GOVERNO DO ESTADO DO PIAUÍ
SECRETARIA DA ADMINISTRAÇÃO DO ESTADO DO PIAUÍ

ASSUNTO: Procedimento público de Intenção de Registro de Preços para subsidiar futura(s) contratação(ões) de empresa(s) para aquisição de solução unificada de segurança para proteção de e-mail, proteção de endpoint e proteção contra ataques avançados, com garantia de 36 meses, contemplando os serviços de desinstalação e configuração, transferência de conhecimento e suporte técnico.

Senhores,

Trata-se o presente de divulgação de procedimento de intenção de registro de preços promovida pela Secretaria de Estado da Administração do Piauí (SEAD), para possibilitar a participação dos Órgãos e Entes que compõem a Administração Pública do Estado do Piauí no **Registro de Preços** que tem por objeto a contratação de solução unificada de segurança para proteção de e-mail, proteção de endpoint e proteção contra ataques avançados, com garantia de 36 meses, contemplando os serviços de desinstalação e configuração, transferência de conhecimento e suporte técnico, na modalidade Pregão Eletrônico, para atender demanda da Secretaria de Estado da Administração do Piauí – SEAD-PI e demais órgãos e entidades da Administração Pública Estadual.

Considerando que a Secretaria de Estado da Administração do Piauí - SEAD é órgão central da administração do Governo do Estado do Piauí e possui competência para realizar procedimento público de intenção de registro de preços – IRP, estabelecendo, quando for o caso, o número máximo de participantes, em conformidade com sua capacidade de gerenciamento, conforme previsto no art. 17, Lei n 7.884, de 08 de dezembro de 2022 (7884.pdf (al.pi.leg.br)).

Cumpre ressaltar que a Intenção de Registro de Preços (IRP) é a ferramenta que permite que Administração Pública compartilhe as suas intenções de realizar licitações para Registro de Preço - SRP, possibilitando a participação de outros órgãos ou entidades que tenham interesse em adquirir o mesmo objeto. Entre os principais benefícios das participações às IRPs, **estão a economia de escala e processual, além de favorecer a redistribuição de agentes públicos para tarefas finalísticas.**

Assim, a presente IRP, visa realizar o estudo para levantamento do quantitativo, a fim de determinar a estimativa total das quantidades de forma clara e precisa para atendimento de toda a necessidade administrativa e tem como alinhamento estratégico o **Documento de Formalização de Demanda nº 41/2023/SEAD**, composto por **1 LOTE contendo 13 (TREZE) ITENS, com descrição resumida dos serviços constante no ANEXO deste ofício**, o qual deve ser avaliado e preenchido pelo setor competente de cada órgão e entidade, conforme a seguir:

a) **Estimativa total de quantidades da contratação**, **com base nas necessidades de contratações dos últimos e para os próximos 12 (doze) meses, com a devida justificativa administrativa do quantitativo indicado, bem como a sua necessidade, demonstrada a sua previsão no Plano Anual de Contratações, se houver**;

O órgão consultado deve demonstrar quais itens e quantitativos precisará para compor a futura Ata de Registro de Preços, como as estimativas das quantidades, acompanhadas das memórias de cálculo e dos documentos que lhes dão suporte, que considerem interdependências com outras contratações, de modo a possibilitar economia de escala.

Por fim, solicita-se que esta Intenção de Registro de Preços – IRP seja respondida pelos órgãos e entidades da administração pública estadual **impreterivelmente ATÉ O DIA 06/12/2023 (8 DIAS ÚTEIS),** com a **urgência** que o caso requer, seguindo os critérios elencados ao longo do ofício e anexo.

Ressalta-se, ainda, que **demandas enviadas após esse prazo** para a SEAD **NÃO serão computadas** no presente procedimento de Registro de Preços.

Certo de nobre colaboração, desde já agradecemos.

ANEXO

(DOCUMENTO DE FORMALIZAÇÃO DE DEMANDA Nº 41/2023/SEAD)

IDENTIFICAÇÃO DO ÓRGÃO GERENCIADOR DA SOLUÇÃO

Órgão Gerenciador:	Secretaria de Estado da Administração do Piauí - SEAD-PI
Unidade:	Diretoria de Planejamento de Licitações/ Superintendência de Licitações e Contratos - SEAD-PI
Nome do Projeto:	**Registro de Preços para subsidiar futura(s) contratação(ões) de empresa(s) especializada(s) na prestação de serviços de solução unificada de segurança para proteção de e-mail, proteção de endpoint e proteção contra ataques avançados, com garantia de 36 meses, contemplando os serviços de desinstalação e configuração, transferência de conhecimento e suporte técnico.**
Responsável pela Demanda:	Diretoria de Planejamento de Licitações da Secretaria de Estado da Administração do Piauí.
E-mail:	diretoriaplanejamentosead@gmail.com

INDICAÇÃO DO REQUISITANTE/PARTICIPANTE DA SOLUÇÃO:

Requisitante:	
Responsável pela Demanda:	
E-mail:	
Telefone:	

1. **ALINHAMENTO ESTRATÉGICO**

1.1. O Alinhamento Estratégico do **Documento de Formalização de Demanda nº 41/2023/SEAD** é composto por **1 LOTE contendo 13 (TREZE) ITENS, conforme tabela abaixo:**

1.2. Solicita-se aos órgãos da Administração Estadual do Estado do Piauí que se manifestem quanto ao interesse de aquisição das soluções de segurança (quadro I) apresentadas a seguir:

ITEM	DESCRIÇÃO DO OBJETO	UNIDADE DE MEDIDA	QUANTIDADE
1	Solução de proteção de Endpoints com abordagem proativa para resposta eficaz a incidentes	Por Endpoint	
	Solução de proteção de Servidores com abordagem proativa para resposta eficaz a incidentes	Por Servidor	
3	Solução de segurança avançada para mitigação de ameaças na rede	Por Throughput de dados	
4	Solução de segurança para e-mail com módulo de resposta a incidente.	Por conta de E-mail	
5	Proteção avançada contra ameaças e dados para Microsoft Office 365, Goolge Workspace e outros serviços em nuvem	Por conta de E-mail	
6	Solução de prevenção de intrusão de próxima geração (NGIPS)	Por Throughput de dados	
7	Solução de visibilidade de superfície de ataques	Por Endpoint	
8	Solução de Gerenciamento de Vulnerabilidades para Endpoints, baseada e com análise contínua e adaptável de riscos e confiança, com o serviço de instalação, implantação dos softwares, garantia técnica e transferência de conhecimento.	Por de dispositivos, assets, aplicações web, contêiner.	
9	Solução de Gerenciamento de Vulnerabilidades e Visibilidade de Ataques em tempo real para estrutura de Diretório de Usuários, com análise contínua e adaptável de riscos e confiança, com o serviço de instalação, implantação dos softwares, garantia técnica e transferência de conhecimento	Por de usuários ativos no Active Directory	
10	Serviço de suporte pro ativo, corretivo e para resposta a incidentes	Por Solução	
11	Serviço de implantação	Por Solução	
12	Serviço de capacitação e repasse de conhecimento	40 Horas	
13	Serviço de monitoramento do ambiente presencial	Por Posto	

Tabela 1: Solução de Segurança.

1.3. **APRESENTAÇÃO DO ITENS**

Item 1.

Oferece uma camada de defesa aos endpoints da rede, ajudando a prevenir, detectar e responder a ataques de malware, ransomware, vírus e outras ameaças. As proteções para endpoint incluem firewalls, antivírus, antimalware, detecção de intrusão, controle de aplicativos, gerenciamento de patches e outras ferramentas de segurança. Elas são essenciais para garantir a segurança dos dispositivos e dos dados armazenados neles, especialmente em ambientes corporativos, onde a proteção dos endpoints é crucial para a segurança global da rede. A integração com XDR (Extended Detection and Response) é crucial para uma visão abrangente e unificada das atividades de segurança cibernética em várias plataformas. Essa integração facilita a detecção avançada de ameaças, permite respostas coordenadas e rápidas a incidentes, reduz falsos positivos, oferece análises forenses detalhadas e ajuda na conformidade com regulamentos de segurança. Em resumo, o XDR melhora a segurança global, fornecendo uma abordagem integrada e proativa contra ameaças cibernéticas.

Item 2.

A proteção para servidores em um ambiente corporativo é de extrema importância porque os servidores são peças fundamentais da infraestrutura de tecnologia da informação de uma empresa. Eles armazenam e processam dados críticos e sensíveis, além de hospedar aplicativos e serviços essenciais para o funcionamento do negócio. Assim como nos endpoints a integração com XDR (Extended Detection and Response) é crucial para uma visão abrangente e unificada das atividades de segurança cibernética em várias plataformas. Essa integração facilita a detecção

avançada de ameaças, permite respostas coordenadas e rápidas a incidentes, reduz falsos positivos, oferece análises forenses detalhadas e ajuda na conformidade com regulamentos de segurança. Em resumo, o XDR melhora a segurança global, fornecendo uma abordagem integrada e proativa contra ameaças cibernéticas.

Item 3.

Solução de segurança que opera como um sistema de detecção de ameaças avançadas e análise de tráfego de rede. Ele utiliza uma variedade de métodos de inspeção, incluindo análise de tráfego, inspeção de pacotes, e técnicas de detecção comportamental para identificar e mitigar potenciais ameaças cibernéticas. Este sistema monitora o tráfego de rede em busca de comportamentos suspeitos, analisa padrões de comunicação e examina a integridade dos pacotes transmitidos espelhando o Throughput dos dados. Por meio de um conjunto diversificado de algoritmos e técnicas de análise procura identificar atividades maliciosas, como tentativas de intrusão, exploits, malware, comunicações suspeitas e outras atividades anômalas que possam indicar uma ameaça à segurança da rede.

Item 4.

O sistema em questão apresenta diversas funcionalidades destinadas a fortalecer a segurança de e-mails. Essas incluem:

Por meio da Filtragem de Conteúdo, são utilizados mecanismos avançados para examinar o conteúdo dos e-mails, verificando minuciosamente anexos, links e textos. Esse processo visa identificar possíveis ameaças, como malware, phishing e spam, antes que alcancem os destinatários. Além disso, há a implementação da Análise Comportamental, onde técnicas específicas são empregadas para identificar padrões de comportamento suspeitos nos e-mails. Essa abordagem busca detectar ameaças que podem passar despercebidas pelos métodos de filtragem tradicionais. A Verificação de URLs e Links é realizada em tempo real para avaliar a legitimidade e os possíveis riscos associados a esses elementos presentes nos e-mails. Essa verificação visa prevenir o acesso a sites maliciosos, protegendo os usuários contra possíveis ataques cibernéticos. O sistema também emprega a Prevenção de Ameaças Avançadas, valendo-se de inteligência artificial e aprendizado de máquina para identificar e bloquear ataques sofisticados e desconhecidos que possam representar riscos para os usuários. Adicionalmente, oferece recursos de Criptografia de E-mail para proteger informações confidenciais e implementar políticas de segurança. Isso reforça as diretrizes de uso seguro de e-mails dentro da organização, garantindo a proteção adequada dos dados sensíveis. Por meio de Relatórios e Análises Detalhadas, o sistema gera informações valiosas sobre as atividades de e-mail, oferecendo insights sobre ameaças bloqueadas, tendências de segurança e eventuais vulnerabilidades.

Item 5.

Solução capaz de monitorar as atividades dos usuários nos aplicativos baseados na nuvem, analisando o comportamento para identificar possíveis ameaças ou violações de segurança. Além disso, implementa políticas de controle de acesso baseadas em identidade, utilizando autenticação multifator e gerenciamento de privilégios para reforçar a segurança e limitar o acesso a dados sensíveis. Utilizando tecnologias de detecção de ameaças, como análise comportamental e algoritmos de inteligência artificial, identifica atividades suspeitas ou maliciosas nos aplicativos em nuvem. Também emprega medidas de criptografia, mascaramento ou tokenização para proteger dados confidenciais armazenados ou compartilhados por meio desses aplicativos. Ainda implementa controles para prevenção de perda de dados (DLP), estabelecendo políticas para evitar vazamentos acidentais ou intencionais de informações sensíveis. Gera relatórios e análises detalhadas sobre as atividades do usuário e as ameaças detectadas nos aplicativos em nuvem, oferecendo insights valiosos para aprimorar a segurança.

A capacidade de integração com outras soluções de segurança permite coordenar defesas em vários pontos e compartilhar informações para uma resposta mais rápida a incidentes de segurança. Todos esses recursos técnicos são direcionados para fornecer uma camada adicional de segurança aos aplicativos usados na nuvem, garantindo proteção, monitoramento eficaz e detecção proativa de ameaças ou violações de segurança. Sendo uma ferramenta muito eficaz para funcionar junto a proteção de email.

Item 6.

O Next-Generation Intrusion Prevention System (NGIPS) é uma solução de segurança avançada projetada para detectar e prevenir ataques cibernéticos em tempo real. Esses sistemas empregam técnicas sofisticadas de detecção e análise de tráfego de rede para identificar ameaças, proporcionando proteção proativa contra diversos tipos de ataques. Utilizando uma combinação de assinaturas de ameaças, análise comportamental e inteligência artificial, o NGIPS é capaz de identificar padrões de tráfego maliciosos ou comportamentos anômalos que indicam possíveis ataques. Ele examina pacotes de dados em tempo real, analisando-os em busca de vulnerabilidades conhecidas, exploits, malware e outras atividades suspeitas. Uma característica fundamental do NGIPS é a capacidade de tomar ações imediatas para bloquear ou mitigar esses ataques. Isso pode incluir o bloqueio de endereços IP suspeitos, a aplicação de regras de segurança para interromper tentativas de intrusão ou a quarentena de dispositivos comprometidos para evitar a propagação de ameaças. Além disso, esses sistemas são frequentemente atualizados com informações de inteligência de ameaças em tempo real, mantendo-se atualizados para reconhecer e se defender contra novas formas de ataques cibernéticos à medida que surgem.

Item 7.

O Automated Security Risk Management (ASRM) representa um avanço significativo na gestão de riscos de segurança em ambientes de rede. Esta abordagem inovadora se destaca pela sua capacidade automatizada de avaliar de forma contínua a postura de segurança de uma organização, oferecendo uma identificação e priorização precisa e eficiente dos riscos. Este sistema automatizado realiza análises e avaliações em tempo real, considerando uma gama diversificada de elementos, tais como vulnerabilidades, ameaças emergentes e conformidade com políticas

de segurança. Essa abordagem abrangente proporciona uma visão holística dos riscos, permitindo que a equipe de segurança concentre seus esforços nas áreas mais críticas. Consequentemente, isso possibilita decisões embasadas sobre onde alocar recursos para mitigar tais riscos, reforçando assim a eficácia das medidas de segurança adotadas pela organização.

Item 8.

A solução de Gerenciamento de Vulnerabilidades para Endpoints baseada em análise contínua e adaptável ofereceria um conjunto de ferramentas para identificar, avaliar e mitigar vulnerabilidades em dispositivos finais, como computadores e dispositivos móveis. Essa solução realizaria uma análise contínua do ambiente dos endpoints, identificando e classificando riscos em tempo real, ela incluiria serviços completos, desde a instalação e implementação dos softwares necessários até a garantia técnica e transferência de conhecimento para a equipe de segurança da organização. Isso garantiria não apenas a correta implementação da solução, mas também o suporte contínuo para o gerenciamento eficaz das vulnerabilidades nos endpoints.

Item 9.

Essa solução proporcionaria uma visão abrangente e contínua das vulnerabilidades existentes, fornecendo insights em tempo real sobre possíveis ameaças e ataques direcionados aos sistemas relacionados aos diretórios de usuários. Isso incluiria análises adaptáveis e em tempo real, permitindo identificar e responder rapidamente a possíveis riscos e ameaças emergentes. Além disso, a solução ofereceria serviços completos, desde a instalação e implantação dos softwares necessários até a garantia técnica e a transferência de conhecimento. Isso significa que a equipe responsável pela segurança cibernética receberia suporte completo durante todo o processo, desde a configuração inicial até o uso contínuo da solução.

Item 10.

O serviço abrange suporte proativo, corretivo e resposta a incidentes, visando prevenir problemas, corrigir falhas e reagir rapidamente a eventos adversos para manter a estabilidade e segurança dos sistemas.

Item 11.

Oferece suporte especializado para implementar soluções de segurança digital em ambientes corporativos. Ele inclui desde a configuração inicial até a integração completa das ferramentas de segurança, garantindo uma instalação eficiente e funcional.

Item 12.

Esse serviço visa fornecer treinamento e transferência de conhecimento para os clientes. Ele oferece capacitação especializada, permitindo que os usuários adquiram habilidades e compreensão sobre o uso eficaz das soluções ou tecnologias implementadas, capacitando-os a gerenciar, operar e manter os sistemas.

Item 13.

Esse serviço consiste na vigilância contínua e física do ambiente local de uma empresa ou espaço específico. Ele envolve a supervisão ativa por meio de pessoal designado para garantir a segurança, monitorar atividades e identificar possíveis ameaças ou irregularidades no local físico da organização.

2. **JUSTIFICATIVA DA NECESSIDADE DO QUANTITATIVO INDICADO PELA UNIDADE REQUISITANTE:**

2.1. *[Digite o texto de explicitação da motivação dos resultados a serem alcançados com o Registro de Preços, que **deverá conter na justificativa o problema, a solução e o quantitativo para justificar a demanda solicitada. É importante que a justificativa seja desenvolvida com todos os aspectos mencionados, pois uma justificativa pouco elaborada impossibilitará o atendimento da demanda].***

2.2. A justificativa há de ser clara, precisa e suficiente, **sendo vedadas justificativas genéricas**, incapazes de demonstrar de forma cabal a necessidade da Administração.

2.3. É imprescindível que o campo aborde o problema identificado a ser resolvido, a real necessidade gerada por ele e o que se almeja alcançar com a contratação.

2.4. Além disso, a descrição da necessidade de contratação deve conter manifestação acerca da essencialidade e interesse público da contratação, devendo, portanto, ser **avaliado o interesse público** também na perspectiva de se haverá impacto ambiental negativo decorrente da contratação e se há opções que atendam ao princípio do desenvolvimento nacional sustentável.

3. **NECESSIDADE DE INCLUSÃO DE NOVOS ITENS MEDIANTE MOTIVAÇÃO/JUSTIFICATIVA:**

3.1. A finalidade principal desta etapa é propiciar que a própria Administração incremente seus conhecimentos sobre o objeto, distinguindo suas características principais, para então, por meio da descrição, possibilitar que todos os fornecedores da solução escolhida venham a saber do interesse administrativo em uma futura contratação.

3.2. **O objeto deve ser descrito de forma detalhada, com todas as especificações necessárias e suficientes para garantir a qualidade da contratação**, cuidando-se para que não sejam admitidas, previstas ou incluídas condições impertinentes ou irrelevantes para o específico objeto do contrato. Deve-se levar em consideração as normas técnicas eventualmente existentes, quanto a requisitos mínimos de qualidade, utilidade, resistência e segurança, inclusive das exigências relacionadas à manutenção e à assistência técnica, quando for o caso:

ORDEM	ESPECIFICAÇÃO COMPLETA (INDICAR CATSER)	UNIDADE DE MEDIDA	QUANTIDADE

3.3. **Seguem orientações para indicação de um novo item não contemplado no Alinhamento Estratégico:**

3.3.1. Apresentar a definição clara, precisa e suficiente do item.

3.3.2. A identificação da necessidade da contratação é essencial justamente para permitir a reflexão sobre os motivos pelos quais determinada contratação foi solicitada, investigando, assim, qual a necessidade final a ser atendida, que pode inclusive ser distinta a depender da finalidade do órgão ou entidade, ainda que o objeto indicado pelo setor requisitante seja o mesmo.

3.3.3. Além disso, a descrição da necessidade de contratação deve conter manifestação conforme descrito no item 2 deste instrumento.

a) **Periodicidade da prestação do serviço:**

[Digite aqui a periodicidade estimada da prestação do serviço após a formalização da futura contratação. Ex: a prestação do serviço é de forma parcelada ou integral]

Diante do exposto, a Secretaria de Estado da Administração do Piauí continua aberta a maiores esclarecimentos de eventuais dúvidas, e devolve-se o **Processo nº 00002.013313/2023-11.**

Atenciosamente,

(Documento datado e assinado eletronicamente)

JÉSSICA KELLY DE SOUSA CARVALHO

Diretora de Planejamento de Licitações- DIP/SLC/SEAD

APROVO:

JACYLENNE COELHO BEZERRA FORTES

Superintendente de Licitações e Contratos - SLC/SEAD

SAMUEL PONTES DO NASCIMENTO

Secretário de Estado da Administração do Piauí - SEAD/PI

Documento assinado eletronicamente por **JESSICA KELLY DE SOUSA CARVALHO - Matr.371411-0**, **Diretora**, em 24/11/2023, às 12:28, conforme horário oficial de Brasília, com fundamento no Cap. III, Art. 14 do Decreto Estadual nº 18.142, de 28 de fevereiro de 2019.

Documento assinado eletronicamente por **SAMUEL PONTES DO NASCIMENTO - Mat.0209541-2**, **Secretário de Estado**, em 24/11/2023, às 14:09, conforme horário oficial de Brasília, com fundamento no Cap. III, Art. 14 do Decreto Estadual nº 18.142, de 28 de fevereiro de 2019.

A autenticidade deste documento pode ser conferida no site https://sei.pi.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **10142662** e o código CRC **3622E6E4**.