INSTITUTO FEDERAL DE SANTA CATARINA
Sistema Integrado de Patrimônio, Administração e Contratos
Emitido em 28/05/2024 08:46

Quadro de especificações mínimas

Licitação: 23292.006156/2024-47 - PE 21005/2024 - REI
Assunto: AQUISIÇÃO DE SOFTWARES NAS DIVERSAS MODALIDADES DE LICITAÇÃO.

Item	Descrição	Unidade	Quant.	Preço Unit. (R$)	Valor Total (R$)
NÃO ASSOCIADO(S) A LOTE/GRUPO					
2	CESSÃO TEMPORÁRIA DE USO DE LICENÇA DE ANTIVÍRUS - 12 MESES Características mínimas: 1. Proteção contra malware conhecido e zero-day; 2. Proteção contra ransomware conhecido e zero-day; 3. Proteção contra ameaças conhecidas e zero-day; 4. Proteção antispyware, antiphishing; 5. Proteção contra vários vetores de ataque (web, e-mail, rede, dispositivos); 6. Proteção tradicional com assinaturas genéricas e otimizadas; 7. Consultas na inteligência coletiva baseada em nuvem; 8. Bloqueio comportamental e detecção de IoA (indicadores de ataques); 9. Firewall pessoal e gerenciado; 10. IDS/HIDS; 11. Controle do dispositivo; 12. Filtragem de URL por categoria (monitoramento da navegação na web); 13. Alertas de risco de segurança totalmente configuráveis e instantâneos; 14. Capacidade de reverter e remediar as ações cometidas pelos invasores; 15. Quarentena centralizada; 16. Análise automática e desinfecção; 17. Informações sobre os componentes de hardware e software de cada computador; 18. Informações sobre as atualizações da Microsoft instaladas em Endpoints; 19. Informações em tempo real sobre o status de todas as proteções e comunicações; 20. Atualizações automáticas; 21. Descoberta automática de Endpoints desprotegidos; 22. Capacidade de proteger imediatamente Endpoints desprotegidos remotamente; 23. Proxy nativo da Panda para oferecer suporte a Endpoints sem conexão com a Internet; 24. Console centralizado baseado em nuvem; 25. Herança de configurações entre grupos e Endpoints; 26. Capacidade de configurar e aplicar configurações por grupo; 27. Capacidade de configurar e aplicar configurações por Endpoint; 28. Implantação em tempo real de configurações do console para Endpoints; 29. Gerenciamento de segurança com base em visualizações de Endpoint e filtros dinâmicos; 30. Capacidade de agendar e executar tarefas em visualizações de Endpoint; 31. Capacidade de atribuir funções pré-configuradas aos usuários do console; 32. Capacidade de atribuir permissões personalizadas para usuários do console; 33. Capacidade de personalizar alertas locais; 34. Auditoria da atividade do usuário; 35. Instalação via pacotes MSI, download de URLs e e-mails enviados aos usuários finais; 36. Relatórios sob demanda e agendados em diferentes níveis e com várias opções de granularidade; 37. Relatórios de status do sistema em diferentes níveis e com várias opções de granularidade; 38. Inventário e auditorias de dispositivos; 39. Monitoramento de dispositivos com e sem agentes; 40. Patch Management; 41. Instalação centralizada de software; 42. Acesso remoto sem interrupções; 43. Desktop remoto; 44. Automação de tarefas e scripts; 45. Suporte para Windows e Linux.	LICENÇA	400	106,44	42.576,00
3	CHATGPT TEAM - SUBSCRIÇÃO ***Configuração mínima*** 1. Mensagens, interações e histórico ilimitados; 2. Acesso na web, iOS, Android; 3. Acesso ao modelo GPT-4; 4. Acesso a ferramentas adicionais como DALL·E, Navegação, Análise Avançada de Dados; 5. Console administrativo para gerenciamento do espaço de trabalho;	LICENÇA	17	1.515,00	25.755,00
6	LICENÇA COMERCIAL, PERPÉTUA, SOFTWARE ASC TIME TABLES PREMIUM - Software para geração de horários escolares.	LICENÇA	5	2.522,50	12.612,50
7	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.	LICENÇA	121	668,36	80.871,56
8	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.	LICENÇA	85	1.326,79	112.777,15

Item	Descrição	Unidade	Quant.	Preço Unit. (R$)	Valor Total (R$)
9	LICENÇA COMERCIAL AUTOCAD LT 2024 - 36 MESES - Assinatura de licença usuário único do Autodesk Autocad LT (última versão disponível), com suporte avançado, pelo período de 03 (três) anos.	LICENÇA	32	5.854,09	187.330,88
10	LICENÇA COMERCIAL 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.	UNIDADE	8	4.058,34	32.466,72
11	LICENÇA DE ANTIVÍRUS F-SECURE - ATUALIZAÇÃO Renovação de licenças de uso de solução antivírus F-Secure Client Security, F-Secure Antivírus for Windows Server, e F-Secure Policy Manager Server e Console de Administração. Atualização por 36 meses.	LICENÇA	585	184,67	108.031,95
12	LICENÇA EDUCACIONAL ATLAS.ti - SUBSCRIÇÃO DE 1 ANO --- CARACTERÍSTICAS MÍNIMAS: - Criar categorias e subcódigos e organizar em pastas. - Explorar dados com listas de palavras e nuvens em mais profundidade, concentrando-se em classes gramaticais selecionadas, como verbos, adjetivos, advérbios, conjunções, etc. - Importar pesquisa simplificada. - Suportar os formatos .xml e .bibTex; - Recuperar comentários de redes sociais por meio de exportcomments.com e importe o arquivo Excel resultante para ATLAS.ti. - Processamento de vídeos, imagens e arquivos de áudio com alta performance. - Trabalhar com documentos de texto em todos os principais formatos - incluindo .txt, .doc, .docx, .odt e, é claro, .pdf. - Realizar pesquisas totalmente automatizadas em um ou vários documentos, auto codificação e outras operações semânticas poderosas. - Trabalhar com formatos gráficos e de áudio (.wav,, mp3, .wma, etc.), bem como com os tipos de vídeo mais comuns (.avi, .mp4, .wmv, entre outros). - Importar dados do Evernote, Twitter e de seu Reference Manager favorito para uma revisão da literatura	LICENÇA	10	1.740,74	17.407,40
13	LICENÇA EDUCACIONAL DE ACESSO REMOTO A WINDOWS SERVER 2022 - CAL -> LICENÇAS POR DISPOSITIVO. PACOTE COM 5 LICENÇAS.	LICENÇA	102	912,36	93.060,72
14	LICENÇA EDUCACIONAL DO SPSS STATISTICS PREMIUM - SUBSCRIÇÃO 1 ANO	LICENÇA	4	2.142,50	8.570,00
15	LICENÇA EDUCACIONAL OGG - SOFTWARE PARA SIMULAÇÃO GERENCIAL - Software para simulação gerencial, baseado em plataforma WEB. Licença para uso simultâneo de até 50 usuários. Utilização em Processos Gerenciais - Jogos de Empresas.	LICENÇA	1	3.025,00	3.025,00
16	LICENÇA EDUCACIONAL, PERPÉTUA, DE SO WINDOWS SERVER 2022 STANDARD 16 CORE Marca: Microsoft Licenciamento: ESD Idioma: Português Licenciamento para: Uso corporativo Núcleos: Até 16 - 32bits ou 64bits	LICENÇA	5	6.989,49	34.947,45
17	LICENÇA EDUCACIONAL, PERPÉTUA, SOFTWARE COREL DRAW - Aquisição de licença perpétua, educacional, software Corel Draw Graphics 2023 em Português do Brasil, compatível com Windows 7, 8, 10, 11 (32 e 64 bits).	LICENÇA	10	4.095,00	40.950,00
18	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	LICENÇA	35	5.287,35	185.057,25

Item	Descrição	Unidade	Quant.	Preço Unit. (R$)	Valor Total (R$)
	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.				
19	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.	LICENÇA	30	5.157,79	154.733,70
20	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.	LICENÇA	350	1.391,60	487.060,00
21	LICENÇA EDUCACIONAL PARA SOFTWARE PARA GERENCIAMENTO DE SISTEMAS OPERACIONAIS - 36 MESES -> CARACTERÍSTICAS: 1. 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; 2. 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; 3. 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; 4. 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; 5. Instalação do gerenciador de boot local via PXE (boot de rede) ou via USB (para clientes remotos); 6. 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; 7. 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; 8. 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; 9. 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; 10. 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; 11. Acionamento de bloqueio de periféricos e portas de acesso (USB e outros).	LICENÇA	100	1.500,00	150.000,00
22	LICENÇA EDUCACIONAL SOFTWARE ADOBE CREATIVE CLOUD - 12 MESES 1. Aquisição de licença (educacional) ADOBE CREATIVE CLOUD em Português. 2. ADOBE CREATIVE CLOUD FOR ENTERPRISE ALL APPS - EDUCACIONAL NEW SDL 3. ITEM PASSÍVEL DE CONTRATAÇÃO VIA ASSINATURA DE INSTRUMENTO DE CONTRATO	LICENÇA	31	1.616,75	50.119,25
23	LICENÇA EDUCACIONAL SOFTWARE ADOBE CREATIVE CLOUD - 36 MESES 1. Aquisição de licença (educacional) ADOBE CREATIVE CLOUD em Português. 2. ADOBE CREATIVE CLOUD FOR ENTERPRISE ALL APPS - EDUCACIONAL NEW SDL 3. ITEM PASSÍVEL DE CONTRATAÇÃO VIA ASSINATURA DE INSTRUMENTO DE CONTRATO	LICENÇA	56	4.579,17	256.433,52

Item	Descrição	Unidade	Quant.	Preço Unit. (R$)	Valor Total (R$)
24	LICENÇA EDUCACIONAL ADOBE ILLUSTRATOR 12 MESES	LICENÇA	26	852,00	22.152,00
25	LICENÇA EDUCACIONAL ADOBE PHOTOSHOP 12 MESES	LICENÇA	36	852,00	30.672,00
26	LICENÇA EDUCACIONAL, SAAS, DEEP FREEZE CLOUD - 36 MESES - SW.FR.DF.CL.BAS.EDU.S3Y	LICENÇA	360	300,24	108.086,40
27	LICENÇA EDUCACIONAL, WINDOWS SERVER 2022 REMOTE DESKTOP SERVICES - 1 CAL POR DISPOSITIVO.	LICENÇA	5	177,03	885,15
28	LICENÇA MATH TYPE - Criação de equações profissionais em documentos digitais. Software: Math Type. Desenvolvedor: Design Science. Plataforma: Windows	UNIDADE	1	280,00	280,00
29	LICENÇA MLABS - Licença do Software MLABS Profissional, com validade de 1 ano.	UNIDADE	1	392,08	392,08
30	LICENÇA PERPÉTUA EDUCACIONAL NVIVO - ÚLTIMA VERSÃO DISPONÍVEL ---- Características mínimas: - Importar e analisar documentos de texto, imagens e documentos escaneados. - Importar áudio e vídeo em diversos formatos. - Categorizar e classificar dados por tema ou tópico e analisar como os itens são conectados usando Codificação In-Vivo. - Revisar codificação utilizando barras de codificação e destaques. - Fazer buscas de texto específicos, frequência de palavras e codificação. - Criar hiperlinks para anotar uma comparação ou evidência, vinculando páginas da web e arquivos fora do seu projeto. - Gráficos, nuvem de palavras, árvore de palavras, explore e compare diagramas. - Coletar dados de planilhas e formulários e importe para formatos populares. - Capturar páginas de sites e importe em formato PDF. - Importar comentários do Twitter, Facebook e YouTube. - Importar vídeos do YouTube. - Importar e-mails do Outlook e criar automaticamente conexões entre remetentes e destinatários. - Criar um sistema de arquivamento, permitindo que você procure, separe e acesse itens do seu projeto com facilidade. - Importar ou crie transcrições e ligue aos arquivos de vídeo ou áudio correspondentes. - Proteger o acesso aos projetos com perfis de usuário, senhas e tipos de permissões diferentes. - Acompanhar o que os membros da sua equipe estão fazendo, registrando as alterações do seu projeto em um log de ações do usuário. - Identificar as palavras mais frequentes em materiais selecionados e explore o contexto envolvendo essas palavras. - Diagramas dinâmicos que mostram conexões entre um item de um projeto central e o conteúdo de projetos relacionados. - Verificar ortografia (português, inglês, espanhol, francês, alemão, japonês e chinês). - Unir projetos separados em um só projeto. - Analisar de rede social: crie e analise conexões entre pessoas ou outras entidades. Visualize conexões entre uma população e obtenha mais dados através da métrica de rede. Suporte para PAJEK. - Categorizar e classifique os dados automaticamente com base nos padrões de codificação existentes. - Analisar automaticamente temas: encontrar e classificar temas entre seus dados automaticamente. - Sociogramas: Visualizar como um tema central se conecta a outros casos, e como esses casos se conectam uns aos outros. - Autocodificação baseada em padrões.	LICENÇA	4	7.503,50	30.014,00
31	LICENÇA, PERPÉTUA, DE SOFTWARE SQL SERVER 2019 STANDARD ------- Licenciamento de direitos permanentes de uso de software para servidor - SQL Server 2019 Standard Core - 2 Core License Pack Edu.	LICENÇA	2	7.330,77	14.661,54
32	LICENÇA DE SOFTWARE DETECTOR DE PLÁGIO 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.	LICENÇA	12	2.228,50	26.742,00
33	RENOVAÇÃO DA VALIDADE TÉCNICA DO SOFTWARE 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.	LICENÇA	2	600,00	1.200,00
34	RENOVAÇÃO DE VALIDADE TÉCNICA - LICENÇA VITALÍCIA ASC TIMETABLES PREMIUM - 1 ANO	SERVIÇO	9	600,00	5.400,00
35	SOFTWARE PARA AVALIAÇÃO DE IMÓVEIS URBANOS. Software para avaliação imobiliária conforme preconiza a NBR 14.653 da ABNT. Permite o uso de diversas técnicas matemáticas e estatísticas que favorecem a obtenção de uma avaliação precisa e confiável, como inferência estatística, regressão linear, análise de dados, redes neurais artificiais e outras. Deve possibilitar o cadastramento de informações completas referentes aos dados da amostra, fornecendo gráficos e tabelas. Possibilidade de montagem de laudos personalizados, possibilitando transformações de variáveis, de forma dirigida ou automática, manipulação de gráficos e tabelas com inúmeras ordenações, navegação pelos resultados obtidos, entre outros recursos. Interface de dados com software de dados livre. Referência: 1: TS-Sisreg (https://tecsys.eng.br/) 2: SisDEA (https://pellisistemas.com	LICENÇA	24	1.779,50	42.708,00

Item	Descrição	Unidade	Quant.	Preço Unit. (R$)	Valor Total (R$)
	/software/sisdea-avaliacao-de-imoveis/) 3: INFER32 (https://ariainformatica.com.br/infer-32/)				
38	TEAM VIEWER - CESSÃO TEMPORÁRIA DE DIREITOS DE USO DE LICENÇA DE SOFTWARE - 12 MESES ***Características Mínimas*** 1 - 15 usuários licenciados; 2 - 1 Conexão (canal); 3 - 300 dispositivos gerenciados; 4 - Conexão a partir de um número ilimitado de dispositivos; 5 - Conexão com um número ilimitado de dispositivos; 6 - 10 Sessões simultâneas (em abas) por canal; 7 - Relatórios de conexões realizadas;	LICENÇA	8	6.370,00	50.960,00
LOTE/GRUPO 1: AUTOMATION STUDIO					
1	ATUALIZAÇÃO DA VERSÃO 7.1 PARA 8.0 EDUC - AUTOMATION STUDIO ***Características Mínimas*** Pacote Premium - Biblioteca Hidráulica; - Biblioteca Hidráulica Proporcional; - Biblioteca Pneumática; - Biblioteca Pneumática Proporcional; - Ligações Mecânicas; - Módulo de dimensionamento de componentes; - Biblioteca de controles elétricos (inclui padrões IEC e JIC); - Biblioteca Eletrotécnica (AC e DC, inclui padrões IEC e NEMA); - Módulo de diagrama elétrico unifilar; - Biblioteca Lógica Ladder PLC (Allen Bradley™); - Biblioteca Lógica Ladder PLC (Siemens™); - Biblioteca Lógica Ladder PLC (IEC 61131-3); - Biblioteca de painéis de controle e HMI 2D/3D; - SFC - Biblioteca Grafcet IEC 61131; - Biblioteca Eletrônica Digital; - Módulo de diagnóstico e solução de problemas; - Lista de materiais (BOM) e módulo de relatório; - Módulo de comunicação cliente OPC para simulação de E/S e monitoramento de controle; - Workshop de Diagrama de Blocos (Matemática); - Biblioteca Lógica Ladder PLC (LSIS); - Diagrama de sequência; - Visualização incorporada; - Biblioteca lógica ladder PLC (série Mitsubishi MELSEC iQ-R); Usuário final: Instituto Federal de Ciências e Tecnologia de Santa Catarina - Campus Florianópolis	LICENÇA	31	2.917,52	90.443,12
4	EDIÇÃO EDUCACIONAL DE RENOVAÇÃO DO PROGRAMA DE MANUTENÇÃO E SUPORTE ESTENDIDO DE SOFTWARE - AUTOMATION STUDIO Duração: 1 ano a partir da data de compra Inclui: - Catálogos de Fabricantes; - Licenciamento de Acesso Remoto (WAN1) para Configuração de Rede com 3 licenças ou mais em todo o seu período de validade; - Atualizações de software, lançamentos de serviços, novas versões; - Treinamento online predefinido pela Famic Technologies - 2 horas por ano, por cliente; - Acesso ilimitado ao suporte técnico através do nosso portal de suporte técnico; - Teachware (Hidráulica, Pneumática, Elétrica); - Acesso ao sistema virtual 3D já feito; Usuário final: Instituto Federal de Ciências e Tecnologia de Santa Catarina - Campus Florianópolis	LICENÇA	1	56.527,20	56.527,20
5	EDIÇÃO EDUCACIONAL DE RENOVAÇÃO DO PROGRAMA DE MANUTENÇÃO E SUPORTE ESTENDIDO DE SOFTWARE - AUTOMATION STUDIO - 36 MESES - Catálogos de Fabricantes; - Licenciamento de acesso remoto (WAN1) para configuração de rede com 3 licenças ou mais durante todo o seu período de validade; - Atualizações de software, lançamentos de serviços, novas versões; - Treinamento online predefinido pela Famic Technologies - 2 horas por ano, por cliente; - Acesso ilimitado ao suporte técnico através do nosso portal de suporte técnico; - Teachware (Hidráulica, Pneumática, Elétrica); - Acesso ao sistema virtual 3D já feito; Usuário final: Instituto Federal de Ciências e Tecnologia de Santa Catarina - Campus Florianópolis	LICENÇA	1	133.650,00	133.650,00
				Valor Total do Lote/Grupo: R$ 280.620,32	
LOTE/GRUPO 2: SOLUÇÃO ZTNA					
36	SOLUÇÃO DE PROXY EM NUVEM ZERO TRUST ***Características de proxy em nuvem Zero Trust*** 1 - Todas as funcionalidades devem ser ofertadas em modalidade de "Nuvem como Serviço", utilizando um único agente instalado no dispositivo de acesso do usuário e console única de administração para todas as características técnicas descritas neste documento. A "Nuvem como Serviço" deve ser distribuída a nível nacional no Brasil com, no mínimo, 4 datacenters físicos e redundantes no país. 2 - O fabricante da solução de segurança em nuvem deve ter ponto de presença local no Brasil, onde todos os usuários em território nacional terão suas transações processadas dentro país; 3 - Garantir disponibilidade de 99.999% das estruturas de processamento de dados; 4 - O fabricante deve garantir o funcionamento integral até 6 meses pós fim do contrato; 5 - O fabricante da plataforma deve garantir: 5.1 - Metodologias para codificação segura durante o ciclo de vida de desenvolvimento da solução; 5.2 - PSIRT capaz de gerir vulnerabilidade, incidentes de segurança e problemas de segurança reportados inerentes à plataforma em questão; 6 - Os Data Centers localizados no Brasil devem ter rede independente com Sistema Autônomo e conectividade, redundante, em PTT (Ponto de Troca de Tráfego) no Brasil com "peering" com provedores de serviços, empresas de telecomunicações, CDNs (Content Delivery Network) e provedores de nuvem pública tais como (AWS, Microsoft e Google). Desta forma assegurando a melhor experiência e baixa latência aos usuários; 7 - Os datacenters do fabricante devem estar distribuídos em, no mínimo, 3 estados brasileiros de forma que o haja redundância geográfica da nuvem do fabricante da	LICENÇA	3000	1.009,08	3.027.240,00

Item	Descrição	Unidade	Quant.	Preço Unit. (R$)	Valor Total (R$)
	solução. 8 - O fabricante deverá prover, no mínimo, 3 (três) estruturas de processamento de dados no Brasil para melhor experiência do usuário. 9 - O licenciamento deverá contemplar: 9.1 - Uso global, com mais de 50 pontos no mundo, da infraestrutura do fabricante. 9.2 - Uso irrestrito de banda por parte dos usuários. 9.3 - 50 túneis IPSEC. 9.4 - Disponibilidade de 99.9999% dos datacenters no Brasil e no mundo. 9.5 - 30 ms para tráfego não criptografado e 70 ms para tráfego criptografado. 9.6 - Armazenamento de eventos para os módulos supracitados no período de 90 dias. 10 - Deve possuir um motor único e integrado para proteção de dados nos módulos Proxy em nuvem e ZTNA. Ex: o mesmo profile de LGPD customizado pelo IFSC deve poder ser aplicado em ambas as regras de Proxy e ZTNA; 11 - Deve ser permitido, sem custo adicional, o uso de todos os Datacenters do fabricante no mundo, garantindo assim a mobilidade segura dos usuários; 13 - Todas as inspeções e aplicações de políticas devem ser realizadas diretamente na solução na "Nuvem como Serviço"; 14 - O cliente instalado no dispositivo do usuário deve executar apenas as funções de redirecionamento de tráfego para nuvem, identificação do usuário e checagem de conformidade. Todo o processamento, incluindo controle de aplicações, proteção de dados, proteção contra ameaças, deve ocorrer na nuvem; 15 - No caso da utilização de agentes, a gestão de como o tráfego será encaminhado a plataforma, incluindo eventuais exclusões específicas (bypass), deve ser gerenciada da maneira centralizada na console Web da solução com o contexto de usuário e grupos de usuários; 16 - A solução não poderá exigir para o seu funcionamento, qualquer alteração ou customizações diretamente nos dispositivos dos usuários, exceto eventuais necessidades ajustes para convivências com soluções de antivírus/EDR; 17 - O agente único deve ser compatível com, no mínimo, os seguintes sistemas operacionais: 17.1 - Windows 10 e 11; 17.2 - Windows Server 2016, 2019, 2022 17.3 - MacOS 11, 12, 13, 14; 17.4 - IOS 15.1, 16, 17; 17.5 - Android 11, 12, 13, 14; 17.6 - Linux Ubuntu 18.04, 20.04 18 - Toda a solução proposta deve ser implementada com autenticação dos usuários integrada e suportar aplicações de políticas granulares com base em nome do usuário, departamento e grupos, integrados com a plataforma de base de usuário e diretório da contratante; 19 - A solução deve habilitar uma arquitetura de privilégio mínimo e confiança zero, "Zero Trust", definindo uma política de acesso granular para fornecer às pessoas certas no contexto certo, o acesso menos privilegiado aos aplicativos ou recursos e reduzir a superfície de ataque; 20 - Possuir peering com os principais provedores SaaS/IaaS, dentre eles: Amazon, Microsoft, Google, Akamai, Cloudflare, Facebook e Oracle Cloud. ***CONSOLE DE GESTÃO:*** 21 - A solução deve possuir capacidade de gestão centralizada, mantendo um painel único de administração e visibilidade para todos os módulos descritos neste termo de referência; 22 - Toda a parte de gestão deve ser centralizada em uma única console, garantindo a aplicação das políticas criadas em todos os datacenters disponíveis pelo fabricante no mundo e independente de qual data center que o usuário faça uso, a política deve estar vigente para proteção e controle do tráfego; 23 - Os dados disponíveis para a consulta e criação de relatórios, deve residir no plano de gestão por, no mínimo, 90 dias; 24 - A plataforma deve permitir a criação de diferentes perfis de acesso a console de administração com, no mínimo, as seguintes possibilidades: 24.1 - Perfil de administrador geral: acesso total às funções da solução, acesso aos logs de auditoria dos outros usuários, criação e administração de outras contas de acesso; 24.2 - Perfil de administrador intermediário: acesso total às funções da solução, exceto criação e administração de outras contas de acesso; 24.3 - Perfil de DPO: acesso ao painel de incidentes relacionados ao motor de prevenção de vazamento de dados; 24.4 - Perfil de Cibersegurança: acesso ao painel para análise de ameaças encontradas pela solução. 25 - A solução deve permitir associar as regras de proxy, DLP, proteção de ameaças e ZTNA em grupos distintos na tabela e associar aos grupos quais usuários administradores da console podem enxergá-los e administrá-los; 26 - A tabela de regras ainda deve possuir regras de topo de tabela que não possa ser sobreposta em uma estratégia de leitura "top-down"; 27 - A solução deve apresentar dashboard situacional referente ao tráfego processado contendo: 27.1 - Shadow IT: quantidade de aplicações descobertas e novas aplicações; 27.2 - Malware: Visão geral sobre os artefatos maliciosos encontrados 27.3 - DLP: visão geral sobre os incidentes gerados pelo motor de prevenção contra vazamento de dados; 27.4 - URLs: Domínios com maior registro de bloqueio pela ferramenta 28 - O painel de dashboard ofertado pela solução deve ser acionável, ou seja, para cada resultado ao clicar o administrador deve ser redirecionado para o evento em questão contendo mais detalhes sobre o ocorrido; 29 - O referido painel deve conter ainda capacidade de adicionar dashboards adicionais para fins de aumentar a visibilidade sobre o tráfego processado, contendo categorias como: 29.1 - Data loss prevention; 29.2 - Malware; 29.3 - Behavior Analytics; 29.4 - Dispositivos; 29.5 - Aplicações SaaS. 30 - A solução deve apresentar os incidentes em painéis especializados, contendo eventos subdivididos por: 30.1 - DLP; 30.2 - Malware; 30.3 - Análise comportamental dos usuários; 30.4 - Sites maliciosos; 31 - O painel de DLP deve apresentar todos os				

Item	Descrição	Unidade	Quant.	Preço Unit. (R$)	Valor Total (R$)
	incidentes relacionados a vazamento de dados, contendo informações que auxiliem na mitigação do evento de vazamento, apresentando ao DPO do IFSC os seguintes campos: 31.1 - Objeto/Arquivo; 31.2 - Aplicação/Site; 31.3 - Quantidade de violações; 31.4 - Ação realizada pela solução; 31.5 - Severidade; 31.6 - Data. 32 - Os incidentes de DLP deverão ser acionáveis, permitindo o aprofundamento da visibilidade do incidente e inclusive apresentar os dados que indicam o vazamento em questão na própria console da solução; 33 - A solução deve apresentar painel de comportamento para cada usuário do IFSC, identificando a nota de risco atual, bem como todo o histórico e atividades que levaram ao acréscimo ou decréscimo do risco; 34 - A solução deverá analisar o comportamento dos usuários através de regras sequenciais, detectando minimamente: 34.1 - Detectar atividades anômalas relacionadas a upload, download e deleção de arquivos em massa, falhas de login, compartilhamento de credencial, eventos raros, acesso ou tentativa de acesso a partir de países não confiáveis. 34.2 - Detectar a movimentação de dados a partir da tenant corporativa do Microsoft Office 365 com destino a instâncias pessoais SaaS; 35 - Os incidentes de malware devem ser acionáveis, permitindo aprofundamento do incidente, apresentando os usuários afetados, os arquivos relacionados a atividade maliciosa e a aplicação envolvida no incidente; 36 - A solução deve apresentar o HASH do arquivo para comparativo com base aberta de ameaças (VirusTotal) para identificar se a solução de endpoint corporativa do IFSC já possui assinatura preventiva contra a ameaça; 37 - Para todo o tráfego Web admitido, a solução deve realizar normalização e descoberta de aplicações SaaS – ShadowIT, sem a necessidade de importação de logs; 38 - Para as aplicações SaaS descobertas a solução deve realizar a classificação quanto à categoria (Ex: Cloud Storage), bem como o risco de tal aplicação; 39 - Minimamente apresentar se a aplicação SaaS possui em seu histórico recente vazamento de dados e vulnerabilidades em seus serviços; 40 - O risco deve ser uma das condicionantes para construção de regras de acesso web para os usuários do IFSC; 41 - Solução deve possuir capacidade de apresentar os logs de acesso em painel específico, garantindo a identificação do usuário, máquina, domínio, regra de processamento do tráfego e localização do acesso; 42 - Como forma de facilitar a visualização, a solução deve possuir painéis específicos que garantam: 42.1 - Visibilidade por aplicação – apresentando quais usuários acessaram tal aplicação, bem como os incidentes de malware e vazamento de dados, caso existam; 42.2 - Visibilidade por domínio – apresentando quais usuários acessaram tal domínio, bem como os incidentes de malware e vazamento de dados, caso existam; 42.3 - Visibilidade por usuário – apresentando os acessos, ações, geolocalização e incidentes de malware, comportamento e vazamento de dados; 43 - Deve possuir base própria de aplicações SaaS, com capacidade de controle granular, oferecendo no mínimo: 43.1 - O centro de inteligência do fabricante deve pontuar o índice de risco no uso de cada uma as aplicações SaaS não sancionadas (Shadow IT); 43.2 - Deve poder associar o índice de risco de uma determinada aplicação ou categoria de aplicações a uma regra de bloqueio em tempo real; 43.3 - A solução deve ser capaz de apresentar se uma aplicação SaaS, em uso por parte dos usuários do IFSC, possui em seu histórico algum registro de vazamento de dados e vulnerabilidades associados; 44 - A solução deve gerar relatórios baseado no tráfego processado, suportando no mínimo: 44.1 - Relatório de risco das nuvens SaaS acessadas – ShadowIT; 44.2 - Relatório do acesso Web; 44.3 - Relatório do acesso SaaS; 45 - A solução deve prover mecanismos capazes de monitorar a experiência do usuário, garantindo: 45.1 - Telemetria detalhada para análise fim-a-fim e identificar problemas de performance através de painel específico para apresentar as latências entre o cliente e a unidade de processamento do fabricante e da unidade de processamento do fabricante até o serviço SaaS Microsoft Office 365 45.2 - Deve possuir dashboard específico para apresentar a volumetria de tráfego por unidade de processamento do fabricante (pop); 46 - Deve possuir painel específico com dados relacionados ao cliente, garantindo visibilidade quanto a versões em uso, usuário ativos, Bytes baixados e carregados, quantidade de sessões diárias; 47 - A console deve possuir, dentre suas características, solução de relatório com capacidade de apresentar as mais diversas dimensões, medidas e outros campos que se façam necessários para a construção de relatórios e dashboards analíticos, com as seguintes capacidades: 47.1 - Permitir a construção de relatórios customizados, utilizando os atributos disponíveis e os mais diversos formatos de exposição dos dados: Bar, Pie, Table, Trend, Sankey, Treemap, Pivots; 48 - Disponibilizar ao administrador 20 dashboards/relatórios pré-definidos, incluindo assessment de risco de acordo com a aplicações em nuvem em uso, governança de dados, CISO, uso de nuvens SaaS, uso de Web, proteção de dados, uso de aplicações privadas dentre outros; 49 - Deve permitir a exportação e agendamento dos dashboards nos formatos Excel, PDF, CSV e texto; 50 - Ao criar um dashboard ou relatório, a solução deve permitir o uso de campos customizados, cálculo de tabelas e filtros customizados com múltiplas opções de organização dos valores/resultados; 51 - A solução deve prover monitoramento proativo para identificação de Insider				

Item	Descrição	Unidade	Quant.	Preço Unit. (R$)	Valor Total (R$)
	Threats; ********** 53 - SERVIÇO DE SUPORTE 24X7 (nível 1, 2 e 3) do fabricante: 53.1 - Atendimento 24x7; 53.2 - Suporte por E-mail/Web; 53.3 - Suporte por telefone; 53.4 - Suporte por plantão (após horário comercial) 53.4 - Disponibilidade de documentação dos produtos do fabricante; ********** 54 - A solução de proxy em nuvem, deve oferecer controles de proteção de dados e de ameaças com visibilidade e controle granular das atividades em aplicações SaaS para os protocolos HTTP e HTTPS. 55 - Deve ser capaz de processar tráfego HTTP/HTTPS nas portas 80, 443 e em portas customizadas, a exemplo: 8443, 8080, 8081; 56 - A solução de proxy em nuvem deve prover: 56.1 - Descoberta, visibilidade e controle do tráfego Shadow IT; 56.2 - Visibilidade e controle do tráfego corporativo com direção aplicações SaaS sancionadas pela TI, em tempo real; 56.3 - Visibilidade e controle em tempo real de acesso a URLs, por meio de classificação baseado em categorias; 56.4 - Prevenção contra vazamento de dados no nas aplicações sancionadas, Shadow IT e aplicações Web 2.0; 56.5 - Prevenção contra acesso a sites maliciosos; 56.7 - Prevenção contra acesso a artefatos maliciosos; 57 - A solução deve estar licenciada e suportar os seguintes métodos para encaminhamento do tráfego para a solução de Proxy em nuvem: 57.1 - Integração com o FW (Fortigate 600F) do IFSC via túnel IPSEC; 57.2 - Integração com o FW (Fortigate 600F) do IFSC via túnel GRE; 57.3 - Proxy Explícito em nuvem; 57.4 - Cliente nativo do próprio fabricante para as plataformas Windows, MacOS, Linux e iOS; 58 - A solução deve ser capaz de atuar diretamente no tráfego, sem a necessidade de integração via API, para processar o tráfego nas estruturas de processamento de dados posicionadas em território nacional, garantindo, no mínimo, as seguintes funções: Shadow IT; 58.1 - Proteção contra vazamento de dados; 58.2 - Proteção contra malwares; 58.3 - Análise comportamental dos usuários. 59 - Dentre as capacidades da solução para o entendimento do tráfego a ser inspecionado, deve constar: 59.1 - Base contendo, no mínimo, 100 categorias de URLs; 59.2 - Deve ser capaz de identificar e controlar nativamente, no mínimo, 2.500 aplicações SaaS e 40 Categorias nativas de aplicações SaaS; 60 - Aplicar ação de bloqueio em tempo real para Google Workspace, Microsoft Office 365, aplicações SaaS terceiras e Web; 61 - Deve suportar e estar licenciado para que o usuário que estiver fora do Brasil se conecte ao POP mais próximo geograficamente na nuvem do fabricante ou com menor latência para acesso a internet obedecendo a mesma política de segurança dos usuários localizados no Brasil; 62 - Deve ser capaz de inspecionar túneis criptografados baseados no TLS 1.3; 63 - A solução deve oferecer controle e proteção para o acesso Web dos usuários garantindo o controle de acesso a categorias não autorizadas; 64 - Controle de acesso a categorias que impõem risco de segurança aos usuários do IFSC, incluindo, mas não limitado a URLs associadas às categorias de Botnets, DGA, Command Control, Sites Maliciosos e Phishing; 65 - Deve permitir o bloqueio automático a URLs desconhecidas não categorizadas pelo fabricante; 66 - Permitir a criação de categorias customizadas baseadas em listas contendo regex e domínios; 67 - A solução deve permitir a criação de listas de by-pass, onde o tráfego não deve ser encaminhado à nuvem do fabricante, como, por exemplo: categoria de sites financeiros ou de bancos; 68 - A solução deve de-criptografa o tráfego automaticamente e permitir criar regras de exceção para o tráfego que não deva ser decriptado; 69 - O controle nativo de aplicações SaaS deve apresentar visibilidade mínima sobre os seguintes contextos: 69.1 - Identificação do usuário e grupo; 69.2 - Validação do dispositivo (gerenciado ou não gerenciado); 69.3 - Categoria da aplicação SaaS; 69.4 - Nível de risco da aplicação SaaS; 69.5 - Geolocalização; 69.6 - Controle granular de atividades (upload, post, edit, share, view, download, send). 70 - Para aplicações Web 2.0 a solução deve oferecer controles granulares, dentre eles: 70.1 - Facebook: Prevenir o vazamento de dados na ação de POST e bloquear as ações de POST, LIKE, SHARE e UPLOAD; 70.2 - Youtube: bloquear as ações de DELETE, LIKE, SHARE, POST e VIEW para categorias de canais específicos 70.3 - Twitter: Prevenir o vazamento de dados nas ações POST e UPLOAD e ser capaz de bloquear as ações de POST, SHARE, FOLLOW e DELETE 70.4 - Pastebin: Prevenir o vazamento de dados via ação POST e controlar ações de POST, DELETE e CREATE. 71 - A solução deve possibilitar a liberação de um período de hora por dia para acesso a aplicações, sites e categorias; 72 - A solução deve permitir, de maneira nativa, a criação de regras para permitir o acesso à plataforma do Google Workspace e o 365 Corporativo e negar o acesso às instâncias pessoais da Google e Microsoft Office. Exemplo: Gmail, Outlook, Gdrive e Onedrive; 73 - A solução deve ser capaz controlar o upload de arquivos para o WhatsApp Web; 75 - A solução deve possuir a capacidade de criar políticas onde o upload/download de arquivos com destino a instância de SaaS/IaaS corporativo do IFSC é permitido e o upload a outras instâncias nos demais serviços é bloqueado, incluindo, mas não limitado a GitHub (mediante licenciamento adicional), AWS, Microsoft Office, Google Worksapces; 76 - Capacidade de aplicar políticas granulares, a nível de atividade, em aplicativos do pacote Microsoft Office 365 e Google Workspace: 76.1 - Aplicar políticas				

Item	Descrição	Unidade	Quant.	Preço Unit. (R$)	Valor Total (R$)
	granulares a nível de atividade para OneDrive; 76.2 - Aplicar políticas granulares a nível de atividade para o SharePoint; 76.3 - Aplicar políticas granulares a nível de atividade para o Word Online; 76.4 - Aplicar políticas granulares a atividade granular para o Outlook.com; 76.5 - Aplicar políticas granulares a nível de atividade para o Exchange Online; 76.6 - Aplicar políticas granulares a nível de atividade para Teams; 76.7 - Aplicar políticas granulares a nível de atividades para Power BI; 76.8 - Aplicar políticas granulares a nível de atividade para Gmail; 76.9 - Aplicar políticas granulares a nível de atividade para Gdrive. 77 - A solução deve possuir as seguintes características mínimas para o motor contra vazamento de dados: 77.1 - Deve possuir nativamente perfis de DLP pré-definidos baseados em normas regulamentares, incluindo, mas não limitado a LGPD e permitir também a criação de perfis customizados; 77.2 - Deve permitir a criação de dicionários de dados baseados em palavras-chave, frases e expressões regulares para serem usados nas regras de DLP; 77.3 - Deve permitir a criação de regras customizadas de DLP através de expressão regulares, dicionários e palavras chaves com opção de uso de operadores booleanos; 77.4 - Deve possuir a capacidade de detectar informações confidenciais em, no mínimo, 300 tipos de arquivos distinto; 78 - A solução deve ser capaz de empregar controle contra vazamento de dados em: 78.1 - Aplicação SaaS corporativa; 78.2 - Aplicação SaaS terceiras (Shadow IT) – Microsoft Live Suite, Onedrive, Outlook, 4yshare. 78.3 - Sites Web –Twitter, Pastebin, Facebook. 79 - A solução deve ter a capacidade de identificar máscara de dados relacionados a LGPD nativamente, incluindo, mas não limitado a: CPF, CNH, RG, Título de Eleitor, PIS-PASEP, Passaporte Brasileiro, RENAVAM, Placa de Veículo, Endereços Brasileiros, CNPJ e prevenir a ação caso viole a política de segurança estabelecida. 80 - Para os dados pessoais brasileiros que possuam algoritmo validador, a solução deve possuir nativamente a capacidade de validar os dados a fim de evitar falso positivo; 81 - Deve proteger o acesso do usuário aos dados corporativos, controlando a exposição dos mesmos quanto a movimentação entre nuvens (Serviço SaaS sancionado e para Serviço SaaS não sancionado); 82 - A solução deve prover capacidade de proteção dos usuários do IFSC contra malwares: 82.1 - Análise de artefatos por meio de assinaturas; 83 - Deve realizar análise do tráfego web para evitar explorações de vulnerabilidades no cliente a partir de sites comprometidos/maliciosos; 84 - Deve ser capaz de inspecionar o tráfego criptografado e identificar artefatos maliciosos em ações de download em aplicações SaaS ShadowIT; 85 - A Engine de malware deve suportar inspeção de arquivos carregado (upload) na instância corporativa de aplicações sancionadas e prevenir o (download) a partir de instâncias pessoais de aplicações SaaS (Exemplo: Google Drive, Microsoft Onedrive, Bucket S3, Bloob Azure); 86 - A solução deve realizar monitoramento do comportamento dos usuários gerenciados pela solução: 86.1 - Detectar atividade suspeita de violação de proximidade no acesso às aplicações quando, por exemplo, em um curto intervalo de tempo, as mesmas credenciais de acesso forem usadas para fazer login na mesma aplicação a partir de localidades distantes; 86.2 - Detectar atividade suspeita de usuários que fizerem download/upload em massa de arquivos das aplicações em nuvem corporativa do IFSC e nuvens pessoais; 86.3 - Detectar atividade suspeita de credenciais sendo compartilhadas entre usuários da instituição; 86.4 - Detectar exfiltração de dados a partir da instância do IFSC com destino a SaaS terceiros (Shadow IT). 87 - A solução deve permitir a inspeção de downloads relacionados a categorias Web relacionadas a algum risco de segurança, exemplo: Phishing; 88 - A solução deve permitir o controle de quais tipos de anexos os usuários podem realizar download e se estes estão livres de malwares; 89 - Deve ser capaz, por meio de integração com SIEM, NGFW e EDR, suplementar o SOC com IOC's (Hashes e URL), para que seja possível rastrear um ataque onde quer que ele aconteça; 90 - O cliente do próprio fabricante deve avaliar a postura do dispositivo, liberando ou não de acesso a aplicações SaaS corporativas ou SaaS terceiras baseando-se na identificação de itens, como: 90.1 - Processo em execução; 90.2 - Presença de arquivos armazenados em disco local; 90.3 - Presença de um domínio Windows; 90.4 - Presença de um certificado digital no dispositivo. 91 - Para tráfego não WEB a solução deve possuir as capacidades descritas abaixo; 92 - Deve ser capaz de controlar e bloquear o uso de protocolos não WEB para conexões com destino a internet, originadas por usuários remotos usando máquinas corporativas do IFSC; 93 - O filtro deverá suportar os protocolos baseados em TCP, UDP e ICMP; 94 - A identificação do destino deverá suportar os seguintes parâmetros: 94.1 - FQDN; 94.2 - PQDN; 94.3 - Wildcard; 94.4 - IP; 94.5 - CIDR; 94.6 - Range de IP. 95 - Para a filtragem do tráfego, deverá suportar os seguintes métodos de redirecionamento a nuvem do fabricante: 95.1 - Túnel GRE; 95.2 - Túnel IPSEC. 95.3 - Agente instalado no dispositivo do usuário sendo o mesmo para o tráfego WEB e para o tráfego do ZTNA (ztna sendo uma solução à parte do web gateway, porém utilizam a mesma console e agente); 96 - Para a identificação da origem do tráfego, deverá aplicar a identificação do usuário e grupo de usuário, minimamente; 97 - Deverá suportar o controle de comandos FTP no modo passivo; 98 - Deverá suportar a				

Item	Descrição	Unidade	Quant.	Preço Unit. (R$)	Valor Total (R$)
	criação de aplicações baseando-se em: 98.1 - Destino; 98.2 - Protocolo; 98.3 - Porta (uma, múltiplas e range). 99 - Deverá ser capaz de reconhecer o tráfego e aplicações não web em camada 7; 100 - O reconhecimento de aplicações deve englobar minimamente SSH, RDP, SMB, SAP, Zoom e Git; 101 - Deve ser capaz de identificar e bloquear aplicações não autorizadas, como exemplo: Ultrasurf, BitTorrent, Teamviewer e RealVNC; 103 - Possibilitar a criação e modificação de atributos dos alarmes (p.e. status, inclusão de campos textuais, cálculo do tempo de tratamento dos alarmes); 104 - Gerar relatórios, padronizados ou customizados, podendo apresentar informações agrupadas ou expandidas pelos atributos utilizados para caracterizar os alarmes; 105 - Deve permitir a geração de relatórios sob demanda para emissão pontual ou periódica, possibilitando a exportação em PDF ou CSV. 106 - Os relatórios devem possibilitar listar os sites mais acessados e os mais bloqueados com suas respectivas categorias e URLs, permitindo a busca por IP, URL ou domínio por intervalo de tempo. 107 - Capacidade de automatizar o envio de relatórios customizados, via e-mail, a usuários específicos; 108 - Possibilitar a criação e modificação de atributos dos alarmes (p.e. status, inclusão de campos textuais, cálculo do tempo de tratamento dos alarmes); 109 - Gerar relatórios, padronizados ou customizados, podendo apresentar informações agrupadas ou expandidas pelos atributos utilizados para caracterizar os alarmes; ***GERÊNCIA DE PROJETO, IMPLEMENTAÇÃO, CUSTOMIZAÇÃO E SUPORTE:*** 110 - Deve ser alocado pela CONTRATADA da solução, no mínimo, um Gerente de Projetos com certificação PMP e que possua fluência na língua portuguesa para a gerência de todo o projeto; 111 - Deve ser alocado pela CONTRATADA da solução, no mínimo, dois Professional Services que possuam fluência na língua portuguesa para devida implementação, configurações e customizações da solução contratada; 112 - Deve ser alocado pela CONTRATADA, no mínimo, um Instrutor de treinamento que possua fluência na língua portuguesa para entrega dos treinamentos em língua portuguesa; 113 - Apresentação e validação de plano de implementação do projeto com detalhamento das atividades, cronograma previsto, duração, prazos, profissionais envolvidos, necessidades, premissas etc. seguindo as melhores práticas de gerenciamento de projetos, p.e., PmBOK/PMI; 114 - Devem estar em conjunto o profissional do fabricante da solução e o parceiro fornecedor; 115 - Realização de reunião de Kick-off de projeto, reuniões semanais e sempre que necessário, de apresentação de Status Report do andamento do projeto; 116 - Devem estar em conjunto o profissional do parceiro fornecedor; 117 - Elaboração e apresentação de relatórios detalhado e executivo de Status Report do andamento do projeto; 118 - Devem estar em conjunto o profissional do parceiro fornecedor; 119 - Após a finalização do escopo proposto a ser implantado pelo fabricante ou parceiro, um profissional do fabricante ou do parceiro fornecedor, customer success, deve prestar os seguintes serviços durante todo o contrato em língua portuguesa no Brasil: 119.1 - Apoio técnico para os administradores da solução; 119.2 - Apoio executivo para CISO/CSO; 119.3 - O apoio se baseia em: 119.3.1 - Compartilhar boas práticas de administração da solução; 119.3.1 - Documentação técnica para apoiar e sustentar uma determinada decisão técnica 119.3.1 - Desenhar e apresentar junto aos decisores um roadmap estratégico para determinar os passos de proteção e governança; 119.3.1 - Prover Transferência de conhecimento pós-implantação; 119.3.1 - Fornecer liderança técnica e orientação para conduzir a implantação e operacionalização da plataforma; 119.3.1 - Auxiliar na configuração e ajuste de políticas, configuração de aprimoramentos do produto e revisões periódicas de políticas; 119.3.1 - Executar um plano estratégico de realização e obtenção de valor e retorno sobre investimento, conforme casos de uso que estejam alinhados às necessidades de segurança e do negócio. 119.4 - As atividades macro de implantação do projeto: 119.4.1 - Configurações básicas de acesso para administradores do tenant; 119.4.2 - Definição das ROLES de cada administrador do tenant; 119.4.3 - Integração de AD/Azure AD de grupos e usuários; 119.4.4 - Configuração de tráfego de grupos sincronizados do AD/Azure AD e definição de exceções desse tráfego; 119.4.5 - Configuração dos Clients, por grupo, conforme os grupos sincronizados do AD/Azure AD; 119.4.6 - Configurações de URL lists, incluindo lista de Bypass; 119.4.7 - Configuração de regras de DLP (ex.: LGPD - CPF, CNH, RENAVAM, PASSAPORTE, NOME PRÓXIMO A E-MAIL,) e DLP Profiles; 119.4.8 - Configuração de políticas de acesso WEB e aplicações SaaS com e sem DLP; 119.4.9 - Configuração de políticas de acesso WEB e aplicações SaaS com e sem Threat Protection; 119.4.10 - Criação de templates de notificação (pop-up) customizados. *********SUBSCRIÇÃO = 36 MESES********** *****TREINAMENTO***** 120 - ADMINISTRAÇÃO E OPERAÇÃO DA SOLUÇÃO: 120 .1 - Segurança em nuvem; 120 .2 - Arquitetura; 120 .3 - Níveis de risco de aplicações SaaS; 120 .4 - Proteção via API; 120 .5 - Políticas; 120.6 - Client da solução; 120.7 - Threat Protection; 120.8 - Relatórios; 120.9 - Relatórios avançados; 120.10 - IaaS; 120.11 - Segurança Web; 120.12 - ROLES (Role-Based Access Control); 120.13 - Segurança IoT ; 121 - IMPLEMENTAÇÃO E INTEGRAÇÃO: 121.1 - SAML; 121.2 -ZTNA; 121.3 -DLP; 121.4 -Segurança Web ; 121.5 -Relatórios				

Item	Descrição	Unidade	Quant.	Preço Unit. (R$)	Valor Total (R$)
	avançados; 121.6 -REST API; 121.7 -Security Posture Management; 121.8 -Remote Browser Isolation (RBI);				
37	SOLUÇÃO DE ZERO TRUST NETWORK ACCESS PARA ACESSO A APLICAÇÕES PRIVADAS ***Características Mínimas*** 1 - Todas as funcionalidades devem ser ofertadas em modalidade de "Nuvem como Serviço", utilizando um único agente instalado no dispositivo de acesso do usuário e console única de administração para todas as características técnicas descritas neste documento. A "Nuvem como Serviço" deve ser distribuída a nível nacional no Brasil com, no mínimo, 4 datacenters físicos e redundantes no país. 2 - O fabricante da solução de segurança em nuvem deve ter ponto de presença local no Brasil, onde todos os usuários em território nacional terão suas transações processadas dentro país; 3 - Garantir disponibilidade de 99.999% das estruturas de processamento de dados; 4 - O fabricante deve garantir o funcionamento integral até 6 meses pós fim do contrato; 5 - O fabricante da plataforma deve garantir: 5.1 - Metodologias para codificação segura durante o ciclo de vida de desenvolvimento da solução; 5.2 - PSIRT capaz de gerir vulnerabilidade, incidentes de segurança e problemas de segurança reportados inerentes à plataforma em questão 6 - Os Data Centers localizados no Brasil dever ter rede independente com Sistema Autônomo e conectividade, redundante, em PTT (Ponto de Troca de Tráfego) no Brasil com "peering" com provedores de serviços, empresas de telecomunicações, CDNs (Content Delivery Network) e provedores de nuvem pública tais como (AWS, Microsoft e Google). Desta forma assegurando a melhor experiência e baixa latência aos usuários; 7 - Os datacenters do fabricante devem estar distribuídos em, no mínimo, 3 estados brasileiros de forma que o haja redundância geográfica da nuvem do fabricante da solução. 8 - O fabricante deverá prover, no mínimo, 3 (três) estruturas de processamento de dados no Brasil para melhor experiência do usuário. 9 - O licenciamento deverá contemplar: 9.1 - Uso global, com mais de 50 pontos no mundo, da infraestrutura do fabricante. 9.2 - Uso irrestrito de banda por parte dos usuários. 9.3 - 50 túneis IPSEC. 9.4 - Disponibilidade de 99.9999% dos datacenters no Brasil e no mundo. 9.5 - 30 ms para tráfego não criptografado e 70 ms para tráfego criptografado. 9.6 - Armazenamento de eventos para os módulos supracitados no período de 90 dias. 10 - Deve possuir um motor único e integrado para proteção de dados nos módulos Proxy em nuvem e ZTNA. Ex: o mesmo profile de LGPD customizado pelo IFSC deve poder ser aplicado em ambas as regras de Proxy e ZTNA; 11 - Deve ser permitido, sem custo adicional, o uso de todos os Datacenters do fabricante no mundo, garantindo assim a mobilidade segura dos usuários; 13 - Todas as inspeções e aplicações de políticas devem ser realizadas diretamente na solução na "Nuvem como Serviço"; 14 - O cliente instalado no dispositivo do usuário deve executar apenas as funções de redirecionamento de tráfego para nuvem, identificação do usuário e checagem de conformidade. Todo o processamento, incluindo controle de aplicações, proteção de dados, proteção contra ameaças, deve ocorrer na nuvem; 15 - No caso da utilização de agentes, a gestão de como o tráfego será encaminhado a plataforma, incluindo eventuais exclusões específicas (bypass), deve ser gerenciada da maneira centralizada na console Web da solução com o contexto de usuário e grupos de usuários; 16 - A solução não poderá exigir para o seu funcionamento, qualquer alteração ou customizações diretamente nos dispositivos dos usuários, exceto eventuais necessidades ajustes para convivências com soluções de antivírus/EDR; 17 - O agente único deve ser compatível com, no mínimo, os seguintes sistemas operacionais: 17.1 - Windows 10 e 11; 17.2 - Windows Server 2016, 2019, 2022 17.3 - MacOS 11, 12, 13, 14; 17.4 - IOS 15.1, 16, 17; 17.5 - Android 11, 12, 13, 14; 17.6 - Linux Ubuntu 18.04, 20.04 18 - Toda a solução proposta deve ser implementada com autenticação dos usuários integrada e suportar aplicações de políticas granulares com base em nome do usuário, departamento e grupos, integrados com a plataforma de base de usuário e diretório da contratante; 19 - A solução deve habilitar uma arquitetura de privilégio mínimo e confiança zero, "Zero Trust", definindo uma política de acesso granular para fornecer às pessoas certas no contexto certo, o acesso menos privilegiado aos aplicativos ou recursos e reduzir a superfície de ataque; 20 - Possuir peering com os principais provedores SaaS/IaaS, dentre eles: Amazon, Microsoft, Google, Akamai, Cloudflare, Facebook e Oracle Cloud. ***CONSOLE DE GESTÃO:*** 21 - A solução deve possuir capacidade de gestão centralizada, mantendo um painel único de administração e visibilidade para todos os módulos descritos neste termo de referência; 22 - Toda a parte de gestão deve ser centralizada em uma única console, garantindo a aplicação das políticas criadas em todos os datacenters disponíveis pelo fabricante no mundo e independente de qual data center o usuário faça uso, a política deve estar vigente para proteção e controle do tráfego; 23 - Os dados disponíveis para a consulta e criação de relatórios, deve residir no plano de gestão por, no mínimo, 90 dias; 24 - A plataforma deve permitir a criação de diferentes perfis de acesso a console de administração com, no mínimo, as seguintes possibilidades: 24.1 - Perfil de administrador geral: acesso total às funções da solução, acesso aos logs de auditoria dos outros	LICENÇA	3000	1.009,08	3.027.240,00

Item	Descrição	Unidade	Quant.	Preço Unit. (R$)	Valor Total (R$)
	usuários, criação e administração de outras contas de acesso; 24.2 - Perfil de administrador intermediário: acesso total às funções da solução, exceto criação e administração de outras contas de acesso; 24.3 - Perfil de DPO: acesso ao painel de incidentes relacionados ao motor de prevenção de vazamento de dados; 24.4 - Perfil de Cibersegurança: acesso ao painel para análise de ameaças encontradas pela solução. 25 - A solução deve permitir associar as regras de proxy, DLP, proteção de ameaças e ZTNA em grupos distintos na tabela e associar aos grupos quais usuários administradores da console podem enxergá-los e administrá-los; 26 - A tabela de regras ainda deve possuir regras de topo de tabela que não possa ser sobreposta em uma estratégia de leitura "top-down"; 27 - A solução deve apresentar dashboard situacional referente ao tráfego processado contendo: 27.1 - Shadow IT: quantidade de aplicações descobertas e novas aplicações; 27.2 - Malware: Visão geral sobre os artefatos maliciosos encontrados; 27.3 - DLP: visão geral sobre os incidentes gerados pelo motor de prevenção contra vazamento de dados; 27.4 - URLs: Domínios com maior registro de bloqueio pela ferramenta; 28 - O painel de dashboard ofertado pela solução deve ser acionável, ou seja, para cada resultado ao clicar o administrador deve ser redirecionado para o evento em questão contendo mais detalhes sobre o ocorrido; 29 - O referido painel deve conter ainda capacidade de adicionar dashboards adicionais para fins de aumentar a visibilidade sobre o tráfego processado, contendo categorias como: 29.1 - Data loss prevention; 29.2 - Malware; 29.3 - Behavior Analytics; 29.4 - Dispositivos; 29.5 - Aplicações SaaS. 30 - A solução deve apresentar os incidentes em painéis especializados, contendo eventos subdivididos por: 30.1 - DLP; 30.2 - Malware; 30.3 - Análise comportamental dos usuários; 30.4 - Sites maliciosos; 31 - O painel de DLP deve apresentar todos os incidentes relacionados a vazamento de dados, contendo informações que auxiliem na mitigação do evento de vazamento, apresentando ao DPO do IFSC os seguintes campos: 31.1 - Objeto/Arquivo; 31.2 - Aplicação/Site; 31.3 - Quantidade de violações; 31.4 - Ação realizada pela solução; 31.5 - Severidade; 31.6 - Data. 32 - Os incidentes de DLP deverão ser acionáveis, permitindo o aprofundamento da visibilidade do incidente e inclusive apresentar os dados que indicam o vazamento em questão na própria console da solução; 33 - A solução deve apresentar painel de comportamento para cada usuário do IFSC, identificando a nota de risco atual, bem como todo o histórico e atividades que levaram ao acréscimo ou decréscimo do risco; 34 - Os incidentes de malware devem ser acionáveis, permitindo aprofundamento do incidente, apresentando os usuários afetados, os arquivos relacionados a atividade maliciosa e a aplicação envolvida no incidente; 35 - A solução deve apresentar o HASH do arquivo para comparativo com base aberta de ameaças (VirusTotal) para identificar se a solução de endpoint corporativa do IFSC já possui assinatura preventiva contra a ameaça; 36 - Para todo o tráfego Web admitido, a solução deve realizar normalização e descoberta de aplicações SaaS – ShadowIT, sem a necessidade de importação de logs; 37 - Para as aplicações SaaS descobertas a solução deve realizar a classificação quanto à categoria (Ex: Cloud Storage), bem como o risco de tal aplicação; 38 - Minimamente apresentar se a aplicação SaaS possui em seu histórico recente vazamento de dados e vulnerabilidades em seus serviços; 39 - O risco deve ser uma das condicionantes para construção de regras de acesso web para os usuários do IFSC; 40 - Solução deve possuir capacidade de apresentar os logs de acesso em painel específico, garantindo a identificação do usuário, máquina, domínio, regra de processamento do tráfego e localização do acesso; 41 - Como forma de facilitar a visualização, a solução deve possuir painéis específicos que garantam: 42 - Visibilidade por aplicação – apresentando quais usuários acessaram tal aplicação, bem como os incidentes de malware e vazamento de dados, caso existam; 43 - Visibilidade por domínio – apresentando quais usuários acessaram tal domínio, bem como os incidentes de malware e vazamento de dados, caso existam; 44 - Visibilidade por usuário – apresentando os acessos, ações, geolocalização e incidentes de malware, comportamento e vazamento de dados; 45 - Deve possuir base própria de aplicações SaaS, com capacidade de controle granular, oferecendo no mínimo: 45.1 - O centro de inteligência do fabricante deve pontuar o índice de risco no uso de cada uma as aplicações SaaS não sancionadas (Shadow IT); 46 - Deve possuir associar o índice de risco de uma determinada aplicação ou categoria de aplicações a uma regra de bloqueio em tempo real; 47 - A solução deve ser capaz de apresentar se uma aplicação SaaS, em uso por parte dos usuários do IFSC, possui em seu histórico algum registro de vazamento de dados e vulnerabilidades associados; 48 - A solução deve gerar relatórios baseado no tráfego processado, suportando no mínimo: 48.1 - Relatório de risco das nuvens SaaS acessadas – ShadowIT; 48.2 - Relatório do acesso Web; 48.3 - Relatório do acesso SaaS; 49 - A solução deve prover mecanismos capazes de monitorar a experiência do usuário, garantindo: 49.1 - Telemetria detalhada para análise fim-a-fim e identificar problemas de performance através de painel específico para apresentar as latências entre o cliente e a unidade de processamento do fabricante e da unidade de processamento do fabricante até o serviço SaaS Microsoft Office 365; 49.2 - Deve possuir				

Item	Descrição	Unidade	Quant.	Preço Unit. (R$)	Valor Total (R$)
	dashboard específico para apresentar a volumetria de tráfego por unidade de processamento do fabricante (pop); 50 - Deve possuir painel específico com dados relacionados ao cliente, garantindo visibilidade quanto a versões em uso, usuário ativos, Bytes baixados e carregados, quantidade de sessões diárias; 51 - A console deve possuir, dentre suas características, solução de relatório com capacidade de apresentar as mais diversas dimensões, medidas e outros campos que se façam necessários para a construção de relatórios e dashboards analíticos, com as seguintes capacidades: 51.1 - Permitir a construção de relatórios customizados, utilizando os atributos disponíveis e os mais diversos formatos de exposição dos dados: Bar, Pie, Table, Trend, Sankey, Treemap, Pivots; 52 - Disponibilizar ao administrador 20 dashboards/relatórios pré-definidos, incluindo assessment de risco de acordo com a aplicações em nuvem em uso, governança de dados, CISO, uso de nuvens SaaS, uso de Web, proteção de dados, uso de aplicações privadas dentre outros; 53 - Deve permitir a exportação e agendamento dos dashboards nos formatos Excel, PDF, CSV e texto; 54 - Ao criar um dashboard ou relatório, a solução deve permitir o uso de campos customizados, cálculo de tabelas e filtros customizados com múltiplas opções de organização dos valores/resultados; 55 - A solução deve prover monitoramento proativo para identificação de Insider Threats; 57 - SERVIÇO DE SUPORTE 24X7 (nível 1, 2 e 3) do fabricante: 57.1 - Atendimento 24x7; 57.2 - Suporte por E-mail/Web; 57.3 - Suporte por telefone; 58.3 - Suporte por plantão (após horário comercial) 58.4 - Disponibilidade de documentação dos produtos do fabricante; 59 - A solução deve ter arquitetura de alta disponibilidade e realizar o balanceamento de carga automaticamente entre os Datacenters no Brasil, sem depender de nenhum componente de rede da infraestrutura da contratante; 60 - A solução deve permitir a instalação, quando necessário, de forma flexível em qualquer ponto/dispositivo da rede da Contratante, como por exemplo, atrás de uma configuração NAT (Network Address Translation); 61 - Deve suportar e estar licenciado para que o usuário que estiver fora do Brasil se conecte ao POP mais próximo geograficamente na nuvem do fabricante ou com menor latência para acesso as aplicações privadas localizadas no Brasil; 62 - Deve suportar e estar licenciado para acesso a, no mínimo, 1600 aplicações privadas, permitidas individualmente em regras de acesso por usuários e grupo de usuários, seguindo os conceitos de ZTNA e não agrupadas em segmentos; 63 - A solução deve autenticar o usuário em um provedor de identidade (IdP) e com base em identidade, políticas granulares, segmentação de aplicações e posturas específicas fornecer acesso a aplicações Web, ou qualquer outra com protocolo TCP e UDP, tais como (SSH, RDP, SQL, aplicações client-to-server, compartilhamento de arquivos, etc. de forma transparente, sem a necessidade de alteração do cliente original da aplicação, criando um túnel encriptado que conectará o usuário até a aplicação e não a rede da contratante; 64 - A solução não deve operar como uma Rede Privada Virtual (VPN) fornecendo um IP da rede local, e sim conectar o usuário direto, após validação de política de identidade, postura e políticas de acesso, aos recursos e aplicações com túneis encriptados específicos; 65 - Os usuários remotos não devem possuir visibilidade de aplicativos não autorizados. Os recursos não autorizados não devem apenas ser inacessíveis, mas também completamente invisíveis para os usuários; 66 - Todas as comunicações entre os componentes da solução e a infraestrutura em nuvem do fabricante devem mutuamente utilizar certificados pinados; 67 - A solução deve ser protegida, blindada contra ataques de "Man-in-the-middle" (MITM); 68 - A solução deve possuir recursos de monitoramento da atividade dos usuários, dando a equipe de TI da contratante alternativas de monitorar e gerenciar todas as atividades de forma granular, informando p.e., qual usuário, quando, qual aplicação, qual política autorizou ou negou o acesso, status da postura e localização do usuário; 69 - A solução deve suportar diferentes tipos de validação de perfil de acesso/postura, de acordo com cada plataforma/sistema operacional usado para o acesso remoto (Windows, Mac, iOS, Android e Linux), mas não somente: 69.1 - Validação da presença de um Antivírus; 69.2 - Validação de Certificado Cliente (chave privada e pública) assinada por um CA específico; 69.3 - Validação de Certificado confiável no dispositivo; 69.4 - Validação de qualquer processo executando na máquina; 69.5 - Validação de máquina no domínio; 69.6 - Validação de disco encriptado; 69.7 - Validação de Registro de chave no Windows; 69.8 - Validação de presença de um arquivo; 70 - Os componentes publicadores devem atualizar suas versões de forma automática e realizar suas atualizações em janelas pré-definidas e configuradas pela contratante (p.e. finais de semana, em horários pré-estabelecidos) de forma 100% automatizada, sem causar interrupção dos serviços e sem intervenção do administrador/equipe de TI da contratante; 71 - Permitir a utilização, quando necessário, de múltiplos fatores de autenticação dos usuários/acessos (MFA) através de integração com o IDP da contratante; 72 - Possibilitar a configuração de controles de acesso baseados em funções ("Role Based Access Control" - RBAC) com capacidade de criação de funções personalizadas; 73 - Possibilitar a integração com Microsoft AD (on premisses) e Azure AD (na "Nuvem") 74 - Possibilitar a implementação de políticas através de				

Item	Descrição	Unidade	Quant.	Preço Unit. (R$)	Valor Total (R$)
	Grupos do AD ("Microsoft Active Directory") e/ou Azure AD; 75 - Possibilitar a integração com plataformas de solução "Single Signon" (SSO); 76 - Disponibilizar Servidor de Armazenamento de Logs ("Log Server") próprio que permita o armazenamento de logs por, no mínimo, 90 dias e que possa ser integrado com plataformas "Security Information and Events Management" (SIEM) de terceiros; 77 - Possibilitar desabilitar formas legadas de autenticação; 78 - Permitir a implementação e utilização em ambientes de mais de uma Nuvem ("Cloud Computing"), nuvens híbridas, nuvens privadas, ou em instalações próprias da empresa ("on-premise"); 79 - Disponibilizar dados em formatos compatíveis para importação/upload em outras plataformas/sistemas (p.e., SOAR, SIEM, Excel, etc.); 80 - Disponibilizar informações granulares para revisões de acesso, independentemente da existência de uma solução de gestão de identidades; 81 - Acesso Remoto seguro sem VPN para proteção da rede e sistemas/aplicações internas; 82 - O ZTNA deve suportar os principais protocolos de comunicação, por exemplo, mas não somente, HTTPS, RDP, SSH, SFTP etc.; 83 - Aplicação ("Enforcement") de política baseada em controles de acesso por aplicações; 84 - Viabilizar a descoberta contínua de "ShadowIT", incluindo aplicativos não autorizados pela empresa; 85 - Proteção de acessos administrativos provendo acesso "just-in-time", de mínimo privilégio para reduzir o risco de permissões de acesso permanentes (sem expiração controlada); 86 - Permitir registrar os dispositivos de acesso em num provedor de identidade; 87 - Possuir validação de antivírus implementado e ativo; 88 - Possuir validação de criptografia de disco; 89 - Possuir validação se o dispositivo está no domínio corporativo; 90 - Possuir validação do sistema operacional do dispositivo; 91 - Possuir validação da localização do dispositivo; 92 - Possuir validação da rede do dispositivo; 93 - Permitir a customização dos controles de validação do dispositivo; 94 - Permitir a configuração de acesso aos recursos/sistemas internos sem necessidade de instalação software "Cliente" ("Clientless") nos dispositivos; 95 - Possuir um cliente/agente unificado para validação do dispositivo e aplicações instaladas no sistema operacional; 96 - Permitir verificar a conformidade dos dispositivos com as políticas de configuração e segurança de TI antes de iniciar o processo de log-in; 97 - Permitir implementar de forma obrigatória as políticas de configuração e segurança de TI nos dispositivos antes de iniciar o processo de log-in. 98 - Possuir recursos de monitoramento para identificação e análise de possíveis problemas de conectividade no ambiente; 99 - Possuir recurso de envio logs gerados para soluções externas de gerenciamento de logs para automatizar ações por meio de sistemas (p.e., SIEM) e/ou Centro de Operações de Segurança (SOC); 100 - Possuir recurso de auditoria de configurações aplicadas no sistema de Acesso Remoto de Confiança Zero (Zero Trust Network Access); 101 - Possuir recurso de auditoria de acessos realizados. 104 - A solução deve suportar SYSLOG para enviar mensagens para servidores de terceiros em eventos de rede e segurança; 105 - Portabilidade: todos os dados estruturados e não estruturados devem estar disponíveis para o cliente e fornecidos a eles mediante solicitação em um formato padrão da indústria (por exemplo, .docx, .xlsx, .pdf, logs e arquivos simples). O fornecedor deve utilizar protocolos de rede padronizados e seguros para a importação e exportação dos dados. 106 - Capacidade de ajustar os níveis de log seletivamente, por função ou por população de usuários finais. 107 - Integração com ferramenta de tickets: 107.1 - Automatização de serviços de ticket 107.2 - Detalhes do evento selecionado 107.3 - Mapeamento dos tickets para fluxo de trabalho 107.4 - Mute & De-duplication 108 - Troca de Ameaças: 108.1 - Compartilhar IOCs com solução de Endpoint Protection (EPP) utilizado pelo cliente (EDR/XDR /etc); 108.2 - Atualizações bidirecionais (tanto da SOLUÇÃO DE ZERO TRUST NETWORK ACCESS A APLICAÇÕES PRIVADAS quanto do EPP); 108.3 - File hases (DLP, Threat); 108.4 - URLs maliciosas; 109 - Troca de risco: 109.1 - Troca de nível de risco; 109.2 - Envolvendo: Usuários, dispositivos, e/ou aplicações; 109.3 - Gatilhos para ações integradas para abertura de ticket; 110 - Relatórios Avançados: 110.1 - Capacidade de automatizar o envio de relatórios customizados, via e- mail, a usuários específicos; 110.2 - Possibilitar a criação e modificação de atributos dos alarmes (p.e. status, inclusão de campos textuais, cálculo do tempo de tratamento dos alarmes); 110.3 - Gerar relatórios, padronizados ou customizados, podendo apresentar informações agrupadas ou expandidas pelos atributos utilizados para caracterizar os alarmes; 110.4 - Deve permitir a geração de relatórios sob demanda para emissão pontual ou periódica, possibilitando a exportação em PDF ou CSV. 110.5 - Os relatórios devem possibilitar listar os sites mais acessados e os mais bloqueados com suas respectivas categorias e URLs, permitindo a busca por IP, URL ou domínio por intervalo de tempo. 110.6 - Capacidade de automatizar o envio de relatórios customizados, via e- mail, a usuários específicos; 110.7 - Possibilitar a criação e modificação de atributos dos alarmes (p.e. status, inclusão de campos textuais, cálculo do tempo de tratamento dos alarmes); 110.8 - Gerar relatórios, padronizados ou customizados, podendo apresentar informações agrupadas ou expandidas pelos atributos utilizados para caracterizar os alarmes; ***GERÊNCIA DE PROJETO, IMPLEMENTAÇÃO,				

Item	Descrição	Unidade	Quant.	Preço Unit. (R$)	Valor Total (R$)
	CUSTOMIZAÇÃO E SUPORTE:*** 111 - Deve ser alocado pela CONTRATADA da solução, no mínimo, um Gerente de Projetos com certificação PMP e que possua fluência na língua portuguesa para a gerência de todo o projeto; 112 - Deve ser alocado pela CONTRATADA da solução, no mínimo, dois Professional Services que possuam fluência na língua portuguesa para devida implementação, configurações e customizações da solução contratada; 113 - Deve ser alocado pela CONTRATADA, no mínimo, um Instrutor de treinamento que possua fluência na língua portuguesa para entrega dos treinamentos em língua portuguesa; 114 - Apresentação e validação de plano de implementação do projeto com detalhamento das atividades, cronograma previsto, duração, prazos, profissionais envolvidos, necessidades, premissas etc. seguindo as melhores práticas de gerenciamento de projetos, p.e., PmBOK/PMI; 115 - Devem estar em conjunto o profissional do fabricante da solução e o parceiro fornecedor; 116 - Realização de reunião de Kick-off de projeto, reuniões semanais e sempre que necessário, de apresentação de Status Report do andamento do projeto; 117 - Devem estar em conjunto o profissional do parceiro fornecedor; 118 - Elaboração e apresentação de relatórios detalhado e executivo de Status Report do andamento do projeto; 119 - Devem estar em conjunto o profissional do parceiro fornecedor; 120 - Após a finalização do escopo proposto a ser implantado pelo fabricante ou parceiro, um profissional do fabricante ou do parceiro fornecedor, customer success, deve prestar os seguintes serviços durante todo o contrato em língua portuguesa no Brasil: 120.1 - Apoio técnico para os administradores da solução; 120.2 - Apoio executivo para CISO/CSO; 121 - O apoio se baseia em: 121.1 - Compartilhar boas práticas de administração da solução; 121.2 - Documentação técnica para apoiar e sustentar uma determinada decisão técnica 121.3 - Desenhar e apresentar junto aos decisores um roadmap estratégico para determinar os passos de proteção e governança; 121.4 - Prover Transferência de conhecimento pós-implantação; 121.5 - Fornecer liderança técnica e orientação para conduzir a implantação e operacionalização da plataforma; 121.6 - Auxiliar na configuração e ajuste de políticas, configuração de aprimoramentos do produto e revisões periódicas de políticas; 121.7 - Executar um plano estratégico de realização e obtenção de valor e retorno sobre investimento, conforme casos de uso que estejam alinhados às necessidades de segurança e do negócio. 122 - As atividades macro de implantação do projeto: 122.1 - Configurações básicas de acesso para administradores do tenant; 122.2 - Definição das ROLES de cada administrador do tenant; 122.3 - Integração de AD/Azure AD de grupos e usuários; 122.4 - Configuração de tráfego de grupos sincronizados do AD/Azure AD e definição de exceções desse tráfego; 122.5 - Configuração dos Clients, por grupo, conforme os grupos sincronizados do AD/Azure AD; 122.6 - Criação de templates de notificação (pop-up) customizados; 122.7 - Criação de aplicações de acesso via ZTNA; 122.8 - Definição de políticas de acesso para as aplicações utilizadas via ZTNA; *********SUBSCRIÇÃO = 36 MESES********** *****TREINAMENTO***** 123 - ADMINISTRAÇÃO E OPERAÇÃO DA SOLUÇÃO: 123.1 - Segurança em nuvem; 123.2 - Arquitetura; 123.3 - Níveis de risco de aplicações SaaS; 123.4 - Proteção via API; 123.5 - Políticas; 123.6 - Client da solução; 123.7 - Threat Protection; 123.8 - Relatórios; 123.9 - Relatórios avançados; 123.10 - IaaS; 123.11 - Segurança Web; 123.12 - ROLES (Role-Based Access Control); 123.13 - Segurança IoT ; 124 - IMPLEMENTAÇÃO E INTEGRAÇÃO: 124.1 - SAML; 124.2 -ZTNA; 124.3 -DLP; 124.4 -Segurança Web ; 124.5 -Relatórios avançados; 124.6 -REST API; 124.7 -Security Posture Management; 124.8 -Remote Browser Isolation (RBI);				
				Valor Total do Lote/Grupo: R$ 6.054.480,00	

Valor Total do Processo: R$ 8.753.039,54