ATA DE REGISTRO DE PREÇOS Nº 21005/2022
PREGÃO ELETRÔNICO PARA REGISTRO DE PREÇOS
IFSC

Pregão Nº 21005/2022 – SRP
Processo nº 23292.016668/2022-72

O **INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SANTA CATARINA,** CNPJ nº 11.402.887/0001-60, Rua 14 de Julho, 150 – Enseada dos Marinheiros – Coqueiros, Florianópolis/SC – CEP: 88.075-010, doravante denominado apenas CONTRATANTE, neste ato representado pelo seu Reitor, Sr. MAURÍCIO GARIBA JÚNIOR RG 986.743 CPF 464.505.729-49, realizou no site www.comprasnet.gov.br Pregão Eletrônico para Registro de Preços e, nos termos da Lei nº 10.520/02 e os Decretos nº 5.450/05, 7.892/13, 8.250/14, Instrução Normativa N° 6, de 25 de julho de 2014, Lei nº 8.666/93 e das demais normas aplicáveis, em razão da classificação das propostas apresentadas no **Pregão Eletrônico de Registro de Preços nº 21005/2022**, Ata de Julgamento de Preços, divulgada no Comprasnet e homologada pelo Ordenador de Despesas deste IFSC, RESOLVE registrar os preços para a aquisição dos produtos, objeto do Pregão acima citado, que passa a fazer parte desta, tendo sido os referidos preços oferecidos pelas empresas cujas propostas foram classificadas em primeiro lugar no certame acima enumerado.

CLÁUSULA PRIMEIRA – DO OBJETO

A presente Ata tem por objeto assegurar o compromisso de possível contratação entre o IFSC e as empresas vencedoras do certame licitatório referente ao **Pregão Eletrônico nº 21005/2022**, cujo objeto é a contratação de pessoa jurídica para **AQUISIÇÃO DE MATERIAL PERMANENTE SERVIDORES, EXPANSÃO DE ARMAZENAMENTO, SOFTWARES E PERIFÉRICOS.** PARA O INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SANTA CATARINA, IFSC **,** conforme descrito no Anexo I desta Ata e ratificado por todas as empresas vencedoras através das declarações anexas.

CLÁUSULA SEGUNDA – DA VALIDADE DA ATA

A presente Ata de registro de Preços terá a validade de 12 (Doze) meses, compreendendo o período de **28/09/2022 a 28/09/2023.**

Subcláusula Primeira – Durante o prazo de validade desta Ata de Registro de Preço, o IFSC não será obrigado a firmar as contratações que dela poderão advir, facultando-se-lhe a realização de licitação específica para a aquisição pretendida, sendo assegurado ao beneficiário do registro preferência de favorecimento em igualdade de condições.

Subcláusula Segunda - Os preços registrados poderão ser revistos em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo dos serviços ou bens registrados, cabendo ao órgão gerenciador promover as negociações junto aos fornecedores, observadas as disposições contidas na alínea “d” do inciso II do caput do art. 65 da Lei nº 8.666, de 1993.

Subcláusula Terceira - A Ata poderá sofrer alterações de preços de acordo com as condições estabelecidas no arts. 18 e 19 do Decreto nº 7.892, de 23 de janeiro de 2013.

CLÁUSULA TERCEIRA – DA UTILIZAÇÃO DA ATA DE REGISTRO DE PREÇOS

A presente Ata de Registro de Preços poderá ser usada por todos os órgãos da Administração Pública Federal, desde que autorizados pelo IFSC.

Subcláusula Primeira - O preço ofertado pela(s) empresa(s) signatária(s) a presente Ata de Registro de Preços é especificado conforme o Anexo I.
Subcláusula Segunda - Em cada fornecedor decorrente desta Ata, serão observadas, quanto ao preço, as cláusulas e condições constantes do Edital referente a mesma.
Subcláusula Terceira - Em cada aquisição, o preço unitário a ser pago será o constante da proposta apresentada pela(s) empresa(s) detentora(s) da presente Ata, a(s) qual(is) também a integram.

CLÁUSULA QUARTA – DA CLASSIFICAÇÃO DAS PROPOSTAS

A relação do(s) item(ns) com a(s) respectiva(s) empresa(s) ofertante(s) do menor valor por item, a(s) qual(is) terá(ão) preferência de contratação constitui o Anexo I desta Ata.

CLÁUSULA QUINTA – DO LOCAL E PRAZO DE ENTREGA.

Em cada aquisição, o prazo de entrega do objeto desta licitação será aquele definido no edital do pregão eletrônico que originou esta Ata e os quantitativos serão os informados na Autorização de Fornecimento, conforme Anexo IV do Edital.

CLÁUSULA SEXTA – DO PAGAMENTO

Em todas as aquisições, o pagamento será feito por meio de ordem bancária transmitida ao Banco do Brasil, para crédito em banco, agência e conta-corrente indicados pelo contratado até 15 (quinze) dias do aceite na respectiva Nota Fiscal pelo órgão requisitante.
Subcláusula Primeira - Para os produtos com entregas diárias e semanais, o IFSC estimará o consumo mensal e emitirá uma Autorização de Fornecimento, sendo que o pagamento se dará após as entregas das quantidades previstas na referida autorização.

CLÁUSULA SÉTIMA – DA ENTREGA

A entrega dos produtos só estará caracterizada mediante o recebimento definitivo do mesmo, ou seja, o aceite na respectiva Nota Fiscal correspondente pelo fiscal do contrato.
Subcláusula Primeira - O fornecedor ficará obrigado a atender todos os pedidos efetuados durante a vigência desta Ata, mesmo que a entrega deles decorrente estiver prevista para data posterior à do seu vencimento.

Subcláusula Segunda - Os materiais deverão ser entregues acompanhados da Nota Fiscal ou Nota Fiscal Fatura correspondente.

CLÁUSULA OITAVA – DAS PENALIDADES

A licitante que ensejar o retardamento da execução do certame, não mantiver a proposta, falhar ou fraudar na execução do contrato, comportar-se de modo inidôneo, fizer declaração falsa ou cometer fraude fiscal, garantido o direito de ampla defesa, ficará impedida de licitar e contratar com a União, e será descredenciada do SICAF, pelo prazo de até 05 (cinco) anos, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade sem prejuízo das multas previstas em edital e no contrato, e das demais cominações legais.

Subcláusula Única - A contratada ficará sujeita, ainda, as penalidades previstas no edital do Pregão que originou esta Ata.

CLÁUSULA NONA – DO REAJUSTE DE PREÇOS

Considerando o prazo de validade estabelecido na Cláusula Segunda da presente Ata, e em atendimento ao §1º, art.28, da Lei Federal 9.069 de 29.6.1995 e demais legislação, é vedado qualquer reajuste de preços.

Subcláusula Única - Fica ressalvada a possibilidade de Alteração das condições para a concessão de reajuste em face da superveniência de normas federais aplicáveis à espécie. 03/12

CLÁUSULA DÉCIMA – DAS CONDIÇÕES DE RECEBIMENTO

Os materiais objetos desta Ata de Registro de preços serão recebidos pelo requisitante consoante o disposto no art. 73 da Lei 8.666/93 e demais normas pertinentes.

CLÁUSULA DÉCIMA PRIMEIRA – DO CANCELAMENTO DA ATA DE REGISTRO DE PREÇOS

Esta Ata de Registro de Preços poderá ser cancelada, de pleno direito:

I – Pela Administração, quando:

a- a detentora não cumprir as obrigações constantes desta Ata de Registro de Preços;
b- a detentora não assinar a Ata no prazo estabelecido e a Administração não aceitar a sua justificativa;
c- a detentora der causa a rescisão administrativa de contrato decorrente de registro de preços;
d- em qualquer das hipóteses de inexecução total ou parcial de contrato decorrente de registro de preços;
e- os preços registrados se apresentarem superiores aos praticados no mercado;
f- por razões de interesse público devidamente demonstradas e justificadas pela Administração;
g- a comunicação do cancelamento do preço registrado, nos casos previstos neste Edital, será feita pessoalmente ou por correspondência com aviso de recebimento, juntando-se o comprovante aos autos que deram origem ao registro de preços;

h- no caso de ser ignorado, incerto ou inacessível o endereço da detentora, a comunicação será feita por publicação no Diário Oficial da União, considerando-se cancelado o preço registrado após a publicação.

II- Pelas detentoras, quando:

a- mediante solicitação por escrito, comprovarem estar impossibilitadas de cumprir as exigências desta Ata de Registro de Preços;

b- o fornecedor poderá solicitar o cancelamento do seu registro de preços na ocorrência de fato superveniente que venha compromete a perfeita execução contratual, decorrente de caso fortuito ou de força maior, devidamente comprovados;

c- à solicitação das detentoras para cancelamento dos preços registrados deverá ser formulada com a antecedência de 30 (trinta) dias, facultada à Administração a aplicação das penalidades previstas na Lei, caso não aceitas as razões do pedido.

CLÁUSULA DÉCIMA SEGUNDA – DA AUTORIZAÇÃO PARA AQUISIÇÃO E EMISSÃO DAS AUTORIZAÇÕES DE FORNECIMENTO

As aquisições do objeto da presente Ata de Registro de Preço serão autorizadas, caso a caso, pelo Ordenador de Despesas do IFSC.

Subcláusula Primeira - A emissão das autorizações de fornecimento, sua retificação ou cancelamento, total ou parcial serão igualmente autorizados pelo órgão requisitante.

Subcláusula Segunda - Durante o prazo de validade do Registro de Preços, o IFSC poderá ou não contratar o objeto deste pregão.

CLÁUSULA DÉCIMA TERCEIRA – DAS DISPOSIÇÕES FINAIS E DO FORO

Integram esta Ata, o Anexo I (preços registrados) e as declarações de concordância das empresas vencedoras.

Esta Ata está vinculada ao Edital do **Pregão Eletrônico para Registro de Preços nº 21005/2022** e às propostas aceitas durante a sessão do referido certame pelas empresas relacionadas no Anexo I desta Ata.

Fica eleito o Foro da Justiça Federal, Seção Judiciária Florianópolis para dirimir quaisquer questões decorrentes da utilização da presente ata.

Os casos omissos serão resolvidos de acordo com a Lei 10.520/2002 e Decreto 5.450/2005, Lei 8.666/93 e demais normas aplicáveis.

Florianópolis, 28 de Setembro de 2022.

MAURÍCIO GARIBA JÚNIOR
REITOR DO IFSC
(Autorizado conforme despacho no Documento nº 23292.033984/2022-80 em 28/09/2022).

OBS: A adesão das empresas vencedoras a esta Ata se dá pelas Declarações de Concordância anexas

ANEXO I - DA ATA DE REGISTRO DE PREÇOS

EMPRESAS E PREÇOS REGISTRADOS

Pregão Nº 21005 / 2022 – SRP
Processo nº 23292.016668/2022-72
Relação de empresas vencedoras, contendo a descrição dos itens e preços negociados na sessão do Pregão.

EMPRESA (1)	BASE INFORMATICA LTDA
ENDEREÇO	**RUA DR.ABEL CAPELA. Bairro: COQUEIROS, FLORIANÓPOLIS / SC CEP: 88.080-25**
CNPJ	95.795.290/0001-13
TELEFONE/FAX	4830180072
REPRESENTANTE LEGAL	JOSE ARNALDO BAHIA SPINOLA BITTENCOURT
CPF REPRESENTANTE	000.079.899-11
Email	jose.bittencourt@base.inf.br

ITEM	UNID.	QTD.	ESPECIFICAÇÃO	Preço Unitário (R$)	Preço Total (R$)
36	LICENÇA	96.0	Código: 33904019001000068 RENOVAÇÃO DE ASSINATURA - SOFTWARE PHANTOSYS LITE - 36 MESES Marca: SEM MARCA Fabricante: -	600,00	57.600,00
				Total	R$ 57.600,00

EMPRESA (2)	CYBER WAN TECNOLOGIA LTDA
ENDEREÇO	**AV. CARLOS DE LIMA CAVALCANTE, 2821, LJ 09 - CASA CAIADA, OLINDA - PE, 53130-555. Bairro: CASA CAIADA, OLINDA / PE CEP: 53130-555**
CNPJ	47.247.764/0001-40
TELEFONE/FAX	81 3771-0084
REPRESENTANTE LEGAL	JOSÉ ZILMENS RODRIGUES CARTAXO
CPF REPRESENTANTE	709.044.614-08
Email	jose@cyberwan.com.br

ITEM	UNID.	QTD.	ESPECIFICAÇÃO	Preço Unitário	Preço Total (R$)

				(R$)	
6	LICENÇA	9.0	Código: 33904019001000054 LICENÇA COMERCIAL, SAAS, AUTOCAD LT 2021 - 36 MESES - Assinatura de licença usuário único do Autodesk Autocad LT (última versão disponível), com suporte avançado, pelo período de 03 (três) anos. Requisições: 3666/2020 - 119001 - COORDENADORIA DE COMPRAS - JAR - 1 Licença; 3723/2020 - 1106 - DEPARTAMENTO DE ADMINISTRAÇÃO - CDR - 1 Licença; Marca: SEM MARCA Fabricante: -	5.080,00	45.720,00
				Total	R$ 45.720,00

EMPRESA (3)			DUOWARE SOFTWARES LTDA		
ENDEREÇO			**RUA SENADOR DANTAS, 75, SALA 2403. Bairro: CENTRO, RIO DE JANEIRO / RJ**		
CNPJ			19.885.972/0001-39		
TELEFONE/FAX			2139429988		
REPRESENTANTE LEGAL			Ozilio Campos Simão		
CPF REPRESENTANTE			012.295.577-33		
Email			contato@camposemenezes.com		
ITEM	**UNID.**	**QTD.**	**ESPECIFICAÇÃO**	**Preço Unitário (R$)**	**Preço Total (R$)**
25	ANUAL	22.0	Código: 33904019001000063 LICENÇA EDUCACIONAL, SAAS, DE ACESSO A PLATAFORMA DE CRIAÇÃO DE MAPAS MENTAIS -> Características mínimas: 1. Mapas mentais ilimitados; 2. Arquivos e imagens anexos; 3. Exportar como PDF; 4. Exportar imagem; 5. Impressão de mapas mentais; 6. Exportar para o Word; 7. Exportar para o PowerPoint; 8. Uso por múltiplos membros de equipe; 9. Conta de administrador (gerenciar licenças); 10. Login no Google Workspace para domínios;	3.477,88	76.513,36

			11. Exportações e backups de conformidade; 12. Domínio personalizado (ex. empresa.com); 13. Múltiplos administradores de equipe; 14. Suporte prioritário por e-mail e telefone; 15. Plano com pagamento ANUAL. 16. Licença por usuário; 17. Referência: MindMeister Marca: SEM MARCA Fabricante: -		
				Total	R$ 76.513,36

EMPRESA (4)			HORIZON INOVACAO E TECNOLOGIA LTDA		
ENDEREÇO			**R ALCEU AMOROSO LIMAEDIF CENTRO EMPRESARIAL METROPOLINAO SALVADOR OFFICE POOL SALA 701 E 702 CAMINHO DAS ARVORES SALVADOR - BA 41.820-770. Bairro: CAMINHO DAS ÁRVORES, SALVADOR / BA**		
CNPJ			14.497.724/0001-05		
TELEFONE/FAX			(71) 3342 6700		
REPRESENTANTE LEGAL			Alessandro Gustavo Marques Passos		
CPF REPRESENTANTE			016.390.525-85		
Email			contato@hrzon.com.br		
ITEM	**UNID.**	**QTD.**	**ESPECIFICAÇÃO**	**Preço Unitário (R$)**	**Preço Total (R$)**
9	LICENÇA	27.0	Código: 44904005001000099 LICENÇA EDUCACIONAL, PERPÉTUA, SOFTWARE DE AEROFOTOGRAMETRIA - FLUTUANTE (VERSÃO PROFISSIONAL) Características: 1. Triangulação fotogramétrica; 2. Densa nuvem de pontos: edição e classificação; 3. Modelo de Elevação Digital: Exportação DSM/DTM; 4. Exportação de ortomosaicos georreferenciados; 5. Medidas: distâncias, áreas, volume; 6. Pontos de controle em terra: levantamento topográfico; 7. Processamento de imagem multiespectral; 8. Modelagem 4D para cenas dinâmicas; 9. Modelado 4D para escenas dinámicas; 10. Panoramas de 360 graus armados;	3.578,66	96.623,82

			11. Rede de processamento. Suporte técnico em horário comercial para dúvidas operacionais específicas sobre o software. Software de Referência: Agisoft Metashape Professional Flutuante uso educacional. Marca: SEM MARCA Fabricante: -		
26	ANUAL	27.0	Código: 33904019001000064 LICENÇA EDUCACIONAL, SAAS, DE ACESSO A PLATAFORMA DE CRIAÇÃO DE CONTEÚDOS DINÂMICOS -> Características mínimas: 1. Deve ser possível criar diversos modelos de perguntas, como: 1.1. Verdadeiro e falso; 1.2. Resposta digitada; 1.3. Múltipla escolha; 1.4. Enquete ou votação; 1.5. De coleta de feedbacks; 1.6. De revisão de conteúdos; 1.7. De preparação para vestibulares; 1.8. Incluir slides; 1.9. Quebra-cabeça; 1.10. Com imagens e/ou desenhos e vídeos do Youtube; 1.11. Com cronômetro ou de tempo livre; 1.12. Com elevação ou diminuição dos níveis de dificuldade, conforme o ritmo do aluno; 1.13. Com ranking, para estimular a competitividade; 2. Atribuir de forma aleatória as questões para que os alunos respondam individualmente ou em equipe, na sala de aula ou na sala virtual. 3.Geração de relatórios para: 3.1. Escalar os níveis de dificuldade das aulas e das lições; 3.2. Medir o desempenho dos alunos, individual e coletivo, inclusive instantaneamente; 3.3. Identificar o quanto um aluno sabe sobre uma matéria específica; 3.4. Compartilhar informações sobre cada aluno com outros professores; 3.5. Medir o nível de conhecimento da sala toda sobre determinado assunto. 4. Até 2000 participantes por sessão; 5. Licença ANUAL. 6. Licença por usuário. Referência: Kahoot! Marca: SEM MARCA Fabricante: -	4.709,38	127.153,26
				Total	R$ 223.777,08

EMPRESA (5)	PISONTEC COMERCIO E SERVICOS EM TECNOLOGIA DA INFORMACA
ENDEREÇO	**AV. PRESIDENTE GETÚLIO VARGAS 1038 SL 13. Bairro: BAIRRO NOVO, OLINDA / PE**
CNPJ	12.007.998/0001-35
TELEFONE/FAX	(81)32575110
REPRESENTANTE LEGAL	Carla Patricia Carvalho da Silva.
CPF REPRESENTANTE	855.883.004-59
Email	gestao.licitacao@pisontec.com

ITEM	UNID.	QTD.	ESPECIFICAÇÃO	Preço Unitário (R$)	Preço Total (R$)
3	LICENÇA	7.0	Código: 44904005001000071 LICENÇA COMERCIAL, PERPÉTUA, SOFTWARE ASC TIME TABLES PREMIUM - Software para geração de horários escolares. Marca: SEM MARCA Fabricante: -	2.733,00	19.131,00
5	LICENÇA	92.0	Código: 44904005001000089 LICENÇA COMERCIAL, PERPÉTUA, SOFTWARE OFFICE 2021 - Office Home & Business 2021; ➓ Compra única para 1 PC ou Mac; ➓ Versões 2021 clássicas do Word, Excel, PowerPoint e Outlook; ➓ Suporte da Microsoft incluído pelos primeiros 60 dias sem custo adicional; ➓ Compatível com Windows 11, Windows 10 ou macOS; ➓ Funciona com o Microsoft Teams; ➓ Licenciado para uso comercial e doméstico. Marca: SEM MARCA Fabricante: -	1.300,00	119.600,00
7	UNIDADE	9.0	Código: 33904019001000051 LICENÇA COMERCIAL, SAAS, SOFTWARE STREAM YARD - 12 MESES Estúdio virtual. Ferramenta que transmite transmite vídeos nas principais redes sociais, como Facebook, YouTube, LinkedIn, Twitch e Periscope e facilita a realização entrevistas, rodas de discussões e eventos online. Marca: SEM MARCA Fabricante: -	3.175,20	28.576,80
8	LICENÇA	9.0	Código: 44904005001000091 LICENÇA EDUCACIONAL, PERPÉTUA, DE SO WINDOWS SERVER 2022 STANDARD 16 CORE	2.043,00	18.387,00

			Marca: Microsoft Licenciamento: ESD Idioma: Português Licenciamento para: Uso corporativo Núcleos: Até 16 - 32bits ou 64bits Marca: SEM MARCA Fabricante: -		
11	LICENÇA	30.0	Código: 44904005001000078 LICENÇA EDUCACIONAL, PERPÉTUA, SOFTWARE FACTORY I/O. Com atualização por tempo indeterminado e gratuita. Sistema de Treinamento em Realidade Virtual para Aplicação do Controlador Lógico Programável (CLP). Deverá ser um conjunto que forneça interface e ambiente industrial virtual para que os alunos possam montar um projeto de planta industrial utilizando uma biblioteca de equipamentos que podem ser encontrados em ambientes industriais reais. Após a montagem de uma planta virtual, deverá possibilitar controlar todos os atuadores e ler os sinais provenientes dos sensores através de um controlador lógico programável (CLP) ou relé programável real. Deverá ser fornecido drivers que permitam a programação direta através de interface de comunicação TCP/IP por meio de software de programação de CLP TIA Portal da linha Siemens LOGO!, S7-300/400, S7-1200 e S7-1500. Deverá ser fornecido um datasheet dos componentes contidos no software de realidade virtual descrevendo suas características. Ferramenta simuladora para a educação e treinamento de programação de CLP recorrendo a gráficos 3D em tempo real, com som e total interatividade nos ambientes virtuais. Deverá possibilitar a montagem de processos industriais utilizando equipamentos virtuais de características fiéis a de equipamentos encontrados no mercado como esteiras, elevadores, sensores e etc. Deverá possibilitar a construção de diferentes projetos, salvá-los e protegê-los com senha para evitar edições, podendo assim propor diferentes desafios aos alunos, permitindo que possam evoluir de forma natural na sua formação. Após a etapa de lances serão solicitados documentos que comprovem o pleno atendimento a todas as exigências apresentadas para hardware e software,	4.158,00	124.740,00

			entre os documentos solicitados estarão, catálogos, manuais, capturas de telas de software, etc., os quais deverão apresentar correlação técnica entre si. Não sendo suficiente poderá ser solicitada a apresentação de amostras dos softwares de forma a fundamentar perfeitamente o aceite ou recusa da proposta. Sistema de treinamento em automação industrial deverá incluir 1 (uma) licença do tipo autônomo de software de simulação em sistemas industriais em tempo real, com: variáveis discretas e analógicas, com pelo menos 20 (vinte) projetos pré-construídos e editáveis (estação de buffer, estação de classificação, estação de convergência, estação de teste, classificação, pick and place e armazém, fabricação, paletização e controle com fluidos) o que cobre todos os conceitos básicos e intermediários em programação. Além disso, deverá conter uma biblioteca ampla com pelo menos 80 (oitenta) componentes como: Emissor de peças; Removedor de peças; Pallets; Transportadores de roletes; Transportador de correia; Esteira elevadiça; Esteira com balança; Rampa; Braço articulado separador; Separador com rodas ascendentes; Separador pneumático empurrador; Barreira de retenção; Mesa rotativa; Sensor capacitivo; Sensor fotoelétrico; Sensor retroreflectivo com refletor; Barreira de luz; Painel elétrico; Botão de emergência; Botão luminoso; Potenciômetro; Sinalizador luminoso de três cores; Display; Elevador; Pick & Place; Plataformas; Escadas; Centro de usinagem; Paletizador; Pick & Place de dois eixos; Tanque; Entre outros componentes para constituir uma planta fabril com o máximo de fidelidade real. É necessário poder criar situações de erro ou encravamento nos sistemas; Testar partes do circuito de produção, como por exemplo: testar uma mesa transportadora. Deve também mostrar o estado atual dos sensores e atuadores utilizados no ambiente virtual bem como forçar o estado dos atuadores. Deve incluir módulo de inserção de falhas. O fornecedor deverá disponibilizar capacitação com carga horária de 10 horas para 6 professores do câmpus, podendo ser remota ou on-line. Marca: SEM MARCA Fabricante: -		
21	LICENÇA	603.0	Código: 44904005001000102 LICENÇA EDUCACIONAL, WINDOWS SERVER 2022	221,00	133.263,00

			REMOTE DESKTOP SERVICES - 1 CAL POR DISPOSITIVO. Marca: SEM MARCA Fabricante: -		
32	LICENÇA	2.0	Código: 33904019001000070 LICENÇA, SAAS, PARA SOFTWARE DE GESTÃO DE VULNERABILIDADE E AUDITORIA - SUBSCRIÇÃO POR 12 MESES (COM POSSIBILIDADE DE RENOVAÇÃO POR 48 MESES) ---------- Plataforma de gestão de vulnerabilidade e auditoria de configuração de ativos de rede, endereços IP, contêineres, ativos em Nuvem e aplicações Web. O licenciamento da plataforma deverá ser por ativo, seguindo os quantitativos abaixo: 270 ativos de rede (Servidores, Estações de trabalho, Notebooks e Servidores em Cloud) 1 Imagem de Contêiner; 270 Aplicações Web; ---------- 1. Características Gerais: 1.1. O licenciamento da plataforma deverá ser por ativo, sendo este um dos abaixo: 1.1.1.1. Ativos em rede; 1.1.1.2.Servidores e Estações de trabalho ou Notebooks; 1.1.1.3.Servidores em Cloud; 1.1.1.4.Contêineres; 1.1.1.5.Aplicações Web e API; 1.2. O licenciamento deverá ser flexível, ou seja, não limitado por módulo. Cada licença adquirida deverá possibilitar a utilização para qualquer um dos ativos do item anterior; 1.3. Deverá ser possível alterar o uso da licença entre os ativos acima. Caso haja algum prazo mínimo para esta mudança de uso de licenciamento, está deverá ser de no máximo 90 dias; 1.4.O gerenciamento da plataforma deverá ser centralizado e único para todos os módulos descritos neste documento; 1.5.O gerenciamento da solução deverá ser em nuvem; 1.6.O processo de análises de vulnerabilidades e conformidade, quando executados on-premisses, deverá ser efetuado localmente, ou seja, na própria	218.241,40	436.482,80

			rede da CONTRATANTE ou com agente instalado no próprio computador. Os dados então serão sincronizados com a console em nuvem para análise; 1.7.A solução em nuvem deverá atender, no mínimo, os seguintes requerimentos de segurança: 1.7.1.A solução deve prover no minínimo 99.95% de disponibilidade no nível de serviço; 1.7.2. A solução deve criptografar todas as informações em trânsito; 1.7.3. Deve utilizar no mínimo chave AES-256 para criptografar os dados armazenados; 1.7.4. A solução deve ser capaz de gerar uma chave randômica com no mínimo 256 bits para cada scanner conectado na plataforma de gerência; 1.7.5. Todos os dados enviados para a plataforma de gerenciamento devem ser criptografados no mínimo com protocolo TLS 1.2 com tamanho de chave de 4096 bits; 1.7.6. Dados indexados devem possuir no mínimo criptografia utilizando algoritmo AES-256; 1.7.7. A plataforma deve ser capaz de gerar uma chave randômica de no mínimo 128 bits para qualquer ❽Job❾ gerado; 1.7.8. A plataforma deve utilizar no mínimo chave AES-256 para Backups e dados Replicados; 1.7.9. Todas as credenciais armazenadas na plataforma deverão ser criptografadas com algoritmo AES-256, no mínimo; 1.7.10. A solução deve possuir no mínimo as seguintes certificações de privacidade e segurança: 1.7.10.1. EU-U.S. Privacy Shield Framework; 1.7.10.2. Swiss-U.S. Privacy Shield Framework; 1.7.10.3. Cloud Security Alliance (CSA) STAR; 1.7.11. A solução deve possuir ferramentas e processos automatizados para monitorar: Uptime, Comportamentos anômalos e performance da plataforma; 1.7.12. Deve possuir retenção na nuvem de no mínimo 12 meses dos resultados dos scans realizados no ambiente; 1.7.13. Os dados de clientes deverão ser totalmente separados um dos outros, não possuindo compartilhamento de dados; 1.7.14. O fabricante da solução deverá implementar controles de segurança, como Análise de Vulnerabilidade no mínimo semanal, Firewalls, segmentação de rede, e monitoramento de segurança 24/7/365, para garantir a segurança da		

			aplicação; 1.7.15. O desenvolvimento da solução deverá seguir metodologias de Desenvolvimento Seguro; A fabricante da solução deverá possuir ISO 27001; ---------- 2. PLATAFORMA DE GESTÃO DE VULNERABILIDADE EM ATIVOS DE REDE E NUVEM 2.1CARACTERÍSTICAS GERAIS 2.1.1. Toda a solução deverá ser do mesmo fabricante, sem qualquer tipo de customização não autorizada pelo mesmo; 2.1.2. O gerenciamento da solução deve ser 100% em nuvem; 2.1.3. A solução deve prover no mínimo 99.95% de disponibilidade no nível de serviço; 2.1.4. A solução deve ser licenciada de modo a realizar varreduras (scans) de vulnerabilidades, avaliação de configuração e conformidade (baseline e compliance) e indícios e padrões de códigos maliciosos conhecidos (malware); 2.1.5. A solução deve possuir recurso de varredura ativa, onde o scanner comunica-se com os alvos (ativos) através da rede; 2.1.6. Deve possibilitar, por meio da console, no mínimo 4 (três) métodos de escaneamento: 2.1.6.1. Scan ativo; 2.1.6.2. Scan com uso de agentes; 2.1.6.3. Scan passivo; 2.1.6.4. Scanner em nuvem; 2.1.7. A solução deverá possuir Scanners em Nuvem em diversas localidades, possibilitando a escolha da localidade no momento do Scan. O uso destes scanners deverá estar contemplado no licenciamento; 2.1.8. Os Scanners em Nuvem devem estar disponíveis, no mínimo, nas seguintes localidades: EUA, Europa e Brasil; 2.1.9. Deve ser capaz de identificar no mínimo 60.000 CVE´S; 2.1.10. Deverá possuir, através de site público, uma lista com todas as vulnerabilidades identificadas pela solução; 2.1.11. A solução deve possuir um sistema próprio de pontuação e priorização das vulnerabilidades diferente do padrão CVSS; 2.1.12. Deve possuir mecanismo de priorização dinâmico baseado em algoritmos de inteligência		

			artificial (machine learning); 2.1.13. O Algoritmo de priorização deve considerar no mínimo 100.000 vulnerabilidades distintas para realizar o cálculo do score da vulnerabilidade; 2.1.14. Toda vulnerabilidade que possuir um CVE associado deve receber uma nota dinâmica da solução de gestão de vulnerabilidades; 2.1.15. A solução deve ser capaz de aplicar algoritmos de inteligência artificial (Machine learning) para analisar mais de 130 fontes de dados relacionadas a vulnerabilidades; 2.1.16. O sistema de pontuação e priorização de vulnerabilidades deve avaliar no mínimo as seguintes características: 2.1.16.1. CVSSv3 Impact Score; 2.1.16.2. Idade da Vulnerabilidade; 2.1.16.3. Se existe ameaça ou Exploit que explore a vulnerabilidade; 2.1.16.4. Número de produtos afetados pela vulnerabilidade; 2.1.16.5. Intensidade baseada no Número e Frequência de ameaças que utilizaram a vulnerabilidade ao longo do tempo; 2.1.16.6. Lista de todas as fontes (canais de mídia social, Dark Web etc.) em que ocorreram eventos de ameaças relacionados a vulnerabilidade; 2.1.17. A solução de gestão de vulnerabilidades deve suportar análise de vulnerabilidades de ambientes industriais (Tecnologias de Automação); 2.1.18. Deve possuir uma API abrangente para automação de processos e integração com aplicações terceiras; 2.1.19. Deve ser capaz de fazer a correlação diária de ameaças ativas contra as vulnerabilidades existentes na infraestrutura, incluindo feeds de inteligência de ameaças, tanto de fontes públicas como também de fontes não gratuitas; 2.1.20. A solução deve permitir a instalação de agentes em estações de trabalho e servidores, para varredura diretamente no sistema operacional; 2.1.21. A solução deve possuir conectores para a seguintes plataformas: 2.1.21.1. Amazon Web Service (AWS); 2.1.21.2. Microsoft Azure; 2.1.21.3. Google Cloud Platform; 2.1.22. A solução deve ser capaz de analisar vulnerabilidades em servidores na AWS utilizando somente o conector, sem a necessidade de		

			instalação de agente ou uso de qualquer outro tipo de sensor de rede da solução. 2.1.23. A solução deve ser capaz de produzir relatórios nos seguintes formatos: PDF, CSV e HTML; 2.1.24. A solução deve ser PCI ASV (Approved Scanning Vendor); 2.1.25. A solução deve ser capaz de identificar novos hosts no ambiente sem a necessidade de um scan; 2.1.26. A solução deve possuir recurso de monitoria passiva do tráfego de rede para identificação de anomalias, novos dispositivos e desvios de padrões observados; 2.1.27. A solução deve ser licenciada para no mínimo 50 scanners ativos; 2.1.28. A solução deve ser licenciada para o uso de no mínimo 20 sensores passivos de rede para realizar o monitoramento em tempo real do ambiente; 2.1.29. Deve ser possível determinar quais portas estão abertas em determinado ativo; 2.1.30. Deve ser capaz de guardar no mínimo os seguintes atributos de um ativo: 2.1.30.1. Endereço IPv4 e IPv6; 2.1.30.2. Sistema Operacional; 2.1.30.3. Nome NetBIOS: 2.1.30.4. FQDN; 2.1.31. A solução deve ser capaz de realizar em tempo real a descoberta de novos ativos para no mínimo: 2.1.31.1. Bancos de dados; 2.1.31.2. Hypervisors; 2.1.31.3. Dispositivos móveis; 2.1.31.4. Dispositivos de rede; 2.1.31.5. Endpoints; 2.1.31.6. Aplicações; 2.1.32. Deve realizar em tempo real a identificação de informações sensíveis no tráfego de rede do ambiente; 2.1.33. A solução deve ser capaz de identificar a comunicação de malwares na rede de forma passiva; 2.1.34. Deve ter a capacidade de guardar em tempo real informações de GET,POST e Download que trafeguem na rede; 2.1.35. A solução deve ser capaz de em tempo real detectar logins e downloads de arquivos em um compartilhamento de rede sem a necessidade de um agente; 2.1.36. Permitir identificar vulnerabilidades associadas a servidores SQL no tráfego de rede em		

			tempo real sem a necessidade de um agente; 2.1.37. A solução deve ser capaz de realizar varreduras (scans) de vulnerabilidades para o número de ativos contratados; 2.1.38. A solução deve ser licenciada pra uso agentes instalados em estações de trabalho e servidores, para varredura diretamente no sistema operacional, para o número total de ativos contratados. 2.1.39. A solução deve realizar varreduras em uma variedade de sistemas operacionais, incluindo no mínimo Windows, Linux e Mac OS, bem como Hypervisors e Dispositivos de Rede; 2.1.40. A solução deverá estar licenciada para varreduras em dispositivos móveis (Ex.: Smartphones, Tablets), sendo realizada através de integração com solução de MDM de mercado ou uso de agente próprio; 2.1.41. A solução deve suportar vários mecanismos de varredura distribuídos em diferentes localidades e regiões e gerenciar todos por uma console central; 2.1.42. A solução deve fornecer agentes instaláveis em sistemas operacionais distintos para monitoramento de configurações e vulnerabilidades; 2.1.43. A solução deve incluir a capacidade de programar períodos onde varreduras não podem ser executadas em determinados ativos, podendo selecionar no mínimo a frequência da agenda (diário, semanal, etc), hora de inicio e fim da janela, quais ativos serão excluídos e o fuso horário do agendamento; 2.1.44. A solução deve ser configurável para permitir a otimização das configurações de varredura, permitindo no mínimo definir o período de timeout, o número de conexões TCP concorrentes e reduzir a análise em execução caso detecte congestionamento de rede; 2.1.45. A solução deve permitir a entrada e o armazenamento seguro de credenciais do usuário, incluindo contas locais, de domínio (LDAP e Active Directory) e root para sistemas Linux; 2.1.46. A solução deve fornecer a capacidade de escalar privilégios nos destinos, do acesso de usuário padrão até acesso de sistema ou administrativo; 2.1.47. A solução deve ser capaz de realizar pesquisas de dados confidenciais; 2.1.48. Deve permitir executar uma análise de remediação, para verificar que uma solução foi aplicada corretamente. Essa análise de remediação		

			será executada somente nos ativos impactados, analisando somente a vulnerabilidade remediada, sendo sua política criada especificamente para esta finalidade; 2.1.49. Deverá ser possível agrupar sensores em grupos. A solução deverá automaticamente distribuir uma atividade de análise entre os sensores pertencentes ao grupo, para aumentar a performance de um scan; 2.1.50. A solução deverá apresentar o status da vulnerabilidade, demonstrando na interface de gerenciamento se a mesma é Nova, Persistente, Corrigida ou Reapareceu no ativo; 2.1.51. Deverá ser possível aceitar uma vulnerabilidade, onde a mesma não irá mais aparecer na console. Este processo poderá ser feito para um único ativo ou múltiplos ativos. Ainda, deverá ser possível definir uma data de expiração para a Aceitação. 2.1.52. Deverá ser possível modificar a severidade das vulnerabilidades, de um único ativo ou múltiplos ativos, podendo ainda definir uma data de expiração para esta modificação; 2.1.53. A solução deve suportar o uso de Tags nos ativos, sendo estes aplicados de forma manual ou automaticamente; 2.1.54. No caso de Tags automáticas, deverá ser possível configurar regras para atender, no mínimo: 2.1.54.1. Ativo analisado ou não em relação a vulnerabilidades; 2.1.54.2. Informações de nuvem pública, como por exemplo Região na AWS, Azure Resource ID ou GCP Cloud Project ID; 2.1.54.3. Software instalado no ativo; 2.1.54.4. Sub-rede; 2.1.54.5. Sistema Operacional; 2.1.55. Deverá ser possível configurar quais usuários, ou grupos de usuários, podem editar as Tags; 2.1.56. A solução deverá usar as Tags como filtros, podendo ser utilizadas na lista de vulnerabilidades, onde o objetivo é ver todas as vulnerabilidades existentes nos ativos que possuem determinada Tag; 2.1.57. Ser possível fazer análise dos ativos através de Tags, como exemplo todos os Ativos que possuem a Tag Linux; --- --- 3. CONTROLE DE USUÁRIOS		

			3.1. A solução deve suportar RBAC (Role Based Access Control) com no mínimo 5 tipos de usuários pré-definidos; 3.2. Deve possuir no mínimo um perfil administrador e um perfil somente leitura; 3.3. Deve permitir autenticação com Single Sign On suportando os padrões SAML 2.0 ou Shibboleth 1.3; 3.4. A solução deve possibilitar a criação de Grupos de Usuários; 3.5 Deve permitir configurar quais usuários, ou grupos de usuários, tem permissão de visualizar determinados ativos da organização e suas vulnerabilidades, e quais tem permissão de executar análises de vulnerabilidades nesses ativos; 3.6. Possuir duplo fato de autenticação nativo na própria solução; 3.7. Deve possibilitar configurar permissões, por usuário e grupo de usuário, específicas para cada política de análise de vulnerabilidades. No mínimo deverá ser possível configurar permissões de Nenhum Acesso, Somente Ver Resultados, Configuração ou Execução das políticas; --- 4. RELATÓRIOS E DASHBOARDS 4.1.Deve ser capaz de exportar dashboards em modelo de relatórios, tanto de forma manual e periódico de acordo com a frequência estabelecida pelo administrador; 4.2. Deve suportar a criação de relatórios criptografados (protegidos por senha configurável) ; 4.3. A solução deve suportar o envio automático de relatórios para destinatários específicos; 4.4. Deve ser possível definir a frequência na geração dos relatórios para no mínimo: Diário, Mensal, Semanal e Anual; 4.5. A solução deve possuir dashboards customizáveis onde o administrador pode deletar, editar ou criar painéis de acordo com a necessidade; 4.6. Deve possuir ao menos 10 modelos de dashboards já criados, podendo ser customizados; 4.7. A solução deve permitir exportar dados do que está sendo apresentado na tela, no mínimo para: 4.7.1. Ativos gerenciados pela solução 4.7.2. Todas as vulnerabilidades existentes nos ambientes e em quais ativos ela existe; 4.7.3. Vulnerabilidades por ativo gerenciado pela solução;		

			4.7.4. Vulnerabilidades de um único ativo; 4.7.5. Uma única vulnerabilidade e todos os ativos que possuem; 4.8. Deve ser possível exportar os dados em HTML, PDF ou CSV; 4.9. Em caso de exportação por CSV deve ser possível selecionar, via console de gerenciamento, quais campos deseja exportar; 4.10. Deve ser possível exportar somente os gráficos dos dashboards, através da console de gerenciamento, em PDF, PNG e JPG; 4.11. Deve ser possível criar um novo Dashboard e definir este como padrão de visualização do usuário, ou seja, o primeiro Dashboard a aparecer na console no acesso; 4.12. Deve ser possível configurar um filtro permanente no Dashboards para apresentar informações de todos os ativos, ou somente ativos específicos do ambiente; 4.13. A solução deve permitir compartilhar Dashboards com um ou mais usuários, bem como com grupo de usuários da aplicação; 4.14. Deve ser possível configurar SLAs em dias, representando a idade das vulnerabilidades no ambiente, sendo o período onde a mesma foi encontrada até a resolução. Esta informação deverá ser apresentada no Dashboard da solução. ---------- 5. ANÁLISE DE CONFORMIDADE 5.1. A solução deve ser totalmente licenciada para realizar scans de auditoria e compliance; 5.2. A solução deve ser capaz de realizar auditoria de conformidade sem a necessidade de agente instalado no dispositivo de destino; 5.3. A solução deve ser licenciada para realizar scans de conformidade e compliance de forma ilimitada; 5.4 Toda a solução deve ser licenciada de modo a realizar scans de conformidade para os seguintes padrões: CIS, SCAP e OVAL; 5.5. A solução deverá possuir modelos prontos de padrões de configuração, no mínimo para: CIS, DISA e MSCT (Microsoft Security Compliance Toolkit); 5.6. Deve suportar a verificação de compliance para no mínimo: 5.6.1. Bluecoat ProxySG; 5.6.2. Brocade Fabric OS; 5.6.3. Checkpoint;		

			5.6.4. Cisco IOS; 5.6.5. Citrix Xenserver; 5.6.6. Fireeye; 5.6.7. Fortinet FortiOS; 5.6.8. IBM iSeries; 5.6.9. Netapp Data ONTAP; 5.6.10. Palo Alto Firewall; 5.6.11. Red Hat Enterprise Virtualization; 5.6.12. Unix; 5.6.13. Windows; 5.6.14. VMware. 5.7. A solução deve mostrar se o critério de compliance foi atendido ou não fornecendo no mínimo os seguintes status: 5.7.1. Passou; 5.7.2. Falhou; 5.7.3. Atenção; ---------- ---------- 6. ANÁLISE DE RISCO DO AMBIENTE 6.1. A solução deve gerar um score que combine dados de vulnerabilidades com a criticidade dos ativos do ambiente computacional; 6.2. O score deve ser gerado automaticamente por meio de algoritmos de inteligência artificial (Machine Learning) e deve calcular a probabilidade de exploração de uma determinada vulnerabilidade; 6.3. Deve ser capaz de calcular a criticidade dos ativos da organização; 6.4. A solução deve ser capaz de realizar um benchmark no ambiente da CONTRATANTE comparando sua maturidade com outras organizações do mesmo setor; 6.5. A solução deve permitir modificar a qualquer momento o tipo de indústria para comparação. 6.6. Deve fornecer uma lista com as principais recomendações para o ambiente com foco na redução da exposição cibernética da organização; 6.7. A solução deve gerar uma pontuação para cada um dos ativos onde é levado em conta as vulnerabilidades presentes naquele ativo assim como a classificação do ativo na rede (peso do ativo). 6.8. A solução deve gerar uma pontuação global referente a exposição cibernética da organização baseado nas pontuações de cada um dos ativos. 6.9. A solução deve permitir um acompanhamento histórico do nível de exposição da organização; 6.10. Permitir realizar alterações na classificação dos		

			ativos (atribuição de pesos diferentes) podendo sobrescrever a classificação atribuída automaticamente pela solução. 6.11. A solução deverá apresentar indicadores específicos referentes a remediação, possuindo no mínimo informações referentes ao tempo entre remediação e o tempo o qual a vulnerabilidade foi descoberta no ambiente, tempo entre a remediação e a data de publicação da vulnerabilidade, quantidade média de vulnerabilidades criticas por ativo e a comparação da quantidade de vulnerabilidades corrigidas por criticidade. 6.11. A solução deve possuir um gráfico indicativo do percentual de ativos com soluções de proteção de endpoint instaladas, bem como o nome e a versão da solução. 6.12. A solução deve permitir a segregação lógica entre áreas distintas da empresa afim de obter a pontuação referente exposição cibernética por área. 6.13. A solução deve permitir a segregação lógica entre aplicações distintas da empresa afim de obter a pontuação referente exposição cibernética por aplicação. ---------- 7. PLATAFORMA DE GESTÃO DE VULNERABILIDADE EM APLICAÇÕES WEB CARACTERÍSTICAS GERAIS 7.1 A solução de gestão de vulnerabilidades deve ser capaz de analisar, testar e reportar falhas de segurança em aplicações Web como parte dos ativos a serem inspecionados; 7.2 A solução deverá capaz de executar varreduras em sistemas web através de seus endereços FQDN (DNS); 7.3. A plataforma deverá avaliar no mínimo os padrões de segurança OWASP Top 10 e PCI (payment card industry data security standard); 7.4. A solução deverá ser homologada como PCI ASV; 7.5. Deve suportar as diretivas PCI ASV 6.1 para definição de balanceadores de carga das aplicações bem como suas configurações para inclusão no relatório de resultados; 7.6. Deve possui modelos (templates) prontos de varreduras e também ser possível a criação de modelos customizados; 7.7. Para varreduras extensas e detalhadas, deve		

			varrer e auditar no mínimo os seguintes elementos: 7.7.1. Cookies, Headers, Formulários e Links; 7.7.2. Nomes e valores de parâmetros da aplicação; 7.7.3. Elementos JSON e XML; 7.7.4. Elementos DOM; 7.8. Deverá também permitir somente a execução da função crawler, que consiste na navegação para descoberta das URLs existentes na aplicação; 7.9. Deve ser capaz de utilizar scripts customizados de crawl com parâmetros definidos pelo usuário; 7.10. Deve ser capaz de excluir determinadas URLs da varredura através de expressões regulares; 7.11. Deve ser capaz de excluir determinados tipos de arquivos através de suas extensões; 7.12. Deve ser capaz de instituir no mínimo os seguintes limites: 7.12.1. Número máximo de URLs para crawl e navegação; 7.12.2. Número máximo de diretórios para varreduras; 7.12.3. Número máximo de profundidade dos elementos DOM; 7.12.4. Tamanho máximo de respostas; 7.12.5. Limite de requisições de redirecionamentos; 7.12.6. Tempo máximo para a varredura; 7.12.7. Número máximo de conexões HTTP ao servidor hospedando a aplicação Web; 7.12.8. Número máximo de requisições HTTP por segundo; 7.13. A solução deve ser capaz de detectar congestionamento de rede e limitar os seguintes aspectos da varredura: 7.13.1. Limite em segundos para timeout de requisições de rede; 7.13.2. Número máximo de timeouts antes que a varredura seja abortada; 7.14. Deve ser capaz de agendar a varredura e determinar sua frequência entre uma única vez, diária, semanal, mensal e anual; 7.15. Deve ser capaz de enviar notificações através de no mínimo E-mail; 7.16. Deve possuir a flexibilidade de selecionar quais testes serão realizados de forma granular, através da seleção de testes, plug-ins ou ataques; 7.17. Deverá avaliar sistemas web utilizando frameworks modermos, como AJAX, HTML5 e SPA; 7.18. Deverá possibilitar a definição de atributos no cabeçalho (HEADER) da requisição HTTP de forma		

			personalizado a ser enviada durante os testes; 7.19. Deverá ser compatível com avaliação de RESTful APIs, utilizando o padrão OpenAPI (Swagger); 7.20. Deverá suportar no mínimo os seguintes esquemas de autenticação: 7.20.1. Autenticação básica (digest); 7.20.2. NTLM; 7.20.3. Form de login; 7.20.4. Autenticação de Cookies; 7.20.5. Autenticação através de Selenium; 7.21. Deve ser capaz de importar scripts de autenticação selenium previamente configurados pelo usuário; 7.22. Deve ser capaz de customizar parâmetros Selenium como delay de exibição da página, delay de execução de comandos e delay de comandos para recepção de novos comandos; 7.23. Deve ser capaz de exibir os resultados das varreduras em dashboard dedicados para este tipo de análise; 7.24. Deve ser capaz de exibir os resultados agregados de acordo com as categorias do OWASP Top 10 (https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project); 7.25. Os resultados devem ser apresentados agregados por vulnerabilidades ou por aplicações; 7.26. Para cada vulnerabilidade encontrada, deve ser exibido evidências da mesma em seus detalhes; 7.27. Para vulnerabilidades de injeção de código (SQL, XSS, XSRF, etc), deve evidenciar nos detalhes do evento encontrado: 7.27.1. Payload injetado; 7.27.2. Evidência em forma de resposta da aplicação; 7.27.3. Detalhes da requisição HTTP; 7.27.4. Detalhes da resposta HTTP; 7.28. Os detalhes das vulnerabilidades devem conter descrição da falha e referências didáticas para a revisão dos analistas; 7.29. Cada vulnerabilidade encontrada deve conter também soluções propostas para mitigação ou remediação das mesmas; 7.30. A solução deve possuir suporte a varreduras de componentes para no mínimo: Wordpress, Blog Designer Plugin for Wordpress, Event Calendar Plugin for Wordpress, Convert Plus Plugin for Wordpress, AngularJS, Apache, Apache Tomcat,		

			Apache Spark e Apache Struts, Atlassian Confluence, Atlassian Crowd e Atlassian Jira, Backbone.js, ASP.NET, Bootstrap, Drupal, Joomla!, jQuery, Lighttpd, Magento, Modernizr, Nginx, PHP, AJAX, Sitefinity, Telerik, ThinkPHP, Webmin e YUI; 7.31. A solução deverá possuir controle de permissão de usuários, com no mínimo menos 3 níveis, sendo: Administrador, Operador de Scan e Somente Leitura; 7.32. Deverá possuir a capacidade de manter privado os resultados de um scan, ou seja, não aparecendo o resultado no dashboard da solução; 7.33. A solução deverá possuir um Add-on para o browser que permite gravar uma macro de autenticação para criação do Selenium; 7.34. Deverá ser possível excluir a interação com elementos DOM durante o Scan. Está exclusão poderá ser configurada para cada elemento, sendo possível escolher o Conteúdo do texto ou do Atributo CSS. 7.35. A solução deverá possuir nativamente scanners pré-configurados em nuvem, para realização de scans externos. Estes scanner deverão obrigatoriamente possuir IP dedicado, com divulgação pública, para configuração de whitelist em Firewalls, WAFs, ou outros sistemas de proteção. 7.36. A solução deve possuir também sensores (scanner) on-premisses. A solução deverá estar licenciada para o uso de no mímino 10 sensores deste tipo. 7.37. Deverá ser possível exportar os gráficos do dashboard em PDF, PNG ou JPEG, nativamente pela console de gerência. 7.38. Deve ser possível alterar o user agent utilizado pela solução; 7.39. A solução deve suportar listas de exclusão globais; 7.40. Deve possuir um dicionário já criado com as principais páginas comuns e páginas de backup existentes. 7.41. Deve apresentar a nota do CVSSv3 nas vulnerabilidades encontradas; 7.42. Ser possível gerar relatório das vulnerabilidades, no mínimo em PDF, HTML e CSV; ---------- ---------- 8. PLATAFORMA DE GESTÃO DE VULNERABILIDADE EM CONTÊINERES		

			CARACTERÍSTICAS GERAIS: 8.1. A solução deverá ser licenciada contabilizando o número de imagens únicas, não sendo contabilizadas novas versões de uma mesma imagem; 8.1. A solução de gestão de vulnerabilidades deve ser capaz de analisar, testar e reportar falhas de segurança em aplicações em 8.1. 8.2. Containers Docker como parte dos ativos a serem inspecionados; 8.3. A solução deve ser capaz de analisar imagens preparadas pelos desenvolvedores na esteira DevOps em busca de imagens com 8.4. vulnerabilidades identificadas e malware residente no sistema de arquivos; 8.5. A solução deve ser capaz de se integrar a esteira DevOps através de API, invocando o envio da imagem para análise em repositório próprio da solução ou utilizando scanner implementado em infraestrutura proprietária do órgão com a finalidade de evitar o envio de imagens e propriedade intelectual da CONTRATANTE; 8.6. A documentação de API da solução deverá ter acesso público através de website ou documentação do próprio fabricante; 8.7. A console de administração deverá possuir controle de acesso no mínimo permitindo usuários com capacidade de somente visualizar as informações, e usuários com capacidade para efetuar análise das imagens; 8.8. A solução deve inventariar o sistema operacional de cada imagem analisada e suas vulnerabilidades encontradas; 8.9. A solução deve ser capaz de identificar containers que não foram analisados antes de sua implementação em produção; 8.10. A solução deve analisar as camadas (layers) de um container; 8.11. A solução deve ser capaz de identificar containers que tiveram mudanças de arquivos entre a análise e a sua implementação em produção; 8.12. A solução deve ser capaz de identificar as devidas tags das imagens avaliadas; 8.13. A solução deve informar os CVEs para cada vulnerabilidade encontrada nos pacotes e bibliotecas residentes na imagem; 8.14. A solução deve ter a capacidade de testar automaticamente todas as imagens armazenadas, ou previamente testadas, sempre que uma nova		

			vulnerabilidade for publicada e atualizada no banco de dados de vulnerabilidade da solução, sem qualquer tipo intervenção manual; 8.15. Deve ser capaz de inventariar os pacotes e bibliotecas e suas respectivas versões e listar as mesmas dentro do relatório de resultados de análise de cada imagem; 8.16. A solução deve possuir conectores e permitir importação de imagens dos seguintes repositórios: 8.16.1. Docker; 8.16.2. Docker EE; 8.16.3. AWS ECR; 8.16.4. JFrog Artifactory; 8.17. A solução deve possuir integração com Microsoft Azure Container, Vmware Harbor e Sonatype Nexus para importar e analisar imagens; 8.18. A solução deve fornecer scanner em formato Docker para implementação local e análise de imagens sem a necessidade de envio destas para repositório remoto, fora do ambiente da CONTRATANTE; 8.19. A solução ser capaz de configurar políticas usando como condições: CVSS Score, CVEs específicos e Malware identificado; 8.20. Caso a condição da política seja verdadeira, a solução deve ser capaz de prevenir o pull destas para implementação ou identificar a falha de compliance das imagens para ação do time de segurança; 8.21. A solução deve permitir a criação de politicas especificas por repositório; 8.22. A solução deve prover integração com as seguintes plataformas de integração contínua: Bamboo, CircleCI, Codeship, Distelli, Drone.io, Jenkins, Shippable, Solano Labs, Travis CI, Wrecker e Kubernets; 8.23. A solução deverá ser capaz de analisar vulnerabilidades também na infraestrutura onde as imagens de container são executadas, tanto do sistema operacional quanto das aplicações que nele estão instaladas. Esta capacidade poderá ser: 8.23.1. Nativa da solução, desde que exista uma extensa compatibilidade de sistemas operacionais e aplicações relacionadas a container, algumas já explicitadas em itens anteriores, e já licenciada para uso; 8.23.2. Executada através de integração com terceiros, desde que toda a solução esteja licenciada para a CONTRATANTE;		

			Softawre de Referência: Tenable. Marca: SEM MARCA Fabricante: -		
33	SERVIÇO	2.0	Código: 33904021006000169 PLATAFORMA DE GESTÃO DE VULNERABILIDADE E AUDITORIA - CONFIGURAÇÃO 1. Para fins de cálculo, considera-se cada unidade deste item igual a 01 (unidade) 20 horas. 2. Antes de iniciar uma ordem de serviço, a Contratada, junto com a Contratante, deverá estimar o esforço para execução do serviço. 3. Compreende-se nesta etapa a instalação da solução a ser realizada no prazo de até 60 dias consecutivos, contados a partir do primeiro dia útil após a data da última assinatura do Contrato. 4. No momento anterior da assinatura do termo de recebimento provisório, a Contratada será requisitada para reunião de kick-off do projeto com a finalidade de montar o escopo de trabalho. Este escopo deverá conter as atividades, prazos e responsáveis da execução para acompanhamento da evolução do projeto. 5. Durante esta etapa, a equipe da Contratada deverá estar disponível nos horários de instalação definidos pela equipe da Contratante. 6. As atividades de instalação e configuração, de acordo com a necessidade, poderão ser executadas em horário comercial, período noturno ou final de semana. 7. Para esta etapa a Contratante disponibilizará a infraestrutura de hardware e software necessários e já existentes em seu ambiente, incluindo o ambiente virtualizado, sistema operacional, banco de dados, e outros, para a instalação e configuração da solução. 8. A montagem e instalação de todos os componentes que componham solução adquirida são de responsabilidade da Contratada. 9. Os componentes de software deverão estar na versão mais atualizada da solução. 10. A Contratada deverá listar a Contratante todas as informações necessárias para a correta instalação e configuração da solução. 11. A Contratante deverá providenciar as informações necessárias para a correta instalação da solução. 12. A Contratada prestará a transferência de conhecimento no formato hands-on para a equipe técnica da instituição na implantação da solução, ao longo das atividades de configuração, bem como durante atividades de suporte e customização.	82.661,56	165.323,12

			13. A Contratada deverá ao final da implantação elaborar documentação técnica dos procedimentos realizados durante a implantação. 14. A Contratada prestará o serviço de customização com a equipe técnica do contratante no decorrer da vigência do contrato oriundo do presente processo. As customizações são incrementos no uso da ferramenta que extrapolem a mera configuração dos recursos já existentes ou não se caracterizem como serviço de suporte. 15. Consultoria utilizando as melhoras práticas adotadas para as soluções. 16. A Contratante acompanhará e contabilizará a utilização de dias/horas. 17. A prestação dos serviços de instalação/configuração deverá ser realizada por profissionais especializados, que possuam certificação do fabricante da solução adquirida, que lhes confiram as competências necessárias para a realização dos respectivos serviços ou pelo próprio fabricante da solução ofertada. Marca: SEM MARCA Fabricante: -		
34	SERVIÇO	2.0	Código: 33904020001000004 PLATAFORMA DE GESTÃO DE VULNERABILIDADE E AUDITORIA - TREINAMENTO 1. Para fins de cálculo, considera-se cada unidade deste item igual a 01 banco de 40 horas, sendo dessas pelo menos, 12 horas para Treinamento e o saldo para suporte. 2. O treinamento deve conter ementa que contemple o conteúdo necessário para operação e manutenção dos itens deste projeto. 3. O treinamento será realizado no modelo tele presencial para até 4 participantes. 4. A Contratante disponibilizará os computadores a serem utilizados pelos participantes do treinamento; 5. A Contratada disponibilizará material didático em formato digital (PDF) aos participantes e quaisquer conteúdos e ferramentas adicionais que venham a ser necessárias; 6. Contratada deverá emitir um certificado de conclusão do treinamento. Marca: SEM MARCA Fabricante: -	27.958,06	55.916,12
				Total	R$ 1.101.419,84

EMPRESA (6)	RM SERVIÇOS TI LTDA

ENDEREÇO	**Rua Marechal Floriano, 654 sala 1011, centro. Bairro: CENTRO, Governador Valadares / SC CEP: 35010-140**
CNPJ	21.769.908/0001-34
TELEFONE/FAX	(33)3022-0102
REPRESENTANTE LEGAL	MIGUEL LEA
CPF REPRESENTANTE	104345726-75
Email	rmlicitacao@outlook.com

ITEM	UNID.	QTD.	ESPECIFICAÇÃO	Preço Unitário (R$)	Preço Total (R$)
2	LICENÇA	603.0	Código: 44904005001000093 LICENÇA EDUCACIONAL DE ACESSO REMOTO A WINDOWS SERVER 2022 - CAL -> LICENÇAS POR DISPOSITIVO. PACOTE COM 5 LICENÇAS. Marca: SEM MARCA Fabricante: -	250,00	150.750,00
4	LICENÇA	413.0	Código: 44904005001000082 LICENÇA COMERCIAL, PERPÉTUA, SOFTWARE MICROSOFT WINDOWS 10 PRO 64 BITS COEM - Pt Br. - Tipo de mídia: DVD; - Idioma: Português; - Tipo de licença: COEM; - Família Windows 10 Pro; - Versão Professional: 64-bits; - Uso em Notebook e PCs novos sem Windows, ou que nunca tenham tido Windows instalado. Marca: SEM MARCA Fabricante: -	650,00	268.450,00
13	LICENÇA	360.0	Código: 44904005001000077 LICENÇA EDUCACIONAL, PERPÉTUA, SOFTWARE WINDOWS 10 PRO - WinPro 10 SNGL Upgrd OLP NL Acdmc Windows Professional 10 Upgrade é uma licença perpétua do Microsoft Windows 10 Pro para uso de quem já tem uma versão anterior regularizada instalada nas máquinas e vai fazer apenas atualização. Marca: SEM MARCA Fabricante: -	420,00	151.200,00
22	LICENÇA	2.0	Código: 44904005001000096 LICENÇA OPEN DE VMWARE vCENTER SERVER STANDARD FOR vSPHERE (versão mais recente) - Acadêmica. Atualizações de segurança e suporte de, no mínimo, 3 (três) anos. Suporte no horário comercial (8 x 5), de segunda a sexta-feira, através de ligação telefônica	46.000,00	92.000,00

			gratuita (DDG); Marca: SEM MARCA Fabricante: -		
38	LICENÇA	6.0	Código: 44904005001000097 LICENÇA, PERPÉTUA, DE SOFTWARE SQL SERVER 2019 STANDARD ------- Licenciamento de direitos permanentes de uso de software para servidor - Microsoft®SQLSvrStandardCore AllLng License/SoftwareAssurancePack MVL 2Licenses CoreLic. Perpétua - Licença + Suporte e Atualização (SA) por 36 meses. Marca: SEM MARCA Fabricante: -	5.915,00	35.490,00
				Total	R$ 697.890,00

EMPRESA (7)			UHLIG & KOROVSKY TECNOLOGIA LTDA.		
ENDEREÇO			**TRAVESSA THEODORO KOCK, 30, SL 32,. Bairro: CENTRO, SÃO BENTO DO SUL / SC**		
CNPJ			17.011.419/0001-41		
TELEFONE/FAX			(47)32518200 (47)996633083		
REPRESENTANTE LEGAL			Carlos Alberto Cipriano Korovsky		
CPF REPRESENTANTE			031.269.749-02		
Email			contato@uktech.com.br		
ITEM	**UNID.**	**QTD.**	**ESPECIFICAÇÃO**	**Preço Unitário (R$)**	**Preço Total (R$)**
14	LICENÇA	100.0	Código: 33904019001000066 LICENÇA EDUCACIONAL, SAAS, DEEP FREEZE CLOUD - 12 MESES - SW.FR.DF.CL.BAS.EDU.S1Y Marca: SEM MARCA Fabricante: -	197,77	19.777,00
15	LICENÇA	1312.0	Código: 33904019001000067 LICENÇA EDUCACIONAL, SAAS, DEEP FREEZE CLOUD - 36 MESES - SW.FR.DF.CL.BAS.EDU.S3Y Marca: SEM MARCA Fabricante: -	219,97	288.600,64
				Total	R$ 308.377,64

VALOR TOTAL DA ATA	**R$ 2.511.297,92**