ATA DE REGISTRO DE PREÇOS

INSTITUTO FEDERAL DE SANTA CATARINA

ATA DE REGISTRO DE PREÇOS N.º 21117/2023

O INSTITUTO FEDERAL DE SANTA CATARINA - IFSC, com sede na Rua 14 de Julho, 150, Coqueiros, 88075-010, na cidade de Florianópolis/SC, inscrito(a) no CNPJ/MF sob o nº 11.402.887/0001-60, neste ato representado pelo Reitor, Maurício Gariba Junior, nomeado pelo Decreto de 9 de Agosto de 2021, publicado no DOU de 10 de agosto de 2021, portador da Matrícula Funcional no 0277933, , considerando o julgamento da licitação na modalidade de pregão, na forma eletrônica, para REGISTRO DE PREÇOS nº 21117/2023, publicada no Diário Oficial da União de 10/01/2024, processo administrativo n.º 23292.015079/2023-35, RESOLVE registrar os preços da(s) empresa(s) indicada(s) e qualificada(s) nesta ATA, de acordo com a classificação por ela(s) alcançada(s) e na(s) quantidade(s) cotada(s), atendendo as condições previstas no Edital de licitação, sujeitando-se as partes às normas constantes na Lei nº 14.133, de 1º de abril de 2021, no Decreto n.º 11.462, de 31 de março de 2023, e em conformidade com as disposições a seguir:

1. DO OBJETO

1.1. A presente Ata tem por objeto o registro de preços para a eventual AQUISIÇÃO DE CESSÃO TEMPORÁRIA DE DIREITOS DE USO DE SOFTWARES DE SEGURANÇA CIBERNÉTICA , especificado(s) no Termo de Referência, anexo I do edital de Licitação nº 21117/2023 , que é parte integrante desta Ata, assim como as propostas cujos preços tenham sido registrados, independentemente de transcrição.

2. DOS PREÇOS, ESPECIFICAÇÕES E QUANTITATIVOS

2.1. O preço registrado, as especificações do objeto, as quantidades mínimas e máximas de cada item, fornecedor(es) e as demais condições ofertadas na(s) proposta(s) são as que seguem:

ANEXO I - DA ATA DE REGISTRO DE PREÇOS

EMPRESAS E PREÇOS REGISTRADOS

Pregão Nº 21117 / 2023 – SRP
Processo nº 23292.015079/2023-35

Relação de empresas vencedoras, contendo a descrição dos itens e preços negociados na sessão do Pregão. Prazo para entrega: **Item 1**: 15 (quinze)dias após o recebimento da AF para os **demais itens**: 30(trinta) dias após o recebimento da AF.

EMPRESA (1)			ADVANTA SISTEMAS DE TELECOMUNICACOES E SERVICOS DE INFORMATICA LTDA		
ENDEREÇO			**AV. COPACABANA, 325 ☙ 18º ANDAR ☙ SALA 1810 A 1814. Bairro: DEZOITO DO FORTE EMPRESARIAL, BARUERI / SC CEP: 06472-001**		
CNPJ			03.232.670/0001-21		
TELEFONE/FAX			11 4504 5900		
REPRESENTANTE LEGAL			Wilson Roberto Piedade		
CPF REPRESENTANTE			087.941.398-06		
Email			will.sebben@oakmontgroup.com.br		
ITEM	**UNID.**	**QTD.**	**ESPECIFICAÇÃO**	**Preço Unitário (R$)**	**Preço Total (R$)**
1	UNIDADE	20.0	Código: 33904021006000257 SERVIÇO DE IMPLEMENTAÇÃO DE SOLUÇÃO DE SEGURANÇA DE DADOS 1. FASES: a. Avaliação de Pré-implementação: i. A CONTRATADA deve prover um especialista com certificação nas ferramentas ofertadas ao CONTRATANTE, sendo necessária comprovação técnica delas. ii. O especialista da CONTRATADA analisará os requisitos da CONTRATANTE e compreenderá as necessidades de segurança,	7.489,23	149.784,60

			ambiente de rede e objetivos de negócios na implementação. Além disso, o plano de rollout também será avaliado e as inadequações serão previamente apontadas. b. Cronograma do plano de implementação: i. Reunião de alinhamento inicial, em conjunto com o Consultor Técnico de Cibersegurança da CONTRATADA, com as áreas internas da CONTRATANTE para estabelecimento de metas, cronogramas e prazos médios; ii. Após a avaliação, o especialista da CONTRATADA designado deverá desenvolver o plano de implementação, incluindo o escopo da implementação, marcos e tarefas operacionais para atender aos requisitos. O escopo de implementação não deve ser alterado depois de confirmado pelo cliente. Não faz parte do escopo: 1. Avaliação referente a processos e adequações internas de utilização da ferramenta; c. Execução: i. A implementação deverá ser realizada de acordo com o plano aceito pela CONTRATANTE anteriormente, este baseado nas melhores práticas recomendadas pelo FABRICANTE. ii. A implementação será realizada de maneira remota, sendo de responsabilidade da CONTRATANTE disponibilizar os acessos necessários à equipe técnica da CONTRATADA. iii. Será de responsabilidade da CONTRATADA definir o meio de implementação da ferramenta mais eficaz para o ambiente de acordo com a necessidade da CONTRATANTE, podendo esta ser realizada por agente ou por scanners. Devendo a CONTRATANTE designar equipe técnica que possa auxiliar em qualquer demanda referente		

			ao processo de deploy. iv. Para fins de eficiência, o planejamento inicial deve ser executado considerando uma margem máxima de 5% de atraso, seja da CONTRATANTE ou da CONTRATADA. Caso ocorram atrasos de maior proporção, este contrato poderá ser renegociado entre as partes. d. Relatório de Implementação: i. O Relatório de Implantação de Lançamento deverá ser entregue para resumir o procedimento de implementação e os resultados. O relatório fornecerá à CONTRATANTE uma compreensão da implantação, configuração, tarefas de operação e alguns recursos dos produtos ofertados. 2. IMPLEMENTAÇÃO a. Os serviços de instalação deverão ser executados pela CONTRATADA durante o horário comercial compreendido entre 8h e 17h, de segunda à sexta-feira, devendo, eventualmente, atender a CONTRATANTE em finais de semana e feriados para atendimento ou acompanhamento de configurações que necessitem ser executadas nestes horários, cabendo à CONTRATANTE informar tais atendimentos à CONTRATADA, antecipadamente e de comum acordo entre as partes; b. A CONTRATADA, depois de concluído o serviço de configuração da solução, deverá realizar, com o acompanhamento remoto dos técnicos da CONTRATANTE, testes de operação para constatar que a solução foi devidamente instalada e configurada de acordo com o cenário requerido pela CONTRATANTE, período este não excedente a 48 horas.		

			c. Após a reunião final de Golive, o suporte, bem como abertura de chamados e sustentação relacionados a ferramenta é de responsabilidade da CONTRATANTE e do FABRICANTE. Marca: ADVANTA Fabricante: ADVANTA		
2	UNIDADE	3000.0	Código: 33904006002000004 SOLUÇÃO DE DETECÇÃO, RESPOSTA E PROTEÇÃO CONTRA MALWARE - SEGURANÇA DE DADOS 1. A solução deve ser entregue como um serviço Software-as-a-Service (SaaS) em nuvem para todos os seus serviços e aplicativos exigidos neste documento. 2.Todos os serviços da plataforma devem estar disponíveis sob o mesmo padrão de qualidade de serviço 24x7x365 e garantir 99% de disponibilidade. 3. A FABRICANTE deve oferecer manutenção e atualização constante da plataforma durante todo o período de vigência do contrato de serviço. 4. As atualizações de serviço devem ser transparentes para o administrador da solução, sem afetar nenhum dos dados armazenados e serviços fornecidos. 5. As janelas de manutenção programada deverão ocorrer dentro do período de indisponibilidade aceita (1%) e previamente avisada. 6. A plataforma que fornece os serviços deve ser certificada pela FedRAMP e certificada para os procedimentos de segurança SSAE 18 SOC 2. 7. Todas as comunicações entre componentes, transferência de dados e sincronização da solução devem ser criptografadas de ponta a ponta, fazendo uso de no mínimo TLS 1.2, certificados assinados	222,12	666.360,00

			com RSA 2048 bits e algoritmo de assinatura SHA256. 8. A solução deve permitir: 8.1. a criação de usuários distintos; 8.2. a separação de funções e permissões na console; 8.3. a integração através de SSO com, pelo menos, Okta e Azure Active Directory; 8.4. acessibilidade a partir de, pelo menos, um dos navegadores comerciais dentre Google Chrome, Microsoft Edge e Firefox. 9. A solução proposta deve permitir administração centralizada via interface gráfica WEB usando HTTPS. 10. A solução deve possibilitar o acesso a console de todos os componentes do serviço a partir de um único ponto. 11. A solução deve permitir a definição de diferentes perfis de usuários e funções para administração. 12. A solução deve fornecer controles de acesso de usuário hierárquicos e baseados em funções que permitem a delegação de responsabilidades para refletir a estrutura organizacional. 13. A solução deve permitir o acesso de um usuário autorizado de qualquer local. 14. A solução deve suportar autenticação de dois fatores para usuários e login. 15. A solução deve suportar configurações de segurança de senha. 16. A solução deve suportar personalizar a política de segurança para configurações de gerenciamento de senha, por: 16.1. idade e expiração da senha; 16.2. conta do usuário bloqueada após uma série de logins com falha; 16.3. comprimento mínimo da senha; 16.4. complexidade da senha, caracteres alfanuméricos e numéricos a serem usados;		

			16.5. forçar mudança de senha no login inicial; 16.6. notificação de senha expirada antes de vários dias.  17. A solução deve suportar a capacidade de restringir o acesso apenas de rede interna da empresa. 18. A solução deve suportar a capacidade de rastrear a atividade do usuário por nome da conta do usuário, data, ação e informações sobre a ação. 19. A solução deve suportar acesso por SSO (Single Sign-on) usando SAML 2.0. 20. A solução deve possuir um painel (dashboard) que, por padrão, permite que você veja as tendências de fragilidades por gravidade, plataforma, idade e status de remediação. ---------- AGENTES (ENDPOINTS) 1. A solução proposta deve oferecer um agente de baixo impacto nos sistemas operacionais onde está instalado e no consumo de largura de banda que utilizará na rede. 2. A solução deve ser instalada em servidores, estações de trabalho e máquinas virtuais, suportando sua implantação em rede local, em rede doméstica e na nuvem. 3. A solução deve oferecer suporte para sua implantação em pelo menos os seguintes sistemas operacionais: 3.1. Windows 7/Windows Server 2003 SP2 e posterior (x86, x64); 3.2. Red Hat Enterprise Linux/CentOS 6.5+, 7.x (x64), 8.x (x64); 3.3. Ubuntu 14, 16,18,19,20 (x64); 3.4. Oracle Enterpise Linux 8, Oracle Enterprise Linux (OEL) 7 até 7.5, Oracle Enterprise Linux (OEL) 6; 3.5. Amazon Linux 2, Amazon Linux 2018.03,		

			Amazon Linux 2017.09, Amazon Linux 2017.03; 3.6. SUSE Linux Enterprise Server (SLES) 12, SUSE Linux Enterprise Server (SLES) 11; 4. O agente da solução deve se atualizar automaticamente e gerir as suas atualizações automaticamente. 5. A solução deve suportar plataformas de nuvem AWS, GCP e Azure. 6. A solução deve prover nativamente um dispositivo capaz de concentrar requisições dos agentes para encaminhamento a console de gerenciamento de forma a evitar a conexão direta de agentes com a plataforma. 7. O agente de gerenciamento deve suportar o uso de proxy. 8. Deve ser possível definir o intervalo de comunicação entre o agente e a console de gerenciamento. 9. Deve ser possível limitar o consumo de CPU e memória do agente. 10. Deve permitir a definição de um período global de inatividade dos agentes. 11. A solução deve prover nativamente um mecanismo de cache dos principais patches aplicados no ambiente visando a redução do consumo de banda. --- MÓDULO 1 1. A solução deve permitir armazenamento de eventos com a finalidade de busca histórica e pesquisa de comportamentos maliciosos. 2. Os eventos devem ser coletados independentemente da localização do equipamento monitorado e enviados ao console de gerenciamento. 3. Não deve ser necessário utilização de VPN e proxy configurados nos equipamentos para que seja possível receber eventos. 4. A solução deve permitir a coleta e busca de		

			informações sobre atividades de sistemas operacionais para, no mínimo: a. Criação e encerramento de processos; b. Modificações de registro; c. Comunicação de rede; d. Criação e modificação de arquivos. 5. Atividades de processo deverão incluir as seguintes informações: a. Argumentos que foram utilizados para execução do binário; b. Usuário associado; c. Caminho completo do processo; d. Hash SHA256; e. Módulos e DLL carregadas; f. Hostname, endereço IP do ativo associado; g. PID. 6. A solução deve: a. Possuir árvore de processo, incluindo a cadeia de processos pai, filho e atividades detalhadas do processo. b. Permitir navegação interativa na árvore de processos, exibindo detalhes para cada processo e evento envolvido na trilha de execução. c. Informar táticas, técnicas e softwares com classificação do MITRE ATT&CK quando aplicável. d. Atribuir uma pontuação de risco para eventos coletados de desktop e servidores. e. Permitir encerramento de processos a partir da console de gerenciamento de forma nativa, sem utilização de scripts ou softwares auxiliares. f. Permitir colocar ativos específicos em isolamento da rede a partir da console de gerenciamento. 7. Em ativos em isolamento, deverá ser possível criar uma whitelist de aplicações permitidas durante o período de isolamento. 8. Para eventos relacionados a arquivos, a		

			solução deve ser capaz de apontar o tipo de arquivo e extensão. 9. Para arquivos criados e modificados, a solução deve ser capaz de apresentar o processo pai que realizou a ação de criação ou modificação no evento. 10. Deve permitir que a partir da console o arquivo possa ser colocado em quarentena ou removido, sem necessidade de softwares auxiliares. 11. Deve apresentar no mínimo as seguintes informações para eventos relacionados a conexões de rede: a. Endereço IP de destino; b. Porta de destino; c. Porta local; d. Endereço FQDN do host de destino. 12. Deve ser capaz de mostrar portas em modo listening para processos e serviços iniciados. 13. Deve monitorar atividades de registro do Windows para, no mínimo, os seguintes critérios: a. Escrita de chaves de registro; b. Modificação de chaves de registro; c. Endereço IP e hostname do ativo envolvido. 14. Deve apontar a chave exata objeto do evento. 15. Deve apontar valores alterados de chave de registro. 16. Deve apontar o processo responsável pela modificação de chaves de registro. 17. Deve apontar táticas e técnicas do MITRE ATT&CK de ameaças associadas ao registro do Windows. 18. Deve monitorar eventos relacionados a MUTEX. 19. A solução deve prover uma interface gráfica para busca de eventos. 20. Deve ser possível a busca por		

			propriedades do evento de forma facilitada aos administradores da solução. 21. Deve ser possível listar as propriedades disponíveis para busca com um breve exemplo de como devem ser utilizadas. 22. Deve ser possível realizar buscas para os cenários abaixo: a. Todas as alterações de registro de um determinado ativo no último dia; b. Alterações de chave de registro tendo como origem um processo específico; c. Arquivos PDF renomeados por um determinado processo; d. Conexões de rede com uma determinada porta de destino e para FQDNs específicos; e. Todos os processos que iniciaram conexão de rede para um determinado IP no último mês; 21. Deve ser permitido salvar buscas realizadas na própria console. 22. Deve permitir a criação de dashboards com base em buscas de eventos existentes. 23. ALERTAS: a. A solução deve permitir a criação de alertas aos administradores caso eventos específicos sejam encontrados no ambiente. b. Os alertas devem permitir a utilização de filtros de eventos. c. Deve conter um histórico de alertas gerados e sua ação. d. As ações resultantes de um alerta devem permitir, pelo menos, o envio de Email. e. Deve ser permitido a customização de mensagens e destinatários dos alertas. f. A solução deve permitir agregar alertas em intervalos pré-determinados para evitar um número excessivo de mensagens. g. O intervalo de agregação deve ser configurável em minutos ou em um intervalo de horas.		

			DO ANTI-MALWARE 24. A solução deve permitir detecção e bloqueio de ataques incluindo malwares, ataques sem arquivo (Fileless), phishing, roubo de credenciais, entre outros. 25. Deverá permitir varreduras em tempo real e agendadas. 26. Para varreduras em tempo real, deverá permitir pelo menos as ações abaixo: a. Negar acesso ao arquivo infectado; b. Limpar o arquivo infectado; c. Deletar o arquivo infectado. 27. Deverá permitir a inspeção de arquivos comprimidos para varredura em tempo real. 28. Deve manter uma cópia de arquivos detectados. 29. Deverá permitir agendamento de varreduras em disco, com agendamento pré-definido. 30. Deverá permitir exclusões com base em informações de detecção para pelo menos, arquivos e pastas, processos detectados, endereços IP e domínios envolvidos em um evento de detecção. 31. Deverá conter mecanismos específicos para proteção de ataques de rede, sendo capaz de detectar, pelo menos, os seguintes comportamentos: a. Acesso inicial; b. Roubo de credenciais; c. Movimentação lateral; d. Ações de descoberta com finalidade maliciosa. 32. Deverá analisar o tráfego de rede dos equipamentos incluindo inspeção SSL. 33. Deverá permitir aplicação de políticas diferentes para equipamentos que estejam fora da rede interna. 34. Deve ser possível configurar alertas locais para detecção de malwares ou atividades		

			suspeitas. 35. Deve ser possível proteger contra alteração de configurações locais através de definição de senha. 36. Os eventos gerados devem ser enviados ao console centralizado da solução. 37. Deve ser possível limitar o consumo de CPU. 38. Deve ser possível pesquisar os incidentes gerados a partir da console de gerenciamento. 39. Cada incidente deve conter, no mínimo, as seguintes informações: a. Nome da ameaça; b. Nome do arquivo; c. Caminho do arquivo; d. Ação realizada; e. Hash SHA 256; f. Fragilidades associadas; g. Permitir pesquisar pela presença de fragilidades associadas. 40. A solução deve agrupar eventos relacionados a uma mesma ameaça, permitindo uma investigação assertiva. 41. Deverá mostrar o processo responsável pela execução de uma ameaça. 42. A console deverá prover uma interface para pesquisa rápida de incidentes. 43. Deve suportar ao menos as pesquisas abaixo para incidentes encontrados: a. Táticas e técnicas do MITRE ATT&CK e ativo específico; b. Incidente de detecção de arquivos no último mês; c. Agrupar incidentes por nível de risco e categoria de malware específica; d. Detecções de um sistema operacional específico. RELATÓRIOS E DASHBOARDS: 44. A solução deve conter painéis que exibam,		

			no mínimo, as seguintes informações: a. Ativos com anti-malware habilitado; b. Ativos sem proteção instalada; c. Agrupar em tabela quantidade de incidentes por ativo; d. Agrupar em gráfico incidentes separados por tipo de malware; e. Detecções separadas por tática e técnica do MITRE ATT&CK; f. Gráfico em linha mostrando detecções por dia nos últimos 30 dias; g. Quantidade de conexões de rede de endpoints para uma determinada porta. 45. A solução deve permitir a customização dos painéis fazendo uso de qualquer um dos dados disponíveis associados aos ativos protegidos para selecionar diferentes tipos de gráficos, tabelas e visualizações sobre incidentes. 46. A solução deve fornecer painéis executivos personalizáveis com uma visão unificada de todos os componentes da solução. 47. Deve ser possível criar dashboards que mostrem a pontuação de risco global de ativos e sua variação ao longo do tempo. 48. Deve permitir a criação de um painel que mostre quantidade de softwares instalados nos ativos protegidos. 49. A solução deve conter painéis previamente criados que possam ser importados pelos administradores. Marca: ADVANTA Fabricante: ADVANTA		
3	UNIDADE	3000.0	Código: 33904006002000006 SOLUÇÃO DE GERENCIAMENTO DE FRAGILIDADES - SEGURANÇA DE DADOS 1. A solução deve ser entregue como um serviço Software-as-a-Service (SaaS) em nuvem para todos os seus serviços e aplicativos exigidos neste documento.	158,31	474.930,00

			2.Todos os serviços da plataforma devem estar disponíveis sob o mesmo padrão de qualidade de serviço 24x7x365 e garantir 99% de disponibilidade. 3. A FABRICANTE deve oferecer manutenção e atualização constante da plataforma durante todo o período de vigência do contrato de serviço. 4. As atualizações de serviço devem ser transparentes para o administrador da solução, sem afetar nenhum dos dados armazenados e serviços fornecidos. 5. As janelas de manutenção programada deverão ocorrer dentro do período de indisponibilidade aceita (1%) e previamente avisada. 6. A plataforma que fornece os serviços deve ser certificada pela FedRAMP e certificada para os procedimentos de segurança SSAE 18 SOC 2. 7. Todas as comunicações entre componentes, transferência de dados e sincronização da solução devem ser criptografadas de ponta a ponta, fazendo uso de no mínimo TLS 1.2, certificados assinados com RSA 2048 bits e algoritmo de assinatura SHA256. 8. A solução deve permitir: 8.1. a criação de usuários distintos; 8.2. a separação de funções e permissões na console; 8.3. a integração através de SSO com, pelo menos, Okta e Azure Active Directory; 8.4. acessibilidade a partir de, pelo menos, um dos navegadores comerciais dentre Google Chrome, Microsoft Edge e Firefox. 9. A solução proposta deve permitir administração centralizada via interface gráfica WEB usando HTTPS. 10. A solução deve possibilitar o acesso a		

			console de todos os componentes do serviço a partir de um único ponto. 11. A solução deve permitir a definição de diferentes perfis de usuários e funções para administração. 12. A solução deve fornecer controles de acesso de usuário hierárquicos e baseados em funções que permitem a delegação de responsabilidades para refletir a estrutura organizacional. 13. A solução deve permitir o acesso de um usuário autorizado de qualquer local. 14. A solução deve suportar autenticação de dois fatores para usuários e login. 15. A solução deve suportar configurações de segurança de senha. 16. A solução deve suportar personalizar a política de segurança para configurações de gerenciamento de senha, por: 16.1. idade e expiração da senha; 16.2. conta do usuário bloqueada após uma série de logins com falha; 16.3. comprimento mínimo da senha; 16.4. complexidade da senha, caracteres alfanuméricos e numéricos a serem usados; 16.5. forçar mudança de senha no login inicial; 16.6. notificação de senha expirada antes de vários dias.  17. A solução deve suportar a capacidade de restringir o acesso apenas de rede interna da empresa. 18. A solução deve suportar a capacidade de rastrear a atividade do usuário por nome da conta do usuário, data, ação e informações sobre a ação. 19. A solução deve suportar acesso por SSO (Single Sign-on) usando SAML 2.0. 20. A solução deve possuir um painel (dashboard) que, por padrão, permite que você veja as tendências de fragilidades por		

			gravidade, plataforma, idade e status de remediação. ---------- AGENTES (ENDPOINTS) 1. A solução proposta deve oferecer um agente de baixo impacto nos sistemas operacionais onde está instalado e no consumo de largura de banda que utilizará na rede. 2. A solução deve ser instalada em servidores, estações de trabalho e máquinas virtuais, suportando sua implantação em rede local, em rede doméstica e na nuvem. 3. A solução deve oferecer suporte para sua implantação em pelo menos os seguintes sistemas operacionais: 3.1. Windows 7/Windows Server 2003 SP2 e posterior (x86, x64); 3.2. Red Hat Enterprise Linux/CentOS 6.5+, 7.x (x64), 8.x (x64); 3.3. Ubuntu 14, 16,18,19,20 (x64); 3.4. Oracle Enterpise Linux 8, Oracle Enterprise Linux (OEL) 7 até 7.5, Oracle Enterprise Linux (OEL) 6; 3.5. Amazon Linux 2, Amazon Linux 2018.03, Amazon Linux 2017.09, Amazon Linux 2017.03; 3.6. SUSE Linux Enterprise Server (SLES) 12, SUSE Linux Enterprise Server (SLES) 11; 4. O agente da solução deve se atualizar automaticamente e gerir as suas atualizações automaticamente. 5. A solução deve suportar plataformas de nuvem AWS, GCP e Azure. 6. A solução deve prover nativamente um dispositivo capaz de concentrar requisições dos agentes para encaminhamento a console de gerenciamento de forma a evitar a conexão direta de agentes com a plataforma. 7. O agente de gerenciamento deve suportar o		

			uso de proxy. 8. Deve ser possível definir o intervalo de comunicação entre o agente e a console de gerenciamento. 9. Deve ser possível limitar o consumo de CPU e memória do agente. 10. Deve permitir a definição de um período global de inatividade dos agentes. 11. A solução deve prover nativamente um mecanismo de cache dos principais patches aplicados no ambiente visando a redução do consumo de banda. ---------- MÓDULO 2 1. A solução deve permitir varreduras com base em: a. Sistemas Operacionais; b. Serviços WEB; c. Portas TCP e UDP; d. Serviços; e. Aplicações; f. Bancos de dados; g. Dispositivos de rede como switches, roteadores e balanceadores de carga; 2. No mínimo, a ferramenta deve abranger os seguintes sistemas operacionais, bancos de dados e aplicativos: a. Microsoft Windows; b. UNIX; c. LINUX; d. MacOS; e. Mac OS X; f. Cisco; g. Vmware; h. FortiOS; 3. Detectar e analisar fragilidades nas principais versões de Bancos de Dados, pelo menos: a. Microsoft SQL Server;		

			b. MySQL; c. Oracle; d. Sybase; 4. Detectar e analisar fragilidades em plataformas WEB, pelo menos: a. IIS; b. Apache Tomcat; 5. Detectar e analisar fragilidades em portas e serviços TCP e UDP. 6. Detectar fragilidades em pelo menos os seguintes aplicativos ou plataformas: a. Adobe; b. Apple; c. HP; d. McAfee; e. Microsoft (Office, IIS, Exchange); f. Oracle; g. Oracle Java; h. VMware; 7. Permitir a descoberta de fragilidades na rede, oferecendo as seguintes alternativas de varredura: a. Varredura ativa de rede não autenticada; b. Varredura ativa de rede autenticada; c. Agente; d. Varreduras externas; 8. A base de conhecimento de fragilidade deve ser atualizada semanalmente, garantindo a incorporação de pelo menos 20 CVEs a ela e deve ter pelo menos uma base de conhecimento de 35.000 CVEs relacionados incluindo tecnologias legadas e atuais. 9. A solução deve oferecer suporte ao padrão da indústria para pontuação de fragilidade do Common Vulnerability Scoring System (CVSS). 10. A solução deve oferecer suporte ao padrão da indústria para adicionar detecções personalizadas usando Open Vulnerability Assessment Language (OVAL).		

			11. A solução deve permitir vincular as fragilidades detectadas e indicar sua relação com ameaças como Vírus, Trojan e Malware. 12. A solução deve ser capaz de indicar explorações disponíveis e códigos disponíveis para uma fragilidade, quando aplicável. 13. O banco de dados deve relacionar a maioria das fragilidades ao CVE e Bugtraq. 14. A solução deve oferecer suporte à integração para autenticação por ferramentas de cofres de senha com ao menos dois dos seguintes fabricantes: Thycotic/Centrify, CyberArk, BeyondTrust. 15. A solução deve permitir buscas interativas de fragilidade utilizando filtros como severidade, categoria, sistema operacional, status, classificação do CVSS, CVE ou KB. 16. A solução deve permitir a utilização de operadores lógicos na busca de fragilidades para que seja possível encontrar, no mínimo, as seguintes informações: a. Fragilidades associadas a ransomware e que possuem patches disponíveis; b. Fragilidades detectadas em um segmento de rede; c. Fragilidades detectadas em serviços específicos; d. Fragilidades detectadas por um usuário específico; e. Fragilidades detectadas por tag AWS ou Azure específicas; f. Vulnerabildiades detectadas em hardware específico; 17. Na busca de fragilidades deve permitir agrupamento para mostrar, no mínimo, as seguintes visualizações: a. Quantidade de ocorrências de uma mesma fragilidade; b. Quantidade de fragilidades por sistema operacional;		

			c. Quantidade de fragilidades por host; d. Quantidade de fragilidades por Exploit disponível; e. Quantidade de fragilidades por produto /software vulnerável; 18. A solução deve permitir exportar buscas e filtros criados para um dashboard. 19. A solução deve permitir salvar filtros criados em buscas para reutilização. 20. Deve mostrar dashboards que consigam mostrar variação histórica de fragilidades novas, corrigidas, reabertas. 21. Deve permitir mostrar dashboards que contenham quantidades de fragilidades associadas a ransomware, que contém exploits públicos e que permitem exploração sem autenticação. 22. Deve mostrar dashboards que mostrem o racional de fragilidades que podem ser corrigidas através de patches. 23. Deve mostrar patches faltantes em sistemas operacionais independente da relação com uma fragilidade existente. 24. A solução deve oferecer a possibilidade de monitorar dispositivos móveis Android, IOS, IpadOS. Marca: ADVANTA Fabricante: ADVANTA		
4	UNIDADE	3000.0	Código: 33904006002000008 SOLUÇÃO DE GERENCIAMENTO DE PATCH (REMEDIAÇÃO DE ATIVOS) - SEGURANÇA DE DADOS 1. A solução deve ser entregue como um serviço Software-as-a-Service (SaaS) em nuvem para todos os seus serviços e aplicativos exigidos neste documento. 2.Todos os serviços da plataforma devem estar disponíveis sob o mesmo padrão de qualidade de serviço 24x7x365 e garantir 99% de disponibilidade.	287,75	863.250,00

			3. A FABRICANTE deve oferecer manutenção e atualização constante da plataforma durante todo o período de vigência do contrato de serviço. 4. As atualizações de serviço devem ser transparentes para o administrador da solução, sem afetar nenhum dos dados armazenados e serviços fornecidos. 5. As janelas de manutenção programada deverão ocorrer dentro do período de indisponibilidade aceita (1%) e previamente avisada. 6. A plataforma que fornece os serviços deve ser certificada pela FedRAMP e certificada para os procedimentos de segurança SSAE 18 SOC 2. 7. Todas as comunicações entre componentes, transferência de dados e sincronização da solução devem ser criptografadas de ponta a ponta, fazendo uso de no mínimo TLS 1.2, certificados assinados com RSA 2048 bits e algoritmo de assinatura SHA256. 8. A solução deve permitir: 8.1. a criação de usuários distintos; 8.2. a separação de funções e permissões na console; 8.3. a integração através de SSO com, pelo menos, Okta e Azure Active Directory; 8.4. acessibilidade a partir de, pelo menos, um dos navegadores comerciais dentre Google Chrome, Microsoft Edge e Firefox. 9. A solução proposta deve permitir administração centralizada via interface gráfica WEB usando HTTPS. 10. A solução deve possibilitar o acesso a console de todos os componentes do serviço a partir de um único ponto. 11. A solução deve permitir a definição de diferentes perfis de usuários e funções para		

			administração. 12. A solução deve fornecer controles de acesso de usuário hierárquicos e baseados em funções que permitem a delegação de responsabilidades para refletir a estrutura organizacional. 13. A solução deve permitir o acesso de um usuário autorizado de qualquer local. 14. A solução deve suportar autenticação de dois fatores para usuários e login. 15. A solução deve suportar configurações de segurança de senha. 16. A solução deve suportar personalizar a política de segurança para configurações de gerenciamento de senha, por: 16.1. idade e expiração da senha; 16.2. conta do usuário bloqueada após uma série de logins com falha; 16.3. comprimento mínimo da senha; 16.4. complexidade da senha, caracteres alfanuméricos e numéricos a serem usados; 16.5. forçar mudança de senha no login inicial; 16.6. notificação de senha expirada antes de vários dias.  17. A solução deve suportar a capacidade de restringir o acesso apenas de rede interna da empresa. 18. A solução deve suportar a capacidade de rastrear a atividade do usuário por nome da conta do usuário, data, ação e informações sobre a ação. 19. A solução deve suportar acesso por SSO (Single Sign-on) usando SAML 2.0. 20. A solução deve possuir um painel (dashboard) que, por padrão, permite que você veja as tendências de fragilidades por gravidade, plataforma, idade e status de remediação. ---------- AGENTES (ENDPOINTS)		

			1. A solução proposta deve oferecer um agente de baixo impacto nos sistemas operacionais onde está instalado e no consumo de largura de banda que utilizará na rede. 2. A solução deve ser instalada em servidores, estações de trabalho e máquinas virtuais, suportando sua implantação em rede local, em rede doméstica e na nuvem. 3. A solução deve oferecer suporte para sua implantação em pelo menos os seguintes sistemas operacionais: 3.1. Windows 7/Windows Server 2003 SP2 e posterior (x86, x64); 3.2. Red Hat Enterprise Linux/CentOS 6.5+, 7.x (x64), 8.x (x64); 3.3. Ubuntu 14, 16,18,19,20 (x64); 3.4. Oracle Enterpise Linux 8, Oracle Enterprise Linux (OEL) 7 até 7.5, Oracle Enterprise Linux (OEL) 6; 3.5. Amazon Linux 2, Amazon Linux 2018.03, Amazon Linux 2017.09, Amazon Linux 2017.03; 3.6. SUSE Linux Enterprise Server (SLES) 12, SUSE Linux Enterprise Server (SLES) 11; 4. O agente da solução deve se atualizar automaticamente e gerir as suas atualizações automaticamente. 5. A solução deve suportar plataformas de nuvem AWS, GCP e Azure. 6. A solução deve prover nativamente um dispositivo capaz de concentrar requisições dos agentes para encaminhamento a console de gerenciamento de forma a evitar a conexão direta de agentes com a plataforma. 7. O agente de gerenciamento deve suportar o uso de proxy. 8. Deve ser possível definir o intervalo de comunicação entre o agente e a console de gerenciamento.		

			9. Deve ser possível limitar o consumo de CPU e memória do agente. 10. Deve permitir a definição de um período global de inatividade dos agentes. 11. A solução deve prover nativamente um mecanismo de cache dos principais patches aplicados no ambiente visando a redução do consumo de banda. --- MÓDULO 3 1. A solução deve permitir aplicação de patches de segurança para, no mínimo, as plataformas abaixo: 1.1. Windows Embedded 7; 1.2. Windows 7; 1.3. Windows 8/8.1; 1.4. Windows 10** (1507 até 21H2); 1.5. Windows 11; 1.6. Windows Server 2022; 1.7. Red Hat Enterprise Linux 6; 1.8. Red Hat Enterprise Linux 7 até 7.9; 1.9. Red Hat Enterprise Linux 8 até 8.5; 1.10. CentOS 6 até 6.7; 1.11. CentOS 7 até 7.8; 2. A solução deve possuir um catálogo com no mínimo 35.000 patches e permitir aplicação de patches para, no mínimo, os produtos abaixo: 2.1. 7-Zip; 2.2. Adobe Acrobat; 2.3. Adobe Flash; 2.4. Adobe Reader; 2.5. Adobe Shockwave; 2.6. AIMP DevTeam; 2.7. Apache Software Foundation Tomcat; 2.8. Apple iCloud; 2.9. Apple iTunes; 2.10. Apple Mobile Device Support; 2.11. Apple Software Update; 2.12. Audacity;		

			2.13. Box Drive; 2.14. Box Edit; 2.15.Box Sync; 2.16. Cisco Jabber; 2.17. Cisco WebEx Teams; 2.18. CoreFTP; 2.19. Corel WinDVD Pro; 2.20. Dropbox; 2.21. Evernote; 2.22. FileZilla; 2.23. Foxit PhantomPDF; 2.24. Foxit Reader; 2.25. Gimp; 2.26. GIT; 2.27. Chrome; 2.28. Google Drive; 2.29. Google Desktop; 2.30. Google Drive File Stream; 2.31. Google Earth Pro; 2.32. KeePass; 2.33. LibreOffice; 2.34. Microsoft .Net; 2.35. Microsoft .Net Core; 2.36. Microsoft Commerce Server; 2.37. Microsoft Content Management Server; 2.38. Windows Defender; 2.39. Microsoft Digital Image; 2.40. DirectX; 2.41. Microsoft Dynamics; 2.42. Microsoft Edge; 2.43. Microsoft Enhanced Mitigation Experience Toolkit; 2.44. Exchange Server; 2.45. Exchange System Manager; 2.46. Microsoft Expression; 2.47. Forefront Server; 2.48. Front Page Server; 2.49. Host Integration Server; 2.50. Microsoft Identity Manager; 2.51. Internet Explorer;		

			2.52. Internet Information Server; 2.53. ISA Server; 2.54. Live Meeting; 2.55. Live Messenger; 2.56. Lync; 2.57. Lync Server; 2.58. Skype for Business Server; 2.59. MDAC; 2.60. Microsoft Mouse and Keyboard Center; 2.61. Microsoft Step By Step Interactive Training; 2.62. Mscomctl; 2.63. MSN Messenger; 2.64. MSXML; 2.65. Suíte Office nas versões 2000, 2002, 2003, 2007, 2010, 2013, 2016; 2.66. System Center Operations Manager; 2.67. Microsoft SQL Server nas versões 2005, 2008, 2008 R2, 2012, 2014, 2016, 2017, 2019; 2.68. SQL Management Studio; 2.69. Microsoft Visual Studio; 2.70. Windows Server 2012, 2016, 2019; 2.71. Windows 7, 8, 8.1, 10, 11; 3. A solução deve permitir a criação de dashboards para acompanhamento de aplicação de patches. 4. Os Dashboards devem permitir inclusão de filtros personalizados para incluir, no mínimo, os requisitos abaixo: 4.1. Ativos que não possuem patches de segurança instalados; 4.2. Ativos pendente de boot para aplicação de patches; 4.3. Patches faltantes por fabricante; 4.4. Status de aplicação de patches; 4.5. Patches faltantes por severidade. 5. A solução deve permitir mostrar em um mesmo dashboard a quantidade de ativos que possuem um software instalado e quantidade		

			de patches relevantes a esse mesmo software. 6. A solução deve conter uma lista de produtos e softwares priorizados, permitindo visualizar patches relevantes a esses produtos. 7. A solução deve permitir a criação de tarefas de instalação a partir de produtos e softwares priorizados. 8. A solução deve oferecer uma interface que permita buscas com uma sintaxe lógica para visualizar detalhes de um patch específico. 9. As buscas devem considerar, no mínimo, os filtros abaixo: 9.1. Fabricante da aplicação ou software; 9.2. Patches que corrigem falhas de segurança; 9.3. Patches de sistema operacional ou aplicações; 9.4. Severidade do fabricante; 9.5. Número do KB ou boletim; 9.6. CVE associado. 10. A solução deve ser capaz de apresentar informações de patches que já consideram e resolvem correções anteriores. 11. A solução deve apontar fragilidades resolvidas por um determinado patch. 12. A solução deve apontar todas as versões da aplicação que são afetadas e precisam de correção. 13. A solução deve conter referências do fabricante do software ou sistema operacional contendo descrição dos patches disponíveis. 14. Deve ser possível visualizar agentes e último status de comunicação, a quantidade de patches aplicados e faltantes. 15. Deve ser possível definir o intervalo em horas para verificação de patches e reporte à console. 16. A solução deve suportar tarefas de instalação e remoção dos patches.		

			17. A solução deve permitir a execução de scripts personalizados durante a tarefa de instalação de patches. 18. Deve ser possível executar scripts Powershell antes e depois da instalação de correções. 19. A solução deve permitir a instalação de softwares através de scripts. 20. A tarefa de aplicação de patches deve permitir alteração de chaves de registro. 21. A tarefa de aplicação de correções deve permitir selecionar manualmente os patches a serem aplicados ou através de um filtro de seleção que considere, no mínimo, severidade do patch, fabricante, associação a uma fragilidade, associação a riscos de segurança. 22. Deve ser possível restringir a aplicação de patches a um grupo de máquinas baseados em ranges de IP, software instalado, portas abertas, serviços em execução. 23. Deve ser possível o agendamento de execução de tarefas de patch de forma imediata. 24. Deve ser possível agendar a execução de tarefas de patch em um horário específico com recorrência diária, semanal ou mensal. 25. Deve ser possível agendar a execução de tarefas de patch com agendamento a partir do Patch Tuesday, da Microsoft, de forma automática. 26. Deve ser possível configurar uma janela de tempo máximo para execução de patches em intervalo de horas ou minutos. 27. A solução deve permitir customização de mensagens para o usuário antes, durante e após a aplicação de patches. 28. Deve permitir o download de patches antes do início da tarefa, de forma a otimizar o processo de instalação. 29. A solução deve permitir a supressão do		

			reinício do sistema operacional, forçá-la ou permitir que o usuário reinicie o sistema, caso o patch aplicado exija o reinício. 30. Deve ser possível restringir o licenciamento a um determinado grupo de máquinas baseado em critérios como sistema operacional, presença de softwares instalados e ranges de IPs. 31. A solução deve conter a inteligência de filtrar automaticamente, sem intervenção, quais ativos receberão os patches selecionados na tarefa de patch considerando a arquitetura do sistema operacional e a pré-existência de determinada aplicação, evitando assim instalações indesejadas. 32. Deve ser possível gerar relatórios a partir do catálogo de patches a serem aplicados considerando filtros dos patches e dos ativos. 33. O catálogo de patches a serem aplicados deve filtrar de forma simples quais são os patches que precisam ser instalados e exibir somente as últimas versões disponíveis de cada um deles, considerando a obsolescência de versões antigas. 34. Deve ser possível visualizar, pela interface, o status de instalação de cada uma das tarefas de patch criadas. 35. O status individual de cada tarefa de patch deve mostrar quais patches foram instalados com sucesso, os que falharam e quais não foram instalados por não serem necessários. 36. A solução deve exibir, para os patches que não foram instalados com sucesso, qual o motivo do erro. 37. Deve ser possível gerar um relatório CSV para uma tarefa de patch específica, com a finalidade de validar seu progresso e situação final de execução. 38. A solução deve possuir controle de acesso no modelo Role Based Access Control, para		

			que sejam definidos no mínimo dois perfis de usuários caso seja necessário, sendo um deles, necessariamente, incapaz de iniciar uma tarefa de execução de patch. 39. A solução deve possuir uma interface de API para permitir automatização de ativadas com no mínimo as seguintes funções: 39.1. Criação de tarefa de patch; 39.2. Listagem de ativos; 39.3. Listagem de patches; 39.4. Listagem de tarefas de patch. Marca: ADVANTA Fabricante: ADVANTA		
5	UNIDADE	25.0	Código: 33904006002000010 SOLUÇÃO DE VERIFICAÇÃO E SCAN DE APLICAÇÕES WEB - SEGURANÇA DE DADOS 1. A solução deve ser entregue como um serviço Software-as-a-Service (SaaS) em nuvem para todos os seus serviços e aplicativos exigidos neste documento. 2.Todos os serviços da plataforma devem estar disponíveis sob o mesmo padrão de qualidade de serviço 24x7x365 e garantir 99% de disponibilidade. 3. A FABRICANTE deve oferecer manutenção e atualização constante da plataforma durante todo o período de vigência do contrato de serviço. 4. As atualizações de serviço devem ser transparentes para o administrador da solução, sem afetar nenhum dos dados armazenados e serviços fornecidos. 5. As janelas de manutenção programada deverão ocorrer dentro do período de indisponibilidade aceita (1%) e previamente avisada. 6. A plataforma que fornece os serviços deve ser certificada pela FedRAMP e certificada para os procedimentos de segurança SSAE 18 SOC 2.	3.788,90	94.722,50

			7. Todas as comunicações entre componentes, transferência de dados e sincronização da solução devem ser criptografadas de ponta a ponta, fazendo uso de no mínimo TLS 1.2, certificados assinados com RSA 2048 bits e algoritmo de assinatura SHA256. 8. A solução deve permitir: 8.1. a criação de usuários distintos; 8.2. a separação de funções e permissões na console; 8.3. a integração através de SSO com, pelo menos, Okta e Azure Active Directory; 8.4. acessibilidade a partir de, pelo menos, um dos navegadores comerciais dentre Google Chrome, Microsoft Edge e Firefox. 9. A solução proposta deve permitir administração centralizada via interface gráfica WEB usando HTTPS. 10. A solução deve possibilitar o acesso a console de todos os componentes do serviço a partir de um único ponto. 11. A solução deve permitir a definição de diferentes perfis de usuários e funções para administração. 12. A solução deve fornecer controles de acesso de usuário hierárquicos e baseados em funções que permitem a delegação de responsabilidades para refletir a estrutura organizacional. 13. A solução deve permitir o acesso de um usuário autorizado de qualquer local. 14. A solução deve suportar autenticação de dois fatores para usuários e login. 15. A solução deve suportar configurações de segurança de senha. 16. A solução deve suportar personalizar a política de segurança para configurações de gerenciamento de senha, por: 16.1. idade e expiração da senha;		

			16.2. conta do usuário bloqueada após uma série de logins com falha; 16.3. comprimento mínimo da senha; 16.4. complexidade da senha, caracteres alfanuméricos e numéricos a serem usados; 16.5. forçar mudança de senha no login inicial; 16.6. notificação de senha expirada antes de vários dias.  17. A solução deve suportar a capacidade de restringir o acesso apenas de rede interna da empresa. 18. A solução deve suportar a capacidade de rastrear a atividade do usuário por nome da conta do usuário, data, ação e informações sobre a ação. 19. A solução deve suportar acesso por SSO (Single Sign-on) usando SAML 2.0. 20. A solução deve possuir um painel (dashboard) que, por padrão, permite que você veja as tendências de fragilidades por gravidade, plataforma, idade e status de remediação. ---------- AGENTES (ENDPOINTS) 1. A solução proposta deve oferecer um agente de baixo impacto nos sistemas operacionais onde está instalado e no consumo de largura de banda que utilizará na rede. 2. A solução deve ser instalada em servidores, estações de trabalho e máquinas virtuais, suportando sua implantação em rede local, em rede doméstica e na nuvem. 3. A solução deve oferecer suporte para sua implantação em pelo menos os seguintes sistemas operacionais: 3.1. Windows 7/Windows Server 2003 SP2 e posterior (x86, x64); 3.2. Red Hat Enterprise Linux/CentOS 6.5+, 7.x (x64), 8.x (x64);		

			3.3. Ubuntu 14, 16,18,19,20 (x64); 3.4. Oracle Enterpise Linux 8, Oracle Enterprise Linux (OEL) 7 até 7.5, Oracle Enterprise Linux (OEL) 6; 3.5. Amazon Linux 2, Amazon Linux 2018.03, Amazon Linux 2017.09, Amazon Linux 2017.03; 3.6. SUSE Linux Enterprise Server (SLES) 12, SUSE Linux Enterprise Server (SLES) 11; 4. O agente da solução deve se atualizar automaticamente e gerir as suas atualizações automaticamente. 5. A solução deve suportar plataformas de nuvem AWS, GCP e Azure. 6. A solução deve prover nativamente um dispositivo capaz de concentrar requisições dos agentes para encaminhamento a console de gerenciamento de forma a evitar a conexão direta de agentes com a plataforma. 7. O agente de gerenciamento deve suportar o uso de proxy. 8. Deve ser possível definir o intervalo de comunicação entre o agente e a console de gerenciamento. 9. Deve ser possível limitar o consumo de CPU e memória do agente. 10. Deve permitir a definição de um período global de inatividade dos agentes. 11. A solução deve prover nativamente um mecanismo de cache dos principais patches aplicados no ambiente visando a redução do consumo de banda. --- MÓDULO 4 1. A solução proposta deve habilitar varreduras dinâmicas para descobrir e catalogar todos os aplicativos da web e APIs na rede corporativa externa, redes corporativas internas e instâncias de nuvem.		

			2. A solução deve permitir varreduras autenticadas, complexas e progressivas. 3. A solução deve suportar varreduras programadas de serviços SOAP e REST API. 4. A solução deve contar com uma API e integração com Jenkins para automação em um ambiente de CI / CD. 5. A solução deve detectar, identificar, avaliar, rastrear os 10 principais riscos OWASP (Top 10), como injeção de SQL, Cross-site script (XSS), XML External Entity (XXE), autenticação interrompida e configurações incorretas, também ameaças de WASC, fragilidades CWE e CVEs associados em aplicações da web. 6. A solução deve suportar a capacidade de re-testar uma fragilidade específica que foi detectada anteriormente na aplicação web. 7. A solução deve ter capacidade de encontrar aplicações web aprovadas e não aprovadas em sua rede, gerando um processo contínuo de catalogação e descoberta de aplicações web. 8. A solução deve gerar tags para facilitar a localização e o uso de ativos de aplicações web encontrados. 9. A solução deve permitir que se faça a varredura de grandes aplicações da web usando um mecanismo de varredura progressiva, que deve permitir a varredura em estágios incrementais e evitar quaisquer restrições que possam surgir ao tentar fazer a varredura de um aplicativo de uma vez. 10. A solução deve definir a hora exata de início e duração das verificações. 11. A solução deve permitir gerenciar várias varreduras de aplicações web, combinando vários scanners para acelerar o processo e obter resultados mais rapidamente. 12. A solução deve permitir integração nativa		

			com uma das seguintes ferramentas de WAF: F5, Fortinet, Imperva, Citrix NetScaler. 13. A solução deve consolidar os dados de varredura automatizada da solução com dados de ferramentas que permitem a avaliação manual de fragilidades por meio do Burp Suite e Bugcrowd, para uma visão unificada de fragilidades de aplicações web detectadas automática e manualmente. 14. A solução deve fornecer relatórios resumidos e de varredura do site que podem ser exportados para os formatos HTML e PDF. 15. A solução deve oferecer suporte à criação de escopos e funções definidos pelo usuário e permitir que as permissões apropriadas sejam atribuídas a cada função. Marca: ADVANTA Fabricante: ADVANTA		
				Total	R$ 2.249.047,10

VALOR TOTAL DA ATA	**R$ 2.249.047,10**

2.2. A listagem do cadastro de reserva referente ao presente registro de preços consta como anexo a esta Ata.

3. ÓRGÃO(S) GERENCIADOR E PARTICIPANTE(S)

3.1. O órgão gerenciador será o Instituto Fedral De Santa Catarina – IFSC UG – 158516

3.2. Além do gerenciador, não há órgãos e entidades públicas participantes do registro de preços.

4. DA ADESÃO À ATA DE REGISTRO DE PREÇOS

4.1. Durante a vigência da ata, os órgãos e as entidades da Administração Pública federal, estadual, distrital e municipal que não participaram do procedimento de IRP poderão aderir à

ata de registro de preços na condição de não participantes, observados os seguintes requisitos:

4.1.1. Apresentação de justificativa da vantagem da adesão, inclusive em situações de provável desabastecimento ou descontinuidade de serviço público;

4.1.2. Demonstração de que os valores registrados estão compatíveis com os valores praticados pelo mercado na forma do art. 23 da Lei nº 14.133, de 2021; e

4.1.3. Consulta e aceitação prévias do órgão ou da entidade gerenciadora e do fornecedor.

4.2. A autorização do órgão ou entidade gerenciadora apenas será realizada após a aceitação da adesão pelo fornecedor.

4.2.1. O órgão ou entidade gerenciadora poderá rejeitar adesões caso elas possam acarretar prejuízo à execução de seus próprios contratos ou à sua capacidade de gerenciamento.

4.3. Após a autorização do órgão ou da entidade gerenciadora, o órgão ou entidade não participante deverá efetivar a aquisição ou a contratação solicitada em até noventa dias, observado o prazo de vigência da ata.

4.4. O prazo de que trata o subitem anterior, relativo à efetivação da contratação, poderá ser prorrogado excepcionalmente, mediante solicitação do órgão ou da entidade não participante aceita pelo órgão ou pela entidade gerenciadora, desde que respeitado o limite temporal de vigência da ata de registro de preços.

4.5. O órgão ou a entidade poderá aderir a item da ata de registro de preços da qual seja integrante, na qualidade de não participante, para aqueles itens para os quais não tenha quantitativo registrado, observados os requisitos do item 4.1. Dos limites para as adesões

4.6. As aquisições ou contratações adicionais não poderão exceder, por órgão ou entidade, a cinquenta por cento dos quantitativos dos itens do instrumento convocatório registrados na ata de registro de preços para o gerenciador e para os participantes.

4.7. O quantitativo decorrente das adesões não poderá exceder, na totalidade, ao dobro do quantitativo de cada item registrado na ata de registro de preços para o gerenciador e os participantes, independentemente do número de órgãos ou entidades não participantes que aderirem à ata de registro de preços.

4.8. Para aquisição emergencial de medicamentos e material de consumo médico-hospitalar por órgãos e entidades da Administração Pública federal, estadual, distrital e municipal, a adesão à ata de registro de preços gerenciada pelo Ministério da Saúde não estará sujeita ao limite previsto no item 4.7.

4.9. A adesão à ata de registro de preços por órgãos e entidades da Administração Pública estadual, distrital e municipal poderá ser exigida para fins de transferências voluntárias, não ficando sujeita ao limite de que trata o item 4.7, desde que seja destinada à execução descentralizada de programa ou projeto federal e comprovada a compatibilidade dos preços registrados com os valores praticados no mercado na forma do art. 23 da Lei nº 14.133, de 2021. Vedação a acréscimo de quantitativos 4.10. É vedado efetuar acréscimos nos quantitativos fixados na ata de registro de preços.

5. VALIDADE, FORMALIZAÇÃO DA ATA DE REGISTRO DE PREÇOS E CADASTRO RESERVA

5.1. A validade da Ata de Registro de Preços será de 1 (um) ano, contado a partir do primeiro dia útil subsequente à data de divulgação no PNCP, podendo ser prorrogada por igual período, mediante a anuência do fornecedor, desde que comprovado o preço vantajoso.

5.1.1. O contrato decorrente da ata de registro de preços terá sua vigência estabelecida no próprio instrumento contratual e observará no momento da contratação e a cada exercício financeiro a disponibilidade de créditos orçamentários, bem como a previsão no plano plurianual, quando ultrapassar 1 (um) exercício financeiro.

5.1.2. Na formalização do contrato ou do instrumento substituto deverá haver a indicação da disponibilidade dos créditos orçamentários respectivos.

5.2. A contratação com os fornecedores registrados na ata será formalizada pelo órgão ou pela entidade interessada por intermédio de instrumento contratual, emissão de nota de empenho de despesa, autorização de compra ou outro instrumento hábil, conforme o art. 95 da Lei nº 14.133, de 2021.

5.2.1. O instrumento contratual de que trata o item 5.2. deverá ser assinado no prazo de validade da ata de registro de preços.

5.3. Os contratos decorrentes do sistema de registro de preços poderão ser alterados, observado o art. 124 da Lei nº 14.133, de 2021.

5.4. Após a homologação da licitação ou da contratação direta, deverão ser observadas as seguintes condições para formalização da ata de registro de preços:

5.4.1. Serão registrados na ata os preços e os quantitativos do adjudicatário, devendo ser observada a possibilidade de o licitante oferecer ou não proposta em quantitativo inferior ao máximo previsto no edital e se obrigar nos limites dela;

5.4.2. Será incluído na ata, na forma de anexo, o registro dos licitantes ou dos fornecedores que:

5.4.2.1. Aceitarem cotar os bens, as obras ou os serviços com preços iguais aos do adjudicatário, observada a classificação da licitação; e

5.4.2.2. Mantiverem sua proposta original.

5.4.3. Será respeitada, nas contratações, a ordem de classificação dos licitantes ou dos fornecedores registrados na ata.

5.5. O registro a que se refere o item 5.4.2 tem por objetivo a formação de cadastro de reserva para o caso de impossibilidade de atendimento pelo signatário da ata.

5.6. Para fins da ordem de classificação, os licitantes ou fornecedores que aceitarem reduzir suas propostas para o preço do adjudicatário antecederão aqueles que mantiverem sua proposta original.

5.7. A habilitação dos licitantes que comporão o cadastro de reserva a que se refere o item 5.4.2.2 somente será efetuada quando houver necessidade de contratação dos licitantes remanescentes, nas seguintes hipóteses:

5.7.1. Quando o licitante vencedor não assinar a ata de registro de preços, no prazo e nas condições estabelecidos no edital; e

5.7.2. Quando houver o cancelamento do registro do licitante ou do registro de preços nas hipóteses previstas no item 9.

5.8. O preço registrado com indicação dos licitantes e fornecedores será divulgado no PNCP e ficará disponibilizado durante a vigência da ata de registro de preços.

5.9. Após a homologação da licitação ou da contratação direta, o licitante mais bem classificado ou o fornecedor, no caso da contratação direta, será convocado para assinar a ata de registro de preços, no prazo e nas condições estabelecidos no edital de licitação ou no aviso de contratação direta, sob pena de decair o direito, sem prejuízo das sanções previstas na Lei nº 14.133, de 2021. 5.9.1. O prazo de convocação poderá ser prorrogado 1 (uma) vez, por igual período, mediante solicitação do licitante ou fornecedor convocado, desde que apresentada dentro do prazo, devidamente justificada, e que a justificativa seja aceita pela Administração.

5.10. A ata de registro de preços será assinada por meio de assinatura digital e disponibilizada no Sistema de Registro de Preços.

5.11. Quando o convocado não assinar a ata de registro de preços no prazo e nas condições estabelecidos no edital ou no aviso de contratação, e observado o disposto no item 5.7, observando o item 5.7 e subitens, fica facultado à Administração convocar os licitantes remanescentes do cadastro de reserva, na ordem de classificação, para fazê-lo em igual prazo e nas condições propostas pelo primeiro classificado.

5.12. Na hipótese de nenhum dos licitantes que trata o item 5.4.2.1, aceitar a contratação nos termos do item anterior, a Administração, observados o valor estimado e sua eventual atualização nos termos do edital , poderá:

5.12.1. Convocar para negociação os demais licitantes ou fornecedores remanescentes cujos preços foram registrados sem redução, observada a ordem de classificação, com vistas à obtenção de preço melhor, mesmo que acima do preço do adjudicatário; ou

5.12.2. Adjudicar e firmar o contrato nas condições ofertadas pelos licitantes ou fornecedores remanescentes, atendida a ordem classificatória, quando frustrada a negociação de melhor condição.

5.13. A existência de preços registrados implicará compromisso de fornecimento nas condições estabelecidas, mas não obrigará a Administração a contratar, facultada a realização de licitação específica para a aquisição pretendida, desde que devidamente justificada.

6. ALTERAÇÃO OU ATUALIZAÇÃO DOS PREÇOS REGISTRADOS

6.1. Os preços registrados poderão ser alterados ou atualizados em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo dos bens, das obras ou dos serviços registrados, nas seguintes situações:

6.1.1. Em caso de força maior, caso fortuito ou fato do príncipe ou em decorrência de fatos imprevisíveis ou previsíveis de consequências incalculáveis, que inviabilizem a execução da ata tal como pactuada, nos termos da alínea “d” do inciso II do caput do art. 124 da Lei nº 14.133, de 2021;

6.1.2. Em caso de criação, alteração ou extinção de quaisquer tributos ou encargos legais ou a superveniência de disposições legais, com comprovada repercussão sobre os preços registrados;

6.1.3. Na hipótese de previsão no edital ou no aviso de contratação direta de cláusula de reajustamento ou repactuação sobre os preços registrados, nos termos da Lei nº 14.133, de 2021.

6.1.3.1. No caso do reajustamento, deverá ser respeitada a contagem da anualidade e o índice previstos para a contratação;

6.1.3.2. No caso da repactuação, poderá ser a pedido do interessado, conforme critérios definidos para a contratação.

7. NEGOCIAÇÃO DE PREÇOS REGISTRADOS

7.1. Na hipótese de o preço registrado tornar-se superior ao preço praticado no mercado por motivo superveniente, o órgão ou entidade gerenciadora convocará o fornecedor para negociar a redução do preço registrado.

7.1.1. Caso não aceite reduzir seu preço aos valores praticados pelo mercado, o fornecedor será liberado do compromisso assumido quanto ao item registrado, sem aplicação de penalidades administrativas.

7.1.2. Na hipótese prevista no item anterior, o gerenciador convocará os fornecedores do cadastro de reserva, na ordem de classificação, para verificar se aceitam reduzir seus preços aos valores de mercado e não convocará os licitantes ou fornecedores que tiveram seu registro cancelado.

7.1.3. Se não obtiver êxito nas negociações, o órgão ou entidade gerenciadora procederá ao cancelamento da ata de registro de preços, adotando as medidas cabíveis para obtenção de contratação mais vantajosa.

7.1.4. Na hipótese de redução do preço registrado, o gerenciador comunicará aos órgãos e às entidades que tiverem firmado contratos decorrentes da ata de registro de preços para que avaliem a conveniência e a oportunidade de diligenciarem negociação com vistas à alteração contratual, observado o disposto no art. 124 da Lei nº 14.133, de 2021.

7.2. Na hipótese de o preço de mercado tornar-se superior ao preço registrado e o fornecedor não poder cumprir as obrigações estabelecidas na ata, será facultado ao fornecedor requerer ao gerenciador a alteração do preço registrado, mediante comprovação de fato superveniente que supostamente o impossibilite de cumprir o compromisso.

7.2.1. Neste caso, o fornecedor encaminhará, juntamente com o pedido de alteração, a documentação comprobatória ou a planilha de custos que demonstre a inviabilidade do preço registrado em relação às condições inicialmente pactuadas.

7.2.2. Não hipótese de não comprovação da existência de fato superveniente que inviabilize o preço registrado, o pedido será indeferido pelo órgão ou entidade gerenciadora e o fornecedor deverá cumprir as obrigações estabelecidas na ata, sob pena de cancelamento do seu registro, nos termos do item 9.1, sem prejuízo das sanções previstas na Lei nº 14.133, de 2021, e na legislação aplicável.

7.2.3. Na hipótese de cancelamento do registro do fornecedor, nos termos do item anterior, o gerenciador convocará os fornecedores do cadastro de reserva, na ordem de classificação, para verificar se aceitam manter seus preços registrados, observado o disposto no item 5.7.

7.2.4. Se não obtiver êxito nas negociações, o órgão ou entidade gerenciadora procederá ao cancelamento da ata de registro de preços, nos termos do item 9.4, e adotará as medidas cabíveis para a obtenção da contratação mais vantajosa.

7.2.5. Na hipótese de comprovação da majoração do preço de mercado que inviabilize o preço registrado, conforme previsto no item 7.2 e no item 7.2.1, o órgão ou entidade gerenciadora atualizará o preço registrado, de acordo com a realidade dos valores praticados pelo mercado.

7.2.6. O órgão ou entidade gerenciadora comunicará aos órgãos e às entidades que tiverem firmado contratos decorrentes da ata de registro de preços sobre a efetiva alteração do preço registrado, para que avaliem a necessidade de alteração contratual, observado o disposto no art. 124 da Lei nº 14.133, de 2021.

8. REMANEJAMENTO DAS QUANTIDADES REGISTRADAS NA ATA DE REGISTRO DE PREÇOS

8.1. As quantidades previstas para os itens com preços registrados nas atas de registro de preços poderão ser remanejadas pelo órgão ou entidade gerenciadora entre os órgãos ou as entidades participantes e não participantes do registro de preços.

8.2. O remanejamento somente poderá ser feito:

8.2.1. De órgão ou entidade participante para órgão ou entidade participante; ou

8.2.2. De órgão ou entidade participante para órgão ou entidade não participante.

8.3. O órgão ou entidade gerenciadora que tiver estimado as quantidades que pretende contratar será considerado participante para efeito do remanejamento.

8.4. Na hipótese de remanejamento de órgão ou entidade participante para órgão ou entidade não participante, serão observados os limites previstos no art. 32 do Decreto nº 11.462, de 2023.

8.5. Competirá ao órgão ou à entidade gerenciadora autorizar o remanejamento solicitado, com a redução do quantitativo inicialmente informado pelo órgão ou pela entidade participante, desde que haja prévia anuência do órgão ou da entidade que sofrer redução dos quantitativos informados.

8.6. Caso o remanejamento seja feito entre órgãos ou entidades dos Estados, do Distrito Federal ou de Municípios distintos, caberá ao fornecedor beneficiário da ata de registro de

preços, observadas as condições nela estabelecidas, optar pela aceitação ou não do fornecimento decorrente do remanejamento dos itens.

8.7. Na hipótese da compra centralizada, não havendo indicação pelo órgão ou pela entidade gerenciadora, dos quantitativos dos participantes da compra centralizada, nos termos do item 8.3, a distribuição das quantidades para a execução descentralizada será por meio do remanejamento.

9. CANCELAMENTO DO REGISTRO DO LICITANTE VENCEDOR E DOS PREÇOS REGISTRADOS

9.1. O registro do fornecedor será cancelado pelo gerenciador, quando o fornecedor:

9.1.1. Descumprir as condições da ata de registro de preços, sem motivo justificado;

9.1.2. Não retirar a nota de empenho, ou instrumento equivalente, no prazo estabelecido pela Administração sem justificativa razoável;

9.1.3. Não aceitar manter seu preço registrado, na hipótese prevista no artigo 27, § 2º, do Decreto nº 11.462, de 2023; ou

9.1.4. Sofrer sanção prevista nos incisos III ou IV do caput do art. 156 da Lei nº 14.133, de 2021. 9.1.4.1. Na hipótese de aplicação de sanção prevista nos incisos III ou IV do caput do art. 156 da Lei nº 14.133, de 2021, caso a penalidade aplicada ao fornecedor não ultrapasse o prazo de vigência da ata de registro de preços, poderá o órgão ou a entidade gerenciadora poderá, mediante decisão fundamentada, decidir pela manutenção do registro de preços, vedadas contratações derivadas da ata enquanto perdurarem os efeitos da sanção.

9.2. O cancelamento de registros nas hipóteses previstas no item 9.1 será formalizado por despacho do órgão ou da entidade gerenciadora, garantidos os princípios do contraditório e da ampla defesa.

9.3. Na hipótese de cancelamento do registro do fornecedor, o órgão ou a entidade gerenciadora poderá convocar os licitantes que compõem o cadastro de reserva, observada a ordem de classificação.

9.4. O cancelamento dos preços registrados poderá ser realizado pelo gerenciador, em determinada ata de registro de preços, total ou parcialmente, nas seguintes hipóteses, desde que devidamente comprovadas e justificadas:

9.4.1. Por razão de interesse público;

9.4.2. A pedido do fornecedor, decorrente de caso fortuito ou força maior; ou

9.4.3. Se não houver êxito nas negociações, nas hipóteses em que o preço de mercado tornar-se superior ou inferior ao preço registrado, nos termos do artigos 26, § 3º e 27, § 4º, ambos do Decreto nº 11.462, de 2023.

10. DAS PENALIDADES

10.1. O descumprimento da Ata de Registro de Preços ensejará aplicação das penalidades estabelecidas no edital .

10.1.1. As sanções também se aplicam aos integrantes do cadastro de reserva no registro de preços que, convocados, não honrarem o compromisso assumido injustificadamente após terem assinado a ata.

10.2. É da competência do gerenciador a aplicação das penalidades decorrentes do descumprimento do pactuado nesta ata de registro de preço (art. 7º, inc. XIV, do Decreto nº 11.462, de 2023), exceto nas hipóteses em que o descumprimento disser respeito às contratações dos órgãos ou entidade participante, caso no qual caberá ao respectivo órgão participante a aplicação da penalidade (art. 8º, inc. IX, do Decreto nº 11.462, de 2023).

10.3. O órgão ou entidade participante deverá comunicar ao órgão gerenciador qualquer das ocorrências previstas no item 9.1, dada a necessidade de instauração de procedimento para cancelamento do registro do fornecedor.

11. CONDIÇÕES GERAIS

11.1. As condições gerais de execução do objeto, tais como os prazos para entrega e recebimento, as obrigações da Administração e do fornecedor registrado, penalidades e demais condições do ajuste, encontram-se definidos no Termo de Referência, ANEXO AO EDITAL .

11.2. No caso de adjudicação por preço global de grupo de itens, só será admitida a contratação de parte de itens do grupo se houver prévia pesquisa de mercado e demonstração de sua vantagem para o órgão ou a entidade. Para firmeza e validade do pactuado, a presente Ata foi lavrada em 1 (uma) via digital,, que, depois de lida e achada em ordem, vai assinada pelas partes por meio de assinatura à declaração de concordância à ata de registro de preços..

12. Anexo II

DECLARAÇÃO DE CONCORDÂNCIA À ATA DE REGISTRO DE PREÇOS PREGÃO ELETRÔNICO (SRP) 21117/2023 – IFSC

A empresa **ADVANTA SISTEMAS DE TELECOMUNICACOES E SERVICOS DE INFORMATICA LTDA,** declara para os devidos fins, que:

1. Recebeu a Ata de Registros de Preços do Pregão Eletrônico nº 21117/2023 do IFSC, contendo 44(quarenta e quatro) páginas (incluindo Ata e anexos) e;

2. Concorda com todos os termos da referida Ata e o Anexo I, com os preços registrados.

3. Assume o compromisso de receber as Autorizações de Fornecimento e Empenhos pelo e-mail institucional will.sebben@oakmontgroup.com.br

Concordando que não sendo confirmado o recebimento do e-mail, o IFSC considerará como recebido, iniciando a contagem do prazo de entrega. Assumindo o compromisso de avisar o IFSC quando houver mudança do e-mail

Florianópolis, 07 de março de 2024.

Representante legal do órgão gerenciador

gov.br
Documento assinado digitalmente
ALOISIO SILVA JUNIOR
Data: 07/03/2024 14:04:57-0300
Verifique em https://validar.iti.gov.br

Documento assinado de acordo com
Portaria do Reitor nº 1.452, de 19 de maio de 2021
MAURÍCIO GARIBA JÚNIOR
REITOR DO IFSC

(assinatura e identificação do Representante Legal e Carimbo da Empresa/ ou assinatura dig

WILSON ROBERTO PIEDADE:08794139806
Assinado de forma digital por WILSON ROBERTO PIEDADE:08794139806
Dados: 2024.03.07 19:48:13 -03'00'

Representante legal do fornecedor registrado:
ADVANTA SISTEMAS DE TELECOMUNICACOES E SERVICOS DE INFORMATICA LTDA

Wilson Roberto Piedade