PROPOSTA TÉCNICA

À

DIRETORIA DE CONTRATAÇÕES E AQUISIÇÕES DO CBMDF
Endereço: Setor de Administração Municipal – SAM, Quadra "B", Bloco "D", CEP 70610-600, Brasília/DF (ao lado do DER)

LICITAÇÃO ELETRÔNICA - P.E. Nº 90045/2025 - DICOA/DEALF/CBMDF
PROCESSO Nº 00053-00033059/2025-80

DESCRIÇÃO SOLUÇÃO DE SEGURANÇA	ATENDE: S/N	DOCUMENTO	PÁG. PARAGRAFO DO ATENDIMENTO DO ITEM
• Licença subscrições de software de segurança composta por um conjunto de módulos de software integrados gerenciados por um único fabricante de forma que atende ao conjunto de requisitos técnicos exigidos.	S	capture_client-getting_started	Pág 5: Before provisioning your Capture Client subscription
• Devido ao progresso de ataques a dispositivos e regulamentações nacionais e internacionais, será fornecido módulo de detecção e resposta de endpoints, coletando, inspecionando e centralizando as informações importantes que acontecem em tempo real, para que, a qualquer momento, mesmo após a ocorrência de um incidente de segurança, a equipe técnica possa investigar a causa raiz e responder/mitigar o impacto com o máximo de informações possíveis remediando os endpoints da rede corporativa por ventura comprometidos com maior rapidez.	S	SonicWall Capture Client	SonicWall Capture Client is a unified client platform that delivers multiple Endpoint Detection & Response (EDR) capabilities, including behavior-based malware protection, advanced threat hunting and visibility into application vulnerabilities Capture Client's integration with the Capture Security Center creates a single pane of glass across network and endpoint security operations for centralized control of attack visualization, rollback and remediation, network control and remote shell troubleshooting abilities
• Permite a integração de forma nativa com gerencia centralizada da solução de segurança, para trabalhar de forma harmônica e sincronizada com os demais componentes de segurança da solução do fabricante.	S	SonicWall Capture Client E SonicWall Capture Security Center	Capture Client's integration with the Capture Security Center creates a single pane of glass across network and endpoint security operations for centralized control of attack visualization, rollback and remediation, network control and remote shell troubleshooting abilities SonicWall Capture Security Center: Single pane of glass (SPOG) cloud management is unified cybersecurity and comprehensive management. SonicWall engineers designed it with agility and scalability in mind. And if you have SonicWall firewalls and other security services, you already have Capture Security Center.

• Será entregue com o gerenciamento do sistema ofertado baseado em modelo de nuvem computacional.	S	Client Getting Sttardted Guide	Cloud-based management console reduces the footprint and overhead of management. It improves the deployability and enforceability of Endpoint Protection, irrespective of where the endpoint is.
• Será implementado mecanismo de descoberta de ameaças cibernéticas baseado em análise de inteligência artificial permitindo a coleta de dados dos endpoints e seu armazenamento centralizado em console de gerência em ambiente de nuvem (SaaS).	S	SonicWall Capture Client E Datasheet: SonicWall Capture Advanced Threat Protection Service	Capture Advanced Threat Protection (ATP) integration to automatically test suspicious files Capture ATP file verdict lookup A Inteligencia artifical (machine learning) é comprovada no datasheet do "Capture ATP": A Inteligencia artifical (machine learning) é comprovada no datasheet do "Capture ATP": Datasheet: SonicWall Capture Advanced Threat Protection Service Item: MACHINE LEARNING
• A solução ofertada não depende para sua operação de atualizações de assinaturas.	S	Capture Client Getting Started Guide	Não possuímos assinaturas (signatureless): Capture Client Getting Started Guide Procurar por "signatureless techniques"
• Todos os módulos de software do sistema ofertado atendem às especificações técnicas descritas neste documento em sua integralidade.	S	PROPOSTA PREÇOS	CONFORME DECLARAÇÃO NA PROPOSTA DE PREÇOS
• Suporte total para os seguintes sistemas operacionais ou superiores: • Windows 7 (32 e 64 bits); • Windows Server 2008 R2 (32 e 64 bits); • Mac OS X 10.10 (Yosemite); • LINUX ou Unix em alguma versão recente recomendada.	S	Capture Client - System Requirements	Windows: Capture Client Agent OS Requirements : Windows & Windows Server MacOS: Capture Client Agent OS Requirements : Mac LINUX: Capture Client Agent OS Requirements : Linux
• A console de gerência é centralizada com interface gráfica web.	S	SonicWall Capture Security Center	o painel unificado de todos os produtos SonicWall: SonicWall Capture Security Center Capture Security Center is a scalable cloud security management system that's a built-in and ready to use component of your SonicWall product or service. It features single-sign-on and 'single-pane-of-glass' management. It integrates the functionality of the Capture Cloud Platform to deliver robust security management, analytics, and real-time threat intelligence for your entire portfolio of network, email, endpoint, mobile, and cloud security resources Link do Capture Security Center (Interface Gráfica): http://cloud.sonicwall.com

• A solução permite a instalação inicial de agentes de segurança nos endpoints pelos administradores de forma silenciosa.	S	Capture Client Installation via Command Line Interface or PowerShell	Procurar por: the client can be downloaded and packaged with specific command-line parameters for silent installation on the clients
• A gerência centralizada permite a distribuição de atualizações nos módulos de Next Generation antivirus em execução nos agentes de segurança.	S	SonicWall Capture Security Center	Feito através do Cloud Security Center, o console centralizador da Sonicwall: https://www.sonicwall.com/capture-security-center Procurar por: Unify and synchronize updates and support, monitor security risks, fulfill regulatory compliance – do everything with greater clarity, precision and speed
• Provê a detecção e prevenção de ameaças em real- time;	S	Capture Client Getting Started Guide	Sim, possui um "monitoramento continuo comportamental", ou seja, "em tempo real": Capture Client Getting Started Guide Pág 3: Continuous behavioral monitoring
• O funcionamento da solução opera analisando a pré-execuçao e pós-execução da ameaça em potencial, em nível de sistema operacional (O/S), memória e prevenindo a entrada de códigos maliciosos.	S	SonicWall Capture Client	Pré-execução: Stop Attacks Before Execution Pós execução: Remediate & Rollback Memória: Memory em nível de sistema operacional: Atendido através do Capture ATP, que é "Full System emulation":Datasheet: SonicWall Capture Advanced Threat Protection Service Procurar por: full system emulation technology
• Capacidade de análise automática do código do arquivo, identificando suas características antes da sua capacidade de execução.	S	Capture Client Datasheet	ability to manipulate and test files in ways that endpoints can't. Discovering, quarantining, and removing undercover threats before they execute saves time for end users and administrators
• A solução aplica analise baseada em código algoritmo, para identificar programas maliciosos antes da sua execução.	S	Capture Client Getting Started Guide	Pág 3: Continuous behavioral monitoring of the client that helps create a complete profile of file activity, application & process activity, and network activity. This protects against both file-based and fileless malware and delivers a 360º attack view with actionable intelligence relevant for investigations Análise baseada em código de algoritmo feita pelo "Capture ATP": Datasheet: SonicWall Capture Advanced Threat Protection Service Pág 2: executes suspicious code and analyzes behavior

• Caso seja encontrado um programa malicioso a sua execução não é permitida.	S	SonicWall Capture Client	Com a proteção pré execução: SonicWall Capture Client **S**top Attacks Before Execution Protects against ransomware, known and unknown malware, memory exploits, and more
• A solução identifica e bloqueia a execução de códigos executáveis, scripts ou comandos.	S	Datasheet: SonicWall Capture Advanced Threat Protection Service	Pág 2: BROAD FILE TYPE ANALYSIS: range of file types and sizes, including executables (PE), DLLs, PDFs, MS Office documents, archives, JARs, and APKs Scripts: Analyze threats detected by Capture Client using the Attack Storyline If a threat is detected by the behavioral engine, an Attack Storyline is generated (e.g. Fileless malware, Scripts, Lateral Movement etc) Comandos: Capture Client Protecting Assets with Security Policies PowerShell or CMD
• A solução de endpoint previne e detecta qualquer alteração oriunda de código malicioso em programas que sejam executados em memória.	S	Real-Time Deep Memory Inspection	Pág 1: Procurar por: Real-Time Deep Memory Inspection
• Utiliza a tecnologia de “Machine Learning” para identificar qualquer ameaça nos arquivos potencialmente perigosos.	S	Datasheet: SonicWall Capture Advanced Threat Protection Service	Procurar por: "MACHINE LEARNING " (Pág 1)
• Caso necessário a solução tem a capacidade de encaminhar arquivos identificados como ameaças para uma solução de “Sandbox On-premises ou On-Cloud”, com o objetivo de fazer uma segunda analise em diferentes sistemas operacionais.	S	Datasheet: SonicWall Capture Advanced Threat Protection Service	On-Cloud Através do Capture ATP: Datasheet: SonicWall Capture Advanced Threat Protection Service Procurar por: Files are sent to the SonicWall Capture ATP Cloud for analysis. The multi-engine sandbox platform, Em diferentes distemas operacionais: https://www.sonicwall.com/resources/datasheet/datasheet-sonicwall-capture-advanced-threat-protection-service Procurar por: full system emulation technology

• Identifica ameaças avançadas, chamadas de “Zero- day”, sem a necessidade de base de assinaturas (DATs) e suas atualizações, detecção por heurística, detecção por comportamento ou sandboxing.	S	Capture ATP Datasheet	A solução é 'signatureless", e não depende de assinaturas (DAT): https://www.sonicwall.com/resources/datasheet/sonicwall-capture-client Procurar por: requires no signatures Outro documento: https://www.sonicwall.com/support/technical-documentation/docs/capture_client-getting_started/Content/Overview/description.htm Procurar por: Multiple layered signatureless techniques Heurística: "Machine Learning": Datasheet: SonicWall Capture Advanced Threat Protection Service Comportamento: dynamic behavioral protection : Capture Client Getting Started Guide Sandboxing: Capture Advanced Threat Protection (ATP) Sandboxing SonicWall Capture Client
• Tem capacidade para expandir funcionalidades habilitando a função de Busca de ameaças avançadas usando mecanismos e filtros de busca por processos ou serviços ou outras características coerentes para buscas de ameaças.	S	Capture Client Datasheet	A busca de ameaças é feita pelo "Threat Hunting: SonicWall Capture Client Pág 1, Procurar por: threat hunting with deep visibility
• Tem passado satisfatoriamente, sob documentação a ser avaliada, nos testes de ameaças mais recentes do MITRE@ATTACK.	S	What the 2023 MITRE ATT&CK Evaluation Results Mean for SonicWall Users	https://www.sonicwall.com/blog/what-the-2023-mitre-attck-evaluation-results-mean-for-sonicwall-users
• Permite controlar dispositivos de conectados via USB, permitindo bloquear ou liberar acesso e adicionalmente criação de exceções na política, pelo número de série, identificador do fabricante e tipo de dispositivo.	S	How Do I Configure Capture Client Device Control Policy	Feito atraves do Device Control : How Do I Configure Capture Client Device Control Policy
• Tem a capacidade de detectar e controlar os seguintes dispositivos USB: • Dispositivos de armazenamento externo; • Dispositivos de áudio e vídeo; • Impressoras; • Dispositivos de leitura de Smart-Cards; • Interfaces Wireless; • Dispositivos conectados nos HUBs USB.	S	How Do I Configure Capture Client Device Control Policy	Feito atraves do Device Control : How Do I Configure Capture Client Device Control Policy
• Para prover maior visibilidade e controle dos acessos dos usuários do ambiente, está incluso um módulo de filtro de URL integrado no cliente instalados nas estações de trabalho;	S	Capture Client Datasheet	Sim, com o "Filtro de conteúdo" integrado: SonicWall Capture Client Pág 2, procurar por: Web Content Filtering

• Possui base contendo, no mínimo, 20 milhões de sites internet web já registrados e classificados com atualização automática;	S	Content Filtering Service (CFS) 4.0 Overview	Nossa base de CFS (Content Filter Service) é a mesma para todas as soluções SonciWall, seja ele um Firewall, SWG ou EPP. Content Filtering Service (CFS) 4.0 Overview Buscar por: There are about ~42M URLs in CFS 4.0 database and the data is increasing day by day
• Atua como filtro de conteúdo transparente de forma a dispensar a configuração dos browsers das máquinas clientes.	S	How to configure Web Content Filtering on Capture Client 3.6	Sim, atua de forma transparente, diretamente pelo agente do Capture Client instalado no dispositivo: https://www.sonicwall.com/support/knowledge-base/how-to-configure-web-content-filtering-on-capture-client-3-6/220427203917200 Pesquisar por: have the ability to perform content filtering through the Capture Client Web Content Filter
• A plataforma possui as seguintes funcionalidades de filtro de URL: • Permite a criação de listas personalizadas de URLs permitidas e bloqueadas (lista branca e lista negra); • Permite proeger os acessos a sites categorizados maliciosos e possui no mínimo 50 categorias de URLs; • Suporta a exclusão ou inclusão de URLs do bloqueio, por categoria; • Possibilita a categorização ou recategorização de URL caso não esteja categorizada ou categorizada incorretamente, utilizando-se ferramenta do próprio fabricante; • A solução permite um mecanismo que permita criar whitelist ou blacklist de URLs; • A solução não depende de base de assinaturas para a identificação de qualquer ameaças. • A solução sempre mantem o monitoramento continuo e ativo no endpoint para remover a necessidade de escaneamentos periódicos.	S	How to configure Web Content Filtering on Capture Client 3.6	Pesquisar por: you have the option to individually allow or block websites. Using the Allowed and Forbidden Web Domains Possuímos 93 categorias catalogadas: Content Filtering Rating Categories CFS5.0 exclusão ou inclusão de URLs :https://www.sonicwall.com/support/knowledge-base/how-to-configure-web-content-filtering-on-capture-client-3-6/220427203917200 Pesquisar por: Using the Allowed and Forbidden Web Domains. You can either block using domain names or IP addresses of the websites you wish to allow or block. You also have the option to block using URL keywords. Atraves do serviço de recategorizacão de filtro de conteúdo da SonicWall: https://cfssupport.sonicwall.com/Support/web/eng/newui/viewRating.jsp Whitelist e Blacklist atraves do Allowed' e do 'forbidden' web domains: https://www.sonicwall.com/support/knowledge-base/how-to-configure-web-content-filtering-on-capture-client-3-6/220427203917200 Pesquisar por: Using the Allowed and Forbidden Web Domains. You can either block using domain names or IP addresses of the websites you wish to allow or block. You also have the option to block using URL keywords. A solução é 'signatureless", e não depende de assinaturas: https://www.sonicwall.com/resources/datasheet/sonicwall-capture-client Procurar por: requires no signatures Sim, possui um "monitoramento continuo comportamental", ou seja, "em tempo real": Capture Client Getting Started Guide Pág 3: Continuous behavioral monitoring

• Provê proteção em real-time, independente do estado de conexão da máquina, sendo: • Online, com conexão com a internet; • Offline, sem conexão com a internet;	S	Capture Client Getting Started Guide	Procurar po: Continuous behavioral monitoring Pág 3, não necessita de estar online para atualizar. Toda análise é comportamental: Multiple layered signatureless techniques include techniques for protecting cloud intelligence, advanced static analysis and dynamic behavioral protection. They help protect against and remediate well known, little known, and even unknown malware, without regular scans or periodic updates. This maintains the highest level of protection at all times, without hampering user productivity
• O módulo de controle e analise de scripts é capaz de analisar no mínimo scripts em powershell, macros ou VBA.	S	Capture Client Protecting Assets with Security Policies Administration Guide	Sim, nosso mecanismo de análise não se limita ao tipo de script: https://www.sonicwall.com/techdocs/pdf/capture_client-protecting_assets.pdf Buscar por: "PowerShell " https://www.sonicwall.com/blog/sonicwall-rtdmi-engine-identifies-malicious-vba-macro-laced-ms-office-document-in-real-time-may-22-2018-2-2 Procurar por "VBA" ou "macro"
• O módulo de controle e analise de scripts possui as seguintes ações em caso se violação: • Alertar; • Bloquear; • Deixar o dispositivo em isolado da rede, podendo optar por deixar o dispositivo isolado ocorra uma violação.	S	Capture Client Premier Administration Guide	1: Alertar: Sim, é possivel alertar em caso de violação. 2: Bloquear: Sim, na política é possivel bloquear e já configurar a ação, como "quarentenar", por exemplo 3: Isolar o dispositivo: Sim, é possivel isolar o dispositivo com o "Network Control" Procurar por: 1 - To enable notifications for Network 2 - Configurable Network Quarantine 3 - You can set the automatic Disconnect from Network option in the Policy Settings

Garantia:

Garantia de 36 (trinta e seis) meses, fornecida pelo FABRICANTE, com suporte técnico de segunda-feira à sexta-feira, exceto feriados, das 8hs às 18hs.

O prazo máximo para atendimento e reparo/solução do problema que ocasionou o chamado, contado a partir da abertura do mesmo, será de até 2 (dois) dias úteis, inclusive quando o mesmo implicar troca de peças ou componentes;

O FABRICANTE possui Central de Atendimento para abertura dos chamados de garantia, comprometendo-se a manter registros dos mesmos constando a descrição do problema;

O FABRICANTE oferece canais de comunicação e ferramentas adicionais de suporte online como "chat", "e-mail" e página de suporte técnico na Internet com disponibilidade de atualizações e "hotfixes" de drivers, do próprio software como todo ou partes e ferramentas de troubleshooting;

- Possuir recurso disponibilizado via web, site do próprio FABRICANTE, que permita verificar a garantia do software através da inserção do seu número de série.

- Devido à necessidade de atendimento de suporte à CONTRATANTE, será enviado juntamente com a proposta uma declaração do FABRICANTE do software informando que estamos aptos a comercializar e dar suporte na solução.

- Na decalração irá constar os P/N do software bem como a garantia ofertada.

São Paulo, 10 de outubro de 2025.

Luis Rogério Oliveira Vieira de Moraes
ESYWORLD SISTEMAS E INFORMÁTICA LDA
CNPJ: 03.899.222/0001-86
Diretor
RG nº: 23585645 SSP/SP
CPF/MF: 165.770.378-92

PROPOSTA DE PREÇOS

À
DIRETORIA DE CONTRATAÇÕES E AQUISIÇÕES DO CBMDF
Endereço: Setor de Administração Municipal – SAM, Quadra "B", Bloco "D", CEP 70610-600, Brasília/DF (ao lado do DER)

LICITAÇÃO ELETRÔNICA - P.E. Nº 90045/2025 - DICOA/DEALF/CBMDF
PROCESSO Nº 00053-00033059/2025-80

Apresentamos **PROPOSTA DE PREÇOS** acordo com as especificações, condições e prazos estabelecidos no **Pregão Eletrônico nº 90045/2025** - DICOA/DEALF/CBMDF, dos quais nos comprometemos a cumprir integralmente.

DADOS DA EMPRESA:

RAZÃO SOCIAL	ESYWORLD SISTEMAS E INFORMATICA LTDA
CNPJ	03.899.222/0001-86
I.E	146.341.168.111
ENDEREÇO	Alameda Araguaia No. 2044, Bloco 1, Sala 1014
BAIRRO	Alphaville
CEP	06.455-000
CIDADE/UF	Barueri - SP
TELEFONES	+55 51 5677-1751
E-MAIL	governo@esy.com.br

DADOS DO REPRESENTANTE LEGAL:

REPRESENTANTE LEGAL	Luis Rogério Moraes
E-MAIL	governo@esy.com. br
CI	23585645 SSP/SP
CPF	165.770.378-92
TELEFONE	+55 51 5677-1751
ENDEREÇO	Av. Jandira 226, Ap 112B
BAIRRO	Moema
CEP	04080-000
CIDADE/UF	São Paulo

BANCO	Banco do Brasil
CÓD. AGÊNCIA	1195-9
NOME DA AGÊNCIA	Bom Retiro
Nº DA CONTA	6830-6

Declaramos que concordamos com todas as condições estabelecidas no Edital e seus respectivos Anexos.

Nossa cotação para entrega do(s) material(is) e/ou equipamentos está especificada, conforme abaixo:

Item	Qtd	Un	Especificação	Marca / Modelo	Valor Unitário (R$)	Valor Total (R$)
11	2250	UN	**SOLUÇÃO DE SEGURANÇA** 1. Licença perpétua ou subscrições de software de segurança composta por um conjunto de módulos de software integrados gerenciados por um único fabricante de forma a atender ao conjunto de requisitos técnicos exigidos nessa especificação. 2. Devido ao progresso de ataques a dispositivos e regulamentações nacionais e internacionais, far-se-á necessário o fornecimento de módulo de detecção e resposta de endpoints, coletando, inspecionando e centralizando as informações importantes que acontecem em tempo real, para que, a qualquer momento, mesmo após a ocorrência de um incidente de segurança, a equipe técnica do contratante possa investigar a causa raiz e responder/mitigar o impacto com o máximo de informações possíveis remediando os endpoints da rede corporativa por ventura comprometidos com maior rapidez. 3. Deve permitir a integração de forma nativa com gerência centralizada da solução de segurança, para trabalhar de forma harmônica e sincronizada com os demais componentes de segurança da solução do fabricante. 4. Deve ser entregue com o gerenciamento do sistema ofertado	SONICWALL CAPTURE CLIENT	R$ 1.100,00	R$ 2.475.000,00

			baseado em modelo de nuvem computacional. 5. Deverá implementar mecanismo de descoberta de ameaças cibernéticas baseado em análise de inteligência artificial permitindo a coleta de dados dos endpoints e seu armazenamento centralizado em console de gerência em ambiente de nuvem (SaaS). 6. Não serão aceitas soluções que dependam para sua operação de atualizações de assinaturas. 7. Todos os módulos de software do sistema ofertado deverão atender às especificações técnicas descritas neste documento em sua integralidade. 8. Suporte total para os seguintes sistemas operacionais ou superiores: 1. Windows 7 (32 e 64 bits); 2. Windows Server 2008 R2 (32 e 64 bits); 3. Mac OS X 10.10 (Yosemite); 4. LINUX ou Unix em alguma versão recente recomendada. 9. A console de gerência deverá ser centralizada cominterface gráfica web. 10. A solução deverá prover permitir a instalação inicial de agentes de segurança nos endpoints pelos administradores de forma silenciosa. 11. A gerência centralizada deverá permitir a distribuição de atualizações nos módulos de Next Generation antivírus em execução nos agentes de segurança. 12. Deve prover detecção e prevenção de ameaças em realtime; 13. O funcionamento da solução deve operar analisando a pré-execuçao e pós-execução da ameaça em potencial, em nível de sistema operacional (O/S), memória e prevenindo a entrada de códigos maliciosos. 14. Capacidade de análise automática do código do arquivo, identificando suas características antes da sua capacidade de execução.			

			15. A solução deve aplicar analise baseada em código algoritmo, para identificar programas maliciosos antes da sua execução. 16. Caso seja encontrado um programa malicioso a sua execução não deve ser permitida. 17. A solução deve identificar e bloquear a execução de códigos executáveis, scripts ou comandos. 18. A solução de endpoint deve prevenir e detectar qualquer alteração oriunda de código malicioso em programas que sejam executados em memória. 19. Deve utilizar a tecnologia de “Machine Learning” para identificar qualquer ameaça nos arquivos potencialmente perigosos. 20. Caso necessário a solução deve ter a capacidade de encaminhar arquivos identificados como ameaças para uma solução de “Sandbox On-premises ou On-Cloud”, com o objetivo de fazer uma segunda analise em diferentes sistemas operacionais. 21. Identificar ameaças avançadas, chamadas de “Zero-day”, sem a necessidade de base de assinaturas (DATs) e suas atualizações, detecção por heurística, detecção por comportamento ou sandboxing. 22. Deve ter capacidade para expandir funcionalidades habilitando a função de Busca de ameaças avançadas usando mecanismos e filtros de busca por processos ou serviços ou outras características coerentes para buscas de ameaças. 23. Deve ter passado satisfatoriamente, sob documentação a ser avaliada , nos testes de ameaças mais recentes do MITRE@ATTACK. 24. Deve permitir controlar dispositivos de conectados via USB, permitindo bloquear ou liberar acesso e adicionalmente criação de exceções na política, pelo número de série, identificador do fabricante e tipo de dispositivo.			

			25. Deve ter a capacidade de detectar e controlar no mínimo os seguintes dispositivos USB: 1. Dispositivos de armazenamento externo; 2. Dispositivos de áudio e vídeo; 3. Impressoras; 4. Dispositivos de leitura de Smart-Cards; 5. Interfaces Wireless; 6. HUBs USB. 26. Para prover maior visibilidade e controle dos acessos dos usuários do ambiente, deve ser incluído um módulo de filtro de URL integrado no cliente instalados nas estações de trabalho; 27. Possuir base contendo, no mínimo, 20 milhões de sites internet web já registrados e classificados com atualização automática; 28. Deve atuar como filtro de conteúdo transparente de forma a dispensar a configuração dos browsers das máquinas clientes. 29. A plataforma deve possuir as seguintes funcionalidades de filtro de URL: 1. Permitir a criação de listas personalizadas de URLs permitidas e bloqueadas (lista branca e lista negra); 2. Permitir proteger os acessos a sites categorizados maliciosos e possuir no mínimo 50 categorias de URLs; 3. Suporta a exclusão ou inclusão de URLs do bloqueio, por categoria; 4. Deverá possibilitar a categorização ou recategorização de URL caso não esteja categorizada ou categorizada incorretamente, utilizando-se ferramenta do próprio fabricante; 5. A solução deverá permitir um mecanismo que permita criar whitelist ou blacklist de URLs; 6. A solução não deve depender de base de assinaturas para a identificação de qualquer ameaças.			

			7. A solução deve sempre manter o monitoramento continuo e ativo no endpoint para remover a necessidade de escaneamentos periódicos. 30. Deve prover proteção em real-time, independente do estado de conexão da máquina, sendo: 1. Online, com conexão com a internet; 2. Offline, sem conexão com a internet; 31. O módulo de controle e analise de scripts deve ser capaz de analisar no mínimo scripts em powershell, macros ou VBA. 32. O módulo de controle e analise de scripts deve possuir as seguintes ações em caso se violação: 1. Alertar; 2. Bloquear; 3. Deixar o dispositivo em isolado da rede, podendo optar por deixar o dispositivo isolado ocorra uma violação. 33. **Garantia** 1. Garantia mínima de 36 (trinta e seis) meses, fornecida pelo FABRICANTE, com suporte técnico de segunda-feira à sexta-feira, exceto feriados, das 8hs às 18hs. A LICITANTE deverá informar na proposta o período da garantia. No momento da análise da proposta será verificado disponibilidade de oferta da garantia e no momento da entrega da solução também será verificado o prazo; 2. O prazo máximo para atendimento e reparo/solução do problema que ocasionou o chamado, contado a partir da abertura do mesmo, será de até 2 (dois) dias úteis, inclusive quando o mesmo implicar troca de peças ou componentes; 3. O FABRICANTE deverá possuir Central de Atendimento para abertura dos chamados de garantia, comprometendo-se a manter registros dos mesmos constando a descrição do problema; 4. O FABRICANTE também deverá oferecer canais de comunicação e ferramentas adicionais de suporte online como "chat", "e-mail" e página de suporte técnico na Internet com isponibilidade de atualizações e			

			"hotfixes" de drivers, do próprio software como todo ou partes e ferramentas de troubleshooting; 5. Possuir recurso disponibilizado via web, site do próprio FABRICANTE, que permita verificar a garantia do software através da inserção do seu número de série. 6. Devido à necessidade de atendimento de suporte à CONTRATANTE, caso a LICITANTE não seja o mesmo FABRICANTE da solução, este deverá enviar juntamente com a sua proposta uma declaração do FABRICANTE do software informando que a licitante esta apta a comercializar e dar suporte na solução. Deverá constar na declaração do fabricante os P/N do software bem como a garantia ofertada.			

Declaramos que esta proposta tem validade de 90 (noventa) dias corridos, contados da data de apresentação.

O prazo para entrega dos materiais e/ou equipamentos será de até 60 (sessenta) dias CORRIDOS, contados a partir da retirada/recebimento da respectiva Nota de Empenho ou da assinatura do Contrato.

Declaro que entregarei o(s) equipamento(s) e/ou peça(s)] comprovadamente novo(s) e sem uso, uma vez que não será(ão) aceito(s) material(is)/equipamento(s) ou peça(s) recondicionado(s), reutilizado(s) ou reformado(s).

Declaramos ainda, que nos preços estão inclusos todos os tributos, fretes, tarifas e demais despesas decorrentes da execução do objeto.

DECLARAMOS QUE ATENDEMOS OS CRITÉRIOS DE SUSTENTABILIDADE AMBIENTAL

previstos no art. 7º da Lei distrital nº 4.770/2012, em especial que produz/comercializa bens:

a) constituídos por material reciclado, atóxico e biodegradável, na forma das normas da Associação Brasileira de Normas Técnicas – ABNT;

b) que ofereçam menor impacto ambiental em relação aos seus similares;

c) que não contém substâncias perigosas acima dos padrões tecnicamente recomendados por organismos nacionais ou internacionais;

d) acondicionados em embalagem adequada, feita com a utilização de material reciclável, com o menor volume possível;

e) que funcionem com baixo consumo de energia ou de água;

f) que sejam potencialmente menos agressivos ao meio ambiente ou que, em sua produção, signifiquem economia no consumo de recursos naturais;

g) que possuam certificado emitido pelos órgãos ambientais;

h) que possuam certificação de procedência de produtos.

São Paulo, 10 de outubro de 2025.

Luis Rogério Oliveira Vieira de Moraes
ESYWORLD SISTEMAS E INFORMÁTICA LDA
CNPJ: 03.899.222/0001-86
Diretor
RG nº: 23585645 SSP/SP
CPF/MF: 165.770.378-92