gerenciamento de serviços de TI do Banco utilizando um dos mecanismos descritos, criando assim, um ticket para o incidente correspondente.

Os seguintes requisitos devem ser respeitados, quando da abertura de um *ticket*, para que não haja inundação de aberturas de *tickets* na solução de gerenciamento de serviço de TI do Banco:

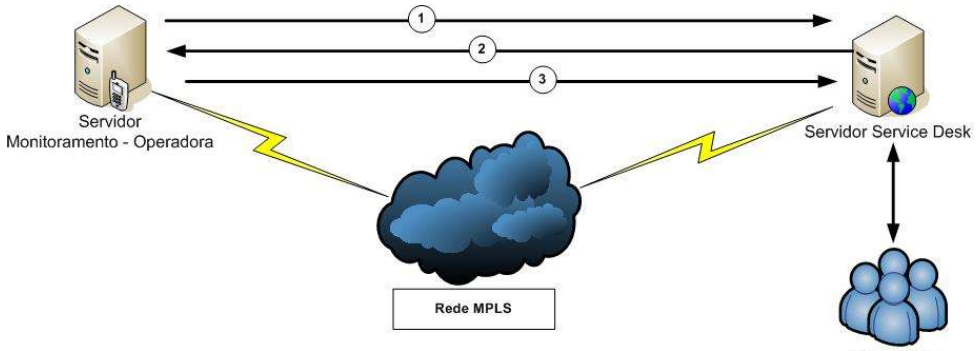
- Mecanismo de correlação de eventos: analisa as informações dos dispositivos e permite identificar eventos relacionados, avaliando a relevância de um determinado evento.

- Mecanismo de relacionamento de causa raiz: analisa as informações dos dispositivos e permite identificar eventos que possuam a mesma causa raiz.

Dessa maneira, o sistema deve filtrar automaticamente os eventos de forma a identificar apenas os eventos relevantes, reduzindo significativamente os falsos positivos.

Quando a ferramenta efetua o registro do ticket, automaticamente é gerado um número identificador (ID) do incidente. Esse número será utilizado posteriormente para fazer a resolução do incidente quando os componentes afetados retornarem ao funcionamento normal. Portanto, o identificador (ID) do ticket deve ser registrado para que o incidente seja finalizado corretamente.

A figura abaixo ilustra um cenário genérico de funcionamento da solução:



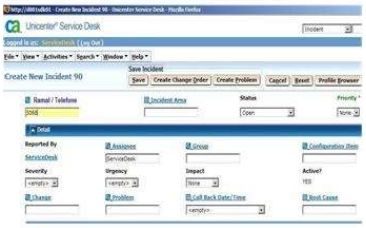
POLITICA DE NOTIFICAÇÕES

1 – Envio de notificações da ferramenta da licitante para a solução de gerenciamento de serviços de TI do Banco (CA Unicenter Service Desk r11)

2 – Retorno informando o identificador do chamado aberto.

3 – Confirmação de resolução do incidente contendo o identificador do chamado, mudando o status para resolvido.

4 – Posteriormente a central irá confirmar o retorno à normalidade dos itens afetados, mudando o status para fechado.



A integração das plataformas será de responsabilidade da CONTRATADA, e deverá ser executada no prazo máximo de **60 (sessenta) dias corridos** contados a partir da data de solicitação formal a ser feita pelo Banco.

3.5 Gerenciamento da Solução de Segurança

A CONTRATADA ficará obrigada a fornecer as informações exigidas no Sistema de Gerenciamento da Solução de Segurança de forma online. Além disso, se obrigará também a, mensalmente, disponibilizar os relatórios do item 4 deste anexo.

As Soluções de Gerenciamento de Segurança (SSE) devem apresentar uma gerência centralizada, através de padrão Web, que deverá permitir a realização de todas as configurações de Segurança necessárias (appliances, firewalls, etc). Acesso ao sistema através de cliente com browser padrão (HTTPS) e implementar o uso de duplo fator de autenticação (2FA ou MFA) para acesso à console de administração da solução.

Permitir a criação de grupos de administração com diferentes perfis de acesso, que possibilitem a separação das atividades administrativas na plataforma de segurança. Deve ser possível a criação de, pelo menos, os seguintes perfis: Operador (somente leitura) e Administrador. Todos os acessos administrativos devem ser autenticados, criptografados e registrados em trilha de auditoria às plataformas de Gerenciamento, e devem obrigatoriamente utilizar segundo fator de autenticação (2FA ou MFA).

Todas as configurações relacionadas aos recursos e regras de segurança deverão ser rigorosa e formalmente documentadas, atualizadas e repassadas ao Banco.

Ainda em caso de perda da comunicação com a plataforma de gerência, deverá disponibilizar de forma automática, uma interface web local, para gerenciamento dos appliances, firewalls e access points, durante o evento de falha.

Possuir capacidade de gerenciamento hierárquico, com possibilidade de definição de grupos de equipamentos e alteração das características de configuração do grupo sem a necessidade de configuração individual de cada equipamento (appliance, firewall, access points, etc). A plataforma de gerencia/controle da rede Wireless poderá ser a diferente do gerenciamento dos FWNG. Deve possuir capacidade de identificação e listagem dos rádios vizinhos e respectivos SSID (Service Set Identifier) que podem ser percebidos pelos Ponto de Acesso;

Deve permitir a realização de atualizações de software através da plataforma de gerência, e permitir também o agendamento para que a atualização seja feita em uma janela de manutenção;

Possuir solução de identificação de aplicações através de técnicas de análise de tráfego, provendo informações das aplicações mais utilizadas na interface gráfica;

4 RELATÓRIOS DE ACOMPANHAMENTO DOS SERVIÇOS

A CONTRATADA será responsável pela geração e emissão de relatórios gerenciais que permitam o acompanhamento da qualidade dos serviços, nos níveis de serviço contratados (SLA) e dos chamados técnicos realizados. Os relatórios deverão ser entregues ao Banco em formato eletrônico (PDF ou DOC) e disponibilizados via Internet ou por correio eletrônico, observando os critérios de segurança definidos pelo Ambiente de Segurança Corporativa do Banco. As informações geradas pelo sistema deverão ser trabalhadas de forma automática ou manual para estarem em conformidade com os *leiautes* dos modelos fornecidos.

4.1 Relatórios estáticos

Os relatórios classificados como estáticos são aqueles que, uma vez emitidos, apenas necessitarão ser novamente emitidos quando ocorrer alguma alteração no seu conteúdo. Devem refletir o histórico das atualizações incorporadas à rede. As informações contidas nesses relatórios caracterizam-se por serem estáveis, somente sendo atualizadas em razão de evento específico, pré-determinado e devidamente conhecido e autorizado pelo Banco.

4.2 Relatórios periódicos

Os relatórios classificados como periódicos são aqueles que devem ser emitidos mensalmente, pela CONTRATADA, refletindo a dinamicidade das informações neles contidas.

4.2.1 Relatório de disponibilidade

Relatório com os descritivos em DOC ou PDF e tabelas em formato de planilha eletrônica que possam ser lidas pelo Microsoft Excel contendo os dados para a análise de disponibilidade de todos os circuitos de comunicação de dados da solução, sendo o relatório gerado em duas versões:

- **Relatório de Disponibilidade Padrão – 24hs**: computado desde a zero hora do primeiro dia do mês até as vinte e quatro horas do último dia do mês, conforme modelo constante no item 5;
- **Relatório de Disponibilidade Comercial**: computado desde as oito horas até as dezoito horas de cada dia útil do mês, conforme modelo constante no item 5.

4.2.2 Relatório de desempenho

Relatório com os descritivos em DOC ou PDF e tabelas em formato de planilha eletrônica que possam ser lidas pelo Microsoft Excel contendo os dados para a análise de desempenho de todos os recursos utilizados para prover o serviço de comunicação fim a fim, sendo o relatório gerado em duas versões:

- **Relatório de Desempenho Padrão – 24hs**: computado desde a zero hora do primeiro dia do mês até as vinte e quatro horas do último dia do mês, conforme modelo constante no item 5;
- **Relatório de Desempenho Comercial**: computado desde as oito horas até as dezoito horas de cada dia útil do mês, conforme modelo constante no item 5

As medições para obtenção destes valores deverão ser realizadas no circuito a intervalos máximos de **5 (cinco) minutos** ao longo do mês;

4.2.3 Relatório de faturamento

Relatório em formato de planilha eletrônica que possam ser lidas pelo Microsoft Excel contendo o faturamento mensal referente aos serviços contratados e os efetivamente prestados no período, conforme modelo constante neste anexo.

4.2.4 Relatório de serviços (chamados técnicos)

Relatório com os descritivos em DOC ou PDF e tabelas em formato de planilha eletrônica (Microsoft Excel) contendo os dados dos chamados técnicos referentes ao mesmo período de dias especificado no relatório de faturamento, conforme modelo constante no item 5.

Nos relatórios de acompanhamento dos chamados deverão existir filtros por tipos de problema e por pontos de presença, que poderão ser utilizados concomitantemente.

Deverá fazer parte do relatório um resumo constando o total de chamados abertos, fechados e pendentes (em andamento), destacando os chamados resolvidos fora do tempo de atendimento contratado, problemas reincidentes e tipos de chamados mais frequentes.

4.2.5 Relatório de Segurança

Relatório com os descritivos em DOC ou PDF e/ou tabelas em formato de planilha eletrônica que possam ser lidas pelo Microsoft Excel contendo os dados para a análise das soluções NGFW e SSE, contendo, no mínimos os seguintes tópicos:

- Utilização de Banda por Aplicação;
- Principais Aplicação;
- ToP users;
- Top Sites
- Top Categorias

- Top Blocked Sites
- Utilização de VPN
- Utilização de Web por usuários
- Emails
- Ameaças detectadas no período;
- Eventos de Sistema;

- **Relatório de Disponibilidade Padrão – 24hs**: computado desde a zero hora do primeiro dia do mês até as vinte e quatro horas do último dia do mês, conforme modelo constante no item 5;
- **Relatório de Disponibilidade Comercial**: computado desde as oito horas até as dezoito horas de cada dia útil do mês, conforme modelo constante no item 5.

A CONTRATADA deverá apresentar semestralmente, até o último dia útil do mês subsequente ao semestre anterior, relatórios de acompanhamento dos controles de segurança executados pela CONTRATADA, assim como potenciais riscos de segurança da informação e cibernéticos identificados, monitorados e mitigados.

4.3 Relatórios online

Deverá ser fornecida visualização de informações *on-line* da solução ofertada apresentando, no mínimo, as seguintes funcionalidades:

- Topologia da rede, incluindo os roteadores CPE e os enlaces entre eles, com visualização do estado operacional, de todos os elementos da rede, incluindo quantitativos absolutos e relativos de enlaces sem conectividade;

- Sinalização de alerta (com gradação de criticidade), em casos de falha e volta à normalidade dos enlaces entre equipamentos roteadores WAN e comutadores LAN;

- Visualização dos módulos componentes de todos os elementos da rede (equipamentos roteadores, appliances, firewalls, access points e comutadores) e de todas as suas portas, interfaces e sub-interfaces, permitindo a verificação, no mínimo, da ocorrência de erros, capacidade de uso, descarte de pacotes;

- Visualização da utilização de banda dos enlaces, devendo ser considerados valores (absolutos e relativos) instantâneos, médios e de pico dos últimos 30 (trinta) dias, separados por semana e dia, com diferenciação de dias úteis e horário comercial;

- Indicação do consumo de banda dos enlaces (entrada e saída), devendo ser indicado o volume de tráfego e a ocupação de memória e CPU dos roteadores CPE, appliances, comutadores, firewall, etc;

- Visualização do retardo do enlace, devendo ser considerados os valores (absolutos e relativos) instantâneos, médios e de pico dos últimos 30 (trinta) dias, separados por semana e dia, com diferenciação de dias úteis e horário comercial;

- Visualização dos chamados registrados, abertos, fechados e encerrados, dentro ou fora do prazo contratual, por tipo de problema, permitindo acesso ao detalhamento dos chamados.

- Relatórios **SDWAN**, que permitam identificar:

  a) Principais aplicativos/aplicações que estão usando mais largura de banda na WAN;
  b) análise de partes da WAN com a latência mais alta em tempo real.
  c) análise de perda média e máxima de pacotes em tempo real, em conjunto e em conexões WAN individuais.
  d) quantidade de pacotes que são entregues fora de ordem na WAN, em média e durante os períodos de pico.

e) informações de fluxo do usuário(ou endereço IP) em tempo real para solução de problemas
f) visualização do túnel Overlay em tempo real para mostrar como vários transportes estão sendo usados pelas políticas de aplicativo
g) gráficos em tempo real que mostram o uso da largura de banda de diferentes classes de tráfego, como voz, vídeo, aplicativos de transferência de arquivos, etc.
h) visualização da latência no caminho WAN

- Relatórios **SSE**, que permitam visualizar:

  a) de forma direta na solução, as aplicações mais utilizadas, os usuários que mais estão utilizando estes recursos informando sua sessão, total de pacotes enviados, total de bytes enviados, URLs acessadas e ameaças identificadas;
  a) de forma direta na solução, o throughput de dados utilizado pela rede de computadores conectados ao serviço em nuvem. Esse requisito poderá ser atendido pela solução SSE ou pela solução SDWAN ofertada;

Caso seja utilizada a Internet como meio de visualização *on-line*, a CONTRATADA deverá garantir a confidencialidade e a integridade das informações.

4.4 Relatórios de Qualificação de Tráfego

Deverão ser providos os seguintes relatórios que permitam a análise do tráfego que passa pelos componentes roteadores concentradores da solução (CAPGV), Unidades e Postos, sob forma *on-line*, e também histórico, com possibilidade de apresentação das informações em formato tabular e gráfico:

- Qualificação de tráfego por classes de serviço (conforme classes definidas no **Anexo VII – Requisitos dos Serviços Integrados de Comunicação**), aplicação, protocolo de transporte; podendo ser aplicados filtros de forma a detalhar o tráfego entre determinadas estações, conversações de rede (*socket)*, unidade ou grupo de unidades distribuídas;

- Verificação do consumo de banda de uma ou mais unidades distribuídas, postos ou parceiros, permitindo filtro por endereço IP.

- Detalhamento das conversações (*socket*) e protocolos de rede utilizados por um determinado endereço IP;

- Verificação do consumo de banda total, sob forma percentual e em *kilobits* por segundo, utilizada por um ou mais aplicativos, com possibilidade de filtro por endereço IP ou faixa de endereços IPs;

- Monitoramento do tempo de resposta de aplicações, permitindo examinar o tempo de resposta percebido pelos usuários das Unidades Distribuídas, conforme indicação do Banco e prévia configuração na ferramenta de gerência.

Deverão ser providos os seguintes relatórios que permitam a análise do tráfego que passa pelos componentes Firewalls dos Postos e Superintendências:

- verificação do consumo de banda de um ou mais pontos de atendimento, permitindo filtro por endereço IP;

- detalhamento das conversações (socket) e protocolos de rede utilizados por um determinado endereço IP;

- Permita visualização de dados de segurança através de gráficos;

- verificação do consumo de banda total, sob forma percentual, utilizada por um ou mais aplicativos, com possibilidade de filtro por endereço IP ou faixa de endereços IPs.

- Monitoramento do tempo de resposta de aplicações trafegadas;

Os relatórios devem ser gerados de forma que a lista de aplicações reconhecidas seja customizável, permitindo a definição de aplicações proprietárias do Banco, a partir das informações de protocolo de transporte e da porta de comunicação utilizada.

4.5 Relatórios de Eventos Específicos

Em caso de eventos imprevistos que afetem a disponibilidade ou o desempenho de 10 (dez) ou mais unidades distribuídas ou Postos de Crédito, o Banco solicitará a emissão de um relatório específico para cada um desses eventos, explicitando as causas do incidente, soluções de contorno adotadas, ações para solução definitiva do problema e respectivo prazo, caso esta ainda não tenha sido efetivada, bem como as medidas de prevenção adotadas para evitar reincidência do evento. Outras informações julgadas pertinentes pela contratada também deverão constar nesse documento, conforme modelo constante no item 5.

5 MODELOS DOS RELATÓRIOS

Nas páginas a seguir estão os modelos de relatórios descritos no item 4, que servirão de exemplo, e devem incluir:

5.1 Modelo de Relatório de Disponibilidade – Padrão 24h
5.2 Modelo de Relatório de Disponibilidade – Comercial
5.3 Modelo de Relatório de Desempenho – Padrão 24h
5.4 Modelo de Relatório de Desempenho – Comercial
5.5 Modelo de Relatório de Faturamento
5.6 Modelo de Relatório de Serviços
5.7 Modelo de Relatório de Eventos Específicos
5.8 Modelo de Relatório de Segurança - Padrão 24h e comercial

Banco do Nordeste do Brasil S/A

Área de Tecnologia da Informação

Ambiente de Operações de Tecnologia da Informação

Central de Recursos de Comunicação

REDE INTEGRADA DE COMUNICAÇÃO

RELATÓRIO DE DISPONIBILIDADE – PADRÃO 24H

Apresenta os dados apurados desde a zero hora do primeiro dia do mês até às vinte e quatro horas do último dia do mês

Versão 1.00

Fortaleza – CE

TOPICOS QUE DEVEM CONSTAR NO RELATÓRIO:

1. Observações iniciais

2. Data de emissão:

3. Versão número:

4. Responsável:

5. Telefone:

6. E-mail:

7. Características Gerais e observações iniciais

8. Tabela de disponibilidade
   - 8.1. Unidades
     - 8.1.1. Número do evento
     - 8.1.2. Unidade
     - 8.1.3. Unidade Federativa (UF)
     - 8.1.4. Disponibilidade
       - 8.1.4.1. Percentual Realizado
       - 8.1.4.2. Percentual de Inoperância excedente ao SLA
       - 8.1.4.3. Multa
     - 8.1.5. Detalhes do evento ocorrido no Circuito Primário ou Secundário
       - 8.1.5.1. Data e Hora da abertura da falha
       - 8.1.5.2. Data e Hora da finalização da falha
       - 8.1.5.3. Tempo total da inoperância
       - 8.1.5.4. Causa da inoperância
     - 8.1.6. Prazo de Reparo (Assistência Técnica)
       - 8.1.6.1. Horas excedentes ao SLA
       - 8.1.6.2. Multa
     - 8.1.7. Tempo Medio entre Falha (*Mean Time Between Failure* – MTBF)

9. Problemas Identificados

Nº	Unidade	UF	Disponibilidade			Circuito Primário ou Secundário				Prazo de Reparo		MTBF
			Realizado (%)	Inoperância Excedente ao SLA (%)	Multa (R$)	Data/Hora Abertura da Falha	Data/Hora Finalização da Falha	Tempo Total de Inoperância	Causa	Horas Excedentes ao SLA	Multa (R$)	
1	Unidade 1	U1	-	-	-	10/3/12 16:59	10/3/12 19:21	2:21:30	Elétrica	-	-	-
2						30/3/12 17:50	30/3/12 19:48	1:57:35	Backbone			
Totalização da Unidade 1			**99%**	**1%**	**R$ 100.000,00**	**-**		**5:34:43**	**-**	**0:55:12**	**R$ 200.000,00**	**12 dias**
1	Unidade 2	U2	-	-	-	10/3/12 16:59	10/3/12 19:21	2:21:30	Elétrica	-	-	-
2						30/3/12 11:38	30/3/12 12:54	1:15:38	Elétrica			
3						30/3/12 17:50	30/3/12 19:48	1:57:35	Backbone			
4						30/3/12 16:50	30/3/12 19:48	2:57:35	Backbone			
Totalização da Unidade 2			**99%**	**1%**	**R$ 100.000,00**	**-**		**6:10:48**	**-**	**1:55:12**	**R$ 410.000,00**	**8 dias**
Total de Multas Indisponibilidade					**R$ 200.000,00**			**Total de Multas Atraso Assistência Técnica**			**R$ 610.000,00**	

Banco do Nordeste do Brasil S/A

Área de Tecnologia da Informação

Ambiente de Operações de Tecnologia da Informação

Central de Recursos de Comunicação

REDE INTEGRADA DE COMUNICAÇÃO

RELATÓRIO DE DISPONIBILIDADE – COMERCIAL

Apresenta os dados apurados desde as oito horas até as dezoito horas de cada dia útil do mês

Versão 1.00

Fortaleza – CE

TOPICOS QUE DEVEM CONSTAR NO RELATÓRIO:

1. Observações iniciais

2. Data de emissão:

3. Versão número:

4. Responsável:

5. Telefone:

6. E-mail:

7. Características Gerais e observações iniciais

8. Tabela de disponibilidade
   - 8.1. Unidades
     - 8.1.1. Número do evento
     - 8.1.2. Unidade
     - 8.1.3. Unidade Federativa (UF)
     - 8.1.4. Disponibilidade
       - 8.1.4.1. Percentual Realizado
       - 8.1.4.2. Percentual de Inoperância excedente ao SLA
       - 8.1.4.3. Multa
     - 8.1.5. Detalhes do evento ocorrido no Circuito Primário ou Secundário
       - 8.1.5.1. Data e Hora da abertura da falha
       - 8.1.5.2. Data e Hora da finalização da falha
       - 8.1.5.3. Tempo total da inoperância
       - 8.1.5.4. Causa da inoperância
     - 8.1.6. Prazo de Reparo (Assistência Técnica)
       - 8.1.6.1. Horas excedentes ao SLA
       - 8.1.6.2. Multa
     - 8.1.7. Tempo Medio entre Falha (*Mean Time Between Failure* – MTBF)

9. Problemas Identificados

Nº	Unidade	UF	Disponibilidade			Circuito Primário ou Secundário				Prazo de Reparo		MTBF
			Realizado (%)	Inoperância Excedente ao SLA (%)	Multa (R$)	Data/Hora Abertura da Falha	Data/Hora Finalização da Falha	Tempo Total de Inoperância	Causa	Horas Excedentes ao SLA	Multa (R$)	
1	Unidade 1	U1	-	-	-	10/3/12 16:59	10/3/12 19:21	2:21:30	Elétrica	-	-	-
2						30/3/12 11:38	30/3/12 12:54	1:15:38	Elétrica			
3						30/3/12 17:50	30/3/12 19:48	1:57:35	Backbone			
Totalização da Unidade 1			**99%**	**1%**	**R$ 100.000,00**	**-**		**5:34:43**	**-**	**0:55:12**	**R$ 200.000,00**	**12 dias**
1	Unidade 2	U2	-	-	-	10/3/12 16:59	10/3/12 19:21	2:21:30	Elétrica	-	-	-
2						30/3/12 11:38	30/3/12 12:54	1:15:38	Elétrica			
3						30/3/12 17:50	30/3/12 19:48	1:57:35	Backbone			
4						30/3/12 16:50	30/3/12 19:48	2:57:35	Backbone			
Totalização da Unidade 2			**99%**	**1%**	**R$ 100.000,00**	**-**		**6:10:48**	**-**	**1:55:12**	**R$ 410.000,00**	**8 dias**
Total de Multas Indisponibilidade					**R$ 200.000,00**			**Total de Multas Atraso Assistência Técnica**			**R$ 610.000,00**	

Banco do Nordeste do Brasil S/A

Área de Tecnologia da Informação

Ambiente de Operações de Tecnologia da Informação

Central de Recursos de Comunicação

REDE INTEGRADA DE COMUNICAÇÃO

RELATÓRIO DE DESEMPENHO – PADRÃO 24H

Apresenta os dados apurados desde a zero hora do primeiro dia do mês até às vinte e quatro horas do último dia do mês

Versão 1.00

Fortaleza – CE

TOPICOS QUE DEVEM CONSTAR NO RELATÓRIO:

1. Observações iniciais

2. Data de emissão:

3. Versão número:

4. Responsável:

5. Telefone:

6. E-mail:

7. Características Gerais e observações iniciais

8. Tabela de disponibilidade
   - 8.1. Número do evento
   - 8.2. Unidade
   - 8.3. Unidade Federativa (UF)
   - 8.4. Velocidade do link principal
   - 8.5. Carga de utilização média do link primário ou secundário
   - 8.6. Latência
     - 8.6.1. Latência máxima
     - 8.6.2. Latência média
     - 8.6.3. Latência excedente ao SLA
     - 8.6.4. Jitter
     - 8.6.5. Jitter excedente ao SLA
   - 8.7. Descarte de pacotes
     - 8.7.1. Descarte de pacotes
     - 8.7.2. Descarte de pacotes excedentes ao SLA
   - 8.8. Taxa de erro de Transmissão (CRC)
     - 8.8.1. CRC
     - 8.8.2. CRC excedente ao SLA
   - 8.9. Roteador
     - 8.9.1. Uso de memória do roteador
     - 8.9.2. Uso de CPU do roteador

9. Multa total

10. Problemas Identificados

Nº	Unidade	UF	Velocidade do Link	Carga de Utilização Média	Latência					Descarte de Pacotes		Taxa de Erro de Transmissão (CRC)		Roteador	
					Latência Máxima	Latência Média	Latência Excedente ao SLA	Jitter	Jitter Excedente ao SLA	Descarte de Pacotes	Descarte de Pacotes Excedente ao SLA	CRC	CRC Excedente ao SLA	Uso de Memória	Uso de CPU
1	Unidade 1	U1													
2	Unidade 2	U2													
3	Unidade 3	U3													
4	Unidade 4	U4													
5	Unidade 5	U5													
6	Unidade 6	U6													

Banco do Nordeste do Brasil S/A

Área de Tecnologia da Informação

Ambiente de Operações de Tecnologia da Informação

Central de Recursos de Comunicação

REDE INTEGRADA DE COMUNICAÇÃO

RELATÓRIO DE DESEMPENHO – COMERCIAL

Apresenta os dados apurados desde as oito horas até as dezoito horas de cada dia útil do mês

Versão 1.00

Fortaleza – CE

TOPICOS QUE DEVEM CONSTAR NO RELATÓRIO:

1. Observações iniciais

2. Data de emissão:

3. Versão número:

4. Responsável:

5. Telefone:

6. E-mail:

7. Características Gerais e observações iniciais

8. Tabela de disponibilidade
   - 8.1. Número do evento
   - 8.2. Unidade
   - 8.3. Unidade Federativa (UF)
   - 8.4. Velocidade do link principal
   - 8.5. Carga de utilização média do link primário ou secundário
   - 8.6. Latência
     - 8.6.1. Latência máxima
     - 8.6.2. Latência média
     - 8.6.3. Latência excedente ao SLA
     - 8.6.4. Jitter
     - 8.6.5. Jitter excedente ao SLA
   - 8.7. Descarte de pacotes
     - 8.7.1. Descarte de pacotes
     - 8.7.2. Descarte de pacotes excedentes ao SLA
   - 8.8. Taxa de erro de transmissão (CRC)
     - 8.8.1. CRC
     - 8.8.2. CRC excedente ao SLA
   - 8.9. Roteador
     - 8.9.1. Uso de memória do roteador
     - 8.9.2. Uso de CPU do roteador

9. Multa total

10. Problemas Identificados

Nº	Unidade	UF	Velocidade do Link	Carga de Utilização Média	Latência					Descarte de Pacotes		Taxa de Erro de Bit (BER)		Roteador	
					Latência Máxima	Latência Média	Latência Excedente ao SLA	Jitter	Jitter Excedente ao SLA	Descarte de Pacotes	Descarte de Pacotes Excedente ao SLA	BER	BER Excedente ao SLA	Uso de Memória	Uso de CPU
1	Unidade 1	U1													
2	Unidade 2	U2													
3	Unidade 3	U3													
4	Unidade 4	U4													
5	Unidade 5	U5													
6	Unidade 6	U6													

Banco do Nordeste do Brasil S/A

Área de Tecnologia da Informação

Ambiente de Operações de Tecnologia da Informação

Central de Recursos de Comunicação

REDE INTEGRADA DE COMUNICAÇÃO

RELATÓRIO DE FATURAMENTO

Versão 1.00

Fortaleza – CE

TOPICOS QUE DEVEM CONSTAR NO RELATÓRIO:

1. Observações iniciais

2. Data de emissão:

3. Versão número:

4. Responsável:

5. Telefone:

6. E-mail:

7. Observações Relevantes:

8. Tabela de Faturamento
   - 8.1. Unidades
     - 8.1.1. Número do evento
     - 8.1.2. Unidade
     - 8.1.3. Unidade Federativa
     - 8.1.4. Velocidade do link
     - 8.1.5. Valor mensal contratado
     - 8.1.6. Multas
     - 8.1.7. Ajustes
     - 8.1.8. Valor da mensalidade
     - 8.1.9. Serviços extras
     - 8.1.10. Total a pagar
     - 8.1.11. Período de referência
     - 8.1.12. Número do último aditivo

Nº	Unidade	UF	Velocidade do Link	Valor mensal contratado	Multas	Ajustes	Valor da mensalidade	Serviços extras	Total a pagar	Período de referência	Nº último aditivo
1	Unidade 1	U1									
2	Unidade 2	U2									
3	Unidade 3	U3									
4	Unidade 4	U4									
5	Unidade 5	U5									
6	Unidade 6	U6									

Banco do Nordeste do Brasil S/A

Área de Tecnologia da Informação

Ambiente de Operações de Tecnologia da Informação

Central de Recursos de Comunicação

REDE INTEGRADA DE COMUNICAÇÃO

RELATÓRIO DE SERVIÇOS

Versão 1.00

Fortaleza – CE

TOPICOS QUE DEVEM CONSTAR NO RELATÓRIO:

1. Observações iniciais

2. Data de emissão:

3. Versão número:

4. Responsável:

5. Telefone:

6. E-mail:

7. Tabela de chamados
   - 7.1. Data e horário da abertura
   - 7.2. Caracterização do chamado
     - 7.2.1. Número de identificação
     - 7.2.2. Elemento afetado
   - 7.3. Data e horário de fechamento
   - 7.4. Tempo entre abertura e fechamento

8. Resumo do relatório
   - 8.1. Total de chamados abertos
   - 8.2. Total de chamados fechados
   - 8.3. Total de chamados pendentes
   - 8.4. Os dez tipos de chamados mais frequentes
   - 8.5. Total de chamados com duração acima do prazo
   - 8.6. Reincidência de problemas

9. Ações ou sugestões decorrentes dos chamados

Nº	Unidade	UF	Caracterização do Chamado		Data/Hora da Abertura	Data/Hora do Fechamento	Tempo entre Abertura e Fechamento	Chamado acima do prazo (sim ou não)
			Número de identificação	Elemento Afetado				
1	Unidade 1	U1						
2	Unidade 2	U2						
3	Unidade 3	U3						
4	Unidade 4	U4						
5	Unidade 5	U5						
6	Unidade 6	U6						

Banco do Nordeste do Brasil S/A

Área de Tecnologia da Informação

Ambiente de Operações de Tecnologia da Informação

Central de Recursos de Comunicação

REDE INTEGRADA DE COMUNICAÇÃO

RELATÓRIO DE EVENTOS ESPECÍFICOS

Versão 1.00

Fortaleza – CE

TOPICOS QUE DEVEM CONSTAR NO RELATÓRIO:

1. Objetivo do Relatório:
2. Descrição do Evento:
    2.1. Cronologia: detalhar o momento (data/hora) de cada evento do incidente
3. Observações Relevantes:
4. Ações Corretivas:
5. Ações Preventivas:

Banco do Nordeste do Brasil S/A

Área de Tecnologia da Informação

Ambiente de Operações de Tecnologia da Informação

Central de Recursos de Comunicação

REDE INTEGRADA DE COMUNICAÇÃO

RELATÓRIO DE SEGURANÇA – PADRÃO 24H
E COMERCIAL

Versão 1.00

Fortaleza – CE

TOPICOS MÍNIMOS QUE DEVEM CONSTAR NO RELATÓRIO:

1. Observações iniciais
2. Data de emissão:
3. Versão número:
4. Responsável:
5. Telefone:
6. E-mail:
7. Características Gerais e observações iniciais
8. Identificação de Unidade: Unidade Distribuída, Postos de Crédito e Superintendências
9. Utilização de Banda por Aplicação;
10. - Principais Aplicação;
11. Too users;
12. Top Sites
13. Top Categorias
14. Top Blocked Sites
15. - Utilização de VPN;
16. - Utilização de Web por usuário;
17. - Emails;
18. - Ameaças detectadas no período;
19. - Eventos de Sistema;