INSTITUTO FEDERAL Santa Catarina
Compras

INSTITUTO FEDERAL DE SANTA CATARINA
SISTEMA INTEGRADO DE PATRIMÔNIO, ADMINISTRAÇÃO E CONTRATOS
PRÓ-REITORIA DE DESENVOLVIMENTO INSTITUCIONAL
DIRETORIA DE TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO
EMITIDO EM 06/06/2022 09:10

RELATÓRIO DOS ITENS COM AS REQUISIÇÕES

Licitação: 23292.016668/2022-72 - PE 21005/2022 - REI
Gestora: 1100 - REI
Assunto: AQUISIÇÃO DE SOFTWARES PRONTOS E SUBSCRIÇÃO DE LICENÇAS SAAS E PAAS.
Tipo: MATERIAIS
Status: SETOR DE COMPRAS - EM ANALISE - SETOR COMPRAS

LISTA DOS ITENS DO PROCESSO

Item	Especificação do Item / Requisição	Unidade / Unidade Gestora	Unid.	Marca	Proposta	Quant. Int.	Quant. Ext.	Quant. Total	Valor Unit.	Total
1	**339040190010000014 - CATMAT: 0**		**LICENÇA**	--	-- --	**385**	**0**	**385**	--	--
	DEEP FREEZE EDUCACIONAL - SAAS									
	DEEP FREEZE EDUCACIONAL - SAAS Software para restauração de sistema operacional nas plataformas windows 7, 8.1, 10 e 11. Licença SaaS - Subscrição de 3 anos com suporte e atualização									
	2921/2022	11003301	COORDENADORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - CCO			235				
	2938/2022	1101260301	COORDENADORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - RAU			150				
2	**449040050010000093 - CATMAT: 0**		**LICENÇA**	--	-- --	**603**	**0**	**603**	--	--
	LICENÇA CAL DE ACESSO REMOTO A WINDOWS SERVER 2022									
	LICENÇA CAL DE ACESSO REMOTO A WINDOWS SERVER 2022 - PACOTE COM 5 LICENÇAS POR DISPOSITIVO									
	2727/2022	1101100303	COORDENADORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - JLE			600				
	2844/2022	112101	COORDENADORIA DE COMPRAS - CAN			1				
	2896/2022	1101180303	COORDENADORIA DE PLANEJAMENTO, MATERIAIS E FINANÇAS - GAS			1				
	3015/2022	1101300303	COORDENADORIA DE ORÇAMENTO E FINANÇAS - SCA			1				
3	**449040050010000071 - CATMAT: 27472**		**LICENÇA**	--	-- --	**7**	**0**	**7**	--	--
	LICENÇA COMERCIAL, PERPÉTUA, SOFTWARE ASC TIME TABLES PREMIUM									
	LICENÇA COMERCIAL, PERPÉTUA, SOFTWARE ASC TIME TABLES PREMIUM - Software para geração de horários escolares.									
	2104/2022	1101080302	COORDENADORIA DE MATERIAIS E FINANÇAS - SJE			1				
	2245/2022	11010702	DIRETORIA DE ENSINO - FLN			1				
	2727/2022	1101100303	COORDENADORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - JLE			2				
	2817/2022	110040	DEPARTAMENTO DE ADMINISTRAÇÃO - SMO			1				
	2837/2022	1101200303	COORDENADORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - CRI			1				
	2844/2022	112101	COORDENADORIA DE COMPRAS - CAN			1				
4	**449040050010000082 - CATMAT: 26077**		**LICENÇA**	--	-- --	**413**	**0**	**413**	--	--
	LICENÇA COMERCIAL, PERPÉTUA, SOFTWARE MICROSOFT WINDOWS 10 PRO 64 BITS COEM.									
	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.									
	2175/2022	11011202	DIRETORIA DE ENSINO, PESQUISA E EXTENSÃO - CTE			3				
	2344/2022	11010706	ASSESSORIA DE COMUNICAÇÃO E MARKETING - FLN			5				
	2727/2022	1101100303	COORDENADORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - JLE			40				
	2813/2022	11004101	COORDENADORIA DE COMPRAS, MATERIAIS E FINANÇAS - TUB			110				
	2817/2022	110040	DEPARTAMENTO DE ADMINISTRAÇÃO - SMO			5				
	2841/2022	1100690101	COORDENADORIA DE COMPRAS, ORÇAMENTOS E FINANÇAS - PHB			75				
	3017/2022	110107020210	COORDENADORIA MESTRADO PROFISSIONAL PROTEÇÃO RADIOLÓGICA - FLN			25				
	3121/2022	111702	DIRETORIA DE TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO			150				
5	**449040050010000089 - CATMAT: 0**		**LICENÇA**	--	-- --	**22**	**0**	**22**	--	--
	LICENÇA COMERCIAL, PERPÉTUA, SOFTWARE OFFICE 2021									
	LICENÇA COMERCIAL, PERPÉTUA, SOFTWARE OFFICE 2021 - Office Home & Business 2021; • Compra única para 1 PC ou Mac; • Versões 2021 clássicas do Word, Excel, PowerPoint e Outlook; • Suporte da Microsoft incluído pelos primeiros 60 dias sem custo adicional; • Compatível com Windows 11, Windows 10 ou macOS; • Funciona com o Microsoft Teams; • Licenciado para uso comercial e doméstico.									
	2165/2022	110079	DIREÇÃO-GERAL DO CAMPUS ITAJAÍ			6				
	2175/2022	11011202	DIRETORIA DE ENSINO, PESQUISA E EXTENSÃO - CTE			1				
	2727/2022	1101100303	COORDENADORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - JLE			10				
	2919/2022	1101070203	DEPARTAMENTO ACADÊMICO DE CONSTRUÇÃO CIVIL - FLN			1				
	3225/2022	110107030204	COORDENADORIA DE ENGENHARIA - FLN			4				
6	**339040190010000054 - CATMAT: 26077**		**LICENÇA**	--	-- --	**9**	**0**	**9**	--	--
	LICENÇA COMERCIAL, SAAS, AUTOCAD LT 2021 - 36 MESES									
	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;									
	2182/2022	110107030204	COORDENADORIA DE ENGENHARIA - FLN			2				
	2247/2022	1101020301	COORDENADORIA DE ENGENHARIA			4				

TOTAL LICITADO: R$ 0,00

LISTA DOS ITENS DO PROCESSO

Item	Especificação do Item		Unid.	Marca	Proposta	Quant. Int.	Quant. Ext.	Quant. Total	Valor Unit.	Total
	Requisição	Unidade Unidade Gestora								
	2726/2022	1101100303	COORDENADORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - JLE			2				
	2912/2022	1190	DEPARTAMENTO DE ADMINISTRAÇÃO - JAR			1				
7	**339040190010000051 - CATMAT: 26077**		**UNIDADE**	**--**	**--** --	**4**	**0**	**4**	**--**	**--**
	LICENÇA COMERCIAL, SAAS, SOFTWARE STREAM YARD - 12 MESES									
	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.									
	2105/2022	1101080302	COORDENADORIA DE MATERIAIS E FINANÇAS - SJE			1				
	2800/2022	11004101	COORDENADORIA DE COMPRAS, MATERIAIS E FINANÇAS - TUB			1				
	2897/2022	1101180303	COORDENADORIA DE PLANEJAMENTO, MATERIAIS E FINANÇAS - GAS			1				
	3018/2022	110107020210	COORDENADORIA MESTRADO PROFISSIONAL PROTEÇÃO RADIOLÓGICA - FLN			1				
8	**449040050010000091 - CATMAT: 0**		**LICENÇA**	**--**	**--** --	**9**	**0**	**9**	**--**	**--**
	LICENÇA DE SO WINDOWS SERVER 2022 STANDARD 16 CORE - VITALÍCIA									
	LICENÇA DE SO WINDOWS SERVER 2022 STANDARD 16 CORE - VITALÍCIA Marca: Microsoft Licenciamento: ESD Idioma: Português Licenciamento para: Uso corporativo Núcleos: Até 16 - 32bits ou 64bits									
	2727/2022	1101100303	COORDENADORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - JLE			4				
	2844/2022	112101	COORDENADORIA DE COMPRAS - CAN			2				
	2896/2022	1101180303	COORDENADORIA DE PLANEJAMENTO, MATERIAIS E FINANÇAS - GAS			1				
	3015/2022	1101300303	COORDENADORIA DE ORÇAMENTO E FINANÇAS - SCA			1				
	3121/2022	111702	DIRETORIA DE TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO			1				
9	**449040050010000078 - CATMAT: 27472**		**LICENÇA**	**--**	**--** --	**30**	**0**	**30**	**--**	**--**
	LICENÇA EDUCACIONAL, PERPÉTUA, SOFTWARE FACTORY I/O									
	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, 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.									
	2818/2022	11004101	COORDENADORIA DE COMPRAS, MATERIAIS E FINANÇAS - TUB			15				
	2908/2022	1101130304	COORDENADORIA DE MATERIAIS E FINANÇAS - ARU			15				
10	**449040050010000076 - CATMAT: 27472**		**LICENÇA**	**--**	**--** --	**14**	**0**	**14**	**--**	**--**
	LICENÇA EDUCACIONAL, PERPÉTUA, SOFTWARE SSCNC									
	LICENÇA EDUCACIONAL, PERPÉTUA, SOFTWARE SSCNC - Recursos de programação e operação que possibilitam o aprendizado e a simulação de programas CNC através de um PC. - TREINAMENTO: Para a compra acima de 20 licenças, está incluso um treinamento para até 6 pessoas in loco no Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina, o treinamento deverá ser realizado em até 90 dias no máximo após confirmação do pedido, os custos de deslocamento, hospedagem e alimentação do técnico serão por conta do contratante.									
	2908/2022	1101130304	COORDENADORIA DE MATERIAIS E FINANÇAS - ARU			14				
11	**449040050010000077 - CATMAT: 27456**		**LICENÇA**	**--**	**--** --	**360**	**0**	**360**	**--**	**--**
	LICENÇA EDUCACIONAL, PERPÉTUA, SOFTWARE WINDOWS 10 PRO									
	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.									
	2727/2022	1101100303	COORDENADORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - JLE			50				
	2812/2022	11003001	DIRETORIA DO CENTRO DE FORMAÇÃO E EDUCAÇÃO A DISTÂNCIA (EAD) (11.00.30.01)			20				
	2813/2022	11004101	COORDENADORIA DE COMPRAS, MATERIAIS E FINANÇAS - TUB			110				
	2817/2022	110040	DEPARTAMENTO DE ADMINISTRAÇÃO - SMO			5				
	3015/2022	1101300303	COORDENADORIA DE ORÇAMENTO E FINANÇAS - SCA			25				
	3121/2022	111702	DIRETORIA DE TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO			150				
12	**339040190010000066 - CATMAT: 0**		**LICENÇA**	**--**	**--** --	**100**	**0**	**100**	**--**	**--**
	LICENÇA EDUCACIONAL, SAAS, DEEP FREEZE CLOUD - 12 MESES									
	LICENÇA EDUCACIONAL, SAAS, DEEP FREEZE CLOUD - 12 MESES - SW.FR.DF.CL.BAS.EDU.S1Y									
	2757/2022	1100680305	COORDENADORIA CURSO TÉCNICO INFORMÁTICA PARA INTERNET - SLO			100				

TOTAL LICITADO: R$ 0,00

LISTA DOS ITENS DO PROCESSO

Item	Especificação do Item		Unid.	Marca	Proposta	Quant. Int.	Quant. Ext.	Quant. Total	Valor Unit.	Total
	Requisição	Unidade Unidade Gestora								
13	**339040190010000067 - CATMAT: 0**		**LICENÇA**	**--**	**--** **--**	**1162**	**0**	**1162**	**--**	**--**
	LICENÇA EDUCACIONAL, SAAS, DEEP FREEZE CLOUD - 36 MESES									
	LICENÇA EDUCACIONAL, SAAS, DEEP FREEZE CLOUD - 36 MESES - SW.FR.DF.CL.BAS.EDU.S3Y									
	2726/2022	1101100303	COORDENADORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - JLE			250				
	2800/2022	11004101	COORDENADORIA DE COMPRAS, MATERIAIS E FINANÇAS - TUB			284				
	2822/2022	110040	DEPARTAMENTO DE ADMINISTRAÇÃO - SMO			41				
	2825/2022	119101	COORDENADORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - XXE			136				
	2840/2022	1100690101	COORDENADORIA DE COMPRAS, ORÇAMENTOS E FINANÇAS - PHB			300				
	2918/2022	1101070203	DEPARTAMENTO ACADÊMICO DE CONSTRUÇÃO CIVIL - FLN			1				
	2938/2022	1101260301	COORDENADORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - RAU			150				
14	**339040190010000010 - CATMAT: 26077**		**LICENÇA**	**--**	**--** **--**	**5**	**0**	**5**	**--**	**--**
	LICENÇA EDUCACIONAL, SAAS, SOFTWARE ADOBE CREATIVE CLOUD - 12 MESES									
	LICENÇA EDUCACIONAL, SAAS, SOFTWARE ADOBE CREATIVE CLOUD - 12 MESES Aquisição de licença (educacional) ADOBE CREATIVE CLOUD em Português. Licença Adobe Creative Cloud for teams All Apps ALL Multiple Platforms Team - Licensing Subscription New Multi Latin American Languages Monthly Education Device license 1 Month Device - Subscrição de 12 meses - ITEM PASSÍVEL DE CONTRATAÇÃO VIA ASSINATURA DE INSTRUMENTO DE CONTRATO									
	2357/2022	11010503	ASSESSORIA DA PRÓ-REITORIA DE EXTENSÃO E RELAÇÕES EXTERNAS			3				
	2895/2022	110107020607	COORDENADORIA CURSO ENGENHARIA MECATRÔNICA - FLN			1				
	2907/2022	1101130304	COORDENADORIA DE MATERIAIS E FINANÇAS - ARU			1				
15	**339040190010000040 - CATMAT: 26077**		**LICENÇA**	**--**	**--** **--**	**79**	**0**	**79**	**--**	**--**
	LICENÇA EDUCACIONAL, SAAS, SOFTWARE ADOBE CREATIVE CLOUD 36 MESES									
	LICENÇA EDUCACIONAL, SAAS, SOFTWARE ADOBE CREATIVE CLOUD - 36 MESES - Creative Cloud é uma coleção de mais de 20 aplicativos e serviços para desktop e dispositivos móveis para fotografia, design, vídeo e Web; Aplicativos inclusos: Photoshop, Lightroom, Illustrator, Premiere Pro, InDesign, Adobe XD, Fresco, Premiere Rush, After Effects, Dimension, Acrobat Pro, Dreamweaver, Animate, Audition, Lightroom Classic, Character Animator, Spark, Bridge, Media Encoder, InCopy, Prelude, Substance, Story Plus e Fuse (beta).									
	2174/2022	11011202	DIRETORIA DE ENSINO, PESQUISA E EXTENSÃO - CTE			1				
	2461/2022	11010706	ASSESSORIA DE COMUNICAÇÃO E MARKETING - FLN			1				
	2726/2022	1101100303	COORDENADORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - JLE			5				
	2783/2022	1101040901	DEPARTAMENTO DE EDUCAÇÃO A DISTÂNCIA			5				
	2840/2022	1100690101	COORDENADORIA DE COMPRAS, ORÇAMENTOS E FINANÇAS - PHB			30				
	2898/2022	1101180303	COORDENADORIA DE PLANEJAMENTO, MATERIAIS E FINANÇAS - GAS			32				
	3167/2022	11003001	DIRETORIA DO CENTRO DE FORMAÇÃO E EDUCAÇÃO A DISTÂNCIA (EAD) (11.00.30.01)			5				
16	**339040190010000041 - CATMAT: 26077**		**LICENÇA**	**--**	**--** **--**	**22**	**0**	**22**	**--**	**--**
	LICENÇA EDUCACIONAL, SAAS, SOFTWARE ADOBE ILLUSTRATOR 12 MESES									
	LICENÇA EDUCACIONAL, SAAS, SOFTWARE ADOBE ILLUSTRATOR 12 MESES									
	2895/2022	110107020607	COORDENADORIA CURSO ENGENHARIA MECATRÔNICA - FLN			20				
	2923/2022	110107020109	ASSESSORIA DE ARTES - FLN			2				
17	**339040190010000043 - CATMAT: 26077**		**LICENÇA**	**--**	**--** **--**	**2**	**0**	**2**	**--**	**--**
	LICENÇA EDUCACIONAL, SAAS, SOFTWARE ADOBE PHOTOSHOP 12 MESES									
	LICENÇA EDUCACIONAL, SAAS, SOFTWARE ADOBE PHOTOSHOP 12 MESES									
	2923/2022	110107020109	ASSESSORIA DE ARTES - FLN			2				
18	**339040190010000050 - CATMAT: 26077**		**LICENÇA**	**--**	**--** **--**	**6**	**0**	**6**	**--**	**--**
	LICENÇA EDUCACIONAL, SAAS, SOFTWARE SKETCHUP 12 MESES									
	LICENÇA EDUCACIONAL, SAAS, SOFTWARE SKETCHUP 12 MESES - Software próprio para a criação de modelos em 3D no computador.									
	2247/2022	1101020301	COORDENADORIA DE ENGENHARIA			3				
	2726/2022	1101100303	COORDENADORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - JLE			2				
	2907/2022	1101130304	COORDENADORIA DE MATERIAIS E FINANÇAS - ARU			1				
19	**449040050010000096 - CATMAT: 0**		**LICENÇA**	**--**	**--** **--**	**2**	**0**	**2**	**--**	**--**
	LICENÇA OPEN DE VMWARE VCENTER SERVER STANDARD FOR VSPHERE									
	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 gratuita (DDG);									
	2727/2022	1101100303	COORDENADORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - JLE			1				
	3121/2022	111702	DIRETORIA DE TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO			1				
20	**449040050010000094 - CATMAT: 0**		**LICENÇA**	**--**	**--** **--**	**20**	**0**	**20**	**--**	**--**

TOTAL LICITADO: R$ 0,00

LISTA DOS ITENS DO PROCESSO

Item	Especificação do Item	Requisição	Unidade / Unidade Gestora	Unid.	Marca	Proposta	Quant. Int.	Quant. Ext.	Quant. Total	Valor Unit.	Total
	LICENÇA PARA SOFTWARE DE USO EM DISCIPLINAS DE ESTRUTURAS LICENÇA PARA SOFTWARE DE USO EM DISCIPLINAS DE ESTRUTURAS - LICENÇA PERPÉTUA Características mínimas: Contempla análise do tipo: 1. Primeira ordem e segunda ordem. 2. Grandes deslocamentos, incluindo estruturas e membranas tensionadas. 3. Análise pós-crítica. 4. Análise estática e dinâmica, espectral modal ou terremoto acelerogramas, " pushover" ou cargas equivalentes bem. 5. Análise vibracional; 6. Análise de estabilidade. 7. Análise elástico linear, não linear, plástico, termo elástica e fissuração. Com a possibilidade de realizar 1. Cálculo linear e não linear. Com elementos do tipo barra não linear, suportes não lineares e materiais não lineares. 2. Cálculo de flambagem com imperfeições. 3. Parametrização de estruturas e utilização como blocos paramétricos. 4. Gerar linhas e superfícies de influência. 5. Cálculo de conexões em aço e madeira. 6. Importação e exportação para outros softwares ao adotar a metodologia BIM. Estruturas do tipo 1. Estruturas de concreto armado e protendido, aço, alumínio, madeira, vidro, alvenaria estrutural e outros materiais; 2. Dimensionamento mecânico de tubulações industriais; 3. Pontes e passarelas; 4. Guindastes, vigas de ponte rolantes, equipamentos fixos e móveis; 5. Torres e estruturas estaiadas ou autoportantes; 6. Membrana tensionadas. 7. Comportas hidráulicas. 8. Túnel de vento digital usando mecânica de fluidos computacional e elementos finitos. Nos segmentos de: 1. Engenharia Civil; 2. Engenharia Mecânica; 3. Engenharia Naval; 4. Engenharia aeronáutica. REFERÊNCIA: Dlubal RFEM5	3015/2022	1101300303	COORDENADORIA DE ORÇAMENTO E FINANÇAS - SCA				20				
21	**449040050010000090 - CATMAT: 0** **LICENÇA PERPÉTUA DO SOFTWARE REMARK OFFICE OMR** LICENÇA PERPÉTUA DO SOFTWARE REMARK OFFICE OMR - Software para processamento de cartões resposta (exames de classificação, vestibulares, concursos, etc); - Licença Perpétua - 1º ano de manutenção e suporte (updates e upgrades) - Serviços adicionais inclusos: um treinamento remoto e o primeiro layout folha de respostas/gabarito;	2209/2022	1101750101	DEPARTAMENTO DE INGRESSO	**LICENÇA**	-- -- --	**1**	**0**	**1**	--	--
22	**339040190010000063 - CATMAT: 0** **LICENÇA SAAS - ACADÊMICA/EDUCACIONAL - DE SOFTWARE PARA CRIAÇÃO DE MAPAS MENTAIS** LICENÇA SAAS - ACADÊMICA/EDUCACIONAL - DE SOFTWARE PARA 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; 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	2783/2022	1101040901	DEPARTAMENTO DE EDUCAÇÃO A DISTÂNCIA	**ANUAL**	-- -- --	**22**	**0**	**22**	--	--
		3167/2022	11003001	DIRETORIA DO CENTRO DE FORMAÇÃO E EDUCAÇÃO A DISTÂNCIA (EAD) (11.00.30.01)			6				
		3195/2022	11011602	DEPARTAMENTO DE ENSINO, PESQUISA E EXTENSÃO - ITJ			10				
23	**339040190010000064 - CATMAT: 0** **LICENÇA SAAS - ACADÊMICA/EDUCACIONAL - PARA ACESSO A PLATAFORMA DE CRIAÇÃO DE CONTEÚDOS DINÂMICOS** LICENÇA SAAS - ACADÊMICA/EDUCACIONAL - PARA 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!	2783/2022	1101040901	DEPARTAMENTO DE EDUCAÇÃO A DISTÂNCIA	**ANUAL**	-- -- --	**27**	**0**	**27**	--	--
		3167/2022	11003001	DIRETORIA DO CENTRO DE FORMAÇÃO E EDUCAÇÃO A DISTÂNCIA (EAD) (11.00.30.01)			6				
		3195/2022	11011602	DEPARTAMENTO DE ENSINO, PESQUISA E EXTENSÃO - ITJ			15				
24	**339040190010000065 - CATMAT: 0** **LICENÇA SAAS - ACADÊMICA/EDUCACIONAL - PARA ACESSO A PLATAFORMA DE CRIAÇÃO DE ENQUETES** LICENÇA SAAS - ACADÊMICA/EDUCACIONAL - PARA ACESSO A PLATAFORMA DE CRIAÇÃO DE ENQUETES Características mínimas: 1. Apresentações ativas - Ilimitado; 2. Tamanho do público - Ilimitado; 3. Slides de conteúdo - Ilimitado; 4. Slides por apresentação - Ilimitado; 5. Quiz por apresentação - Ilimitado; 6. Obter perguntas do público; 7. Importar apresentações; 8. Tornar apresentações privadas; 9. Colaborar em apresentações; 10. Layouts rápidos; 11. Customização de cores; 12. Temas customizados; 13. Branding da empresa; 14. Adicionar logotipo; 15. Criar templates de apresentações; 16. Criar grupos; 17. Análise da área de trabalho; 18. Exportar Imagens e PDF; 19. Exportar Excel; 20. Adicionar Formulários Rápidos; 21. Respostas em um dispositivo; 22. Privacidade e controle; 23. Adicionar e remover membros da equipe automaticamente; 24. Configurações de acesso; 25. Níveis de acesso; 26. Suporte online por chat ou email; 27. Plano ANUAL; 28. Licença por usuário; Referência: Mentimeter	2783/2022	1101040901	DEPARTAMENTO DE EDUCAÇÃO A DISTÂNCIA	**ANUAL**	-- -- --	**27**	**0**	**27**	--	--
		3167/2022	11003001	DIRETORIA DO CENTRO DE FORMAÇÃO E EDUCAÇÃO A DISTÂNCIA (EAD) (11.00.30.01)			6				
		3195/2022	11011602	DEPARTAMENTO DE ENSINO, PESQUISA E EXTENSÃO - ITJ			15				
25	**339040190010000016 - CATMAT: 0** **LICENÇA SAAS - SOFTWARE PARA GERENCIAMENTO DE SISTEMAS OPERACIONAIS - 36 MESES** LICENÇA SAAS - SOFTWARE PARA GERENCIAMENTO DE SISTEMAS OPERACIONAIS - 36 MESES CARACTERÍSTICAS: ● Criação e gerenciamento de discos virtuais armazenados em repositório central e sincronizados com repositórios locais em área criptografada e invisível (no HD de cada PC cliente), utilizando protocolo otimizado de transferência com cópia diferencial; ● Estrutura hierárquica de armazenamento de imagens de discos virtuais em camadas, contendo diferentes sistemas Windows e/ou Linux e/ou diferentes conjuntos de softwares/configurações, permitindo alterações e atualizações centralizadas, e disponibilização dinâmica de discos virtuais em qualquer camada para qualquer estação da rede; ● Compatível com computadores padrão x86 32/64bits com interface de rede com suporte a boot PXE, com processador e memória adequados aos requisitos das versões de sistemas operacionais a serem utilizados por meio dos discos virtuais; ● Montagem e boot de discos virtuais localmente em cada estação, com acesso transparente aos recursos nativos de hardware de cada PC, sem uso de máquinas virtuais ou hipervisores, com operação sem dependência de recursos de processamento do servidor; ● Instalação do gerenciador de boot local via PXE (boot de rede) ou via USB (para clientes remotos); ● Criação de snapshots (imagem do disco em determinado ponto no tempo) salvos no servidor ou em cache local (no HD de cada PC cliente), com opção de snapshot automático quando a imagem de disco virtual é iniciada pela primeira vez; ● Permite a restauração de discos virtuais ao snapshot gravado, independentemente do seu conteúdo (sistema operacional Windows, Linux, ou disco de dados) de forma manual, programada, ou automaticamente a cada reboot; ● Permite configuração de senha de acesso ao gerenciador de discos virtuais em cada PC cliente, e também diferentes senhas de acesso para cada imagem de disco virtual; ● Controle centralizado de autorização de boot pelo endereço MAC do cliente, com a opção de permitir boot de estações sem conexão ao servidor pelo período de até 14 dias; ● Suporte a configuração de rede específica para cada grupo de PCs clientes, via DHCP externo ou diferentes grupos de IPs providos pelo próprio servidor da solução; ● Acionamento de bloqueio de periféricos e portas de acesso (USB e outros).	2726/2022	1101100303	COORDENADORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - JLE	**LICENÇA**	-- -- --	**225**	**0**	**225**	--	--
26	**339040190010000062 - CATMAT: 0** **LICENÇA SOFTWARE REMARK OFFICE OMR - SUBSCRIÇÃO** LICENÇA SOFTWARE REMARK OFFICE OMR - SUBSCRIÇÃO - Pagamento anual; - Sem limite processamento de cartões resposta enquanto a licença estiver ativa; - Incluso manutenção e suporte; - Serviços adicionais inclusos: um treinamento remoto e o primeiro layout folha de respostas/gabarito;	2218/2022	11010401	DIRETORIA DE ENSINO	**LICENÇA**	-- -- --	**1**	**0**	**1**	--	--
										TOTAL LICITADO:	**R$ 0,00**
27	**449040050010000095 - CATMAT: 0**				**LICENÇA**	-- -- --	**9**	**0**	**9**	--	--

LISTA DOS ITENS DO PROCESSO

Item	Especificação do Item		Unid.	Marca	Proposta	Quant. Int.	Quant. Ext.	Quant. Total	Valor Unit.	Total
	Requisição	Unidade Unidade Gestora								

LICENCIAMENTO ACADÊMICO VMWARE VSPHERE ENTERPRISE PLUS - 2022
LICENCIAMENTO ACADÊMICO VMWARE VSPHERE ENTERPRISE PLUS -> Licenciamento Acadêmico VMware vSphere Enterprise Plus para 1 (um) processador com suporte técnico atendido diretamente pela VMware na modalidade Basic (12x5) e atualização pelo período de 36 meses;

2727/2022	1101100303	COORDENADORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - JLE	3
3121/2022	111702	DIRETORIA DE TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO	6

28	**339040190010000061 - CATMAT: 0**	**SERVIÇO**	**--**	**--**	**--**	**2**	**0**	**2**	**--**	**--**

PLATAFORMA DE GESTÃO DE MÍDIAS SOCIAIS
Plataforma de Gestão de Mídias Sociais-->Funcionalidades mínimas: Agendamento de posts com customizações; Ferramentas para criação de posts; Gestão de mensagens - SAC social; Responder comentários de seguidores; Ads (Impulsionar posts); Relatórios de redes sociais (ilimitado); Workflow (Gestão do fluxo de trabalho); Landing Pages e captação de leads; Insights para otimização; Calendário de posts; Monitoramento de concorrentes; Aprovação de posts simplificada; Suporte online (chat); Múltiplos usuários (ilimitado); Páginas de Link na bio; Acesso para 1 perfil. Plataforma de referência: mLabs.

2357/2022	11010503	ASSESSORIA DA PRÓ-REITORIA DE EXTENSÃO E RELAÇÕES EXTERNAS	1
2622/2022	1101280211	ASSESSORIA DO DEPARTAMENTO DE ENSINO, PESQUISA E EXTENSÃO - URP	1

29	**339040190010000070 - CATMAT: 0**	**LICENÇA**	**--**	**--**	**--**	**3**	**0**	**3**	**--**	**--**

PLATAFORMA DE GESTÃO DE VULNERABILIDADE E AUDITORIA
PLATAFORMA 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. 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 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 “Job” 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;

TOTAL LICITADO: R$ 0,00

LISTA DOS ITENS DO PROCESSO

Item	Especificação do Item		Unid.	Marca	Proposta	Quant. Int.	Quant. Ext.	Quant. Total	Valor Unit.	Total
	Requisição	Unidade Unidade Gestora								

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

TOTAL LICITADO: R$ 0,00

LISTA DOS ITENS DO PROCESSO

Item	Especificação do Item	Requisição	Unidade	Unidade Gestora	Unid.	Marca	Proposta	Quant. Int.	Quant. Ext.	Quant. Total	Valor Unit.	Total
	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;										
		3124/2022	111702		DIRETORIA DE TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO			3				
30	339040210060001 69 - CATMAT: 0				SERVIÇO	--	--	--	3	0	3	--	--
	PLATAFORMA DE GESTÃO DE VULNERABILIDADE E AUDITORIA - CONFIGURAÇÃO												
	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 pela 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. 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.										
		3125/2022	111702		DIRETORIA DE TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO			3				
31	339040200010000 04 - CATMAT: 0				SERVIÇO	--	--	--	3	0	3	--	--
	PLATAFORMA DE GESTÃO DE VULNERABILIDADE E AUDITORIA - TREINAMENTO												
	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.										
		3126/2022	111702		DIRETORIA DE TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO			3				
32	339040210040001 64 - CATMAT: 0				LICENÇA	--	--	--	5	0	5	--	--
	RENOVAÇÃO DA VALIDADE TÉCNICA DO ASC TIMETABLES												
	RENOVAÇÃO DA VALIDADE TÉCNICA DO ASC TIMETABLES A Renovação da Validade Técnica inclui: - Validade Técnica (Lei Federal 9609/98 – Garantia e Serviços Técnicos) por 1 ano. - Suporte gratuito por e-mail e telefone. - Novas versões e correções. - aSc TimeTables Online via WEB para qualquer browser. - Permissão para uso gratuito do EDUPAGE APP.										
		2726/2022	1101100303		COORDENADORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - JLE			2				
		3042/2022	1101080302		COORDENADORIA DE MATERIAIS E FINANÇAS - SJE			1				
		3045/2022	110079		DIREÇÃO-GERAL DO CAMPUS ITAJAÍ			2				
33	339040190010000 68 - CATMAT: 0				LICENÇA	--	--	--	96	0	96	--	--
	RENOVAÇÃO DE ASSINATURA - SOFTWARE PHANTOSYS LITE - 36 MESES												
	RENOVAÇÃO DE ASSINATURA - SOFTWARE PHANTOSYS LITE - 36 MESES												
		2532/2022	1101070303		DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - FLN			70				
		2726/2022	1101100303		COORDENADORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - JLE			26				
34	339040210040000 21 - CATMAT: 0				LICENÇA	--	--	--	2	0	2	--	--
	RENOVAÇÃO DO LICENCIAMENTO ACADÊMICO VMWARE VCENTER SERVER STANDARD												
	RENOVAÇÃO DO LICENCIAMENTO ACADÊMICO VMWARE VCENTER SERVER STANDARD -> Renovação do licenciamento Acadêmico VMware vCenter Server Standard para 1 (uma) instancia com suporte técnico na modalidade 12x5 atendido diretamente pela VMware e garantia válida fazendo pro rata com o licenciamento que será adquirido.										
		3125/2022	111702		DIRETORIA DE TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO			2				
35	339040190010000 69 - CATMAT: 0				ANUAL	--	--	--	1	0	1	--	--
	SERVIÇO DE ACESSO A PLATAFORMA DE GESTÃO TRIBUTÁRIA												
	SERVIÇO DE ACESSO A PLATAFORMA DE GESTÃO TRIBUTÁRIA Características Mínimas: 1. Plataforma on-line, com acesso por usuário/senha; 2. Acesso para até 21 usuários; 3. Acesso a artigos publicados; 4. Acesso à legislação selecionada; 5. Acesso aos vídeos; 6. Consultas por mês ilimitadas; 7. Geração de relatório PDF das consultas; 8. Simulador de Cálculo; 9. Consulta de legislação por município; 10. LICENÇA ANUAL 11. REFERÊNCIA: sistema web GESTÃO TRIBUTÁRIA										

TOTAL LICITADO: R$ 0,00

LISTA DOS ITENS DO PROCESSO

Item	Especificação do Item		Unid.	Marca	Proposta	Quant. Int.	Quant. Ext.	Quant. Total	Valor Unit.	Total
	Requisição	Unidade Unidade Gestora								
	2286/2022	1101020101	DEPARTAMENTO DE ORÇAMENTO E EXECUÇÃO FINANCEIRA			1				
36	**339040210150001 65 - CATMAT: 0**		**SERVIÇO**	**--**	**--**	**--**	**2**	**0**	**2**	**--**	**--**

SERVIÇO DE LEVANTAMENTO DE AMBIENTE - SEGURANÇA CIBERNÉTICA

SERVIÇO DE LEVANTAMENTO DE AMBIENTE - SEGURANÇA CIBERNÉTICA 1. O serviço a ser contratado deverá compreender o levantamento do ambiente, baseado em metodologias e estratégias com o objetivo de identificar e classificar riscos e vulnerabilidades trazendo respostas ao negócio para o aumento da maturidade da segurança da informação da organização. 2. Deve ser realizada uma auditoria de segurança da informação, seguindo normas e boas práticas, avaliando a política de segurança da informação e sua eficácia. Vedem ser avaliados procedimentos com aderência a Norma ISO 27001 como: processos de backups, gestão de incidentes, riscos e vulnerabilidades. Serviços a serem executados: 1 - Teste de intrusão; 2 - Avaliação de vulnerabilidades 3 - Testes de aplicações web e mobile; 4 - Avaliação de segurança de infraestrutura de rede; 5 - Avaliação de infraestrutura física; 6 - Engenharia social; 7 - Teste da eficácia das ferramentas de segurança; 8 - Análise dos processos de TIC; 9 - Simulação de furto; 10- Reteste. 1 - Teste de intrusão O teste de intrusão visa encontrar potenciais vulnerabilidades: 1.1 - TESTE DE APLICAÇÕES PÚBLICAS E/OU INTERNAS A. Análise de Vulnerabilidades: A.1. IPs Válidos: A.1.a. DMZ; A.1.b. Cloud; A.1.c. Aplicações Web: A.1.c.1 Proprietárias; A.1.c.2. Terceiras (Termo de aceite); A.1.d. Intranet; A.1.e. Softwares Internos; B. Teste de exploração manual das brechas: B.1. Validação de vulnerabilidades; B.2. Descarte de falsos positivos; C. Identificação de falsos negativos; D. Escalação de privilégio: D.1. Windows; D.2. Linux; D.3. Roteadores; D.4. Outros sistemas; E. Extração de dados: E.1. Dados sensíveis; E.1.a. Dados financeiros; E.1.b. Dados confidenciais; E.1.c. Dados pessoais; 1.2 - ANÁLISE DE CÓDIGO ESTÁTICO A análise de código estático consiste em encontrar vulnerabilidades no código fonte de aplicação, tanto como más práticas de código e bibliotecas desatualizadas. 1.3 - TESTES INTERNO A. Topologia de rede; B. Avaliação de Vulnerabilidades; B.1 Estações de trabalho; B.2 Servidores: B.2.1. LDAP; B.2.2. Servidores de arquivos; B.2.3. Servidores de impressão e impressoras; B.2.4. Servidores de aplicação; B.2.5. Servidores de e-mail; B.3. VoIP; B.4. Firewall: B.4.1. Teste de controle de aplicação; B.4.2. Teste de web filter; B.4.3. Teste de efetividade de UTM; C. Teste de exploração manual das brechas: C.1. Validação de vulnerabilidades; C.2. Descarte de falsos positivos; C.3. Identificação de falsos negativos; C.4. Efetividade de ferramentas de segurança: C.4.1. AV; C.4.2. Firewall C.4.3. Entre outros;; C.5. Análise de falhas em arquitetura de autenticação (Pass-The-Hash). D. Escalação de privilégio: D.1. Windows; D.2. Linux; D.3. Roteadores; D.4. Outros sistemas. E. Extração de dados: E.1. Dados sensíveis: E.1.1. Dados financeiros; E.1.2. Dados confidenciais; E.1.3. Dados pessoais; E.1.4. Entre outros. 2 - Avaliação de vulnerabilidades A avaliação de vulnerabilidades consiste na busca de pontos fracos a serem explorados nos testes de intrusão. 3 - Testes de aplicações web e mobile; São realizados testes tanto em aplicações web, quanto em aplicações mobile para medir a segurança dos mesmos. 4 - Avaliação de segurança de infraestrutura de rede: 4.1 - ANÁLISE DE TRÁFEGO DE REDES A. Sniffer & Spoofing; B. Certificados e criptografia; C. Segmentação de rede. 4.2 - ANÁLISE DE VULNERABILIDADES EM BANCOS DE DADOS A.DAM (Database Activity Monitoring); B. Gestão de acesso; C. Criptografia 5 - Avaliação de infraestrutura física: O processo de auditoria de segurança física visa testar e avaliar os protocolos da organização, como os controles de acesso e infraestrutura das áreas críticas. A. Espionagem Industrial: A.1. Controle de Acesso; A.2. Segurança Física. B. Análise do ambiente de infraestrutura de redes: B.1. Cabeado; B.2. WiFi. C. Data Center: C.1. Cabeamento estruturado; C.2. Ar condicionado corporativo; C.3. Janelas indevidas; C.4. Sistemas de Incêndios; D. Segurança física: D.1. Controle de Acesso. E. Política de Segurança: E.3. Eliminação de dados sensíveis. 6 - Engenharia social (Phishing): 6.1. Campanhas de Phishing aos usuários; 6.2. Avaliação da conscientização de usuários sobre Phishing (educacional); 7 - Teste da eficácia das ferramentas de segurança; Nos processos que são realizados os testes de segurança são testadas as eficácias de todas as ferramentas de segurança, incluindo, AV, NGAV, EDR, Firewall, IPS, IDS, WIPS, entre outras ferramentas de segurança contidas no ambiente. 8 - Análise dos processos de TIC -- deve ser valiado, no mínimo: I. Processos de gestão de patches. II. Gestão de Ativos; III. Gestão de Backups; IV. Gestão de acesso; V. Gestão de chamados; VI. Processo de Inventario; VII. Gestão de softwares; VIII. Política de senhas; IX. Licenciamento; X. Gestão de Vulnerabilidades; XI. Gestão de Segurança da Informação; 9 - Simulação de furto; Na execução da atividade de simulação de furto, o contratante fornecerá um notebook ou gabinete em uso (simulando realmente um furto), mediando autorização do funcionário, assim, os testes de acesso serão realizados com o objetivo de acessar os dados contidos no sistema e testar de efetividade do antivírus, para isso será criado um malware que faz o bypass da solução de antivírus utilizado pela Contratante, sem que o mesmo consiga bloquear ou sequer notificar. As verificações e atividades a serem realizadas são as seguintes: A. Criptografia do Disco; B. Avaliação da ferramenta de Segurança (Antivírus); C. Dados sensíveis; D. Coleta de senhas. 10- Reteste. O reteste tem o objetivo de verificar se uma vulnerabilidade encontrada foi devidamente corrigida, para isso é possível escolher a principal vulnerabilidade e marcar um reteste com 6 meses de antecedência, para que seja verificado a sua devida correção e se não há nenhum outro ponto de exploração.

	3128/2022	111702	DIRETORIA DE TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO			2				
37	**339040190010000 72 - CATMAT: 0**		**LICENÇA**	**--**	**--**	**--**	**2**	**0**	**2**	**--**	**--**

SOFTWARE DE GESTÃO DE PROPRIEDADE INTELECTUAL - SAAS

SOFTWARE DE GESTÃO DE PROPRIEDADE INTELECTUAL - SAAS 1. Licença anual de uso do software de Gestão de Propriedade Intelectual; 2. A empresa contratada deverá disponibilizar o software em infraestrutura de nuvem (SAAS); 3. Deverá ser fornecido suporte aos administradores do ativos e responsáveis pelo uso do sistema; 4. FUNCIONALIDADES: 4.1. Acompanhamento automático das atualizações do Brasil a partir da RPI, apontando prazos, mudanças de status e exigências publicadas; 4.2. Com base nas regras oficiais dos sistemas do Brasil, o sistema deve fornecer um calendário com deadlines de pagamentos e eventos específicos, como data limite para pedido de exame e expiração; 4.3. Deve ser possível acrescentar manualmente outros eventos para cada processo, que funcionam como lembretes; 4.4. Deve ser permitido o envio automático de e-mails informando eventos específicos, como data limite de pagamento ou submissão de documento; 4.5. Deve ser permitido o armazenamento e gestão dos documentos referentes ao processo via sistema (Repositório); 4.6. Os documentos devem ficar associados aos processos de PI para consultas futuras; 4.7. Deve ser permitido a criação de filtros para monitoramento de tecnologias no Brasil a partir da base do INPI. Incluir filtros por palavra chave, resumo, título, titular, inventor, etc. Enviar e-mail automático com novos ativos que se encaixam nos filtros criados. 4.8. Deve ser permitido a pesquisa de anterioridade/colidência de marca e notificação de colidências de marcas registradas através de relatórios automáticos enviados por e-mail, com disponibilidade de pesquisa por termo exato, prefixo, sufixo, contém e distância de caracteres. 4.9. Deve ser permitido a indicação de eventos e pagamentos específicos com base nas regras oficiais de cada país para patentes e D.I.'s; 4.10. Deve ser permitido o armazenamento de todos os custos incorridos no processo de proteção do ativo de PI, apresentando a natureza do custo, a data e o responsável pelo custo (sendo possível anexar um documento comprobatório – recibo); 4.11. Deve ser disponibilizado histórico de custos para consultas e relatórios; 4.12. Deve ser permitido consultar informações gerenciais sobre status dos processos, históricos de custos entre outros; 4.13. Deve ser permitido a indexação e armazenamento automático de emails, e seus anexos, pelo sistema, facilitando o acesso ao histórico de informações; 4.14. Deve ser permitido a consulta do log de informações sobre acessos ao sistema, alterações de informações e armazenamento de documentos e e-mails; 4.15. Deve ser permitido a gestão do fluxo de ações e atividades por responsável com notificação por e-mail e na tela principal. 5.SERVIÇOS 5.1. Suporte ao administrador online; 5.2. Implantação: 5.2.1. Carga no sistema das informações do portfólio de ativos de PI do cliente; 5.2.2. Adequação visual do software para a identidade visual da empresa; 5.2.3. Customização do sistema para particularidades até o limite de 60h de desenvolvimento. 5.2.4. Suporte intensivo de uma semana pós-disponibilização em ambiente de Produção; 5.3. Treinamento: 4 horas de treinamento online para a equipe responsável pela gestão do sistema;

	3129/2022	111702	DIRETORIA DE TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO			2				
38	**339040190010000 73 - CATMAT: 0**		**LICENÇA**	**--**	**--**	**--**	**1**	**0**	**1**	**--**	**--**

SOFTWARE DETECTOR DE PLÁGIO - SAAS

SOFTWARE DETECTOR DE PLÁGIO - SAAS 1.Licença Anual; 2. Software de Referência: Plagius; 3. Formatos de arquivos: doc, docx, pdf, odt, ppt, htm, html, rtf, txt; 4. Suporte gratuito por e-mail; 5. Exibir relatório dinâmico com diversas informações, entre elas: 5.1. Trechos suspeitos e suas fontes; 5.2. Endereços encontrados, com o percentual de semelhança; 5.3. Percentual de suspeitas de plágio e indicadores de qualidade da análise; 5.4. Permite abrir o resultado no seu navegador ou salvar em html.

	2864/2022	11010503	ASSESSORIA DA PRÓ-REITORIA DE EXTENSÃO E RELAÇÕES EXTERNAS			1				
39	**449040050010000 97 - CATMAT: 0**		**LICENÇA**	**--**	**--**	**--**	**6**	**0**	**6**	**--**	**--**

SOFTWARE SQL SERVER 2019 STANDARD

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.

	3121/2022	111702	DIRETORIA DE TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO			6				

TOTAL LICITADO: R$ 0,00

SIPAC | DTIC - Diretoria de Tecnologia da Informação e Comunicação - (48) 3877-9000 | Copyright © 2005-2022 - UFRN - appdocker2-srv2.appdocker2-inst2