

TERMO DE REFERÊNCIA

Processo UDESC SGPe 27843/2025

CENTRO LICITANTE
Coordenadoria de Licitações e Compras da Reitoria

1. OBJETO

Contratação de empresa para renovação de licenças da Solução de Segurança (Firewalls FORTINET), novos equipamentos e IA para toda a UDESC.

1.1. Especificações e quantidades

ESPECIFICAÇÕES E DESCRIÇÃO DETALHADA DOS ITENS:

- 1 Suporte Técnico e Licenciamento para FortiManager (part number) – QUANTIDADE 03**
 - 1.1 Totalmente compatível com a versão atual em uso (FORTIMANAGER v 7.6.3);
 - 1.2 Renovação de licenciamento e suporte Fortinet – coterm para adicionar 12 meses ao vencimento;
 - 1.3 Manter todas as funcionalidades existentes;
- 2 Licença de segurança para FortiGate-100F (part number) – QUANTIDADE 18**
 - 2.1 Totalmente compatível com a versão atual em uso;
 - 2.2 Renovação de licenciamento e suporte Fortinet – coterm para adicionar 12 meses ao vencimento;
 - 2.3 Manter todas as funcionalidades existentes;
- 3 Licença de segurança para FortiGate-201E (part number) – QUANTIDADE 06**
 - 3.1 Totalmente compatível com a versão atual em uso;
 - 3.2 Renovação de licenciamento e suporte Fortinet – coterm para adicionar 12 meses ao vencimento;
 - 3.3 Manter todas as funcionalidades existentes;
- 4 Licença de segurança para FortiGate-501E (part number) – QUANTIDADE 02**
 - 4.1 Totalmente compatível com a versão atual em uso;
 - 4.2 Renovação de licenciamento e suporte Fortinet;
 - 4.3 Manter todas as funcionalidades existentes;
- 5 Suporte Técnico para FortiGate-1001F (part number) – QUANTIDADE 06**
 - 5.1 Totalmente compatível com a versão atual em uso;
 - 5.2 Renovação de licenciamento e suporte Fortinet – coterm para adicionar 12 meses ao vencimento;
 - 5.3 Manter todas as funcionalidades existentes;
- 6 Suporte Técnico e Licenciamento para FortiAnalyzer (part number) – QUANTIDADE 09**
 - 6.1 Totalmente compatível com a versão atual em uso (FORTIANALYZER v 7.6.3);
 - 6.2 Renovação de licenciamento e suporte Fortinet – coterm para adicionar 12 meses ao vencimento;
 - 6.3 Manter todas as funcionalidades existentes (Ex: Suportar a coleta de 50 GB de logs diários).
- 7 Suporte Técnico e Licenciamento para FortiAuthenticator (part number) – QUANTIDADE 03**
 - 7.1 Totalmente compatível com a versão atual em uso (FORTIAUTHENTICATOR v 7.6.3);
 - 7.2 Renovação de licenciamento e suporte Fortinet – coterm para adicionar 12 meses ao vencimento;
 - 7.3 Manter todas as funcionalidades existentes;
- 8 Suporte Técnico e Licenciamento para FortiClient ZTNA Agent Subscription for 500 endpoints (part number) – QUANTIDADE 03**
 - 8.1 Totalmente compatível com a versão atual em uso (FORTICLIENT ZTNA Agent);
 - 8.2 Renovação de licenciamento e suporte Fortinet – coterm para adicionar 12 meses ao vencimento;
 - 8.3 Manter todas as funcionalidades existentes;
- 9 Licenciamento para FortiAnalyzer S-Series ADOM (part number FN-FC-10-AZVMS-230-01-36) – QUANTIDADE 12**

- 9.1 Totalmente compatível com a versão atual em uso (FORTIANALYZER v 7.6.3);
- 9.2 Subscrição para 36 meses;
- 9.3 Adicionar um ADOM aos existentes;

10 Suporte Técnico e Licenciamento para FortiAnalyzer FORTIAI (part number FN-FC2-10-AZVMS-1118-01-12) – QUANTIDADE 09

- 10.1 Totalmente compatível com a versão atual em uso (FORTIANALYZER v 7.6.3);
- 10.2 Licenciamento e suporte de 1 ano ou 12 meses;
- 10.3 Manter todas as funcionalidades para uso com o mínimo de 50 GB de logs diários;

11 Suporte Técnico e Licenciamento para FortiManager FORTIAI (part number FN-FC2-10-M3004-1118-02-12) – QUANTIDADE 03

- 11.1 Totalmente compatível com a versão atual em uso (FORTIMANAGER v 7.6.3);
- 11.2 Licenciamento e suporte de 1 ano ou 12 meses;
- 11.3 Uso de 1 a 110 dispositivos/ domínios virtuais;

12 Licenciamento de Upgrade de tokens para o FortiManager FORTIAI (part number FN-FC1-10-AITMG-1089-02-12) – QUANTIDADE 90

- 12.1 Totalmente compatível com a versão atual em uso (FORTIMANAGER v 7.6.3);
- 12.2 Licenciamento e suporte de 1 ano ou 12 meses;
- 12.3 Para uso de 500.000 Tokens;

13 Solução Firewall de Próxima Geração (NGFW) 1 – Modelo de referência: Fortigate 201G (para Campus) – QUANTIDADE 02

Características Mínimas:

13.1 REQUISITOS GERAIS

- 13.1.1 Deve ter compatibilidade e integração em malha ao Orquestrador e ativos da instituição:
 - FORTIMANAGER v 7.6.3;
 - FORTIGATE FG-1001F
 - FORTIGATE FG-200E
 - FORTIGATE FG-100F
- 13.1.2 Deve ter a função de NGFW (NEXT GENERATION FIREWALL) atuando com o intuito de conexão com enlaces WAN (Wide Área Network), tais como links de Internet, MPLS, entre outros, para utilização da engenharia de tráfego, provendo ainda de modo integrado conectividade segura, viabilizando assim o acesso local à Internet de modo seguro;
- 13.1.3 Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;
- 13.1.4 Os componentes da solução devem ser novos, sem utilização anterior e em linha de fabricação;
- 13.1.5 A solução deve ter arquitetura dedicada, não podendo ser servidor de uso genérico, e o sistema operacional deve estar embutido no hardware proposto, ou seja, hardware e software devem ser integrados em um único equipamento;
- 13.1.6 Deve consistir em plataforma de proteção de rede baseada em equipamento físico com funcionalidades de Next Generation Firewall (NGFW), não sendo permitido appliances virtuais ou solução open source;
- 13.1.7 Todos os equipamentos a serem fornecidos, bem como seu hardware e software, devem ser do mesmo fabricante para assegurar a padronização e compatibilidade funcional de todos os recursos;
- 13.1.8 Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões.
- 13.1.9 A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7 com base no modelo OSI.
- 13.1.10 O gerenciamento da solução deve suportar acesso via SSH, WEB (HTTPS) e via API.
- 13.1.11 Os softwares deverão ser fornecidos em sua versão mais atualizada na data de entrega;
- 13.1.12 Todo hardware e software componentes da solução deve ser do mesmo fabricante, admitido o regime de OEM;
- 13.1.13 Deve possuir interface ethernet “Out-of-Band” dedicada para gerenciamento de

configuração e gerenciamento através de interface de linha de comando CLI (comand line interface);

- 13.1.14 Deve possuir ao menos 8 interfaces 1GE RJ45;
- 13.1.15 Deve possuir ao menos 04 interfaces 1G SFP;
- 13.1.16 Deve possuir ao menos 8 interfaces Multigigabit 5/2.5/GE RJ45 Ports
- 13.1.17 Deve possuir ao menos 8 interfaces 10 GBE SFP+;
- 13.1.18 Devem ser fornecidos 2 cabos DAC (Direct Attach Cable) 10GE SFP+ de 3m de comprimento;
- 13.1.19 Todas as interfaces de rede fornecidas nos appliances devem estar completamente licenciadas e habilitadas para uso imediato;
- 13.1.20 Deve estar licenciado ou ter incluído sem custo adicional, no mínimo, 10 sistemas virtuais lógicos por equipamento. Entende-se por sistema virtual lógico a possibilidade de dividir um único equipamento físico em várias unidades virtuais, tendo um contexto para WAN e outro contexto para LAN, por exemplo.
- 13.1.21 Permitir montagem em rack com largura padrão de 19 polegadas. Deverão ser fornecidos todos os cabos, suportes (se necessários, "gavetas", "braços" e "trilhos") para a instalação dos equipamentos no rack;
- 13.1.22 Deve possuir duas fontes de energia e as faixas de tensão de entrada suportadas devem ser de 100 VAC a 240 VAC, a 60 Hz sem uso de chave de seleção de voltagem (automaticamente), capaz de sustentar a configuração máxima do equipamento;
- 13.1.23 Todas as funcionalidades, features e licenciamentos deverão ser fornecidos pelo mesmo fabricante de maneira integrada e em uma mesma arquitetura, com atualizações no período do contrato;
- 13.1.24 Deve ter armazenamento interno de no mínimo 480GB SSD;
- 13.1.25 Deve suportar o gerenciamento de até 256 (duzentos e cinquenta e seis) pontos de acesso wireless simultaneamente;

13.2 PERFORMANCE:

- 13.2.1 Deve suportar, no mínimo, 26 Gbps de throughput de Firewall stateful;
- 13.2.2 Deve suportar, no mínimo, 9 Gbps de throughput IPS;
- 13.2.3 Deve suportar, no mínimo, 36 Gbps de throughput de VPN IPSec;
- 13.2.4 Deve suportar, no mínimo, 7 Gbps de throughput de Inspeção SSL;
- 13.2.5 Deve suportar, no mínimo, 27 Gbps de throughput de Controle de Aplicação;
- 13.2.6 Deve suportar, no mínimo, 6 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;
- 13.2.7 Deve suportar no mínimo, 7,5 milhões de conexões simultâneas;
- 13.2.8 Deve suportar no mínimo, 400 mil novas conexões por segundo;
- 13.2.9 Deve estar licenciado para, ou suportar sem o uso de licença, 2.000 túneis de VPN IPSec Site-to-Site simultâneos;
- 13.2.10 Deve estar licenciado para, ou suportar sem o uso de licença, 16.000 túneis de clientes VPN IPSec simultâneos;
- 13.2.11 Deve estar licenciado para, ou suportar sem o uso de licença, 500 clientes de VPN SSL simultâneos;

13.3 CARACTERÍSTICAS GERAIS DA SOLUÇÃO DE FIREWALL PRÓXIMA GERAÇÃO (NGFW)

- 13.3.1 Deve estar devidamente licenciada (vide próximo item) para atender as funções, funcionalidades e serviços para no mínimo:
 - Controle de Aplicações;
 - Proteção IPS;
 - Proteção contra Ameaças Avançadas;
 - Filtro Web e de Conteúdo;
 - Análise de malwares modernos em nuvem do mesmo fabricante;
 - Roteamento inteligente de aplicações;
 - VPN site-to-site e client-to-site;
 - Garantia e suporte remoto diretamente com o fabricante na modalidade de 8x5;
- 13.3.2 Deve suportar tags de VLAN (802.1Q);
- 13.3.3 Deve possuir suporte a agregação de links via 802.3ad LACP;

- 13.3.4 Deve possuir ferramenta de diagnóstico do tipo tcpdump e ainda dispor de ferramenta integrada à interface web para capturar informações dos pacotes em tempo real, podendo aplicar filtros, tais como IPs e portas, e ainda ter disponível a possibilidade de exportar a captura para um arquivo do tipo PCAP visando estender a análise para um software terceiro, tal como Wireshark;
- 13.3.5 Deve possuir integração com servidores de autenticação RADIUS, LDAP e Microsoft Active Directory;
- 13.3.6 Deve possuir integração com tokens para autenticação de duplo fator;
- 13.3.7 Deve suportar single-sign-on;
- 13.3.8 Deve possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um, N-para-um, vários para um, NAT64, NAT66, NAT46 e PAT;
- 13.3.9 Deve suportar roteamento estático para IPv4 e IPv6;
- 13.3.10 Deve suportar roteamento dinâmico para IPv4 e IPv6 (OSPF, OSPFv2, OSPFv3, BGP, RIP);
- 13.3.11 Deve suportar ECMP;
- 13.3.12 Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);
- 13.3.13 Deve possuir funcionalidades de DHCP Cliente, Servidor e Relay;
- 13.3.14 Deve suportar aplicações multimídia, tais como: H.323 e SIP;
- 13.3.15 Deve permitir o funcionamento em modo transparente tipo “bridge”;
- 13.3.16 Deve suportar PBR – Policy Based Routing;
- 13.3.17 Deve possuir conexão entre estação de gerência e appliance criptografada, tanto em interface gráfica, quanto em CLI (linha de comando);
- 13.3.18 Deve possuir mecanismo de anti-spoofing;
- 13.3.19 Deve permitir criação de regras definidas pelo usuário;
- 13.3.20 Deve suportar sFlow ou Netflow;
- 13.3.21 Os dispositivos de proteção de rede devem possuir suporte a Jumbo Frames;
- 13.3.22 Deverá permitir autenticação de usuários em base local, servidor LDAP, RADIUS e TACACS;
- 13.3.23 Deve permitir funcionamento em modo bridge em camada 2, roteador em camada 3, proxy explícito e sniffer via espelhamento;
- 13.3.24 Deve possuir mecanismo de tratamento de sessão (session-helpers ou ALGs);
- 13.3.25 Deve possuir suporte a criação de sistemas virtuais no mesmo appliance e que possam ser administrados por equipes distintas;
- 13.3.26 Deve permitir limitar o uso de recursos utilizados por cada sistema virtual;
- 13.3.27 Deve permitir, para o gerenciamento da solução, interface de administração via web no próprio dispositivo;
- 13.3.28 Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e eventos de segurança;
- 13.3.29 Deve disponibilizar controle, inspeção e de-criptografia de SSL para tráfego de entrada e saída, sendo que deve suportar ainda 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;
- 13.3.30 Em caso de ser gerenciado de forma centralizada, o equipamento ofertado deve continuar tratando o tráfego corretamente, sem causar interrupção das comunicações, mesmo no caso de queda da comunicação dos equipamentos com a solução de gerência centralizada;
- 13.3.31 Deve possuir conectores de SDN e dessa forma ser capaz de sincronizar de forma automática objetos;
- 13.3.32 Deve suportar ambientes multi-cloud;
- 13.3.33 Deve possuir a capacidade de criar automações através de gatilhos e ações, possibilitando uma atuação mais proativa;
- 13.3.34 Deve suportar alta disponibilidade (HA), trabalhando no esquema de redundância do tipo Ativo-Passivo e também Ativo-Ativo;
- 13.3.35 A configuração em alta disponibilidade deve sincronizar:
 - Sessões;
 - Configurações, incluindo, mas não limitado às políticas de Firewall, NAT, QoS e objetos de rede;
 - Associações de Segurança das VPNs;

- Tabelas FIB;
 - Assinaturas de IPS, Antivírus e AntiSpyware;
- 13.3.36 A configuração de alta disponibilidade deve possibilitar monitoração de falha de link;
- 13.3.37 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;
- 13.3.38 Deve possuir controle de acesso à Internet por endereço IP de origem e destino;
- 13.3.39 Deve possuir controle de acesso à Internet por subrede;
- 13.3.40 Deve ter a capacidade de criar políticas de firewall baseando-se em endereços MAC;
- 13.3.41 Deve suportar controles por zonas de segurança;
- 13.3.42 Deve suportar controles de políticas por porta e protocolo;
- 13.3.43 Deve suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;
- 13.3.44 Deve suportar controle de políticas por usuários, grupos de usuários, IPs, range de IPs, subrede, FQDN e zonas de segurança;
- 13.3.45 Deve suportar a criação de políticas por geo-localização, permitindo que o tráfego de determinado País/Países seja bloqueado;
- 13.3.46 Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
- 13.3.47 Deve ser viável criar políticas com exceções, onde seja possível especificar que uma política será aplicada somente caso a origem ou destino do tráfego não seja um determinado objeto.
- 13.3.48 Deve ter controle, inspeção e de-criptografia de SSL por política para tráfego de saída;
- 13.3.49 Deve ser possível realizar um espelhamento do tráfego de-criptografado.
- 13.3.50 Deve de-criptografar tráfego de saída em conexões negociadas com TLS 1.2 e TLS 1.3;
- 13.3.51 A inspeção SSL deve ser compatível com HTTP3. Tal inspeção é essencial uma vez que uma grande quantidade de sítios públicos está utilizando o protocolo em questão, tais como serviços de compartilhamento de vídeos, sites de busca e redes sociais, os quais estão sendo diariamente consumidos por usuários corporativos e externos.
- 13.3.52 Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;
- 13.3.53 Deve suportar objetos de endereço IPv4 e IPv6 consolidados na mesma política de firewall;
- 13.3.54 Deve ter suporte a objetos e regras multicast;
- 13.3.55 Deve ser possível criar políticas de firewall utilizando serviços de ameaças de terceiros, onde o firewall receberá uma lista de endereços IPs maliciosos, por exemplo, a qual poderá ser utilizada para bloqueio do tráfego;
- 13.3.56 Deve ser possível criar política de firewall em modo de aprendizado, onde o equipamento deverá monitorar o tráfego que transita nas interfaces de origem e destino e registrar logs de eventos;
- 13.3.57 Deve possuir base com objetos contendo endereços IPs de serviços da Internet como, a citar, mas não se limitando a AWS S3, Microsoft Azure, Oracle, SAP, Google e Microsoft Office 365, atualizados dinamicamente pela solução;
- 13.3.58 Deve suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;
- 13.3.59 Deve dispor de ferramenta para auxiliar a descobrir quais políticas correspondem a um determinado perfil de tráfego, facilitando assim a administração diária da solução e facilmente encontrando quais políticas estão sendo atribuídas a um determinado IP, por exemplo.
- 13.4 FUNCIONALIDADES DE CONTROLE DE APLICAÇÕES:**
- 13.4.1 Deve reconhecer, no mínimo, 2300 (duas mil e trezentas) aplicações com base na camada 7 do modelo OSI;
- 13.4.2 Deve permitir o monitoramento do tráfego de aplicações sem bloqueio de acesso aos usuários;
- 13.4.3 Deve ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando-as apenas pelo comportamento de tráfego da mesma;
- 13.4.4 Para tráfego criptografado SSL, deve de-criptografar os pacotes a fim de possibilitar a leitura do conteúdo do pacote para checagem de assinaturas de aplicações conhecidas pelo fabricante;
- 13.4.5 Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;

- 13.4.6 Deve ser possível bloquear aplicações detectadas em portas não comuns para aquela determinada aplicação;
- 13.4.7 Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory;
- 13.4.8 Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP;
- 13.4.9 Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem;
- 13.4.10 Deve 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;
- 13.4.11 Deve atualizar a base de assinaturas de aplicações automaticamente;
- 13.4.12 O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
- 13.4.13 Deve ser possível a criação de grupos de aplicações baseados em características das aplicações como: Categoria da aplicação;
- 13.4.14 Deve possibilitar a diferenciação de tráfegos Peer-to-Peer (BitTorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;
- 13.4.15 Deve possibilitar a diferenciação de tráfegos de Instant Messaging (Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;
- 13.4.16 Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts chat e bloquear a chamada de vídeo;
- 13.4.17 Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;
- 13.4.18 Deve ser possível limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos;
- 13.4.19 Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Nível de risco da aplicação e Categoria da aplicação;
- 13.4.20 Deve ser possível sobrescrever uma determinada ação para uma aplicação e para um filtro, sendo que os filtros devem ter a possibilidade de ser adicionados com base no comportamento da aplicação, tais como aplicações com alto consumo de banda, evasivas e com comportamento de botnet.
- 13.4.21 Deve ser possível editar uma aplicação associando parâmetros a serem analisados, tal como parâmetros associados a comandos na aplicação FTP.

13.5 FUNCIONALIDADES DE IPS:

- 13.5.1 Deve permitir que seja definido, através de regra por IP de origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão;
- 13.5.2 Deve possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente;
- 13.5.3 Deve possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
- 13.5.4 Deve possuir integração à plataforma de segurança;
- 13.5.5 Deve possuir capacidade de remontagem de pacotes para identificação de ataques;
- 13.5.6 Deve utilizar métodos de prevenção baseados em assinaturas, decodificadores de protocolo, análise heurística (ou monitoramento comportamental), inteligência de ameaças a partir de um centro de inteligência do próprio fabricante e detecção avançada de ameaças para evitar a exploração de ameaças conhecidas e de dia zero desconhecidas.
- 13.5.7 Deve ser capaz de realizar inspeção de pacotes criptografados, a fim de detectar e impedir ameaças de invasores neste perfil de tráfego.
- 13.5.8 Deve possuir capacidade de agrupar assinaturas para um determinado tipo de ataque, tal como agrupar todas as assinaturas relacionadas a servidores web, para que seja usado para proteção específica deste tipo de servidor e perfil de tráfego;
- 13.5.9 Deve possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias, como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;
- 13.5.10 Deve possuir assinaturas para bloqueio de ataques de buffer overflow;
- 13.5.11 Deve implementar os seguintes tipos de ações para ameaças detectadas: permitir, permitir e gerar log, bloquear, reset de conexão e bloquear IP do atacante por um intervalo de tempo;
- 13.5.12 Deve permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoramento;
- 13.5.13 Deve permitir o bloqueio de programas exploradores de vulnerabilidades conhecidos;

- 13.5.14 Deve ser possível criar políticas baseadas no alvo do ataque, seja servidor, cliente ou ambos;
- 13.5.15 Deve ser possível criar políticas com base no sistema operacional envolvido em determinada tentativa de ataque, suportando, no mínimo, Windows, Linux, MacOS, Solaris, BSD, entre outros;
- 13.5.16 Deve ser possível escanear e bloquear conexões a servidores de botnet;
- 13.5.17 Deve dispor de opção para bloquear URLs maliciosas mediante base de dados local;
- 13.5.18 Deve ser possível habilitar a opção de salvar os pacotes correspondentes a uma determinada assinatura de IPS;
- 13.5.19 Deve suportar a possibilidade de criar políticas baseadas em nível de severidade das assinaturas de IPS;
- 13.5.20 Deve suportar a possibilidade de criar políticas baseadas no perfil da aplicação, tais como Apache, IIS, DB2, MySQL, PostgreSQL, MSSQL, MS Exchange, entre outros;
- 13.5.21 Deve ser possível filtrar assinaturas com base no identificador CVE;
- 13.5.22 Deve ser possível criar uma assinatura de IPS utilizando o identificador CVE, bem como um "wildcard" do CVE para abranger mais de um identificador;
- 13.5.23 As assinaturas devem dispor de um resumo explicando o ataque associado, nível de severidade, impacto e uma possível recomendação, bem como deve vincular o(s) CVE(s) correspondente(s) quando aplicável;
- 13.5.24 Deve incluir proteção contra-ataques de negação de serviços;
- 13.5.25 Deve registrar no console de monitoramento 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;
- 13.6 FUNCIONALIDADES DE PROTEÇÃO CONTRA AMEAÇAS AVANÇADAS:**
 - 13.6.1 Deve possuir funções de antivírus e anti-spyware;
 - 13.6.2 Deve possuir antivírus em tempo real, para ambiente de gateway Internet, integrado à plataforma de segurança para os seguintes protocolos: HTTP, SMTP, IMAP, POP3, CIFS e FTP;
 - 13.6.3 Deve permitir o bloqueio de malwares (adware, spyware, hijackers, keyloggers, entre outros);
 - 13.6.4 Deve dispor de detecção baseada em aprendizado de máquina, sendo possível inspecionar e identificar funcionalidades do arquivo que possam determinar se o mesmo tem comportamento de malware, ao invés de simplesmente realizar a análise baseada em assinaturas;
 - 13.6.5 Deve permitir o bloqueio de download de arquivos por extensão, nome do arquivo e tipos de arquivo;
 - 13.6.6 Deve permitir o bloqueio de download de arquivos por tamanho;
 - 13.6.7 Deve ser capaz de mitigar ameaças avançadas persistentes (APT), através de análises dinâmicas para identificação de malwares desconhecidos;
 - 13.6.8 Deve dispor de funcionalidade de desarme e reconstrução visando atuar em cima de arquivos Microsoft Office e PDF, mesmo no caso de o arquivo estar compactado, removendo conteúdo maliciosos como links, JavaScript, Macros, entre outros;
 - 13.6.9 Deve ser possível criar políticas de bloqueio de malware utilizando serviços de terceiros, onde o firewall receberá uma lista de hashes maliciosos;
 - 13.6.10 Deve ser capaz de mitigar ameaças avançadas persistentes (APT), através de análises dinâmicas para identificação de malwares desconhecidos;
 - 13.6.11 A solução de sandbox deve ser capaz de criar assinaturas e ainda as incluir na base de antivírus do firewall, prevenindo a reincidência do ataque;
 - 13.6.12 A solução de sandbox deve ser capaz de incluir no firewall as URLs identificadas como origens de tais ameaças desconhecidas, impedindo que esses endereços sejam acessados pelos usuários de rede novamente;
 - 13.6.13 Dentre as análises efetuadas, a solução deve suportar antivírus, consulta na nuvem, emulação de código, sandboxing e verificação de chamada de call-back;
 - 13.6.14 A solução deve analisar o comportamento de arquivos suspeitos em um ambiente controlado de sandbox. Deve ainda disponibilizar um relatório completo da análise realizada em cada arquivo submetido, o qual poderá ser baixado para auxiliar na análise forense de um evento;
- 13.7 FUNCIONALIDADES DE FILTRO WEB E CONTEÚDO:**
 - 13.7.1 Deve permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
 - 13.7.2 Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de

segurança;

- 13.7.3 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;
- 13.7.4 A identificação pela base do Active Directory deve permitir SSO, de forma que os usuários não precisem logar novamente na rede para navegar pelo firewall;
- 13.7.5 Deve suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
- 13.7.6 Deve possuir a função de exclusão de URLs do bloqueio;
- 13.7.7 Deve permitir a customização de página de bloqueio;
- 13.7.8 Deve 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);
- 13.7.9 Deve dispor de funcionalidade de prevenção contra phishing de credenciais analisando quais estão sendo submetidas em sites externos, permitindo ainda bloquear ou alertar o usuário;
- 13.7.10 Deve possuir a possibilidade de definir uma quota diária de uso web baseado em categoria, sendo possível estipular a quota com base em, no mínimo, tempo de uso e volume de tráfego;
- 13.7.11 Deve ser possível bloquear tráfego HTTP POST, método utilizado para envio de informação a um determinado website;
- 13.7.12 Deve ser possível filtrar e remover Java applets, ActiveX e cookies do tráfego web inspecionado;
- 13.7.13 Deve possuir em sua base de dados uma lista de bloqueio contendo URLs de certificados maliciosos;
- 13.7.14 Deve ser possível filtrar tráfego de vídeo baseado em categoria e até mesmo baseado no identificador de um canal do YouTube, por exemplo;
- 13.7.15 Deve permitir além do Web Proxy explícito, suportar proxy Web transparente;

13.8 IDENTIFICAÇÃO DOS USUÁRIOS

- 13.8.1 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;
- 13.8.2 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, suportando SSO (Single Sign-On). Essa funcionalidade não deve possuir limites quanto a licenciamento de usuários;
- 13.8.3 Deve possuir integração com RADIUS para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 13.8.4 Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;
- 13.8.5 Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a Internet para que antes de iniciar a navegação, apresente-se um portal de autenticação residente no firewall do tipo "captive portal";
- 13.8.6 Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix, VMware Horizon e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
- 13.8.7 Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

13.9 FUNCIONALIDADES DE ROTEAMENTO INTELIGENTE DE APLICAÇÃO:

- 13.9.1 A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para uma aplicação;
- 13.9.2 Deve ser capaz de agregar pelo menos 03 (três) links em uma interface virtual;
- 13.9.3 A solução deve ser capaz de monitorar e identificar falhas mediante a associação de verificações de saúde dos links WAN, permitindo testes de resposta por PING, HTTP, TCP/UDP ECHO, DNS e TWAMP. Deve suportar ainda um método para mensurar a qualidade do tráfego de voz corporativo baseado em MOS (Mean Opinion Score);
- 13.9.4 Deve ser permitida a criação de políticas de roteamento com base nos seguintes critérios: latência, jitter, perda de pacote, banda ocupada ou todos ao mesmo tempo;
- 13.9.5 Diversas formas de escolha do link devem estar presentes, incluindo: melhor link, menor custo e definição de níveis máximos de qualidade a serem aceitos para que tais links possam ser

utilizados em um determinado roteamento de aplicação;

- 13.9.6 Deve suportar o uso de VRF (Virtual Routing and Forwarding);
- 13.9.7 A solução de deve possuir suporte a Policy Based Routing ou Policy Based Forwarding;
- 13.9.8 Deve suportar roteamento estático e dinâmico (OSPFv2/v3, BGPv4/BGP4+);
- 13.9.9 Deve poder adicionar e equilibrar, no mínimo, 06 interfaces de dados (links e VPNs);
- 13.9.10 Deve possibilitar a agregação de túneis IPsec, realizando balanceamento por pacote entre os mesmos;
- 13.9.11 Deve permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da interface virtual;
- 13.9.12 Deve desempenhar a função de duplicidade de pacote permitindo encaminhar o pacote por mais de um circuito para em casos de falhas não ocorrer retransmissão;
- 13.9.13 Deve possuir recurso para correção de erro (FEC), possibilitando a redução das perdas de pacotes nas transmissões;
- 13.9.14 Deve permitir configurar o código de DiffServ (DSCP) do pacote ESP do túnel IPsec;
- 13.9.15 Deve permitir marcar com DSCP os testes de link para obter uma avaliação mais realista da qualidade de um determinado link;
- 13.9.16 Deve possibilitar a distribuição de peso em cada um dos links que compõe a interface virtual, a critério do administrador, de forma em que o algoritmo de balanceamento utilizado possa ser baseado em:
 - Número de Sessões,
 - Volume de Tráfego,
 - IP de Origem e Destino;
 - Transbordo de Link baseado em limite de banda.
- 13.9.17 As regras de escolha de roteamento devem suportar o reconhecimento de aplicações, grupos de usuários, endereço IP de origem e destino e serviços de Internet;
- 13.9.18 Deve permitir a customização dos tempos para detecção de queda de link, bem como tempo necessário para retornar com o link para o balanceamento após restabelecido;
- 13.9.19 Deve prover estatísticas em tempo real na interface web a respeito da ocupação de banda (upload e download) e desempenho das verificações de saúde (perda de pacote, jitter e latência);
- 13.9.20 Deve ser possível configurar a porcentagem de perda de pacote e o tempo de latência e jitter na verificação de estado de saúde do link. Estes valores serão utilizados pela solução para decidir qual link será utilizado;
- 13.9.21 Deve dispor de opção que maximize o uso da largura de banda utilizando os links WANs que estejam dentro do nível de saúde estipulado;
- 13.9.22 Deve ser possível monitorar a saúde do link de modo passivo, sem a emissão de pacotes de verificação, utilizando somente informações das sessões que transitam pelo equipamento;
- 13.9.23 Deve ser possível utilizar o método de verificação de saúde passivo na existência de tráfego e ativo na inexistência de tráfego;
- 13.9.24 Deve suportar balanceamento de tráfego por sessão e pacote;
- 13.9.25 Deve ser possível extrair informações de desempenho das verificações de saúde mediante REST API, permitindo assim a consolidação de tais informações em alguma aplicação terceira;
- 13.9.26 Deve suportar algum método de descoberta automática de VPN, funcionalidade esta que tem o intuito de dinamicamente viabilizar que túneis sejam estabelecidos entre duas localidades remotas, sem necessidade do tráfego transitar pelo ponto central conhecido por HUB;

13.10 QUALITY OF SERVICE (QoS)

- 13.10.1 Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como Youtube, BitTorrent, 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 largura de banda máxima quando forem solicitadas por diferentes usuários ou aplicações.
- 13.10.2 Deve suportar a criação de políticas de QoS e Traffic Shaping para os seguintes itens:
 - por endereço de origem;
 - por endereço de destino;
 - por usuário e grupo;
 - por aplicações;
 - por protocolo e porta;

- por categoria de URL;
 - 13.10.3 O QoS deve possibilitar a definição de tráfego com banda garantida;
 - 13.10.4 O QoS deve possibilitar a definição de tráfego com banda máxima;
 - 13.10.5 Deve possibilitar a marcação de DSCP, a fim de que essa informação possa ser utilizada ao longo do backbone para fins de reserva de banda;
 - 13.10.6 O QoS deve possibilitar a definição de fila de prioridade;
 - 13.10.7 Além de possibilitar a definição de banda máxima e garantida por aplicação, deve também suportar o vínculo com categorias de URL, IPs de origem e destino, grupos de usuários, protocolos e portas;
 - 13.10.8 Deve ter a capacidade de agendar intervalos de tempo onde as políticas de shaping/QoS serão válidas e mandatória;
 - 13.10.9 Uma vez que o tráfego é identificado, as políticas de shaping/QoS podem ser compartilhadas a todos os acessos que tiverem correspondência na regra ou por IP;
 - 13.10.10 Deve possibilitar a definição de bandas distintas para download e upload;
- 13.11 CONTROLADORA DE REDE SEM FIO**
- 13.11.1 Deve administrar e controlar de maneira centralizada os pontos de acesso wireless do mesmo fabricante da solução ofertada;
 - 13.11.2 Deve permitir a conexão de dispositivos wireless que transmitam tráfego IPv4 e IPv6;
 - 13.11.3 Deve ser capaz de gerenciar pontos de acesso que estejam conectados remotamente através de links WAN e Internet;
 - 13.11.4 Deve permitir ser descoberto automaticamente pelos pontos de acesso através de Broadcast, DHCP e consulta DNS;
 - 13.11.5 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;
 - 13.11.6 Deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;
 - 13.11.7 Deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência;
 - 13.11.8 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;
 - 13.11.9 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;
 - 13.11.10 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;
 - 13.11.11 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;
 - 13.11.12 Deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP;
 - 13.11.13 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;
 - 13.11.14 Deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários;
 - 13.11.15 Deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio;

- 13.11.16 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;
- 13.11.17 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;
- 13.11.18 Deve permitir a configuração de quais data rates estarão ativos na ferramenta e quais serão desabilitados;
- 13.11.19 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;
- 13.11.20 Deve suportar a configuração do BLE (Bluetooth Low Energy) nos pontos de acesso que tenham este recurso;
- 13.11.21 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;
- 13.11.22 Deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados;
- 13.11.23 Deve ser capaz de reconfigurar automaticamente os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando for identificado um alto índice de sobreposição de sinal oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências;
- 13.11.24 Deve registrar todos os logs de eventos com bloqueios e liberações das aplicações que foram acessadas na rede wireless;
- 13.11.25 Deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados:
- 13.11.26 Ataques de flood contra o protocolo EAPOL (EAPOL Flooding);
- 13.11.27 Os seguintes ataques de negação de serviço: Association Flood, Authentication Flood, Broadcast Deauthentication e Spoofed Deauthentication;
- 13.11.28 ASLEAP;
- 13.11.29 Null Probe Response or Null SSID Probe Response;
- 13.11.30 Long Duration;
- 13.11.31 Ataques contra Wireless Bridges;
- 13.11.32 Weak WEP;
- 13.11.33 Invalid MAC OUI.
- 13.11.34 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 deauthentication;
- 13.11.35 Deve implementar mecanismos de proteção contra-ataques do tipo ARP Poisoning na rede wireless;
- 13.11.36 Deve permitir configurar o bloqueio na comunicação entre os clientes wireless conectados a um determinado SSID;
- 13.11.37 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;
- 13.11.38 Deve permitir a hospedagem do captive portal na memória interna do controlador wireless;
- 13.11.39 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;
- 13.11.40 Deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede;
- 13.11.41 Deve permitir a configuração do captive portal com endereço IPv6;
- 13.11.42 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;
- 13.11.43 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;
 - 13.11.44 Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado;
 - 13.11.45 Deve identificar automaticamente o tipo de equipamento e sistema operacional utilizado pelo dispositivo conectado à rede wireless;
 - 13.11.46 Deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados;
 - 13.11.47 Deve possuir recurso para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no equipamento ao qual os APs estejam fisicamente conectados;
 - 13.11.48 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;
 - 13.11.49 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;
 - 13.11.50 Deve permitir o gerenciamento unificado e de forma gráfica para redes WiFi e redes cabeadas;
 - 13.11.51 Deve permitir a identificação do firmware utilizado por cada ponto de acesso gerenciado e permitir a atualização via interface gráfica;
 - 13.11.52 Deve permitir a atualização de firmware individualmente nos pontos de acesso, garantindo a gestão e operação simultânea de pontos de acesso com firmwares diferentes;
 - 13.11.53 Deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de um ponto de acesso;
 - 13.11.54 Deve ser compatível e gerenciar os pontos de acesso deste edital;

14 Licenças e Suporte do NGFW (item anterior) - Modelos de Referência: Fortinet UTP (pacote Unified Threat Protection) – QUANTIDADE 02

- 14.1 Devem ser fornecido o Licenciamento de todas as funcionalidades descritas no item 13 (anterior) deste do edital;
- 14.2 Deve ser incluir o suporte do hardware e software referente ao item 13;
- 14.3 Validade do licenciamento e suporte de 3 anos (36 meses);
- 14.4 As funcionalidades 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. Salvo a funcionalidade de Filtro de URL's e Conteúdo;

15 Solução Firewall de Próxima Geração (NGFW) 2 – Modelo de referência: Fortigate 60F (para Apoio) – QUANTIDADE 02

Características Mínimas:

15.1 REQUISITOS GERAIS

- 15.1.1 Deve ter compatibilidade e integração em malha ao Orquestrador e ativos da instituição:
 - FORTIMANAGER v 7.6.3;
 - FORTIGATE FG-1001F
 - FORTIGATE FG-200E
 - FORTIGATE FG-100F
- 15.1.2 Deve ter a função de NGFW (NEXT GENERATION FIREWALL) atuando com o intuito de conexão com enlaces WAN (Wide Área Network), tais como links de Internet, MPLS, entre outros, para utilização da engenharia de tráfego, provendo ainda de modo integrado conectividade segura, viabilizando assim o acesso local à Internet de modo seguro;
- 15.1.3 Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;
- 15.1.4 Os componentes da solução devem ser novos, sem utilização anterior e em linha de fabricação;
- 15.1.5 A solução deve ter arquitetura dedicada, não podendo ser servidor de uso genérico, e o

sistema operacional deve estar embutido no hardware proposto, ou seja, hardware e software devem ser integrados em um único equipamento;

- 15.1.6 Deve consistir em plataforma de proteção de rede baseada em equipamento físico com funcionalidades de Next Generation Firewall (NGFW), não sendo permitido appliances virtuais ou solução open source;
- 15.1.7 Todos os equipamentos a serem fornecidos, bem como seu hardware e software, devem ser do mesmo fabricante para assegurar a padronização e compatibilidade funcional de todos os recursos;
- 15.1.8 Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões.
- 15.1.9 A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7 com base no modelo OSI.
- 15.1.10 O gerenciamento da solução deve suportar acesso via SSH, WEB (HTTPS) e via API.
- 15.1.11 Os softwares deverão ser fornecidos em sua versão mais atualizada na data de entrega;
- 15.1.12 Todo hardware e software componentes da solução deve ser do mesmo fabricante, admitido o regime de OEM;
- 15.1.13 Deve possuir interface ethernet “Out-of-Band” dedicada para gerenciamento de configuração e gerenciamento através de interface de linha de comando CLI (comand line interface);
- 15.1.14 Deve possuir ao menos 5 interfaces 1GE RJ45;
- 15.1.15 Deve possuir ao menos 2 interfaces 1 GE RJ45 WAN;
- 15.1.16 Deve possuir ao menos 1 interfaces 1 GE RJ45 DMZ;
- 15.1.17 Todas as interfaces de rede fornecidas nos appliances devem estar completamente licenciadas e habilitadas para uso imediato;
- 15.1.18 Deve estar licenciado ou ter incluído sem custo adicional, no mínimo, 10 sistemas virtuais lógicos por equipamento. Entende-se por sistema virtual lógico a possibilidade de dividir um único equipamento físico em várias unidades virtuais, tendo um contexto para WAN e outro contexto para LAN, por exemplo.
- 15.1.19 Permitir montagem em rack com largura padrão de 19 polegadas. Deverão ser fornecidos todos os cabos, suportes (se necessários, “gavetas”, “braços” e “trilhos”) para a instalação dos equipamentos no rack;
- 15.1.20 Deve possuir uma fonte de energia e a faixa de tensão de entrada suportada deve ser de 100 VAC a 240 VAC, a 60 Hz sem uso de chave de seleção de voltagem (automaticamente), capaz de sustentar a configuração máxima do equipamento;
- 15.1.21 Todas as funcionalidades, features e licenciamentos deverão ser fornecidos pelo mesmo fabricante de maneira integrada e em uma mesma arquitetura, com atualizações no período do contrato;
- 15.1.22 Deve suportar o gerenciamento de até 30 (trinta) pontos de acesso wireless simultaneamente;

15.2 PERFORMANCE:

- 15.2.1 Deve suportar, no mínimo, 1.0 Gbps de throughput de Firewall stateful;
- 15.2.2 Deve suportar, no mínimo, 1.0 Gbps de throughput IPS;
- 15.2.3 Deve suportar, no mínimo, 6.0 Gbps de throughput de VPN IPsec;
- 15.2.4 Deve suportar, no mínimo, 600 Mbps de throughput de Inspeção SSL;
- 15.2.5 Deve suportar, no mínimo, 800 Mbps de throughput de VPN SSL;
- 15.2.6 Deve suportar, no mínimo, 700 Mbps 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;
- 15.2.7 Deve suportar no mínimo, 700 mil de conexões simultâneas;
- 15.2.8 Deve suportar no mínimo, 35 mil novas conexões por segundo;
- 15.2.9 Deve estar licenciado para, ou suportar sem o uso de licença, 200 túneis de VPN IPsec Site-to-Site simultâneos;
- 15.2.10 Deve estar licenciado para, ou suportar sem o uso de licença, 400 túneis de clientes VPN IPsec simultâneos;
- 15.2.11 Deve estar licenciado para, ou suportar sem o uso de licença, 200 clientes de VPN SSL simultâneos;

15.3 CARACTERÍSTICAS GERAIS DA SOLUÇÃO DE FIREWALL PRÓXIMA GERAÇÃO (NGFW)

- 15.3.1 Deve suportar pela adição de licenciamento, as funcionalidades e serviços abaixo listadas:

- Controle de Aplicações;
 - Proteção IPS;
 - Proteção contra Ameaças Avançadas;
 - Filtro Web e de Conteúdo;
 - Análise de malwares modernos em nuvem do mesmo fabricante;
 - Roteamento inteligente de aplicações;
 - VPN site-to-site e client-to-site;
- 15.3.2 Deve estar devidamente licenciada (vide próximo item) para atender no mínimo:
- Garantia e suporte remoto diretamente com o fabricante na modalidade de 8x5;
- 15.3.3 Deve suportar tags de VLAN (802.1Q);
- 15.3.4 Deve possuir suporte a agregação de links via 802.3ad LACP;
- 15.3.5 Deve possuir ferramenta de diagnóstico do tipo tcpdump e ainda dispor de ferramenta integrada à interface web para capturar informações dos pacotes em tempo real, podendo aplicar filtros, tais como IPs e portas, e ainda ter disponível a possibilidade de exportar a captura para um arquivo do tipo PCAP visando estender a análise para um software terceiro, tal como Wireshark;
- 15.3.6 Deve possuir integração com servidores de autenticação RADIUS, LDAP e Microsoft Active Directory;
- 15.3.7 Deve possuir integração com tokens para autenticação de duplo fator;
- 15.3.8 Deve suportar single-sign-on;
- 15.3.9 Deve possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um, N-para-um, vários para um, NAT64, NAT66, NAT46 e PAT;
- 15.3.10 Deve suportar roteamento estático para IPv4 e IPv6;
- 15.3.11 Deve suportar roteamento dinâmico para IPv4 e IPv6 (OSPF, OSPFv2, OSPFv3, BGP, RIP);
- 15.3.12 Deve suportar ECMP;
- 15.3.13 Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);
- 15.3.14 Deve possuir funcionalidades de DHCP Cliente, Servidor e Relay;
- 15.3.15 Deve suportar aplicações multimídia, tais como: H.323 e SIP;
- 15.3.16 Deve permitir o funcionamento em modo transparente tipo “bridge”;
- 15.3.17 Deve suportar PBR – Policy Based Routing;
- 15.3.18 Deve possuir conexão entre estação de gerência e appliance criptografada, tanto em interface gráfica, quanto em CLI (linha de comando);
- 15.3.19 Deve possuir mecanismo de anti-spoofing;
- 15.3.20 Deve permitir criação de regras definidas pelo usuário;
- 15.3.21 Deve suportar sFlow ou Netflow;
- 15.3.22 Os dispositivos de proteção de rede devem possuir suporte a Jumbo Frames;
- 15.3.23 Deverá permitir autenticação de usuários em base local, servidor LDAP, RADIUS e TACACS;
- 15.3.24 Deve permitir funcionamento em modo bridge em camada 2, roteador em camada 3, e sniffer via espelhamento;
- 15.3.25 Deve possuir mecanismo de tratamento de sessão (session-helpers ou ALGs);
- 15.3.26 Deve possuir suporte a criação de sistemas virtuais no mesmo appliance e que possam ser administrados por equipes distintas;
- 15.3.27 Deve permitir limitar o uso de recursos utilizados por cada sistema virtual;
- 15.3.28 Deve permitir, para o gerenciamento da solução, interface de administração via web no próprio dispositivo;
- 15.3.29 Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e eventos de segurança;
- 15.3.30 Deve disponibilizar controle, inspeção e de-criptografia de SSL para tráfego de entrada e saída, sendo que deve suportar ainda 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;
- 15.3.31 Em caso de ser gerenciado de forma centralizada, o equipamento ofertado deve continuar tratando o tráfego corretamente, sem causar interrupção das comunicações, mesmo no caso de queda da comunicação dos equipamentos com a solução de gerência centralizada;

- 15.3.32 Deve possuir conectores de SDN e dessa forma ser capaz de sincronizar de forma automática objetos;
- 15.3.33 Deve suportar ambientes multi-cloud;
- 15.3.34 Deve possuir a capacidade de criar automações através de gatilhos e ações, possibilitando uma atuação mais proativa;
- 15.3.35 A configuração em alta disponibilidade deve sincronizar:
 - Sessões;
 - Configurações, incluindo, mas não limitado às políticas de Firewall, NAT, QoS e objetos de rede;
 - Associações de Segurança das VPNs;
 - Tabelas FIB;
- 15.3.36 A configuração de alta disponibilidade deve possibilitar monitoração de falha de link;
- 15.3.37 Deve possuir controle de acesso à Internet por endereço IP de origem e destino;
- 15.3.38 Deve possuir controle de acesso à Internet por subrede;
- 15.3.39 Deve ter a capacidade de criar políticas de firewall baseando-se em endereços MAC;
- 15.3.40 Deve suportar controles por zonas de segurança;
- 15.3.41 Deve suportar controles de políticas por porta e protocolo;
- 15.3.42 Deve suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;
- 15.3.43 Deve suportar controle de políticas por usuários, grupos de usuários, IPs, range de IPs, subrede, FQDN e zonas de segurança;
- 15.3.44 Deve suportar a criação de políticas por geo-localização, permitindo que o tráfego de determinado País/Países seja bloqueado;
- 15.3.45 Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
- 15.3.46 Deve ser viável criar políticas com exceções, onde seja possível especificar que uma política será aplicada somente caso a origem ou destino do tráfego não seja um determinado objeto.
- 15.3.47 Deve ter controle, inspeção e de-criptografia de SSL por política para tráfego de saída;
- 15.3.48 Deve ser possível realizar um espelhamento do tráfego de-criptografado.
- 15.3.49 Deve de-criptografar tráfego de saída em conexões negociadas com TLS 1.2 e TLS 1.3;
- 15.3.50 A inspeção SSL deve ser compatível com HTTP3. Tal inspeção é essencial uma vez que uma grande quantidade de sítios públicos está utilizando o protocolo em questão, tais como serviços de compartilhamento de vídeos, sites de busca e redes sociais, os quais estão sendo diariamente consumidos por usuários corporativos e externos.
- 15.3.51 Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;
- 15.3.52 Deve suportar objetos de endereço IPv4 e IPv6 consolidados na mesma política de firewall;
- 15.3.53 Deve ter suporte a objetos e regras multicast;
- 15.3.54 Deve ser possível criar políticas de firewall utilizando serviços de ameaças de terceiros, onde o firewall receberá uma lista de endereços IPs maliciosos, por exemplo, a qual poderá ser utilizada para bloqueio do tráfego;
- 15.3.55 Deve ser possível criar política de firewall em modo de aprendizado, onde o equipamento deverá monitorar o tráfego que transita nas interfaces de origem e destino e registrar logs de eventos;
- 15.3.56 Deve possuir base com objetos contendo endereços IPs de serviços da Internet como, a citar, mas não se limitando a AWS S3, Microsoft Azure, Oracle, SAP, Google e Microsoft Office 365, atualizados dinamicamente pela solução;
- 15.3.57 Deve suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;
- 15.3.58 Deve dispor de ferramenta para auxiliar a descobrir quais políticas correspondem a um determinado perfil de tráfego, facilitando assim a administração diária da solução e facilmente encontrando quais políticas estão sendo atribuídas a um determinado IP, por exemplo.

16 Suporte do NGFW (item anterior) - Modelos de Referência: Forticare Premium – QUANTIDADE 02

- 16.1** Devem ser fornecido o Suporte do item 15 (anterior) deste lote;
- 16.2** Validade do suporte de 3 anos (36 meses).

1.2. Da natureza do objeto

- (X) Não se enquadra como sendo bem de luxo, conforme Decreto nº 2.355, de 16 de dezembro de 2022
- (X) Os bens objeto desta contratação são caracterizados como comuns, com características e especificações usuais de mercado.

2. JUSTIFICATIVA DA CONTRATAÇÃO

A Justificativa da contratação encontra-se pormenorizada em tópico específico dos Estudos Técnicos Preliminares, anexo ao processo.

Resumidamente as justificativas (razão):

- A definição dos quantitativos e necessidades tem como base o histórico de eventos e crescimento das atividades.
- Existe a necessidade de registrar novos equipamentos firewall devido a saída do mercado de um dos modelos que usamos atualmente.
- Acrescentar prazo aos licenciamentos FORTINET para garantir que a rede continue com a segurança no mesmo nível atual, sem perder funcionalidades e atualizações. Alguns equipamentos estão com os prazos em fase final.
- Dar continuidade a ampliação e melhoria da rede lógica da UDESC, que faz parte do planejamento estratégico atendendo as metas de comunicação. A falta de um ativo de rede pode causar a paralisação dos serviços administrativos e acadêmicos.
- Adquirir licenciamentos FORTINET de IA (Inteligência Artificial) para ajudar a equipe técnica que é pequena a resolver os problemas com mais agilidade, melhorando as atividades e o monitoramento da instituição.

O quantitativo de todos os itens do edital é verificado pela equipe da SETIC e CINF, junto aos fabricantes e revendedores, para atender as necessidades futuras e problemas que começam a se apresentar; sempre buscando a melhor solução custo benefício.

3. DOS PARÂMETROS DA LICITAÇÃO

3.1. Será adotado o Sistema de Registro de Preços – SRP?

- (X) Sim
- () Não

3.1.1 Justificativa para adoção do Sistema de Registro de Preços:

- (X) quando, pelas características do bem ou serviço, houver necessidade de contratações frequentes, com maior celeridade e transparência
- (X) quando for conveniente a compra de bens ou a contratação de serviços para atendimento a mais de um órgão ou entidade, ou a programas de governo; e
- () quando, pela natureza do objeto, não for possível definir previamente o quantitativo a ser demandado pela Administração Pública.

3.1.2 Vigência da Ata de Registro de Preços:

- (X) Prazo de um ano, podendo ser prorrogado por igual período;
- () Prazo de um ano, sem a possibilidade de prorrogação.

3.2. Será adotado tratamento diferenciado a microempresas (ME) e empresas de pequeno porte (EPP), conforme o disposto no art. 48 da Lei Complementar nº 123/2006 (alterado pela Lei Complementar nº 147/2014):

- (X) Valor referencial inferior a R\$ 80.000,00 por item (participação exclusiva para ME/EPP).
- () Valor referencial superior a R\$ 80.000,00 por item (participação exclusiva para ME/EPP).
- () Valor referencial superior a R\$ 80.000,00 de natureza divisível (com cota para ME/EPP).
- () Valor referencial superior a R\$ 80.000,00 de natureza divisível, porém não sendo aplicável tratamento

diferenciado e simplificado para as microempresas e empresas de pequeno porte por não ser mais vantajoso para a administração pública.

Justificativa:

--

3.3. Haverá necessidade de vistoria prévia (visita técnica)?

- () Vistoria obrigatória
() Vistoria facultativa
(X) Não será exigida vistoria.

Justificativa:

As licenças e softwares são padrão de mercado, e o equipamento será instalado pela equipe da UDESC.

3.4. Será admitida a participação de consórcios?

- (X) Não
() Sim

Justificativa:

A vedação quanto à participação de consórcio de empresas no presente procedimento licitatório não limitará a competitividade. A participação de consórcios é recomendável quando o objeto considerado for “de alta complexidade ou vulto”, o que não seria o caso do objeto sob exame. Não há nada que justifique a participação de empresas em consórcios no objeto em apreço. Ele não se reveste de alta complexidade, tampouco é serviço de grande vulto econômico, ou seja, o edital não traz em seu termo de referência nenhuma característica própria que justificasse a admissão de empresas em consórcio.

3.5. Será admitida a participação de cooperativas?

- (X) Não
() Sim

3.6. Será admitida a subcontratação?

- (X) Não
() Sim

3.7. Do agrupamento de itens em lotes

A aquisição/contratação se dará em lotes?

- () Não
(X) Sim

Justificativa:

A aglutinação realizada por esta equipe de planejamento, subscritores desta justificativa, foi realizada, após minuciosa análise, reunindo itens que habitualmente são fornecidos por empresas do mesmo ramo de atividade, visando tornar economicamente viável a competição e diante do Princípio de Economicidade ao tentar obter a proposta mais vantajosa para a Administração, mas em um nível “ótimo” possibilitará a maior competitividade possível no certame.
--

3.8. Será admitida adesão à ARP por órgãos não participantes?

- () Não
(x) Sim

Justificativa:

O uso da Ata de Registro de Preços por qualquer órgão ou entidade da Administração Pública do Estado de

Santa Catarina justifica-se, naturalmente, pela economia obtida por não incorrer essas instituições em gastos gerados nos processos licitatórios. Ademais, as ações adotadas por esta Universidade podem ser convenientes a outros órgãos ou entidades da administração do Estado. É vedada a carona a órgãos municipais (inclusive de Santa Catarina), bem como outros Estados, Distrito Federal e União.

4. DOS CRITÉRIOS DE ACEITAÇÃO DA PROPOSTA

4.1. Serão exigidos documentos adicionais juntamente com a proposta de preços (para análise da equipe técnica na fase de julgamento da proposta final de preços):

- () Não
(X) Sim

Se sim, quais?

4.1. Para comprovação das especificações exigidas, dos equipamentos, a licitante deverá apresentar em papel ou em formato digital (disponível no site do fabricante ou fornecido em mídia), sob pena de desclassificação da proposta, os prospectos técnicos e/ou catálogos do fabricante dos equipamentos cotados, informando marca, o modelo e o fabricante do equipamento, não sendo aceita a simples cópia da especificação geral do edital;

4.2. O equipamento cotado deverá constar no portfólio de produtos do fabricante, sendo que o mesmo não deverá estar na lista de produtos a serem descontinuados (End-of-Life e End-of-Sale);

4.3. Deverá ser fornecido, no formato abaixo, um documento que faça a associação do item especificado neste Anexo com o documento técnico que comprove a validação dele, como no exemplo abaixo:

10.10.1 – Característica Datasheet X, página Y, item N

x

10.10.2 – Característica Site: www.fabricante.com/zzzzz

z

4.4. É pré-requisito obrigatório, para fins de comercialização e utilização no país, a certificação de Produtos de Telecomunicação classificáveis nas Categorias I, II e III do artigo 4o da Resolução Anatel 242/2000.

4.2. Será exigido amostra do(s) produto(s)/demonstração do(s) serviço(s):

- () Não
() Sim

(X) A critério da equipe técnica

Se sim ou a critério da equipe técnica:

Prazo para apresentação: 15 dias

Quantidade de amostras: normalmente 1

Unidade técnica responsável pela análise das amostras: SETIC – REITORIA

Local de entrega das amostras: SETIC - REITORIA

Em caso de dúvida técnica, será solicitado uma amostra do item para verificar as especificações e a compatibilidade exigida.

Condições e critérios de avaliação e julgamento da amostra e/ou da demonstração dos serviços:

Item	Código	Critério de avaliação das amostras/protótipos
Todos	Todos	Verificadas as características técnicas, físicas, ergonômicas, aspectos estéticos em geral, dimensões e/ou demais conformidades relativas à qualidade descrita no Termo de Referência
Todos	Todos	Será verificado a compatibilidade exigida para a solução solicitada.

4.2.1. Serão recusados todos os **itens/lotos** em que os materiais não atenderem as especificações técnicas solicitadas ou que apresentarem não conformidade com a qualidade desejada. As amostras entregues para análise deverão ser identificadas com os seguintes dados: Nome da empresa, CNPJ, Nome e telefone do representante legal, Número do processo licitatório, Número do item. As amostras serão válidas somente para esta Licitação.

4.2.2. A solicitação será formalizada via “CHAT”, devendo a empresa entregar no prazo estipulado acima, sob pena de desclassificação do lote, a contar da sessão que definiu a empresa melhor classificada. Caso a empresa não apresente a amostra, além da desclassificação sofrerá as devidas penalizações por não manter a sua proposta no Pregão.

4.2.3. As amostras poderão sofrer danos devido aos testes que serão realizados, portanto, não poderão ser computadas no quantitativo a ser entregue. As amostras ficarão disponíveis para serem retiradas posteriormente a homologação do Pregão.

4.2.4. A não apresentação da(s) amostra(s) ou se a amostra(s) solicitada não corresponder às especificações do edital, o pregoeiro fará a desclassificação de todo o lote da empresa vencedora dos lances, justificando em análise e parecer técnico.

4.2.5. Na hipótese do item anterior, o pregoeiro convocará a empresa seguinte na ordem de classificação das propostas dos lances a apresentar as amostras e assim por diante.

4.3. Será exigida prova de conceito?

(X) Não

() Sim

4.4. Será exigida carta de solidariedade?

(X) Não

() Sim

Se sim, justificativa:

4.5. Será exigida garantia de proposta?

(X) Não

() Sim

Se sim, justificativa:

5. DOS CRITÉRIOS DE HABILITAÇÃO

5.1 (X) Cadastro de fornecedor no Estado de Santa Catarina (CCF);

5.2 Para fins de habilitação, deverá o licitante comprovar os seguintes requisitos, além do Cadastro de fornecedor:

5.2.2 A licitante deve ser parceiro Fortinet, no Brasil, devendo apresentar no momento da habilitação, comprovante desta parceria, através de carta do fabricante ou comprovar constar na lista do site <https://partnerportal.fortinet.com/directory/search?loe=Expert&l=Brazil> . Este documento é obrigatório em razão da garantia do produto.

5.2.1 Qualificação técnica - Conforme descrição do item.

6. DA EXECUÇÃO DO OBJETO

6.1. Local e endereço de entrega:

6.1.1 CAMPUS I – GRANDE FLORIANÓPOLIS:

6.1.1.1 Reitoria

Av. Madre Benvenuta, 2007, Itacorubi, Florianópolis/SC CEP 88035-001.

6.2 Prazo de entrega/execução

6.2.1. O prazo de entrega dos materiais/serviços será de até 90 (noventa) dias corridos após o recebimento da nota de empenho e Contrato/AF autorizando a entrega/prestação do item. Exceto para o lote 1, que será de 30 (trinta) dias;

6.2.1.1. O prazo de entrega dos materiais/serviços poderá ser prorrogado por igual prazo mediante justificativa devidamente apresentada com antecedência e aceita pela Contratante.

6.2.1.2. A Contratada receberá por e-mail o empenho e contrato/AF, a qual começará a contar o prazo para entrega dos materiais/serviços.

6.2.2. O valor mínimo para solicitação de AF, caso seja adotado o Sistema de Registro de Preços, será de R\$ 1.000,00 (Um mil reais).

6.2.3. Os Contratos/AFs podem ter a entrega parcelada, conforme a necessidade do Centro, mediante solicitação formal do Responsável de cada Centro.

6.2.4. Os produtos deverão ser novos (primeiro uso) e entregues acondicionados em suas embalagens originais lacradas, de forma a permitir completa segurança quanto a sua originalidade e integridade, devendo estar acondicionados e embalados conforme praxe do fabricante, protegendo o produto durante o transporte e armazenamento, com indicação do material contido, volume, data de fabricação, fabricante, importador (se for o caso), procedência, bem como demais informações exigidas na legislação em vigor, exceto para os itens a serem entregues à granel (areia, brita, entre outros).

6.2.5. O prazo de validade será “conforme a especificação dos itens do Anexo II”, para os itens que não constam a data validade na descrição, considerar validade de, no mínimo, 12 meses, salvo itens em que a validade definida pelo fabricante é menor que 12 meses.

6.2.6. A Contratante não aceitará, sob nenhum pretexto, a transferência de responsabilidade da Contratada para terceiros.

6.2.7. A Contratante reserva-se o direito de a qualquer tempo, previamente ao aceite, ou durante o prazo de validade do produto, proceder a análise técnica e de qualidade do mesmo, através de Parecer Técnico, realizado diretamente ou por intermédio de terceiros.

6.2.7.1. Caso o Parecer Técnico rejeite o produto analisado este deverá ser substituído imediatamente pela Contratada, sem qualquer ônus para a Contratante.

6.2.8. A Contratada, mesmo não sendo a fabricante da matéria prima empregada na fabricação dos produtos ofertados, responderá inteira e solidariamente pela qualidade e autenticidade destes, obrigando-se a substituir, as suas expensas, no todo ou em parte, o(s) produto(s) em que se verificar(em) vícios, defeitos, incorreções, resultantes da fabricação ou transporte, constatado visualmente ou em laboratório, respondendo por todos os custos.

6.2.9. O aceite dos produtos pela Contratante, não exclui a responsabilidade civil da Contratada por vícios de quantidade ou qualidade do produto ou disparidade com as especificações técnicas exigidas no edital ou atribuídas pela Contratada, verificados posteriormente, garantindo-se à Contratante as faculdades previstas no Art. 18 da Lei Federal 8.078/90 (Código de Defesa do Consumidor).

6.3. Bens perecíveis

(☒) Não

(☐) Sim

6.4. Garantia de execução do contrato

Será exigida garantia de execução do contrato, nos moldes do Arts 96 a 102 da Lei nº 14.133/21, em valor correspondente a 5% do valor total do contrato?

(☒) Não

(☐) Sim

6.5. Garantia do produto/serviço, manutenção e assistência técnica

() Não

(X) Sim

Se sim, observar as condições:

6.5.1. O prazo de garantia do(s) produto(s) cotado(s), será do tipo on-site (no local), de 12 meses para todos os itens do edital;

6.5.2. O prazo será contado a partir da data de aceite dos itens.

6.5.3. A garantia do produto inclui todo hardware, software, licenças ou qualquer outra funcionalidade necessária ao uso do mesmo;

6.5.4. A garantia será "on-site" (no local), ou seja, a ser prestada nos locais constantes nas condições de fornecimento, através de assistência técnica autorizada do fabricante (para não prejudicar a responsabilidade da garantia também do fabricante, nos termos do Código de Defesa do Consumidor), com tempo de solução em até 3 (três) dias úteis contados a partir do comunicado efetuado no horário de expediente. O descumprimento do prazo estipulado implica na substituição do equipamento, bem como demais penalidades;

6.5.5. As informações sobre andamento dos serviços, abertura e situação dos chamados, durante o período de garantia, deverão ser disponibilizadas por sistema on-line, e/ou telefone, e por e-mail com o respectivo número de protocolo, sem custos adicionais para a UDESC;

6.5.5.1. O sistema que se refere o item anterior, bem como o contato via e-mail, sistema ou telefone, deverá ser em português e fornecer, no mínimo, número do protocolo, data/hora do chamado e situação atual, descrevendo o serviço executado (ou a ser executado) e as peças eventualmente utilizadas na execução do serviço, contendo marca, modelo e número de série (se houver);

6.5.6. A cada atendimento presencial, a CONTRATADA apresentará um relatório de visita contendo número do protocolo, data e hora do chamado, data e hora do início e término do atendimento, identificação do defeito, identificação do técnico responsável pela execução do serviço, providências adotadas e outras informações pertinentes. O relatório será assinado pelo responsável técnico da UDESC, para comprovação dos serviços realizados;

6.5.7. Para a correção dos problemas graves (com impossibilidade de uso do equipamento), a CONTRATADA poderá fornecer um equipamento substituto temporariamente, com configuração igual ou superior ao fornecido, levando o equipamento defeituoso para reparo;

6.5.8. Sendo impossível o reparo do equipamento ou componente, a CONTRATADA realizará sua substituição definitiva por um equipamento novo sem uso, nas mesmas condições e prazos previstos nos itens anteriores;

6.5.9. Toda e qualquer substituição de qualquer equipamento e/ou de seus periféricos, por defeito ou deficiência, que se verifique durante o período de garantia, será on-site nos locais onde foram fornecidos os equipamentos.

6.5.10. Os serviços de assistência técnica dos equipamentos (para todos os itens) poderão ser prestados pelo próprio fabricante, fornecedor, ou por meio de empresa de assistência técnica/manutenção, oficialmente credenciada.

6.5.11. Em caso de manutenção, a contratada deverá fornecer todos os recursos necessários à perfeita execução dos serviços, em quantidade, qualidade e tecnologia adequada aos padrões recomendados pelos fabricantes ou padrões determinados no edital.

6.5.12. Na hipótese de não existirem peças de reposição no mercado, é de inteira responsabilidade da CONTRATADA a reposição com especificações equivalentes ou superiores.

6.5.13. Para efeitos de garantia, será suficiente à UDESC a apresentação de cópia da Nota Fiscal de compra.

6.5.14. A incidência de problemas em mais de 20% (vinte) dos itens durante o primeiro ano do período de garantia pode ser considerada baixa qualidade dos itens, e será solicitado a substituição do lote todo; um problema só pode ser considerado mau uso se tiver baixa incidência, senão será considerado baixa qualidade do dispositivo e deverá ser atendido em garantia. No caso de desrespeito dos prazos e qualidade, a empresa responsável, poderá ser penalizada.

6.5.15. Durante o período de garantia o fornecedor deverá manter atualizados todos os softwares dos itens cotados neste edital.

6.5.16. Durante o período de garantia, a contratada deverá prestar suporte e sanar as dúvidas sobre os equipamentos, sendo corresponsável pelo atendimento de chamada em garantia, depois de efetivado contato

formal.

6.5.17. Para todos os itens, onde é solicitado garantia do fabricante, o proponente deverá apresentar comprovação através de documento oficial do fabricante.

7. OBRIGAÇÕES ESPECÍFICAS DAS PARTES

7.1 Da contratada

Obriga-se a empresa vencedora:

- a) Na emissão das Notas Fiscais e DANFES só poderão ser agrupados na mesma nota os itens que possuírem o mesmo detalhamento orçamentário (mesmo empenho), constante na planilha de especificações.
- b) Na emissão das Notas Fiscais e DANFES deverá ser informado o número do empenho
- c) Será de exclusiva responsabilidade da Contratada tudo quanto concorrerem à perfeita execução do Contrato tais como: frete e entrega nos locais especificados neste memorial, fornecimento de materiais e acessórios, transportes de materiais, fornecimento de mão-de-obra especializada para entrega dos materiais, recolhimento de impostos e contribuições, encargos sociais, trabalhistas, previdenciários e demais itens pertinentes, direta e indiretamente necessários à perfeita execução contratual
- d) atender a todas as solicitações de contratação efetuadas durante a vigência do Contrato ou Ata de Registro de Preços, limitada ao quantitativo de cada item;
- e) ao fornecimento do objeto, de acordo com as especificações constantes no Edital, em consonância com a proposta apresentada e com a qualidade e especificações determinadas pela legislação em vigor;
- f) responsabilizar-se pela boa execução e eficiência no fornecimento do produto objeto do edital;
- g) reparar, corrigir, remover as suas expensas, no todo ou em parte o(s) objeto(s) em que se verifiquem danos em decorrência do transporte, bem como, providenciar a imediata substituição dos mesmos;
- h) providenciar a imediata correção das deficiências apontadas pelo contratante quando da entrega do produto;
- i) apresentar, sempre que solicitado documentos que comprovem a procedência do produto fornecido, assim como amostra para análise pela Administração, sem qualquer ônus adicional;
- j) não subcontratar, ceder ou transferir, total ou parcialmente, o objeto do contrato ou da Ata de Registro de Preços;
- k) manter, durante a vigência do contrato ou do Registro de Preços, todas as condições de habilitação e qualificações exigidas na licitação;
- l) a estender aos contratos objeto da Ata, os benefícios e promoções oferecidas aos demais clientes da contratada;
- m) responsabilizar-se por quaisquer danos ou prejuízos físicos ou materiais causados à Administração ou a terceiros, pelos seus prepostos, advindos de imperícia, negligência, imprudência ou desrespeito às normas de segurança, quando da execução do fornecimento;
- n) responsabilizar-se por todas e quaisquer despesas, inclusive, despesa de natureza previdenciária, fiscal, trabalhista ou civil, bem como emolumentos, ônus ou encargos de qualquer espécie e origem, pertinentes à execução do objeto contratado;
- o) mesmo não sendo a fabricante da matéria prima empregada na fabricação de seus produtos, a empresa vencedora, responderá inteira e solidariamente pela qualidade e autenticidade destes, obrigando-se a substituir, as suas expensas, no todo ou em parte, o objeto desta licitação, em que se verificarem vícios, defeitos, incorreções, resultantes da fabricação ou transporte, constatado visualmente ou em laboratório, correndo estes custos por sua conta;
- p) manter endereço eletrônico (e-mail) válido para fins de comunicação com a contratante por todo o período de contratação; comunicando, imediatamente, o Contratante em caso de alteração;

- q) realizar cadastro no Portal Externo do SGP-e (<https://portal.sgpe.sea.sc.gov.br/portal-externo/inicio>) para que possa assinar eletronicamente com certificação digital TODOS os documentos firmados com a contratante (como realizar a assinatura digital: https://sgpe.sea.sc.gov.br/capdoc/pergunta_frequente/nova-como-realizar-a-assinatura-digital-via-portal-externo/).

7.1 Da contratante

Obriga-se a Administração/Contratante:

- a) comunicar a Contratada toda e quaisquer ocorrências relacionadas aos objetos entregues;
- b) efetuar o pagamento da Contratada de acordo com a forma de pagamento estipulada na licitação e no Contrato;
- c) promover o acompanhamento e a fiscalização do fornecimento/prestação dos serviços, sob os aspectos qualitativo e quantitativo, anotando em registro próprio as falhas e solicitando as medidas corretivas;
- d) rejeitar, no todo ou em parte, o objeto entregue pela Contratada fora das especificações do contrato;
- e) observar para que durante a vigência do Contrato sejam cumpridas as obrigações assumidas pela Contratada, bem como sejam mantidas todas as condições de habilitação e qualificação exigidas na licitação;
- f) aplicar as sanções administrativas, quando se fizerem necessárias;
- g) prestar à CONTRATADA informações e esclarecimentos que venham a ser solicitados;
- h) demais condições constantes do edital de licitação.

8. DO CONTRATO

8.1. INSTRUMENTO CONTRATUAL

- ☐ Somente por assinatura de contrato
☒ Autorização de Fornecimento + Contrato de garantia e assistência técnica
☐ Autorização de Fornecimento
☐ Outro. _____

8.2. VIGÊNCIA

☒ O prazo de vigência da contratação é de sua assinatura até o encerramento dos créditos orçamentários do ano de sua emissão.

☐ O prazo de vigência da contratação é de (12 meses ou o máximo de 5 anos) contados da sua assinatura, prorrogável por até 10 anos, na forma dos artigos 106 e 107 da Lei nº 14.133, de 2021.

☐ O fornecimento de bens/prestação dos serviços é enquadrado como continuado tendo em vista que há prejuízos se houver a não continuidade dos mesmos para as atividades da Administração, sendo a vigência plurianual mais vantajosa considerando o Estudo Técnico Preliminar.

8.3. GESTÃO E FISCALIZAÇÃO

Gestor:

Nome: Setor de Contratos da Reitoria da UDESC

E-mail: contratos@udesc.br

Fiscal:

Nome: Dorian Amorim

Cargo: Coordenador de Infraestrutura de TIC

Matrícula: 306.412-3-01

E-mail: dorian.amorim@udesc.br

9. CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

9.1 Prazos

Prazo de troca de bens rejeitados: 5 (cinco) dias corridos.

Prazo de recebimento definitivo do objeto: 30 (trinta) dias corridos.

Prazo de liquidação do documento fiscal: _____

Prazo de pagamento: em até 30 dias conforme edital.

10. DA DOTAÇÃO ORÇAMENTÁRIA

As despesas correrão a conta da dotação:

Órgão/Unidade Orçamentária	Subação	Natureza	Fonte
UDESC	3201 – 11038 – 12758 – 14842 -	449040 - 449052	1.500.100.000

11. DO VALOR ESTIMADO

O preço máximo estimado da contratação é de **R\$ 4.461.770,79 (quatro milhões, quatrocentos e sessenta e um mil, setecentos e setenta reais e setenta e nove centavos).**

12. INFORMAÇÕES ADICIONAIS

Não há.

13. INDICAÇÃO RESPONSÁVEL NO ÓRGÃO PELOS ENCAMINHAMENTOS DE EVENTUAIS IMPUGNAÇÕES E/OU ESCLARECIMENTOS

Nome: Dorian Amorim

E-mail: dorian.amorim@udesc.br

Telefone institucional: (48) 3664-8133

14. INDICAÇÃO E ASSINATURA DA EQUIPE DE PLANEJAMENTO RESPONSÁVEL PELA CONFEÇÃO DO PRESENTE TERMO

Nome: Dorian Amorim
Matrícula: 306.412-3-01
Função: Coordenador de
Infraestrutura de TIC

Assinado Digitalmente

Nome: Marcos Vinícius Linhares
Matrícula: 312.772-9-02
Função: Secretário de TIC

Assinado Digitalmente

Nome: Divonzir Anderson Navrotski
Matrícula: 377358-01-2
Função: Técnico Universitário de
Desenvolvimento

Assinado Digitalmente

15. APROVAÇÃO DO TERMO DE REFERÊNCIA

APROVO O Termo de referência e a realização de processo licitatório conforme acima especificado, por intermédio da Coordenadoria de Compras e Licitações da Reitoria.

JOSÉ FERNANDO FRAGALLI
REITOR DA FUNDAÇÃO UNIVERSIDADE DO ESTADO DE SANTA CATARINA



Assinaturas do documento



Código para verificação: **F4T2L19M**

Este documento foi assinado digitalmente pelos seguintes signatários nas datas indicadas:

- ✓ **DIVONZIR ANDERSON NAVROTSKI** (CPF: 027.XXX.339-XX) em 27/08/2025 às 19:15:45
Emitido por: "SGP-e", emitido em 30/03/2018 - 12:42:52 e válido até 30/03/2118 - 12:42:52.
(Assinatura do sistema)
- ✓ **DORIAN AMORIM** (CPF: 572.XXX.449-XX) em 27/08/2025 às 19:19:29
Emitido por: "SGP-e", emitido em 30/03/2018 - 12:42:53 e válido até 30/03/2118 - 12:42:53.
(Assinatura do sistema)
- ✓ **MARCOS VINICIUS LINHARES** (CPF: 785.XXX.171-XX) em 28/08/2025 às 17:53:09
Emitido por: "SGP-e", emitido em 30/03/2018 - 12:35:15 e válido até 30/03/2118 - 12:35:15.
(Assinatura do sistema)
- ✓ **JOSE FERNANDO FRAGALLI** (CPF: 030.XXX.838-XX) em 28/08/2025 às 18:08:12
Emitido por: "AC ONLINE RFB v5", emitido em 10/04/2024 - 12:34:06 e válido até 10/04/2027 - 12:34:06.
(Assinatura ICP-Brasil)

Para verificar a autenticidade desta cópia, acesse o link <https://portal.sgpe.sea.sc.gov.br/portal-externo/conferencia-documento/VURFU0NfMTlwMjJfMDAwMjc4NDNfMjc4NjNfMjAyNV9GNFQyTDE5TQ==> ou o site <https://portal.sgpe.sea.sc.gov.br/portal-externo> e informe o processo **UDESC 00027843/2025** e o código **F4T2L19M** ou aponte a câmera para o QR Code presente nesta página para realizar a conferência.