



Coren/SC

Fls. nº _____

CONSELHO REGIONAL DE ENFERMAGEM DE SANTA CATARINA

Autarquia Federal criada pela Lei Nº 5.905/73

CONTRATO DE PRESTAÇÃO DE SERVIÇO N.º 008/2022**PREGÃO ELETRÔNICO N.º 004/2022****PROCESSO ADMINISTRATIVO N.º 001.926208/2022****PAD N.º 384/2021**

CONTRATANTE: CONSELHO REGIONAL DE ENFERMAGEM DE SANTA CATARINA – COREN/SC, Autarquia Federal nos termos da Lei n.º 5.905/73, dotada de personalidade jurídica de direito público, inscrito no CNPJ/MF sob o n.º 75.308.106/0001-56, com sede Av. Mauro Ramos, n.º 224, Edifício Centro Executivo Mauro Ramos, 6º, 7º e 8º andares, Centro, Florianópolis/SC, neste ato representado por seu Presidente, **GELSON LUIZ DE ALBUQUERQUE**, brasileiro, divorciado, portadora do RG n.º 5564689 - SSP/SC e do CPF/MF n.º 307.136.330-34 e pela Tesoureira, **DANIELA MAÇANEIRO**, brasileira, solteira, portadora do RG nº 3091217 – SSP/SC e do CPF/MF n.º 017.990.019-62.

CONTRATADA: SIGMAFONE TELECOMUNICAÇÕES LTDA, Pessoa Jurídica de Direito Privado, inscrito no CNPJ sob n.º 78.766.151/0001-42, com sede na Rua Anita Ribas, n.º 365, Bacacheri, na cidade de Curitiba/PR, CEP: 82.520-610, neste ato representada por seu representante legal, **Sr. Reynaldo Costa e Rosa**, brasileiro, casado, portador do RG n.º 07828450-37 SSP/BA, inscrito no CPF sob o n.º 901.580.755-87.

PREPOSTO: Thiago Alfredo Grazzotin Duarte, Consultor Comercial, inscrito no CPF sob n.º 051.396.939-09, telefone 47 99963-1172, e-mail thiago.duarte@sigmatelecom.com.br ;

FISCAIS DE CONTRATO: Michel R. Kannenberg, Técnico Especializado em Administração de Redes, inscrita no CPF sob n.º CPF sob n.º 016.744.919-21, telefone (48) 3029-5467, e-mail: michel.kannenberg@corensc.gov.br.

Tendo em vista o resultado da Licitação na modalidade Pregão Eletrônico n.º 004/2022, para contratação de solução de Firewall de Próxima Geração (Next Generation), bem como a classificação obtida no certame, formulamos e homologamos o presente CONTRATO, de acordo com as especificações, quantitativos e preços ofertados pela empresa classificada no Processo Licitatório n.º 001.926208/2022.

Cláusula 1ª DO OBJETO

- 1.1 Contratação de solução de Firewall de Próxima Geração (Next Generation) para Segurança da Informação de perímetro que possibilite a visibilidade e controle de tráfego, filtragem de conteúdo web, prevenção contra ataques e ameaças modernas, filtro de dados, VPN e controle granular de banda de rede, compreendendo fornecimento de equipamentos e softwares integrados em forma de appliance conforme quantidades e exigências estabelecidas neste Contrato.

Bens e/ou Serviços			
Grupo	Item	Bem/Serviço	QTD

**CONSELHO REGIONAL DE ENFERMAGEM DE SANTA CATARINA**

Autarquia Federal criada pela Lei Nº 5.905/73

1	1	Fornecimento de Firewall NGFW	01
	2	Licença 36 meses de Application Control, IPS, AMP, Web Filtering e Serviço antispam	Única
	3	Licença 36 meses de Solução de logs, análise e relatórios.	Única
	4	Serviço de instalação, configuração e treinamento dos itens 1,2 e 3	Única
	5	Suporte Mensal – período 36 meses	36 meses

Cláusula 2ª VALOR DO CONTRATO

2.1 O presente Contrato obedece aos seguintes valores:

Item	Descrição dos bens/licenças/serviços	Quantidade	Quantidade Licenças	Valor Total
01	Fornecimento de Firewall NGFW	01	Não se aplica	R\$ 51.000,00
02	Licença 36 meses de Application Control, IPS, AMP, Web Filtering e Serviço antispam	Não se aplica	01	R\$ 57.274,32
03	Licença 36 meses de Solução de logs, análise e relatórios	Não se aplica	01	R\$ 27.050,12
04	Serviço de instalação, configuração e treinamento dos itens 1,2 e 3	01	Não se aplica	R\$ 10.546,00
Item	Descrição dos bens/licenças/serviços	Quantidade Meses	Valor Mensal	Valor Total
05	Suporte Mensal	36	R\$ 500,00	R\$ 18.000,00
Custo Total da Contratação.....				R\$ 168.870,44

Cláusula 3ª ESPECIFICAÇÕES TÉCNICAS**3.1 CONSIDERAÇÕES GERAIS**

- 3.1.1 Não deverão ser cotados produtos que não atendam as especificações mínimas previstas nas especificações técnicas, sob pena de desclassificação;
- 3.1.2 O fabricante deve ter obtido mínimo de 75% (setenta e cinco por cento) de efetividade de segurança no teste SVM - Security Value Map de Next Generation Firewall NGFW e à direita da linha da média de custo, que cresce no referido gráfico da direita para a esquerda, executado pela NSS Labs (www.nsslabs.com) em algum dos relatórios entre 2017 a 2021;
- 3.1.3 O fabricante deve ter obtido mínimo de 90% (noventa por cento) de efetividade de segurança no teste SVM – Security Value Map de Next Generation Intrusion Prevention



CONSELHO REGIONAL DE ENFERMAGEM DE SANTA CATARINA

Autorquia Federal criada pela Lei Nº 5.905/73

Systems NGIPS executado pela NSS Labs (www.nsslabs.com) em algum dos relatórios entre 2017 e 2021;

3.1.4 A solução ofertada deve ser de fabricante constante no Quadrante Mágico do Gartner, no quesito NGFW;

3.1.5 Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste Contrato deverão ser fornecidos.

Cláusula 4ª FIREWALL NGFW

4.1 CARACTERÍSTICA DO EQUIPAMENTO

4.1.1 Deve suportar, no mínimo, 18 Gbps com a funcionalidade de firewall habilitada para tráfego IPv4 e IPv6 (considerando pacotes de 512 bytes);

4.1.2 Deve suportar, no mínimo, 2.6 Gbps de throughput IPS;

4.1.3 Deve suportar, no mínimo, 11.5 Gbps de throughput de VPN IPsec;

4.1.4 Deve suportar, no mínimo, 1 Gbps de throughput de VPN SSL;

4.1.5 Deve suportar, no mínimo, 1 Gbps de throughput de Inspeção SSL;

4.1.6 Deve suportar, no mínimo, 2.2 Gbps de throughput de Controle de Aplicação;

4.1.7 Deve suportar, no mínimo, 1 Gbps de throughput com as seguintes funcionalidades habilitadas simultaneamente, para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: firewall, controle de aplicação, IPS e antimalware;

4.1.8 Suporte a, no mínimo, 1.5 milhão de conexões simultâneas;

4.1.9 Suporte a, no mínimo, 56 mil novas conexões por segundo;

4.1.10 Estar licenciado para, ou suportar sem o uso de licença, até 2 mil túneis de VPN IPSEC Site-to-Site simultâneos;

4.1.11 Estar licenciado para, ou suportar sem o uso de licença, até 16 mil túneis de clientes VPN IPSEC simultâneos;

4.1.12 Estar licenciado para, ou suportar sem o uso de licença, até 500 clientes de VPN SSL simultâneos;

4.1.13 Permitir gerenciar ao menos 128 Access Points;

4.1.14 Possuir ao menos 18 interfaces 1Gbps RJ45;

4.1.15 Possuir ao menos 2 interfaces 10Gbps SFP+;

4.1.16 Possuir ao menos 4 interfaces 1Gbps SFP;



CONSELHO REGIONAL DE ENFERMAGEM DE SANTA CATARINA

Autarquia Federal criada pela Lei Nº 5.905/73

- 4.1.17 Estar licenciado e/ou ter incluído sem custo adicional, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance;
- 4.1.18 Suporte a, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance;
- 4.1.19 Possuir fonte de alimentação 100-240V AC interna redundante;
- 4.1.20 Possuir no máximo 1 RU de altura.

4.2 REQUISITOS MÍNIMOS DE FUNCIONALIDADES

4.2.1 Características Gerais

- 4.2.1.1. A solução deve consistir em plataforma de proteção de rede baseada em appliance com funcionalidades de Next Generation Firewall (NGFW), e console de gerência e monitoração;
- 4.2.1.2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
- 4.2.1.3. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação;
- 4.2.1.4. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
- 4.2.1.5. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;
- 4.2.1.6. A gestão do equipamento deve ser compatível através da interface de gestão Web no mesmo dispositivo de proteção da rede;
- 4.2.1.7. Os dispositivos de proteção de rede devem possuir suporte a 4094 VLAN Tags 802.1q;
- 4.2.1.8. Os dispositivos de proteção de rede devem possuir suporte a agregação de links 802.3ad e LACP;
- 4.2.1.9. Os dispositivos de proteção de rede devem possuir suporte a Policy based routing ou policy based forwarding;
- 4.2.1.10. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);
- 4.2.1.11. Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay;
- 4.2.1.12. Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;
- 4.2.1.13. Os dispositivos de proteção de rede devem suportar sFlow;
- 4.2.1.14. Os dispositivos de proteção de rede devem possuir suporte a Jumbo Frames;

**CONSELHO REGIONAL DE ENFERMAGEM DE SANTA CATARINA**

Autarquia Federal criada pela Lei Nº 5.905/73

- 4.2.1.15. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet lógicas;
- 4.2.1.16. Deve suportar NAT dinâmico (Many-to-1);
- 4.2.1.17. Deve suportar NAT dinâmico (Many-to-Many);
- 4.2.1.18. Deve suportar NAT estático (1-to-1);
- 4.2.1.19. Deve suportar NAT estático (Many-to-Many);
- 4.2.1.20. Deve suportar NAT estático bidirecional 1-to-1;
- 4.2.1.21. Deve suportar Tradução de porta (PAT);
- 4.2.1.22. Deve suportar NAT de Origem;
- 4.2.1.23. Deve suportar NAT de Destino;
- 4.2.1.24. Deve suportar NAT de Origem e NAT de Destino simultaneamente;
- 4.2.1.25. Deve poder combinar NAT de origem e NAT de destino na mesma política;
- 4.2.1.26. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
- 4.2.1.27. Deve suportar NAT64 e NAT46;
- 4.2.1.28. Deve implementar o protocolo ECMP;
- 4.2.1.29. Deve permitir monitorar via SNMP falhas de hardware, uso de recursos por número elevado de sessões, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede;
- 4.2.1.30. Enviar log para sistemas de monitoração externos, simultaneamente;
- 4.2.1.31. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;
- 4.2.1.32. Proteção anti-spoofing;
- 4.2.1.33. Suportar otimização do tráfego entre dois equipamentos;
- 4.2.1.34. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
- 4.2.1.35. Para IPv6, deve suportar roteamento estático e dinâmico (RIPng, OSPFv3, BGP4+);
- 4.2.1.36. Suportar OSPF graceful restart;
- 4.2.1.37. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
- 4.2.1.38. Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;



CONSELHO REGIONAL DE ENFERMAGEM DE SANTA CATARINA

Autarquia Federal criada pela Lei Nº 5.905/73

- 4.2.1.39. Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;
- 4.2.1.40. Deve suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
- 4.2.1.41. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em modo transparente;
- 4.2.1.42. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3;
- 4.2.1.43. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3 e com no mínimo 3 equipamentos no cluster;
- 4.2.1.44. A configuração em alta disponibilidade deve sincronizar: Sessões;
- 4.2.1.45. A configuração em alta disponibilidade deve sincronizar: Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede;
- 4.2.1.46. A configuração em alta disponibilidade deve sincronizar: Associações de Segurança das VPNs;
- 4.2.1.47. A configuração em alta disponibilidade deve sincronizar: Tabelas FIB;
- 4.2.1.48. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;
- 4.2.1.49. Deve possuir suporte a criação de sistemas virtuais no mesmo appliance;
- 4.2.1.50. Em alta disponibilidade, deve ser possível o uso de clusters virtuais, seja ativo-ativo ou ativo-passivo, permitindo a distribuição de carga entre diferentes contextos;
- 4.2.1.51. Deve permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados por equipes distintas;
- 4.2.1.52. O gerenciamento da solução deve suportar acesso via SSH e interface WEB (HTTPS), incluindo, mas não limitado à, exportar configuração dos sistemas virtuais (contextos) por ambas interfaces;
- 4.2.1.53. Controle, inspeção e descriptografia de SSL para tráfego de entrada (Inbound) e Saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);
- 4.2.1.54. A solução deve identificar potenciais vulnerabilidades e destacar as melhores práticas que poderiam ser usadas para melhorar a segurança e o desempenho geral de uma rede;
- 4.2.1.55. O console de administração deve suportar pelo menos inglês, espanhol e português do Brasil;



CONSELHO REGIONAL DE ENFERMAGEM DE SANTA CATARINA

Autarquia Federal criada pela Lei Nº 5.905/73

- 4.2.1.56. O console deve suportar o gerenciamento de switches e pontos de acesso wireless para melhorar o nível de segurança;
- 4.2.1.57. A solução deve oferecer suporte à integração nativa de equipamentos de proteção de email, firewall de aplicativos, proxy, cache e ameaças avançadas;
- 4.2.1.58. Deverá ser comprovado que a solução ofertada foi aprovada no conjunto de critérios de avaliação contido nos testes da NSS Labs, da ICSSA Labs, ou por meio de certificação similar, que cumpra a mesma finalidade ou que ateste as mesmas funcionalidades.
- 4.2.2. Controle por Política de Firewall
- 4.2.2.1. Deverá suportar controles por zona de segurança;
- 4.2.2.2. Controles de políticas por porta e protocolo;
- 4.2.2.3. Controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;
- 4.2.2.4. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
- 4.2.2.5. Firewall deve ser capaz de aplicar a inspeção UTM (Application Control e Webfiltering no mínimo) diretamente às políticas de segurança versus via perfis;
- 4.2.2.6. Além dos endereços e serviços de destino, objetos de serviços de Internet devem poder ser adicionados diretamente às políticas de firewall;
- 4.2.2.7. Ele deve suportar a automação de situações como detecção de equipamentos comprometidos, status do sistema, alterações de configuração, eventos específicos e aplicar uma ação que pode ser notificação, bloqueio de um computador, execução de scripts ou funções em nuvem pública;
- 4.2.2.8. Deve suportar o padrão de indústria 'syslog' protocol para armazenamento usando o formato Common Event Format (CEF);
- 4.2.2.9. Deve haver uma maneira de assegurar que o armazenamento dos logs em tempo real não supere a velocidade de upload;
- 4.2.2.10. Deve suportar o protocolo padrão da indústria VXLAN;
- 4.2.2.11. Deve suportar objetos de endereço IPv4 e IPv6, consolidados na mesma regra/política de firewall;
- 4.2.2.12. Deve possuir base com objetos de endereço IP, de serviços da internet como Google e Office 365, atualizados dinamicamente pela solução;
- 4.2.2.13. A solução deve oferecer suporte à integração nativa com a solução de sandbox, proteção de email, cache e firewall de aplicativos da Web.
- 4.2.3. Controle de aplicações



CONSELHO REGIONAL DE ENFERMAGEM DE SANTA CATARINA

Autarquia Federal criada pela Lei Nº 5.905/73

- 4.2.3.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;
- 4.2.3.2. Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado a: tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;
- 4.2.3.3. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, LinkedIn, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;
- 4.2.3.4. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;
- 4.2.3.5. Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
- 4.2.3.6. Identificar o uso de táticas evasivas via comunicações criptografadas;
- 4.2.3.7. Atualizar a base de assinaturas de aplicações automaticamente;
- 4.2.3.8. Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos;
- 4.2.3.9. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;
- 4.2.3.10. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;
- 4.2.3.11. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
- 4.2.3.12. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;
- 4.2.3.13. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;
- 4.2.3.14. Deve possibilitar a diferenciação e controle de partes das aplicações como, por exemplo, permitir o Hangouts chat e bloquear a chamada de vídeo;
- 4.2.3.15. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;



CONSELHO REGIONAL DE ENFERMAGEM DE SANTA CATARINA

Autarquia Federal criada pela Lei Nº 5.905/73

- 4.2.3.16. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);
- 4.2.3.17. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Nível de risco da aplicação;
- 4.2.3.18. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;
- 4.2.3.19. Deve ser possível configurar Application Override permitindo selecionar aplicações individualmente.
- 4.2.4. Prevenção de Ameaças
 - 4.2.4.1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;
 - 4.2.4.2. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
 - 4.2.4.3. As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;
 - 4.2.4.4. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;
 - 4.2.4.5. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
 - 4.2.4.6. Deve permitir o bloqueio de vulnerabilidades;
 - 4.2.4.7. Deve incluir proteção contra ataques de negação de serviços;
 - 4.2.4.8. Deverá possuir o seguinte mecanismo de inspeção de IPS: Análise de decodificação de protocolo;
 - 4.2.4.9. Deverá possuir o seguinte mecanismo de inspeção de IPS: Análise para detecção de anomalias de protocolo;
 - 4.2.4.10. Deverá possuir o seguinte mecanismo de inspeção de IPS: IP Defragmentation;
 - 4.2.4.11. Deverá possuir o seguinte mecanismo de inspeção de IPS: Remontagem de pacotes de TCP;
 - 4.2.4.12. Deverá possuir o seguinte mecanismo de inspeção de IPS: Bloqueio de pacotes malformados;



CONSELHO REGIONAL DE ENFERMAGEM DE SANTA CATARINA

Autarquia Federal criada pela Lei Nº 5.905/73

- 4.2.4.13. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;
 - 4.2.4.14. Detectar e bloquear a origem de portscans;
 - 4.2.4.15. Bloquear ataques efetuados por worms conhecidos;
 - 4.2.4.16. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
 - 4.2.4.17. Possuir assinaturas para bloqueio de ataques de buffer overflow;
 - 4.2.4.18. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
 - 4.2.4.19. Identificar e bloquear comunicação com botnets;
 - 4.2.4.20. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
 - 4.2.4.21. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;
 - 4.2.4.22. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;
 - 4.2.4.23. Os eventos devem identificar o país de onde partiu a ameaça;
 - 4.2.4.24. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;
 - 4.2.4.25. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;
 - 4.2.4.26. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança;
 - 4.2.4.27. Suportar e estar licenciado com proteção contra ataques de dia zero por meio de integração com solução de Sandbox em nuvem, do mesmo fabricante.
- 4.2.5. Filtro de URL
- 4.2.5.1. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
 - 4.2.5.2. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local, em modo de proxy transparente e explícito;



CONSELHO REGIONAL DE ENFERMAGEM DE SANTA CATARINA

Autarquia Federal criada pela Lei Nº 5.905/73

- 4.2.5.3. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
 - 4.2.5.4. Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;
 - 4.2.5.5. Possuir pelo menos 60 categorias de URLs;
 - 4.2.5.6. Deve possuir a função de exclusão de URLs do bloqueio, por categoria;
 - 4.2.5.7. Permitir a customização de página de bloqueio;
 - 4.2.5.8. Permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão continuar para permitir o usuário continuar acessando o site);
 - 4.2.5.9. Além do Explicit Web Proxy, suportar proxy Web transparente.
- 4.2.6. Identificação de Usuários
- 4.2.6.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local;
 - 4.2.6.2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
 - 4.2.6.3. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários ou qualquer tipo de restrição de uso como, mas não limitado à, utilização de sistemas virtuais, segmentos de rede, etc;
 - 4.2.6.4. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
 - 4.2.6.5. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;
 - 4.2.6.6. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);
 - 4.2.6.7. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server,



CONSELHO REGIONAL DE ENFERMAGEM DE SANTA CATARINA

Autarquia Federal criada pela Lei Nº 5.905/73

permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;

- 4.2.6.8. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;
 - 4.2.6.9. Permitir integração com tokens para autenticação dos usuários, incluindo, mas não limitado a acesso a internet e gerenciamento da solução;
 - 4.2.6.10. Prover no mínimo um token nativamente, possibilitando autenticação de duplo fator.
- 4.2.7. QoS e Traffic Shaping
- 4.2.7.1. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como Youtube, Ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máxima largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;
 - 4.2.7.2. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem;
 - 4.2.7.3. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino;
 - 4.2.7.4. Suportar a criação de políticas de QoS e Traffic Shaping por usuário e grupo;
 - 4.2.7.5. Suportar a criação de políticas de QoS e Traffic Shaping por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;
 - 4.2.7.6. Suportar a criação de políticas de QoS e Traffic Shaping por porta;
 - 4.2.7.7. O QoS deve possibilitar a definição de tráfego com banda garantida;
 - 4.2.7.8. O QoS deve possibilitar a definição de tráfego com banda máxima;
 - 4.2.7.9. O QoS deve possibilitar a definição de fila de prioridade;
 - 4.2.7.10. Suportar marcação de pacotes Diffserv, inclusive por aplicação;
 - 4.2.7.11. Suportar modificação de valores DSCP para o Diffserv;
 - 4.2.7.12. Suportar priorização de tráfego usando informação de Type of Service;
 - 4.2.7.13. Deve suportar QOS (traffic-shapping), em interface agregadas ou redundantes.
- 4.2.8. Filtro de Dados
- 4.2.8.1. Permitir a criação de filtros para arquivos e dados pré-definidos;
 - 4.2.8.2. Os arquivos devem ser identificados por extensão e tipo;



CONSELHO REGIONAL DE ENFERMAGEM DE SANTA CATARINA

Autarquia Federal criada pela Lei Nº 5.905/73

- 4.2.8.3. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc);
- 4.2.8.4. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
- 4.2.8.5. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
- 4.2.8.6. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.
- 4.2.9. Geo Localização
 - 4.2.9.1. Suportar a criação de políticas por geo-localização, permitindo o tráfego de determinado País/Países sejam bloqueados;
 - 4.2.9.2. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
 - 4.2.9.3. Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas;
- 4.2.10. VPN (Virtual Private Network);
 - 4.2.10.1. Suportar VPN Site-to-Site e Cliente-To-Site;
 - 4.2.10.2. Suportar IPSec VPN;
 - 4.2.10.3. Suportar SSL VPN;
 - 4.2.10.4. A VPN IPSEC deve suportar Autenticação MD5 e SHA-1;
 - 4.2.10.5. A VPN IPSEC deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;
 - 4.2.10.6. A VPN IPSEC deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);
 - 4.2.10.7. A VPN IPSEC deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);
 - 4.2.10.8. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;
 - 4.2.10.9. Suportar VPN em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6;
 - 4.2.10.10. Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de troubleshooting;
 - 4.2.10.11. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;



CONSELHO REGIONAL DE ENFERMAGEM DE SANTA CATARINA

Autarquia Federal criada pela Lei Nº 5.905/73

- 4.2.10.12. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
- 4.2.10.13. Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;
- 4.2.10.14. Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
- 4.2.10.15. Deverá manter uma conexão segura com o portal durante a sessão;
- 4.2.10.16. O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bit), Windows 8 (32 e 64 bit), Windows 10 (32 e 64 bit) e Mac OS X (v10.10 ou superior);
- 4.2.10.17. Deve suportar Auto-Discovery Virtual Private Network (ADVPN);
- 4.2.10.18. Deve suportar agregação de túneis IPsec;
- 4.2.10.19. Deve suportar algoritmo de balanceamento do tipo WRR (Weighted Round Robin) em agregação de túneis IPsec;
- 4.2.10.20. A VPN IPsec deve suportar Forward Error Correction (FEC);
- 4.2.10.21. Deve suportar TLS 1.3 em VPN SSL.

4.2.11. Wireless Controller

- 4.2.11.1. Deverá administrar e controlar de maneira centralizada os pontos de acesso wireless do mesmo fabricante da solução ofertada;
- 4.2.11.2. Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac e que transmitam tráfego IPv4 e IPv6 através do controlador;
- 4.2.11.3. A solução deverá ser capaz de gerenciar pontos de acesso do tipo indoor e outdoor;
- 4.2.11.4. O controlador wireless deve permitir ser descoberto automaticamente pelos pontos de acesso através de Broadcast, DHCP e consulta DNS;
- 4.2.11.5. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário;
- 4.2.11.6. Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points;
- 4.2.11.7. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes devem ser tunelados até o controlador wireless;



CONSELHO REGIONAL DE ENFERMAGEM DE SANTA CATARINA

Autarquia Federal criada pela Lei Nº 5.905/73

- 4.2.11.7.1. Quando tunelado, o tráfego deve ser criptografado através de DTLS ou IPSEC;
- 4.2.11.8. Deve permitir o gerenciamento de pontos de acesso conectados remotamente através de links WAN. Neste cenário o encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma distribuída (local switching), ou seja, o tráfego deve ser comutado localmente na interface LAN do ponto de acesso e não necessitará de tunelamento até o controlador wireless;
- 4.2.11.9. Quando o encaminhamento do tráfego for distribuído (local switching) e a autenticação via PSK, caso haja falha na comunicação entre os pontos de acesso e o controlador wireless, os usuários associados devem permanecer associados aos pontos de acesso e ao mesmo SSID. Deve ser possível ainda permitir a conexão de novos usuários à rede wireless;
- 4.2.11.10. A solução deve permitir definir quais redes serão tuneladas até a controladora e quais redes serão comutadas diretamente pela interface do ponto de acesso;
- 4.2.11.11. A solução deve suportar recurso de Split-Tunneling de forma que seja possível definir, através das sub-redes de destino, quais pacotes serão tunelados até a controladora e quais serão comutados localmente na interface do ponto de acesso;
- 4.2.11.12. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;
- 4.2.11.13. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado dBm;
- 4.2.11.14. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso;
- 4.2.11.15. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como Rogue APs. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados;
- 4.2.11.16. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN;



CONSELHO REGIONAL DE ENFERMAGEM DE SANTA CATARINA

Autarquia Federal criada pela Lei Nº 5.905/73

- 4.2.11.17. A solução deve detectar os pontos de acesso não autorizados e/ou intrusos através de rádios dedicados para a função de análise ou através de Off-channel/Background scanning. Quando realizada através de Off-channel/Background scanning, a solução deve ser capaz de identificar a utilização do ponto de acesso para, caso necessário, atrasar a análise e desta forma não prejudicar os clientes conectados;
- 4.2.11.18. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless;
- 4.2.11.19. A solução deve permitir a adição de controlador redundante operando em N+1. Neste modo, o controlador redundante deve monitorar a disponibilidade e sincronizar as configurações do principal, além de assumir todas as funções em caso de falha do controlador primário. Desta forma, todos os pontos de acesso devem se associar automaticamente ao controlador redundante que passará a ter função de primário de forma temporária;
- 4.2.11.20. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas sub-redes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP;
- 4.2.11.21. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado;
- 4.2.11.22. A solução deve garantir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários;
- 4.2.11.23. Deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio;
- 4.2.11.24. A solução deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;
- 4.2.11.25. A solução deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;
- 4.2.11.26. A solução deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;
- 4.2.11.27. A solução deve implementar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless;



CONSELHO REGIONAL DE ENFERMAGEM DE SANTA CATARINA

Autarquia Federal criada pela Lei Nº 5.905/73

- 4.2.11.28. A solução deve suportar priorização via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada;
- 4.2.11.29. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas;
- 4.2.11.30. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, Fabricante e sistema operacional do dispositivo, Endereço IP, SSID ao qual está conectado, Ponto de acesso ao qual está conectado, Canal ao qual está conectado, Banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação;
- 4.2.11.31. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering;
- 4.2.11.32. A solução deve permitir a configuração de quais data rates estarão ativos na ferramenta e quais serão desabilitados para as frequências de 2.4 e 5GHz e padrões 802.11a/b/g/n/ac;
- 4.2.11.33. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime;
- 4.2.11.34. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados;
- 4.2.11.35. A solução deve permitir a configuração do valor de Short Guard Interval para 802.11n e 802.11ac em 5GHz;
- 4.2.11.36. A solução deve implementar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime alocando porcentagens a serem utilizadas nos SSIDs;
- 4.2.11.37. A solução deve implementar regras de firewall (stateful) para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que deve usar como critério endereços de origem e destino (IPv4 e IPv6), portas e protocolos;
- 4.2.11.38. A solução deve implementar recurso de web filtering para controle de websites acessados na rede wireless. Deve possuir uma base de conhecimento para categorização dos sites e permitir configurar quais categorias de sites serão permitido e bloqueados para cada perfil de usuário e SSID;

**CONSELHO REGIONAL DE ENFERMAGEM DE SANTA CATARINA**

Autarquia Federal criada pela Lei Nº 5.905/73

- 4.2.11.39. A solução deve possuir capacidade de reconhecimento de aplicações através da técnica de DPI (Deep Packet Inspection) que permita ao administrador da rede monitorar o perfil de acesso dos usuários e implementar políticas de controle. Deve permitir o funcionamento deste recurso e a atualização periódica da base de aplicações durante todo o período de garantia da solução;
- 4.2.11.40. A base de reconhecimento de aplicações através de DPI deve identificar com, no mínimo, 1500 (mil e quinhentas) aplicações;
- 4.2.11.41. A solução deve permitir a criação de regras para bloqueio e limite de banda (em Mbps, Kbps ou Bps) para as aplicações reconhecidas através da técnica de DPI;
- 4.2.11.42. A solução deve ainda, através da técnica de DPI, reconhecer aplicações sensíveis ao negócio e permitir a priorização deste tráfego com marcação QoS;
- 4.2.11.43. A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados:
- 4.2.11.43.1. Ataques de flood contra o protocolo EAPOL (EAPOL Flooding);
- 4.2.11.43.2. Os seguintes ataques de negação de serviço: Association Flood, Authentication Flood, Broadcast Deauthentication e Spoofed Deauthentication; Split-Tunneling
- 4.2.11.43.3. ASLEAP;
- 4.2.11.43.4. Null Probe Response / Null SSID Probe Response;
- 4.2.11.43.5. Long Duration;
- 4.2.11.43.6. Ataques contra Wireless Bridges;
- 4.2.11.43.7. Weak WEP;
- 4.2.11.43.8. Invalid MAC OUI.
- 4.2.11.44. A solução deve implementar mecanismos de proteção para mitigar ataques à infraestrutura wireless. Ao menos ataques de negação de serviço devem ser mitigados pela infraestrutura através do envio de pacotes de autenticação;
- 4.2.11.45. A solução deve implementar mecanismos de proteção contra ataques do tipo ARP Poisoning na rede wireless;
- 4.2.11.46. A solução deve monitorar e classificar o risco das aplicações acessadas pelos clientes wireless;
- 4.2.11.47. Permitir configurar o bloqueio na comunicação entre os clientes wireless conectados a um determinado SSID;



**CONSELHO REGIONAL DE ENFERMAGEM DE SANTA CATARINA**

Autarquia Federal criada pela Lei Nº 5.905/73

- 4.2.11.48. Deve implementar autenticação administrativa através do protocolo RADIUS;
- 4.2.11.49. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);
- 4.2.11.50. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3;
- 4.2.11.51. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID;
- 4.2.11.52. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada;
- 4.2.11.53. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;
- 4.2.11.54. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações 802.1X;
- 4.2.11.55. A solução deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;
- 4.2.11.56. A solução deve implementar recurso para autenticação dos usuários através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informarem as credenciais válidas para acesso à rede;
- 4.2.11.57. A solução deve permitir a hospedagem do captive portal na memória interna do controlador wireless;
- 4.2.11.58. A solução deve permitir a customização da página de autenticação, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens;
- 4.2.11.59. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede;
- 4.2.11.60. A solução deve permitir que a página de autenticação seja hospedada em servidor externo;
- 4.2.11.61. A solução deve permitir o cadastramento de contas para usuários visitantes na memória interna. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada;
- 4.2.11.62. A solução deve garantir que usuários se autenticuem em captive portal que faça uso de endereço IPv6;



CONSELHO REGIONAL DE ENFERMAGEM DE SANTA CATARINA

Autarquia Federal criada pela Lei Nº 5.905/73

- 4.2.11.63. A solução deve possuir interface gráfica para administração e gerenciamento das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução;
- 4.2.11.64. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado;
- 4.2.11.65. A solução deve implementar recurso de DHCP Server (IPv4 e IPv6) para facilitar a configuração de redes visitantes;
- 4.2.11.66. A solução deve identificar automaticamente o tipo de equipamento e sistema operacional utilizado pelo dispositivo conectado à rede wireless;
- 4.2.11.67. A solução deve permitir que os usuários sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras sub-redes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado;
- 4.2.11.68. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados;
- 4.2.11.69. A solução deve permitir a configuração de rede Mesh entre pontos de acesso indoor e outdoor;
- 4.2.11.70. A solução deve permitir ser gerenciada através dos protocolos HTTPS e SSH via IPv4 e IPv6;
- 4.2.11.71. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos;
- 4.2.11.72. A solução deve permitir ser gerenciada através do protocolo SNMP (v1, v2c e v3), além de emitir notificações através da geração de traps;
- 4.2.11.73. A solução deve permitir que softwares de gerenciamento realizem consultas diretamente nos pontos de acesso via protocolo SNMP;
- 4.2.11.74. A solução deve incluir suporte para as RFCs 1213 (MIB II) e RFC 2665 (Ethernet-like MIB);
- 4.2.11.75. A solução deve permitir a captura de pacotes na rede wireless e exporta-los em arquivos no formato .pcap;
- 4.2.11.76. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD;
- 4.2.11.77. A solução deve apresentar graficamente a topologia lógica da rede, representar os elementos da rede gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles;
- 4.2.11.78. A solução deve implementar o gerenciamento unificado e de forma gráfica para redes WiFi e redes cabeadas;



CONSELHO REGIONAL DE ENFERMAGEM DE SANTA CATARINA

Autarquia Federal criada pela Lei Nº 5.905/73

- 4.2.11.79. A solução deve permitir a atualização de firmware do controlador wireless mesmo quando conectado remotamente;
- 4.2.11.80. A solução deve permitir a identificação do firmware utilizado por cada ponto de acesso gerenciado e permitir a atualização individualizada através da interface gráfica;
- 4.2.11.81. A solução deve possuir ferramentas de diagnósticos e debug;
- 4.2.11.82. A solução deve suportar comunicação com elementos externos através de APIs;

4.2.12. SD-WAN

- 4.2.12.1. Deve implementar balanceamento de link por hash do IP de origem;
- 4.2.12.2. Deve implementar balanceamento de link por hash do IP de origem e destino;
- 4.2.12.3. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links;
- 4.2.12.4. Deve implementar balanceamento de link por custo configurado do link;
- 4.2.12.5. Deve suportar o balanceamento de, no mínimo, 256 links;
- 4.2.12.6. Deve suportar o balanceamento de links de interfaces físicas, sub-interfaces lógicas de VLAN e túneis IPsec;
- 4.2.12.7. Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;
- 4.2.12.8. Deve gerar log de eventos que registrem alterações no estado dos links do SDWAN, monitorados pela checagem de saúde.

Deve suportar Zero-Touch Provisioning;

- 4.2.12.9. Possuir checagem do estado de saúde do Link baseando-se em critérios mínimos de: Latência, Jitter e Perda de Pacotes;
- 4.2.12.10. Deve ser possível configurar a porcentagem de perda de pacotes e o tempo de latência e jitter, na medição de estado de link. Estes valores serão utilizados pela solução para decidir qual link será utilizado;
- 4.2.12.11. A solução deve permitir modificar o intervalo de tempo de checagem, em segundos, para cada um dos links;
- 4.2.12.12. A checagem de estado de saúde deve suportar teste com Ping, HTTP e DNS;
- 4.2.12.13. Suportar UDP Hole Punching em arquitetura ADVPN;
- 4.2.12.14. A checagem de estado de saúde deve suportar a marcação de pacotes com DSCP, para avaliação mais precisa de links que possuem QoE configurado;
- 4.2.12.15. As regras de escolha do link SD-WAN devem suportar o reconhecimento de aplicações, grupos de usuários, endereço IP de destino e Protocolo;



CONSELHO REGIONAL DE ENFERMAGEM DE SANTA CATARINA

Autarquia Federal criada pela Lei Nº 5.905/73

- 4.2.12.16. Deve suportar a configuração de nível mínimo de qualidade (latência, jitter e perda de pacotes) para que determinado link seja escolhido pelo SD-WAN;
- 4.2.12.17. Deve suportar envio de BGP route-map para BGP neighbors, caso a qualidade mínima de um link não seja detectada pela checagem de saúde do link.

Cláusula 5ª SOLUÇÃO DE LOGS, ANÁLISE E RELATÓRIOS

5.1. CARACTERÍSTICAS DO SISTEMA

- 5.1.1. Deve ser do mesmo fabricante da solução de firewall (NGFW) ofertada;
- 5.1.2. Deve ser obrigatoriamente uma solução em nuvem do próprio fabricante da solução de firewall (NGFW) ofertada;
- 5.1.3. Possuir capacidade de recebimento e retenção de logs de pelo menos 1 ano.

5.2. REQUISITOS MÍNIMOS DE FUNCIONALIDADE

5.2.1. Funcionalidades Gerais

- 5.2.1.1. Suportar o acesso via SSH e WEB (HTTPS) para gerenciamento de soluções;
- 5.2.1.2. Permitir a criação de administrador geral, que tenha acesso geral a todas as informações;
- 5.2.1.3. Deve possuir a funcionalidade de segundo fator de autenticação via token (aplicação) e email;
- 5.2.1.4. Deve possuir um dashboard centralizado;
- 5.2.1.5. Deve possuir no mínimo as seguintes opções disponíveis no portal de visualização:
 - 5.2.1.5.1. Visão geral da rede
 - 5.2.1.5.1.1. Deve conter no mínimo as seguintes informações para serem customizadas na lista de visualização:
 - 5.2.1.5.1.1.1. Modelo/número de série do equipamento;
 - 5.2.1.5.1.1.2. Versão do firmware;
 - 5.2.1.5.1.1.3. Status (se o equipamento estiver conectado através de um túnel de gerenciamento);
 - 5.2.1.5.1.1.4. Status SD-WAN;
 - 5.2.1.5.1.1.5. Último relatório compilado;

**CONSELHO REGIONAL DE ENFERMAGEM DE SANTA CATARINA**

Autarquia Federal criada pela Lei Nº 5.905/73

- 5.2.1.5.1.1.6. Data de expiração da licença/subscrição;
- 5.2.1.5.1.1.7. Tráfego de entrada/saída;
- 5.2.1.5.1.1.8. Endereço IP público;
- 5.2.1.5.1.1.9. Última vez que uma configuração de backup foi criada.
- 5.2.1.5.1.2. Deve possuir a visualização em formato de mapa, permitindo visualizar a localização geográfica do equipamento.
 - 5.2.1.5.2. Gerenciamento de scripts;
 - 5.2.1.5.3. Criação e alteração de configurações dos relatórios;
 - 5.2.1.5.4. Inventário para visualização de equipamentos sendo monitorados;
 - 5.2.1.5.5. Gerenciamento de contas de administrador.
- 5.2.1.6. Deve possuir visualização de log em tempo real, com filtros;
- 5.2.1.7. Deve possuir análise drilldown para localização em tempo real, usuários, e análise de atividade de rede e alerta de perfis;
- 5.2.1.8. Deve possuir gerador de relatório com modelos de relatórios personalizados e relatórios de agendamento em diferentes formatos para exibir análises baseadas em localização ou ilustrar plataformas de uso de rede;
- 5.2.1.9. Deve mostrar o status de arquivos suspeitos passando por análise de sandbox baseado em nuvem;
- 5.2.1.10. Deve possuir integração com Microsoft Active Directory;
- 5.2.1.11. Deve permitir a configuração de alertas de e-mail para emergências específicas da estrutura de rede, como a Solução de logs, análise e relatórios perdendo conexão com o dispositivo ou falha na fonte de alimentação do dispositivo (firewall);
- 5.2.1.12. Possuir definição de perfis de acesso ao console com permissão granular, como: acesso admin e acesso de somente leitura;
- 5.2.1.13. Deve suportar acesso via API;
- 5.2.1.14. Deve permitir a utilização de Multi-tenancy;
- 5.2.1.15. Deve permitir o gerenciamento de firewalls, bem como a criação de backups e atualização de firmware remotamente;

**CONSELHO REGIONAL DE ENFERMAGEM DE SANTA CATARINA**

Autarquia Federal criada pela Lei Nº 5.905/73

- 5.2.1.16. Deve permitir a utilização de ferramenta de sandbox do mesmo fabricante da solução de firewall (NGFW) fornecida;
- 5.2.1.17. Deve possuir no mínimo os relatórios:
- 5.2.1.17.1. DNS;
 - 5.2.1.17.2. Utilização de aplicação com maior banda consumida;
 - 5.2.1.17.2.1. Deve possuir identificação de aplicação peer-to-peer (bittorrent, xunlei, gnutella, filetopia), compartilhamento e armazenamento de arquivos (onebox, google drive, Dropbox, apple cloud) e aplicações voz/vídeo em streaming (youtube, skype, spotify, vimeo, netflix).
 - 5.2.1.17.3. Resumo:
 - 5.2.1.17.3.1. Análise de ameaças, tráfego, atividade web, análise de VPN, atividade do sistema.
 - 5.2.1.17.4. Atividade WEB:
 - 5.2.1.17.4.1. Categorias web mais visitadas;
 - 5.2.1.17.4.2. Websites mais visitados;
 - 5.2.1.17.4.3. Categorias web e websites mais visitados;
 - 5.2.1.17.4.4. Usuários web mais ativos;
 - 5.2.1.17.4.5. Mais web sites visitados por usuários mais ativos;
 - 5.2.1.17.4.6. Usuários mais ativo dos mais visitados web sites.
 - 5.2.1.17.5. Atividades:
 - 5.2.1.17.5.1. Seções: visibilidade de aplicações, análise de tráfego web, análise de comportamento do usuário.
 - 5.2.1.17.6. Avaliação de ameaças cibernéticas;
 - 5.2.1.17.7. Produtividade do usuário:
 - 5.2.1.17.7.1. Utilização de aplicações;
 - 5.2.1.17.7.2. Utilização da web.
 - 5.2.1.17.8. Prevenção de ameaças:



CONSELHO REGIONAL DE ENFERMAGEM DE SANTA CATARINA

Autarquia Federal criada pela Lei Nº 5.905/73

5.2.1.17.8.1. Exploração de vulnerabilidade de aplicações (exploits);

5.2.1.17.8.2. Prevenção de vírus;

5.2.1.17.8.3. Aplicações de alto risco.

5.2.1.17.9. Utilização de rede:

5.2.1.17.9.1. Largura de banda.

5.2.1.17.10. Relatório de administrador e eventos do sistema:

5.2.1.17.10.1. Admin login

5.2.1.17.10.1.1. Resumo de login;

5.2.1.17.10.1.2. Resumo de login por data;

5.2.1.17.10.1.3. Lista de logins sem sucesso.

5.2.1.17.10.2. Eventos de sistema:

5.2.1.17.10.2.1. Eventos por severidade;

5.2.1.17.10.2.2. Eventos de severidade crítica;

5.2.1.17.10.2.3. Eventos de alta severidade.

5.2.1.17.11. Relatório de VPN:

5.2.1.17.11.1. Resumo:

5.2.1.17.11.1.1. Tendência de utilização de tráfego VPN;

5.2.1.17.11.1.2. Logins de usuários VPN;

5.2.1.17.11.1.3. Tentativas de login sem sucesso;

5.2.1.17.11.1.4. Principais Usuários VPN Dialup.

5.2.1.17.11.2. SSL VPN

5.2.1.17.11.2.1. Principais fontes de túneis VPN SSL por largura de banda;

**CONSELHO REGIONAL DE ENFERMAGEM DE SANTA CATARINA**

Autarquia Federal criada pela Lei Nº 5.905/73

- 5.2.1.17.11.2.2. Principais usuários de túnel SSL VPN por largura de banda;
- 5.2.1.17.11.2.3. Principais usuários de modo web SSL VPN por duração;
- 5.2.1.17.11.2.4. Principais usuários SSL VPN por duração.
- 5.2.1.17.11.3. IPsec VPN:
 - 5.2.1.17.11.3.1. Principais túneis IPsec site-to-site por largura da banda;
 - 5.2.1.17.11.3.2. Principais túneis Dialup IPsec por largura de banda;
 - 5.2.1.17.11.3.3. Principais usuários Dialup IPsec por largura de banda;
 - 5.2.1.17.11.3.4. Principais usuários Dialup IPsec por duração.
- 5.2.1.18. Permitir importação e exportação de relatórios;
- 5.2.1.19. Deve ter a capacidade de criar relatórios no formato HTML;
- 5.2.1.20. Deve ter a capacidade de criar relatórios em formato PDF;
- 5.2.1.21. Deve ter a capacidade de criar relatórios no formato XML;
- 5.2.1.22. Deve ter a capacidade de criar relatórios no formato CSV;
- 5.2.1.23. Deve permitir exportar os logs no formato CSV;
- 5.2.1.24. Deve gerar logs de auditoria, com detalhes da configuração efetuada, o administrador que efetuou a alteração e seu horário;
- 5.2.1.25. Permitir centralmente a exibição de logs recebidos por um ou mais dispositivos, incluindo a capacidade de usar filtros para facilitar a pesquisa nos mesmos logs;
- 5.2.1.26. Os logs de auditoria das regras e alterações na configuração do objeto devem ser exibidos em uma lista diferente dos logs relacionados ao tráfego de dados;
- 5.2.1.27. Ter a capacidade de personalizar gráficos em relatórios, como barras, linhas e tabelas;

**CONSELHO REGIONAL DE ENFERMAGEM DE SANTA CATARINA**

Autarquia Federal criada pela Lei Nº 5.905/73

- 5.2.1.28. Deve ter um mecanismo de "pesquisa detalhada" para navegar pelos relatórios em tempo real;
- 5.2.1.29. Deve permitir que os arquivos de log sejam baixados da plataforma para uso externo;
- 5.2.1.30. Ter a capacidade de gerar e enviar relatórios periódicos automaticamente;
- 5.2.1.31. Permitir a personalização de qualquer relatório pré-estabelecido pela solução, exclusivamente pelo Administrador, para adotá-lo de acordo com suas necessidades;
- 5.2.1.32. Envio por e-mail de relatórios automaticamente;
- 5.2.1.33. Deve permitir que o relatório seja enviado por email ao destinatário específico;
- 5.2.1.34. Permitir a programação da geração de relatórios, conforme calendário definido pelo administrador;
- 5.2.1.35. É necessário exibir graficamente em tempo real a taxa de geração de logs para cada dispositivo gerenciado;
- 5.2.1.36. Deve permitir o uso de filtros nos relatórios;
- 5.2.1.37. Deve permitir definir o design dos relatórios, incluir gráficos, adicionar texto e imagens, alinhamento, quebras de página, fontes, cores, entre outros;
- 5.2.1.38. Permitir especificar o idioma dos relatórios criados;
- 5.2.1.39. Gerar alertas automáticos por email, SNMP e Syslog, com base em eventos especiais em logs, gravidade do evento, entre outros;
- 5.2.1.40. Deve permitir o envio automático de relatórios para um servidor SFTP ou FTP externo;
- 5.2.1.41. Deve ser capaz de criar consultas SQL ou similares nos bancos de dados de logs, para uso em gráficos e tabelas em relatórios;
- 5.2.1.42. Possibilitar visualizar nos relatórios da GUI as informações do sistema, como licenças, memória, disco rígido, uso da CPU, taxa de log por segundo recebido, total de logs diários recebidos, alertas do sistema, entre outros;
- 5.2.1.43. Deve ter uma ferramenta que permita analisar o desempenho na geração de relatórios, a fim de detectar e corrigir problemas na geração deles;
- 5.2.1.44. Importar arquivos com logs de dispositivos compatíveis conhecidos e não conhecidos pela plataforma, para geração posterior de relatórios;



CONSELHO REGIONAL DE ENFERMAGEM DE SANTA CATARINA

Autarquia Federal criada pela Lei Nº 5.905/73

- 5.2.1.45. Deve fornecer as informações da quantidade de logs armazenados e as estatísticas do tempo restante armazenado;
- 5.2.1.46. Deve ser compatível com a autenticação de fator duplo (token) para usuários do administrador da plataforma;
- 5.2.1.47. Gerar alertas de eventos a partir de logs recebidos;
- 5.2.1.48. Oferecer suporte ao serviço Indicadores de Comprometimento (IoC) do mesmo fabricante, que mostra as suspeitas de envolvimento do usuário final na Web e deve relatar pelo menos: endereço IP do usuário, nome do host, sistema operacional, veredicto (classificação geral da ameaça), o número de ameaças detectadas;
- 5.2.1.49. Deve permitir o suporte a logs na nuvem pública do Amazon S3;
- 5.2.1.50. Deve permitir o suporte a logs na nuvem pública do Microsoft Azure;
- 5.2.1.51. Deve permitir o suporte aos registros de nuvem pública do Google Cloud;
- 5.2.1.52. Suportar o padrão SAML para autenticação do usuário administrador.

5.2.2. Relatórios de Firewall

- 5.2.2.1. Deve ter relatório de conformidade com o PCI DSS;
- 5.2.2.2. Possuir relatório de uso do aplicativo SaaS;
- 5.2.2.3. Possuir relatório de prevenção de perda de dados (DLP);
- 5.2.2.4. Possuir relatório IPS (Intruder Prevention System);
- 5.2.2.5. Possuir relatório de reputação do cliente;
- 5.2.2.6. Possuir relatório de análise de segurança do usuário;
- 5.2.2.7. Possuir relatório de análise de ameaças cibernéticas;
- 5.2.2.8. Possuir breve relatório resumido diário de eventos e incidentes de segurança;
- 5.2.2.9. Possuir relatório de tráfego DNS;
- 5.2.2.10. Possuir relatório de tráfego de e-mail;
- 5.2.2.11. Possuir relatório dos 10 principais aplicativos usados na rede;
- 5.2.2.12. Possuir relatório dos 10 principais sites usados na rede;
- 5.2.2.13. Possuir relatório de uso de mídia social;

**CONSELHO REGIONAL DE ENFERMAGEM DE SANTA CATARINA**

Autarquia Federal criada pela Lei Nº 5.905/73

- 5.2.2.14. Possuir relatório de avaliação de risco para email;
- 5.2.2.15. Possuir relatório de conformidade com o PCI sem fio;
- 5.2.2.16. Possuir um relatório de APs e SSIDs autorizados, bem como clientes WiFi;
- 5.2.2.17. Possuir relatório de vulnerabilidades da solução de segurança gerenciada do equipamento terminal (endpoint);

Cláusula 6ª SERVIÇOS DE INSTALAÇÃO, CONFIGURAÇÃO E TREINAMENTO

6.1. Prestar serviço de instalação , configuração e treinamento para a solução ofertada , que compreende, entre outros, os seguintes procedimentos:

- 6.1.1. Reunião de alinhamento para criação do escopo do projeto previamente a instalação;
- 6.1.2. Instalação física do fi rewall adquirido, no local determinado pela equipe de Informática (TI);
- 6.1.3. Configuração do firewall presente neste processo, nas dependências do COREN-SC;
- 6.1.4. Análise da topologia e arquitetura da rede , considerando todos equipamentos já existentes instalados;
- 6.1.5. Análise do acesso à Internet, sites remotos, serviços de rede oferecidos aos funcionários e aos usuários externos;
- 6.1.6. Migração das regras de Firewall existentes e aplicáveis à solução ofertada , considerando a adequação às políticas de camada 7;
- 6.1.7. Análise do posicionamento de qualquer outro equipamento ou sistema relevante na segurança de qualquer perímetro protegido pela solução ;
- 6.1.8. Configuração do sistema de Firewall , VPN, IPS, Filtro URL, Antivírus e Anti malware de acordo com as melhores práticas e exigências levantadas;
- 6.1.9. Repasse no formato hands-on de no mínimo 4 horas para o DTI após validação da migração;
- 6.1.10. Deve haver geração de relatório com as configurações efetuadas e as decisões tomadas em formato legível e tecnicamente fundamentado.
- 6.1.11. A empresa Contratada deverá fornecer projeto de instalação e cronograma em até 5 (cinco) dias úteis após a assinatura do Contrato;
- 6.1.12. As instalações e configurações dos equipamentos deverão obedecer estritamente ao cronograma, de modo a não impactar as atividades cotidianas em horário comercial. A ativação deverá ocorrer fora do horário comercial.



CONSELHO REGIONAL DE ENFERMAGEM DE SANTA CATARINA

Autarquia Federal criada pela Lei Nº 5.905/73

Cláusula 7ª GARANTIA

- 7.1. A Contratada deverá prestar ampla garantia legal a todos os produtos entregues e serviços prestados, no local da instalação deste Coren/SC, durante 5 (cinco) anos, contados do recebimento definitivo pela Contratante do produto ou serviço, corrigindo qualquer vício ou problema encontrado, sem qualquer ônus para a Contratante, prestando os serviços de manutenção preventiva e corretiva;
- 7.1.1. Deve possuir garantia do fabricante no Brasil com validade de 5 (cinco) anos;
- 7.2. Caso o problema não seja solucionado a Contratada deverá substituir o equipamento em, no máximo, 48 (quarenta e oito) horas. Equipamento esse semelhante ou superior ao equipamento a ser substituído. Deverá ser prevista a garantia do fornecimento de qualquer parte, peça ou componente dos equipamentos fornecidos por um período mínimo de 05 (cinco) anos;
- 7.3. A garantia consistirá na reparação das eventuais falhas dos equipamentos, mediante a substituição de peças e/ou componentes que se apresentem defeituosos, de acordo com os manuais e normas técnicas específicas para os equipamentos, devendo ser prestada no local da instalação do equipamento;
- 7.4. Todo e qualquer desligamento que se fizer necessário nos equipamentos durante os serviços de manutenção dar-se-á somente após a prévia informação e consentimento da Contratante;
- 7.5. Capacidade de início de atendimento em até 1 hora para ocasiões de serviço 100% indisponível e verificação remota prévia.
- 7.6. Durante o prazo de garantia, deve ser possível realizar a atualização de sistema operacional dos equipamentos para obter novas funcionalidades e correção de bugs;
- 7.7. A garantia deve incluir envio de peças ou equipamentos de reposição no local de instalação do equipamento, obedecendo a modalidade NBD (Next Business Day);
- 7.8. Os chamados em garantia poderão ser abertos diretamente com a contratada ou autorizada oficial do fabricante através de ligação telefônica gratuita (0800) no idioma Português, website e e-mail durante a vigência da garantia. O suporte deverá ser na modalidade de 24x7 (24 horas por dia, 7 dias por semana).

Cláusula 8ª SUPORTE MENSAL

- 8.1. O suporte será limitado as seguintes características:
- 8.1.1. (quatro) horas de atendimento remoto mensal;
- 8.1.2. (quatro) aberturas de chamado mensal;
- 8.1.3. Será possível com acordo entre as partes acumular chamados não realizados em no máximo 2 (dois) meses antecedentes.



CONSELHO REGIONAL DE ENFERMAGEM DE SANTA CATARINA

Autarquia Federal criada pela Lei Nº 5.905/73

- 8.1.4. A contratada irá disponibilizar sem custo adicional para o Coren/SC até 10 (dez) horas de suporte técnico após a implementação, não subtraindo do suporte contratado nos itens 8.1.1 e 8.1.2, com a finalidade de executar mudanças no firewall devido nova implementação da rede Wi-Fi.
- 8.1.4.1. O controle e a abertura do suporte referente às horas constantes no item 8.1.4, ficará sob responsabilidade de ambos os gestores do Contrato.
- 8.2. Os serviços de suporte técnico e manutenção serão contratados com o objetivo de garantir a sustentação e a plena utilização da solução durante e depois de concluirmos os serviços de implantação e durante a vigência do contrato de 36 (trinta e seis) meses, devendo contemplar a prestação de suporte técnico para esclarecimento de dúvidas e resolução de problemas relacionados à configuração e uso dos componentes da solução contratada, em especial na configuração de acessos, parâmetros, falhas, erros, defeitos ou vícios identificados no funcionamento da solução, sendo exigido suporte técnico local para a solução, para atuar presencialmente quando o suporte remoto não resolver o problema, a solução/correção deverá ser realizada no período conforme item 8.3 deste Contrato, após a abertura do chamado por parte da Contratante;
- 8.3. O suporte deverá ter no mínimo o seguinte tempo de resposta para os níveis de severidade abaixo:
- 8.3.1. Crítico: Significa que o produto ficou inoperante ou ocorreu falha de grande impacto. Para este nível de severidade o atendimento deve ser imediato e com tempo de resposta de até 1 (uma) hora para resolução total ou encontro de solução temporária de contorno;
- 8.3.2. Alta: Impacto moderado no sistema, travamento, ou parada de ambiente parcial. Para este nível de severidade o tempo de resposta deve ser de até 2 (duas) horas, em horário comercial, para resolução total ou encontro de solução temporária de contorno;
- 8.3.3. Média: Redução de performance do equipamento ou aplicação de solução temporária de contorno bem-sucedida. Para este nível de severidade o tempo de resposta deve ser de até 4 (quatro) horas, em horário comercial, para resolução total ou encontro de solução temporária de contorno;
- 8.3.4. Baixa: Dúvidas de configuração ou anomalia de baixo impacto. Para este nível de severidade o tempo de resposta deve ser de até 8 (oito) horas em horário comercial.
- 8.3.5. O Suporte Técnico e Manutenção deve compreender também a manutenção técnica preventiva, corretiva e evolutiva dos componentes da solução, bem como a substituição de peças parcial ou total dos materiais ou equipamentos decorrentes de defeitos de fabricação ou falhas, assim como de demais componentes que venham compor a solução;
- 8.3.6. Deve contemplar a atualização de versões de software e firmwares dos elementos que compõem a solução, as quais incorporam correções de erros ou problemas registrados e melhorias nas funcionalidades implementadas pela empresa

**CONSELHO REGIONAL DE ENFERMAGEM DE SANTA CATARINA**

Autarquia Federal criada pela Lei Nº 5.905/73

FABRICANTE. Os procedimentos de atualização têm por finalidade assegurar a devida atualização da solução durante o período de vigência do contrato. A CONTRATADA será responsável pela implantação das atualizações dos produtos por ela fornecidos como partes do objeto.

8.3.7. Todo e qualquer desligamento que se fizer necessário nos equipamentos durante os serviços de manutenção dar-se-á somente após a prévia informação e consentimento da Contratante;

8.3.8. Capacidade de atender abertura de chamados em regime 24 horas por 7 dias por semana (24/7).

Cláusula 9ª SLA (SERVICE LEVE AGREEMENT)

9.1 Ao serem abertos os chamados referentes a suporte técnico e manutenção pela Contratante, os mesmos deverão ser classificados considerando as situações descritas na “Tabela: Prioridade X SLA” e “Tabela: Nível X Descrição”, devendo a Contratada saná-los dentro do prazo de atendimento;

9.2 Para efeito de apuração do prazo de atendimento de um chamado, será considerada como “data e hora da abertura do chamado” a data e hora que a Contratante realizar a abertura do chamado e como “data e hora de entrega” a data e hora que a Contratante der o aceite técnico em relação ao chamado aberto;

9.3 Para efeito de cálculo dos pontos perdidos serão atribuídos os seguintes valores aos fatores e níveis de criticidade:

9.3.1 Quando da abertura de chamados técnicos, a Contratada deve realizar em primeiro nível o atendimento de suporte remoto. Este atendimento deverá ser realizado conforme níveis de prioridades estabelecidos abaixo:

Tabela: Prioridade X SLA	
Prioridade	SLA
Prioridade 1 – Crítica	Em até 1 hora
Prioridade 2 – Alta	Em até 2 horas
Prioridade 3 – Média	Em até 4 horas
Prioridade 4 - Baixa	Em até 8 horas

9.4 O SLA acima informado é definido pelo período entre a abertura do chamado técnico e o início das atividades. As prioridades de atendimento estão classificadas da seguinte forma:

Tabela: Nível X Descrição	
Nível	Descrição
Prioridade 1 - Crítico	Significa que o produto ficou inoperante ou ocorreu falha de grande impacto. Para este nível de severidade o atendimento deve ser imediato e com tempo de resposta de até 1

**CONSELHO REGIONAL DE ENFERMAGEM DE SANTA CATARINA**

Autarquia Federal criada pela Lei Nº 5.905/73

	(uma) hora para resolução total ou encontro de solução temporária de contorno;
Prioridade 2 - Alto	Impacto moderado no sistema, travamento, ou parada de ambiente parcial. Para este nível de severidade o tempo de resposta deve ser de até 2 (duas) horas, para resolução total ou encontro de solução temporária de contorno;
Prioridade 3 - Média	Redução de performance do equipamento ou aplicação de solução temporária de contorno bem-sucedida. Para este nível de severidade o tempo de resposta deve ser de até 4 (quatro) horas, para resolução total ou encontro de solução temporária de contorno;
Prioridade 4 - Baixo	Dúvidas de configuração ou anomalia de baixo impacto. Para este nível de severidade o tempo de resposta deve ser de até 8 (oito) horas em horário comercial.

- 9.5 Os prejuízos causados pela demora no atendimento técnico serão indenizados pela CONTRATADA, observados os limites previstos neste Termo, da seguinte forma:
- 9.6 Desconto de 2,5% (dois vírgula cinco por cento) do valor mensal da fatura, para cada uma hora de atraso no atendimento de incidentes com prioridade 1 - Crítico;
- 9.7 Desconto de 2% (dois por cento) do valor mensal da fatura, para cada uma hora de atraso no atendimento de incidentes com prioridade 2 – Alta;
- 9.8 Desconto de 1% (um por cento) do valor mensal da fatura, para cada uma hora de atraso no atendimento de incidentes com prioridade 3 – Média;
- 1.1. Desconto de 0,5% (zero vírgula cinco por cento) do valor mensal da fatura, para cada uma hora de atraso no atendimento de incidentes com prioridade 4 – Baixa.
- 1.2. Os descontos serão aplicados sobre o valor mensal da fatura do mês das ocorrências, após comunicação da avaliação pelo Fiscal do Contrato a empresa Contratada;
- 1.3. O total de desconto aplicado está limitado a 10% (dez por cento) do valor mensal em que ocorrer o atraso em questão;
- 1.4. Não incorrerá em desconto a Contratada, o não atendimento decorrente de impedimento de execução por motivo de ambiente fechado ou não autorização do serviço por parte do responsável local, bem como problemas sob responsabilidade de terceiro;
- 1.5. Excluem-se desta garantia os defeitos provocados por mau uso comprovado ou em desacordo com as instruções fornecidas de manuseio e ainda, os causados por descargas atmosféricas e elétricas ou causas de força maior, tais como incêndios, inundações e outras comprováveis por laudo pertinente.



CONSELHO REGIONAL DE ENFERMAGEM DE SANTA CATARINA

Autarquia Federal criada pela Lei Nº 5.905/73

Cláusula 10ª DOS PRAZOS E CONDIÇÕES DE ENTREGA

- 10.1. A Contratada terá o prazo máximo de até 90 (noventa) dias corridos para realizar a implantação/integração e treinamento da solução, contado a partir da assinatura do contrato;
- 10.2. A entrega deve ser agendada com antecedência mínima de 24 horas, sob o risco de não ser autorizada;
- 10.3. Para itens de software, poderá ser fornecido sem mídia de instalação, desde que seja indicado local para download do arquivo de instalação.
- 10.4. A validação da implantação/integração da solução realizada pela Contratada será realizada através do aceite de implantação pelo Coren/SC, em até 02 (dois) dias úteis;
- 10.5. Após o aceite definitivo do Coren/SC referente à implantação/integração da solução serão iniciados no dia útil seguinte, os serviços referentes ao acesso à solução e ao suporte técnico;
- 10.6. Somente serão aceitos equipamentos novos e sem uso. Não serão aceitos equipamentos re-manufaturados, NFR (Not For Resale) ou de demonstração. Os equipamentos deverão ser entregues nas caixas lacradas pelo fabricante, não sendo aceitos equipamentos com caixas violadas;
- 10.7. O aceite do bem somente será dado após comprovação da entrega e o efetivo cumprimento de todas as exigências da presente especificação técnica;
- 10.8. A licitante deverá encaminhar no momento de habilitação, manuais e toda documentação pública para comprovação do pleno atendimento aos requisitos desta especificação técnica.

Cláusula 11ª DO LOCAL DE EXECUÇÃO DOS SERVIÇOS

- 11.1. Os serviços, formalmente solicitados por meio da Ordem de Serviço, deverão ser entregues/efetuados na sede do Coren/SC, localizado na Avenida Mauro Ramos 224, Centro, Ed. Centro Executivo Mauro Ramos 6º ao 9º andar, Florianópolis/SC, em horário a ser definido pelo fiscal do contrato.
- 11.2. A instalação de equipamentos/software que componham a solução deverá ser instalada na sede do Coren/SC.

Cláusula 12ª DA VIGÊNCIA

- 12.1. A execução do serviço de suporte mensal técnico terá a duração de 36 (trinta e seis) meses a partir do aceite definitivo da implantação/integração e treinamento, podendo ser prorrogado por mais 12 (doze) meses, por acordo entre as partes, mediante termo aditivo, obedecendo ao prazo máximo de 48 (quarenta e oito) meses, conforme artigo 57, inciso IV, da Lei Federal nº 8.666/93; sendo reajustado a cada 12 (doze) meses pelo INPC (Índice Nacional de Preços ao Consumidor) acumulado dos últimos 12 (doze) meses.



CONSELHO REGIONAL DE ENFERMAGEM DE SANTA CATARINA

Autarquia Federal criada pela Lei Nº 5.905/73

- 12.1.1. A contratação de 36 (trinta e seis) meses se faz necessária por se tratar de serviço essencial ao funcionamento do Coren/SC, atendimento ao público e ao atendimento ao Profissional desta categoria. Pois trata-se de serviço essencial contínuo;
- 12.2. O contrato referente ao serviço poderá ser cancelado mediante prévio aviso, tanto da Contratante como da Contratada, de no mínimo 90 (noventa) dias.

Cláusula 13ª DA FISCALIZAÇÃO DO CONTRATO

- 13.1. A execução do Contrato será acompanhada e fiscalizada pelo empregado Michel R. Kannengerg, Téc. Esp. ADM. de Redes, Chefe do Departamento de Tecnologia da Informação.
- 13.2. O fiscal do contrato terá autoridade para:
 - 13.2.1. Exigir o cumprimento de todos os itens desta especificação;
 - 13.2.2. Rejeitar todo e qualquer material de má qualidade ou não especificado e estipular o prazo para sua retirada do local da execução dos serviços;
 - 13.2.3. Verificar a conformidade da prestação dos serviços de forma a assegurar o perfeito cumprimento do contrato;
 - 13.2.4. Manter registro de ocorrências relacionadas com a execução do Contrato, determinando todas as ações necessárias para a regularização das faltas ou defeitos;
 - 13.2.5. A existência desse acompanhamento não exime a Contratada de quaisquer responsabilidades sobre erros ou omissões que surgirem ou vierem a ser constatados.

Cláusula 14ª DO SIGILO PROPRIEDADE DAS INFORMAÇÕES E ACORDO DE CONFIDENCIALIDADE

- 14.1. Todas as informações obtidas e/ou produzidas decorrentes da contratação e execução das atividades são de propriedade do Coren/SC.
- 14.2. A Contratada e todos os funcionários envolvidos no processo de contratação e execução das atividades deverão manter sigilo absoluto sobre quaisquer informações do Coren/SC.
- 14.3. É proibida a interceptação de qualquer tráfego oriundo ou destinado ao Coren/SC sem autorização judicial.
- 14.4. A Contratada, através de seu representante legal, deverá assinar o Acordo de Confidencialidade, e dar ciência do mesmo a toda sua equipe de profissionais e subcontratados que participarão da execução do contrato.
- 14.5. A Contratada deverá atender às seguintes condições relativas à informação que venha a conhecer, em função da prestação dos serviços ao Coren/SC:



CONSELHO REGIONAL DE ENFERMAGEM DE SANTA CATARINA

Autarquia Federal criada pela Lei Nº 5.905/73

- 14.5.1. Não poderá divulgar ou utilizar nenhuma informação adquirida do Coren/SC ou relativa à solução instalada, sem a autorização prévia do Coren/SC;
- 14.5.2. Respeitar a Confidencialidade da Informação e Propriedade Intelectual do Coren/SC;
- 14.5.3. Manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse do Coren/SC ou de terceiros de que tomar conhecimento em razão da execução do objeto contratado, respeitando todos os critérios estabelecidos, aplicáveis aos dados, informações, regras de negócios, documentos, entre outros.

Cláusula 15ª DAS OBRIGAÇÕES DA CONTRATADA

- 15.1. Entregar os serviços nos prazos, quantidades, características e condições especificados.
 - 15.1.1. Implantar o serviço em até 90 dias corridos, a contar da data da assinatura do referido contrato.
 - 15.1.2. Treinar a equipe técnica logo após a instalação/configuração da solução;
 - 15.1.3. Fornecer todos os equipamentos e quaisquer acessórios, incluindo cabos, material e acessórios necessários para instalação, conexão e identificação adequada para o perfeito funcionamento da solução, conforme determinada pelo Coren/SC, de todos os itens utilizados na instalação e funcionamento dos serviços, caso necessário.
 - 15.1.4. Disponibilizar e manter a solução contratada e prestar o suporte técnico, durante todo o prazo de vigência do contrato, observado o SLA estabelecido.
 - 15.1.5. Informar ao Coren/SC, em até 24 horas de antecedência, possíveis manutenções programadas que impossibilite o acesso a solução.
- 15.2. Fornecer em qualquer época, as informações e os esclarecimentos técnicos solicitados pela contratante sobre a execução dos trabalhos.
- 15.3. Manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse da contratante ou de terceiros de que tomar conhecimento em razão da execução do objeto, devendo orientar seus empregados nesse sentido.
- 15.4. Caso haja a necessidade de alocar equipamentos de informática de propriedade da empresa Contratada nas dependências do Coren/SC, como notebooks, os mesmos deverão, obrigatoriamente, antes de se conectar com a rede interna, estar de acordo com as políticas de segurança interna do Coren/SC.
- 15.5. Comunicar ao Coren/SC, por escrito, qualquer anormalidade de caráter urgente.
- 15.6. Nomear preposto para acompanhamento da prestação dos serviços, que deverá seguir as orientações demandadas pelo Coren/SC.



CONSELHO REGIONAL DE ENFERMAGEM DE SANTA CATARINA

Autarquia Federal criada pela Lei Nº 5.905/73

- 15.7. Assumir todos e quaisquer ônus, referente a salário, horas extras, adicionais e demais encargos sociais relativamente aos seus empregados; assumir a responsabilidade pelos encargos fiscais e comerciais resultante da adjudicação da licitação.
- 15.8. Manter, durante toda a execução do serviço, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação.
- 15.9. Zelar pela perfeita execução dos serviços.
- 15.10. Prover, realizar, manter e priorizar todas as ações necessárias ao fiel cumprimento das cláusulas contidas neste Contrato.
- 15.11. Prestar os serviços de forma meticulosa e constante, mantendo-os sempre em perfeita ordem.
- 15.12. Arcar com eventuais prejuízos causados ao Coren/SC ou a terceiros, provocados por negligência ou irregularidade cometida por seus empregados ou prepostos envolvidos na execução do objeto. A fiscalização ou o acompanhamento do contrato pela Administração não exclui ou reduz a responsabilidade do contratado.
- 15.13. Responsabilizar-se por todas as despesas diretas ou indiretas, tais como: salários, transportes, encargos sociais, fiscais, trabalhistas, previdenciários e de ordem de classe, indenizações e quaisquer outras que forem devidas aos seus empregados no desempenho dos serviços objeto do contrato, ficando o Coren/SC isento de qualquer vínculo empregatício com os mesmos.
- 15.14. Manter seus empregados e/ou prepostos, quando em serviço, devidamente identificados, mediante o uso permanente de crachás, devendo substituí-los imediatamente caso sejam considerados inconvenientes.
- 15.15. Providenciar a imediata correção das deficiências, falhas ou irregularidades apontadas pelo Coren/SC.
- 15.16. A Contratada não poderá cobrar valores adicionais ao valor do contrato, tais como custos de deslocamento, alimentação, transporte, alojamento, trabalho aos sábados, domingos, feriados ou em horário noturno, bem como qualquer outro valor adicional para o pleno atendimento do fornecimento do objeto;
- 15.17. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste Contrato deverão ser fornecidos.

Cláusula 16ª DAS OBRIGAÇÕES DA CONTRATANTE

- 16.1. Fornecer informações e esclarecimentos pertinentes que venham a ser solicitados pelo representante da Contratada.
- 16.2. Realizar os pagamentos devidos à Contratada, nos prazos e condições estabelecidas neste Contrato.



Coren/SC

Fls. nº ____

CONSELHO REGIONAL DE ENFERMAGEM DE SANTA CATARINA

Autarquia Federal criada pela Lei Nº 5.905/73

- 16.3. Receber e atestar as notas apresentadas pela Contratada, de conformidade com o material adquirido/recebido.
- 16.4. Comunicar à Contratada a ocorrência de divergência entre o material adquirido e a nota fiscal, promovendo a devolução da nota para correção.
- 16.5. É prerrogativa do Coren/SC, proceder a mais ampla fiscalização sobre o fiel cumprimento do objeto desta licitação, sem prejuízo da responsabilidade da licitante vencedora, avaliar a qualidade do objeto, podendo rejeitá-los no todo ou em parte, bem como, exigir o cumprimento de todos os itens deste processo, segundo suas especificações.
- 16.6. Notificar a Contratada por escrito de quaisquer ocorrências relacionadas à execução do objeto, fixando prazo para a sua correção;
- 16.7. Comunicar oficialmente a Contratada quaisquer falhas verificadas no cumprimento do contrato.

Cláusula 17ª DOS PAGAMENTOS

- 17.1. A Contratada, durante o prazo de execução do serviço, emitirá mensalmente a nota fiscal do objeto contratado;
- 17.2. A nota fiscal deverá ser emitida pela Contratada, discriminando os itens contratados;
- 17.3. A nota fiscal que for apresentada com erro será devolvida à Contratada para retificação e reapresentação;
- 17.4. O pagamento deverá ser efetuado mediante a apresentação da Nota Fiscal, devidamente atestada pela Contratante;
- 17.5. O prazo para pagamento da Nota Fiscal, devidamente atestada pelo fiscal do contrato, será de até 15 (quinze) dias úteis, contados da data do atesto;
- 17.6. O pagamento será feito por meio de depósito na conta-corrente da Contratada ou boleto bancário, mediante apresentação da respectiva Nota Fiscal do fornecimento, acompanhada do atesto do Fiscal do Contrato;
- 17.7. Para execução do pagamento, a Contratada deverá fazer constar como beneficiário/cliente, da Nota Fiscal correspondente, o Conselho Regional de Enfermagem de Santa Catarina, CNPJ nº 75.308.106/0001-56, e ainda, os números do Banco, da Agência e da Conta Corrente da Contratada, e a descrição clara e sucinta do objeto;
- 17.8. Sobre o valor da nota fiscal, a Contratante fará as retenções devidas ao INSS e as dos impostos e contribuições previstas na Instrução Normativa SRF nº 1.234, de 11/01/2012;
- 17.9. A Contratada deverá, ainda, juntamente com a Nota Fiscal, apresentar os documentos comprobatórios de regularidade fiscal e trabalhista, exigidos no Edital de Licitação;



CONSELHO REGIONAL DE ENFERMAGEM DE SANTA CATARINA

Autarquia Federal criada pela Lei Nº 5.905/73

- 17.10. Caso a Contratada seja optante pelo "SIMPLES" (Lei nº 9.317/96), será obrigada a informar no corpo da nota fiscal e apresentar declaração, na forma da Instrução Normativa SRF nº 1.234, de 11/01/2012, assinada pelo seu representante legal;
- 17.11. Nenhum pagamento será efetuado em caráter antecipado, ou antes, de quitada qualquer penalidade.

Cláusula 18ª DA DOTAÇÃO ORÇAMENTÁRIA E FINANCEIRA

- 18.1 Os recursos para a execução do objeto são próprios do Conselho Regional de Enfermagem de Santa Catarina, e correrá sob a seguinte rubrica orçamentária:
- 18.1.1 Rubrica: 44.90.052.004 – Bens de Informática.

Cláusula 19ª DAS SANÇÕES ADMINISTRATIVAS

- 19.1 Comete infração administrativa, nos termos da Lei nº 10.520/2002, a Contratada que:
- 19.1.1 não assinar o Contrato ou aceitar/retirar o instrumento equivalente, quando convocado dentro do prazo de validade da proposta;
- 19.1.2 não assinar o Contrato ou aceitar/retirar o instrumento equivalente, quando convocado dentro do prazo de validade da proposta;
- 19.1.3 apresente documentação falsa;
- 19.1.4 deixar de entregar os documentos exigidos no certame;
- 19.1.5 ensejar o retardamento da execução do objeto;
- 19.1.6 não mantiver a proposta;
- 19.1.7 cometer fraude fiscal;
- 19.1.8 comporta-se de modo inidôneo.
- 19.2 Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os licitantes, em qualquer momento da licitação, mesmo após o encerramento da fase de lances.
- 19.3 A Contratada que cometer qualquer das infrações discriminadas nos subitens anteriores ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:
- 19.3.1 advertência por faltas leves, assim entendidas como aquelas que não acarretarem prejuízos significativos ao objeto da Contratação;
- 19.3.2 multa de 20% (vinte por cento) sobre o valor do(s) item(s) prejudicado(s) pela conduta da Contratada;
- 19.3.3 suspensão de licitar e impedimento de contratar com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo de até 2 (dois) anos;



CONSELHO REGIONAL DE ENFERMAGEM DE SANTA CATARINA

Autarquia Federal criada pela Lei Nº 5.905/73

- 19.3.4 impedimento de licitar e de contratar com a União e descredenciamento no SICAF, pelo prazo de até 5 (cinco) anos;
- 19.3.5 declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a Contratada ressarcir a Contratante pelos prejuízos causados;
- 19.4 A penalidade de multa pode ser aplicada cumulativamente com as demais sanções.
- 19.5 Se durante o processo de aplicação de penalidade, se houver indícios de prática de infração administrativa tipificada pela Lei nº 12.846, de 1º de agosto de 2013, como ato lesivo à administração pública nacional ou estrangeira, cópias do processo administrativo necessárias à apuração da responsabilidade da empresa deverão ser remetidas à autoridade competente, com despacho fundamentado, para ciência e decisão sobre a eventual instauração de investigação preliminar ou Processo Administrativo de Responsabilização – PAR.
- 19.6 A apuração e o julgamento das demais infrações administrativas não consideradas como ato lesivo à Administração Pública nacional ou estrangeira nos termos da Lei nº 12.846, de 1º de agosto de 2013, seguirão seu rito normal na unidade administrativa.
- 19.7 O processamento do PAR não interfere no seguimento regular dos processos administrativos específicos para apuração da ocorrência de danos e prejuízos à Administração Pública Federal resultantes de ato lesivo cometido por pessoa jurídica, com ou sem a participação de agente público.
- 19.8 Caso o valor da multa não seja suficiente para cobrir os prejuízos causados pela conduta do licitante, a União ou Entidade poderá cobrar o valor remanescente judicialmente, conforme artigo 419 do Código Civil.
- 19.9 A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa a Contratada, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente na Lei nº 9.784, de 1999.
- 19.10 A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.
- 19.11 As penalidades serão obrigatoriamente registradas no SICAF.

Cláusula 20ª DA RESCISÃO DO CONTRATO

- 20.1 A inexecução total ou parcial das condições avençadas poderá acarretar a rescisão do Contrato, com as consequências contratuais e as previstas em lei ou regulamento, conforme disposto nos artigos 77 a 80 da Lei n.º 8.666/93.
- 20.2 A rescisão do Contrato poderá ser:



CONSELHO REGIONAL DE ENFERMAGEM DE SANTA CATARINA

Autarquia Federal criada pela Lei Nº 5.905/73

- 20.2.1 Determinada por ato administrativo unilateral e motivado do Contratante, quando o Contratante, frente a situações de descumprimento de cláusulas contratuais por parte da Contratada, lentidão, atraso, paralisação ou por razões de interesse público, decidir rescindir o Contrato;
- 20.2.2 Amigável, por acordo formalizado no processo entre o Contratante e a Contratada, desde que haja conveniência para o Contratante;
- 20.2.3 Judicial, quando a rescisão for discutida em instância judicial e se dará conforme os termos de sentença transitada em julgado.
- 20.3 Os casos de rescisão contratual serão formalmente motivados nos autos do processo e, no procedimento que visa à rescisão do Contrato, será assegurado o contraditório e a ampla defesa, sendo que, depois de encerrada a instrução inicial, a Contratada terá o prazo de 05 (cinco) dias úteis para se manifestar e produzir provas, sem prejuízo da possibilidade de o Contratante adotar, motivadamente, providências acauteladoras.
- 20.4 A rescisão administrativa ou amigável deverá ser precedida de autorização escrita e fundamentada da autoridade competente.
- 20.5 No caso de rescisão provocada por inadimplemento da Contratada, o Contratante poderá reter, cautelarmente, os créditos decorrentes do Contrato até o valor dos prejuízos causados, já calculados ou estimados.
- 20.6 Quando a rescisão ocorrer com base nos incisos XII a XVII, do artigo 78, da Lei n.º 8.666/1993, sem que haja culpa da Contratada, esta será ressarcida dos prejuízos regularmente comprovados, tendo ainda direito a, principalmente:
- 20.6.1 Pagamento devido pela execução do Contrato até a data da rescisão;
- 20.6.2 Pagamento do custo de desmobilização.

Cláusula 21ª ALTERAÇÕES

- 21.1 Eventuais alterações contratuais reger-se-ão pela disciplina do artigo 65 da Lei nº 8.666/93.
- 21.2 A Contratada é obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.
- 21.3 As supressões resultantes de acordo celebrado entre as partes contratantes poderão exceder o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

Cláusula 22ª DOS CASOS OMISSOS

- 22.1 Os casos omissos serão decididos pela Contratante, segundo as disposições contidas na Lei nº 8.666, de 1993, na Lei nº 10.520, de 2002 e demais normas federais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos.



Coren/SC

Fls. nº _____

CONSELHO REGIONAL DE ENFERMAGEM DE SANTA CATARINA

Autarquia Federal criada pela Lei Nº 5.905/73

Cláusula 23ª PUBLICIDADE

23.1 Incumbirá à Contratante providenciar a publicação deste instrumento, por extrato, no Diário Oficial da União, no prazo previsto na Lei nº 8.666, de 1993.

Cláusula 24ª DO FORO

24.1 Para dirimir as questões oriundas do presente Contrato, será competente o Foro da Justiça Federal, Seção Judiciária de Santa Catarina – Subseção Judiciária de Florianópolis.

E, assim, por estarem justas e contratadas, as partes, por seus representantes legais, assinam o presente contrato, em 03 (três) vias de igual teor e forma, para um só e jurídico efeito, perante as testemunhas abaixo assinados, a tudo presentes.

Florianópolis/SC, 16 de maio de 2022.

GELSON LUIZ DE ALBUQUERQUE:
Assinado de forma digital por
GELSON LUIZ DE ALBUQUERQUE:30713633034
Dados: 2022.05.27 13:19:19 -03'00'

CONTRATANTE:

Gelson L. Albuquerque
Presidente do Coren/SC

DANIELA
MACANEIRO:01799001962
Assinado de forma digital por
DANIELA MACANEIRO:01799001962
Dados: 2022.05.25 08:53:26 -03'00'

CONTRATANTE:

Daniela Maçaneiro
Tesoureira do Coren/SC

REYNALDO COSTA E ROSA:
Assinado de forma digital por
REYNALDO COSTA E ROSA:90158075587
Dados: 2022.05.16 16:44:33 -03'00'

CONTRATADO:

Reynaldo Costa e Rosa
SIGMAFONE TELECOMUNICAÇÕES LTDA

Testemunhas:

1) _____
Nome: _____
CPF: _____

2) _____
Nome: _____
CPF: _____

Visto Dejur:

CLAUDIRENE VILVERT ALVES:
Assinado de forma digital por
CLAUDIRENE VILVERT ALVES
Dados: 2022.05.24 12:21:58 -03'00'

Conforme Portaria Coren/SC nº 518 de 17 de novembro de 2021.