GOVERNO DO ESTADO DE RONDÔNIA
Superintendência Estadual de Compras e Licitações - SUPEL
Comissão de Tecnologia - SUPEL-COTEC

ADENDO

MODIFICADOR Nº 01/2026

PREGÃO ELETRÔNICO nº 90236/2025/SUPEL/RO

PROCESSO ADMINISTRATIVO: 0036.028242/2024-36

Objeto: Registro de Preços para contratação de empresa para fornecimento, sob demanda, de solução de segurança para proteção de e-mail, Endpoint e proteção contra ataques avançados, incluindo instalação, configuração, repasse de conhecimento, suporte técnico e garantia, para atender às necessidades da Secretaria de Estado da Saúde - SESAU/RO, por um período de 01 (um) ano, podendo ser prorrogado, conforme a Lei Federal nº 14.133 de 1° de abril de 2021.

A Superintendência Estadual de Compras e Licitações – SUPEL, através de seu Pregoeiro, designada por força das disposições contidas na **Portaria n.° 158 de 07 de julho de 2026**, informa que elaborou adendo modificador devido ao teor da resposta aos pedidos de Esclarecimentos e Impugnação, apresentados por empresas interessadas, interposto em face do **PE 90236/2025/SUPEL/RO.**

Em atenção à Resposta ao Pedido de Esclarecimento e Impugnação considera-se as seguintes alterações a seguir:

1. **DO TERMO DE REFERÊNCIA, ID. (74300119)**

1 - No Termo de Referência id. (74300119).

ONDE SE LÊ:

3.2. Descrição Detalhada do Objeto:

GRUPO ÚNICO	ITEM	CATMAT	OBJETO	UNIDADE DE MEDIDA	QUANTIDADE
01	1	27499	Solução de proteção de Endpoints com abordagem proativa para resposta eficaz a incidentes	Por Endpoint	2150
	2	27499	Solução de proteção de Servidores com abordagem proativa para resposta eficaz a incidentes	Por Servidor	139
	3	27499	Solução de segurança avançada para mitigação de ameaças na rede	Por Throughput de dados	4
	4	27499	Solução de prevenção de intrusão de próxima geração (NGIPS)	Por Throughput de dados	4
	5	27432	Serviço de suporte pro ativo, corretivo e para resposta a incidentes	Por Solução	4

GRUPO ÚNICO	ITEM	CATMAT	OBJETO	UNIDADE DE MEDIDA	QUANTIDADE
	6	3840	Serviço de implantação	Por Solução	4
	7	3840	Serviço de capacitação e repasse de conhecimento	40 Horas	2

LEIA-SE:

3.2. **Descrição Detalhada do Objeto:**

GRUPO ÚNICO	ITEM	CATMAT	OBJETO	UNIDADE DE MEDIDA	QUANTIDADE
01	1	27499	Solução de proteção de Endpoints com abordagem proativa para resposta eficaz a incidentes	Por Endpoint	2150
	2	27499	Solução de proteção de Servidores com abordagem proativa para resposta eficaz a incidentes	Por Servidor	139
	3	27499	Solução de segurança avançada para mitigação de ameaças na rede	Por Throughput de dados	2
	4	27499	Solução de prevenção de intrusão de próxima geração (NGIPS)	Por Throughput de dados	4
	5	27432	Serviço de suporte pro ativo, corretivo e para resposta a incidentes	Por Solução	4
	6	3840	Serviço de implantação	Por Solução	4
	7	3840	Serviço de capacitação e repasse de conhecimento	40 Horas	2

(...)

ONDE SE LÊ:

8.10.1.1.10. Arquivos compactados automaticamente, em pelo menos nos seguintes formatos: zip, exe, arj, MIME/uu, CAB;

8.10.1.1.11. Arquivos recebidos por meio de programas de comunicação instantânea (MSN messenger, yahoo messenger, google talk, icq, dentre outros).

8.10.1.1.85. Deve possuir no mecanismo de autoproteção as seguintes proteções: Proteção e verificação dos arquivos de assinatura;

8.10.1.1.86. Proteção dos processos do agente de segurança; Proteção das chaves de registro do agente de segurança;

8.10.1.1.87. Proteção do diretório de instalação do agente de segurança. Funcionalidade de HIPS – Host IPS e Host Firewall Deve ser capaz de realizar a detecção/proteção contra exploração de vulnerabilidades nos seguintes sistemas operacionais: Windows 8.1 (x86/x64);

8.10.2.1.1. A solução deverá ser compatível com pelo menos os seguintes sistemas operacionais: Windows Server 2000; Windows Server 2003 SP1 e 2003 R2 SP2; Windows Server 2008 e 2008 R2; Windows Server 2012 e 2012 R2; Windows Server 2016; Windows Server 2019;

8.10.2.1.124 A capacidade de análise de artefatos em sandbox pode ser realizada através de no mesmo equipamento de análise; A solução deverá possuir mecanismo de conhecimento de senhas de pelo menos 90 palavras chaves em seu vocabulário de conhecimento, para derivação de arquivos protegidos;

8.10.3.1.20.Precisa conter regras de defesa para blindagem de vulnerabilidades e ataques que explorem os seguintes sistemas operacionais: Windows 2003, 2008, 2012, 2016, 2019, Linux Red Hat, Suse, CentOS, Ubuntu, Debian, Solaris, AIX além de regras para aplicações padrão de mercado, incluindo Microsoft IIS, SQL Server, Microsoft Exchange, Oracle Database, Adobe Acrobat, Mozilla Firefox, Microsoft Internet Explorer, Google Chrome e Web Server Apache;

8.10.3.1.24 Deve possuir a habilidade de detectar e analisar os seguintes protocolos e aplicativos: P2P, SMTP, POP3, IRC, DNS, HTTP, FTP, TFTP, SMB, MSN, AIM, YMSG, Yahoo Mail, Hotmail, RDP, DHCP, TELNET, File Transfer, VNC, Cisco-TELNET, Kerberos, DCE-RPC, SQL, HTTPS, SMB2, MMS, IMAP4, RTSP/RTP-UDP, RTSP/RTP-TCP, RTSP/RDT-UDP, RTSP/RDTTCP, WMSP, SHOUTCast, RTMP, Bittorent, Kazaa, Blubster, eDonkeyeMule, Gnucleus LAN, Gnutella/Limewire/Bearshare/Shareaza, Winny, WinMX, MLDonkey, DirectConnect, SoulSeek, OpenNap, Kuro, iMesh, Skype, Google Talk, Zultrax, Foxy, eDonkey, Ares, Miranda, Kceasy, MoodAmp, Deepnet Explorer, FreeWire, Gimme, GnucDNA GWebCache, Jubster, MyNapster, Nova GWebCache, Swapper GWebCache, Xnap, Xolox, Ppstream, AIM Express, Chikka SMS Messenger, eBuddy, ICQ2Go, ILoveIM Web Messenger, IMUnitive, mabber, meebo, Yahoo Web Messenger, GPass, IP, ARP, TCP, UDP e IGMP;

8.10.3.1.80. Deve enviar alertas via e-mail para pelo menos 100 e-mails diferentes; Deve permitir a configuração de alarmes personalizados, com base em investigações;

8.10.3.1.87. A console de gerenciamento deverá ser gerenciada por Internet Explorer, Google Chrome e Firefox;

8.10.3.1.111. Caso necessário, a CONTRATANTE pode optar em direcionar parte do licenciamento deste módulo para outros módulos da plataforma de Detecção e Resposta, como o monitoramento do email, endpoint ou servidores, sem acréscimos ou mudanças de licenciamento;

8.10.3.1.20. A capacidade de análise de artefatos em sandbox pode ser realizada através de no mesmo equipamento de análise; A solução deverá possuir mecanismo de conhecimento de senhas de pelo menos 90 palavras chaves em seu vocabulário de conhecimento, para derivação de arquivos protegidos;

8.10.4.6. Deverá ser entregue equipamento NGIPS que atenda às seguintes especificações: IPS com throughput de inspeção de 3Gbps, podendo ser expandido até 5Gbps sem necessitar trocar o equipamento;

8.10.4.39. O fabricante da solução NGIPS deverá possuir times de pesquisa de vulnerabilidades de dia zero e de riscos de segurança, com pelo menos 1500 pesquisadores, sejam contratados ou parceiros, sendo que deverão ser apresentadas estatísticas dos últimos 3 anos de vulnerabilidades pesquisadas e descobertas. O fabricante deverá estar entre os Top 5 maiores pesquisadores do mundo nos relatórios publicados pela entidade Frost & Sullivan (Analysis of the Global Public Vulnerability Research);

8.10.4.63.A solução deverá possuir suporte nativo a pelo menos as seguintes ferramentas: Qualys, Nessus e Nexpose; A solução de gerenciamento centralizado deverá possuir módulo de relatórios próprio, possuindo templates que indiquem os principais riscos de segurança detectados no ambiente, contando com pelo menos 20 modelos pré-estabelecidos.

8.10.4.64. Deverá ser possível agendar o envio destes relatórios, sendo exigidos no mínimo os seguintes formatos de arquivo: PDF, DOCX, XLS, CVS e XML; A solução de gerenciamento centralizado deverá suportar o gerenciamento paralelo de pelo menos 4 IPS. A solução ofertada deverá estar dimensionada para atender o exigido neste edital, com crescimento suportado previsto para até 20 NGIPS;

8.10.4.72. A plataforma deve fornecer as três abordagens de análise: "Orientada por Ameaças, Ativos/Impactos e Vulnerabilidades". Análise rigorosa, a plataforma deve fornecer análises baseadas em gráficos para fornecer uma maneira eficaz de considerar as muitas relações muitos-para-muitos.

8.10.4.75 Devem ser suportadas fontes de dados de terceiros para análises adicionais a nível de identidade, como Azure AD, Office 365, AD local. Devem ser suportadas fontes de dados de terceiros para análises adicionais a nível de dispositivo, como Qualys, Nessus e Tenable.

8.10.4.76 Deseja-se ingestão de dados de terceiros de Firewall (Fortinet/Palo Alto/Cisco) e Portais da Web (Forcepoint/Zscaler/Cisco Umbrella/Symantec ProxySG). A plataforma deve detectar a conta de um usuário na dark web.

8.10.4.84 A plataforma deve permitir as seguintes ações para responder a riscos: Desativar/Ativar conta do usuário - Forçar logout - Redefinir senha - Isolar/Restaurar Endpoint - Monitorar tentativas de login - Monitorar/Bloquear/Desbloquear/Permitir aplicativo interno - Bloquear/Desbloquear/Permitir Acesso a aplicativos ou URLs em nuvem.

LEIA-SE:

8.10.1.1.10. A solução deve realizar a análise de malware no interior de arquivos compactados pelo menos nos formatos: ZIP, RAR, TAR e CAB, removendo seletivamente apenas o(s) arquivo(s) malicioso(s);

8.10.1.1.11.A solução deve inspecionar, em tempo real (real-time), os arquivos gravados em disco por qualquer aplicação, incluindo aplicações de mensageria e de transferência de arquivos;

8.10.1.1.85.Deve possuir mecanismo de proteção contra uso não autorizado no qual o agente do antivírus deve ser protegido contra mudança do seu estado (não possibilitar que um administrador da estação de trabalho e notebook possa parar o serviço do antivírus) bem como mecanismo para restaurar seu estado normal;

8.10.1.1.86. Deve possuir no mecanismo de autoproteção as seguintes proteções: Proteção e verificação dos arquivos de assinatura;

8.10.1.1.87. Proteção dos processos do agente de segurança; Proteção das chaves de registro do agente de segurança;

8.10.2.1.1. A solução deverá ser compatível com pelo menos os seguintes sistemas operacionais: Windows Server 2000; Windows Server 2008 e 2008 R2; Windows Server 2012 e 2012 R2; Windows Server 2016; Windows Server 2019; Windows Server 2022 e Windows Server 2025;

8.10.2.1.124. Precisa conter regras de defesa para blindagem de vulnerabilidades e ataques que explorem os seguintes sistemas operacionais: Windows Server 2008, 2012, 2016, 2019, 2022, 2025, Linux Red Hat, Suse, CentOS, Ubuntu, Debian, Solaris, AIX além de regras para aplicações padrão de mercado, incluindo Microsoft IIS, SQL Server, Microsoft Exchange, Oracle Database, Adobe Acrobat, Mozilla Firefox, Microsoft Internet Explorer, Google Chrome e Web Server Apache;

8.10.3.1.24. Capacidade de detectar ameaças web tais como vulnerabilidades e download de conteúdo malicioso; Os módulos de captura de rede deverão suportar a coleta de arquivos pelo menos nos protocolos HTTP e HTTPS;

8.10.3.1.80. Deve permitir receber logs de diferentes dispositivos;

8.10.3.1.87. A console de gerenciamento deverá ser gerenciada por Internet Explorer, Google Chrome e Firefox;

8.10.3.1.20. A capacidade de análise de artefatos em sandbox pode ser realizada no mesmo equipamento de análise; como funcionalidade complementar, quando disponível, a solução poderá possuir mecanismo de conhecimento de senhas para derivação de arquivos protegidos;

8.10.3.1.111. Deve identificar tentativas de ataques avançados na rede da CONTRATANTE e correlacionar com eventos das soluções de estação de trabalho, servidores e e-mail, a fim de rastrear o passo-a-passo do ataque na rede;

8.10.4.6. Deverá ser entregue equipamento NGIPS que atenda às seguintes especificações: IPS com throughput de inspeção de 4Gbps, podendo ser expandido até 5Gbps sem necessitar trocar o equipamento;

8.10.4.39. O fabricante da solução NGIPS deverá comprovar capacidade contínua de pesquisa de vulnerabilidades de dia zero e de riscos de segurança, mediante laboratório próprio, equipe dedicada, serviço de threat intelligence, publicações técnicas, boletins de segurança, histórico de descobertas, participação em programas de divulgação coordenada de vulnerabilidades ou outros meios

objetivos equivalentes, apresentando estatísticas dos últimos 3 anos de vulnerabilidades pesquisadas e descobertas;

8.10.4.63. A solução deverá possuir suporte nativo à integração com ferramentas de avaliação de vulnerabilidades de mercado, a exemplo de Qualys, Nessus e Nexpose, admitindo-se ferramentas equivalentes por meio de API, conectores suportados ou formatos padronizados; A solução de gerenciamento centralizado deverá possuir módulo de relatórios próprio, com relatórios pré-definidos ou customizáveis que indiquem os principais riscos de segurança detectados no ambiente.

8.10.4.64. Deverá ser possível agendar o envio destes relatórios, sendo exigidos no mínimo os seguintes formatos de arquivo: PDF, DOCX, XLS, CVS e XML;

8.10.4.72. A solução de gerenciamento centralizado deverá atuar como ponto central para o gerenciamento de políticas de IPS, devendo possuir versionamento de políticas, capacidade de rollback, além de capacidade de importação e exportação de configurações.

8.10.4.75. Devem ser suportadas fontes de dados de terceiros para análises adicionais a nível de identidade, como Azure AD, Office 365, AD local. Devem ser suportadas fontes de dados de terceiros para análises adicionais a nível de dispositivo, como Qualys, Nessus e Tenable.

8.10.4.76. A plataforma deve fornecer informações sobre contas de usuários que apresentaram atividades anômalas de alto risco ou que foram especificamente alvo de campanhas de e-mail maliciosas.

Adicionado: 8.10.3.1.112. Caso necessário, a CONTRATANTE pode optar em direcionar parte do licenciamento deste módulo para outros módulos da plataforma de Detecção e Resposta, como o monitoramento do email, endpoint ou servidores, sem acréscimos ou mudanças de licenciamento. Serão aceitas as soluções que tiverem modelo de licenciamento flexível, suíte integrada, plataforma unificada ou arranjo equivalente que permita cobertura dos vetores de e-mail, endpoint, servidores e detecção/resposta, desde que observadas as quantidades contratadas, a cobertura exigida e a ausência de custos adicionais não previstos para as funcionalidades obrigatórias.

(...)

ONDE SE LÊ:

ANEXO V -Suporte Técnico

Criticidade	Descrição	Prazo Máximo de Atendimento	Prazo Máximo de Restauração de Serviço	Glosa (por evento) para eventual descumprimento
		Em até 2 horas deve ter um técnico do fornecedor on-site.	Em até 8 horas	
	Sistema parado ou produto inoperante com impacto nas operações críticas de negócio. Exemplos: Servidor de			

Criticidade	Descrição	Prazo Máximo de Atendimento	Prazo Máximo de Restauração de Serviço	Glosa (por evento) para eventual descumprimento
Severidade 1 (Alta)	produção ou outro sistema inicial está inativo. Parte substancial dos dados essenciais corre risco de perda ou corrupção. Operações relacionadas ao negócio foram afetadas, falha que compromete a integridade geral do sistema ou dos dados.	Em até 4 horas deve ter um técnico do fornecedor on-site.	Entrega da Solução pelo fabricante em até 6 dias.	10%
Severidade 2 (Média/Alta)	Alto impacto no ambiente de produção ou grande restrição de funcionalidade. Exemplo: Ocorreu um problema no qual um recurso importante foi gravemente danificado. As operações podem continuar de forma limitada, embora a produtividade a longo prazo possa ser afetada negativamente.	Em até 4 horas deve ter um técnico do fornecedor on-site.	Em até 4 horas deve ter um técnico do fornecedor on-site.	7,50%
		Em até 2 horas um Engenheiro de Suporte do fabricante deve iniciar o atendimento através de transferência ao telefone ou retorno de chamada. Gerente técnico do fabricante deve estar disponível 24x7 e ser automaticamente notificado na abertura do caso.	Em até 16 horas Entrega da Solução pelo fabricante em até 10 dias.	
Severidade 3	O defeito não gera impacto ao negócio. Exemplo: Ocorreu um erro que causou impacto negativo limitado na operações.	Um técnico do fornecedor on-site ou atendimento remoto.	Em até 24 horas.	5%
		Em até 6 horas um Engenheiro de Suporte do fabricante entra em contato	Entrega da Solução pelo fabricante em até 15 dias ou na próxima atualização do Software.	
	O problema é pequeno, ou de	Em até 12 horas um técnico do fornecedor entra em contato.	Em até 12 horas um técnico do fornecedor entra em contato.	

Criticidade	Descrição	Prazo Máximo de Atendimento	Prazo Máximo de Restauração de Serviço	Glosa (por evento) para eventual descumprimento
Severidade 4 (Baixa)	documentação. Exemplos:O problema não afetou as operações da contratante negativamente; Encaminhamento de solicitações e ou sugestões para novos			2%

LEIA-SE:

ANEXO V -Suporte Técnico

Criticidade	Descrição	Prazo Máximo de Atendimento	Prazo Máximo de Restauração de Serviço	Glosa (por evento) para eventual descumprimento
Severidade 1 (Alta)	Sistema parado ou produto inoperante com impacto nas operações críticas de negócio. Exemplos: Servidor de produção ou outro sistema inicial está inativo. Parte substancial dos dados essenciais corre risco de perda ou corrupção. Operações relacionadas ao negócio foram afetadas, falha que compromete a integridade geral do sistema ou dos dados.	Em até 2 horas deve ter um técnico do fornecedor on-site.	Em até 8 horas	10%
		Em até 4 horas deve ter um técnico do fornecedor on-site.	Entrega da Solução pelo fabricante em até 6 dias.	
	Alto impacto no ambiente de produção ou grande restrição de funcionalidade. Exemplo: Ocorreu um problema no	Em até 4 horas deve ter um técnico do fornecedor on-site.	Em até 4 horas deve ter um técnico do fornecedor on-site.	
			Em até 16 horas	

Criticidade	Descrição	Prazo Máximo de Atendimento	Prazo Máximo de Restauração de Serviço	Glosa (por evento) para eventual descumprimento
Severidade 2 (Média/Alta)	qual um recurso importante foi gravemente danificado. As operações podem continuar de forma limitada, embora a produtividade a longo prazo possa ser afetada negativamente.	Em até 2 horas um Engenheiro de Suporte do fabricante deve iniciar o atendimento através de transferência ao telefone ou retorno de chamada. Gerente técnico do fabricante deve estar disponível 24x7 e ser automaticamente notificado na abertura do caso.	Entrega da Solução pelo fabricante em até 10 dias.	7,50%
Severidade 3	O defeito não gera impacto ao negócio. Exemplo: Ocorreu um erro que causou impacto negativo limitado na operações.	Um técnico do fornecedor on-site ou atendimento remoto.	Em até 24 horas.	5%
		Em até 6 horas um Engenheiro de Suporte do fabricante entra em contato	Entrega da Solução pelo fabricante em até 15 dias ou na próxima atualização do Software.	
Severidade 4 (Baixa)	O problema é pequeno, ou de documentação. Exemplos:O problema não afetou as operações da contratante negativamente; Encaminhamento de solicitações e ou sugestões para novos	Em até 12 horas um técnico do fornecedor entra em contato.	Em até 12 horas um técnico do fornecedor entra em contato.	2%

(...)

ONDE SE LÊ:

Tabela 8 - Sistemas Desenvolvidos e/ou Mantidos pela SESAU (Abrangência)			
Sistema	**Unidade demandante**	**Função**	**Amplitude de atuação**
GERADOR SENHA	POC-CGAF-BARCO	Gerar senhas para Gerenciar a Fila de Atendimento de Pacientes	POC - Policlinica Osvaldo Cruz CGAF - Gerência Farmaceutica

Tabela 8 - Sistemas Desenvolvidos e/ou Mantidos pela SESAU (Abrangência)			
PAINEL CHAMADOR	POC-CGAF-BARCO	Realizar a Chamada da Senha no Painel em Voz, chamando o nome Social do Paciente, juntamente com o número da Senha e Consultório Médico.	POC - Policlinica Osvaldo Cruz CGAF - Gerência Farmaceutica
SAÚDE POC	POC	Realizar a Gestão de Atendimento Administrativo, Atendimento Médico, Prontuário Eletrônico, Configurações de Painéis de Chamada, Configurações de Áreas de Atendimento.	POC - Policlinica Osvaldo Cruz
EPEP POC	POC	Sistema para Estatísticas de Atendimentos da POC, Retirar Relatórios Estratégicos de Atendimento, assim como Dashboard em Tempo Real do Cenário da POC	POC - Policlinica Osvaldo Cruz
ADMINISTRATIVO CGAF	CGAF	Realizar a Gestão de Agendamentos de Pacientes para retirar Medicamentos na Farmácia	CGAF - Gerência Farmaceutica
E-CONSUMO	CAP	Realizar a Gestão de Estoque de Materiais de Consumo	CAP - Coordenadoria de Almoxarifado e Patrimonio HEURO - Hospital de Urgência e Emergência Regional de Cacoal HRC - Hospital Regional de Cacoal Hospital Regional De Buritis JP II - Hospital e Pronto Socorro João Paulo II Cemetron - Centro de Medicina Tropical de Rondônia HB - Hospital de Base Ary Pinheiro HICD - Hospital Infantil Cosme Damião AMI - Assistencia Médica Intensiva HCAMP - Hospital de Campanha de Rondônia HRE - Hospital Regional de Extrema HEURO - Hospital de Urgência e Emergência Regional de Cacoal HRC - Hospital Regional de Cacoal Hospital Regional De São Francisco do Guaporé Hospital Regional De Buritis

Tabela 8 - Sistemas Desenvolvidos e/ou Mantidos pela SESAU (Abrangência)			
E-CONSUMO GASES	Unidades Hospitalares	Realizar a Gestão de Estoque e Solicitação de Medicinais das Unidades Hospitalares	CAP - Coordenadoria de Almoxarifado e Patrimonio HEURO - Hospital de Urgência e Emergência Regional de Cacoal HRC - Hospital Regional de Cacoal Hospital Regional De Buritis JP II - Hospital e Pronto Socorro João Paulo II Cemetron - Centro de Medicina Tropical de Rondônia HB - Hospital de Base Ary Pinheiro HICD - Hospital Infantil Cosme Damião Ami - Assistencia Médica Intensiva HCAMP - Hospital de Campanha de Rondônia HRE - Hospital Regional de Extrema HEURO - Hospital de Urgência e Emergência Regional de Cacoal HRC - Hospital Regional de Cacoal Hospital Regional De São Francisco do Guaporé Hospital Regional De Buritis
HOSPUB	Unidades Hospitalares	Realizar a Gestão de Prontuário Eletrônico	HB - Hospital de Base Ary Pinheiro HICD - Hospital Infantil Cosme Damião JP II - Hospital e Pronto Socorro João Paulo II Cemetron - Centro de Medicina Tropical de Rondônia Ami - Assistencia Médica Intensiva HCAMP - Hospital de Campanha de Rondônia HEURO - Hospital de Urgência e Emergência Regional de Cacoal HRC - Hospital Regional de Cacoal Hospital Regional De São Francisco do Guaporé Hospital Regional de Buritis CAFI NMJ - Nucleo de Mandados Judiciais CDA - Centro de Diálise de Ariquemes POC - Policlinica Osvaldo Cruz
E-LEITOS	Regulação	Painel Dashboard da Taxa de Ocupação dos Leitos de Acordo com as Informações do Hospub, assim como Realizar Pareceres para Solicitação de Leitos para as Unidades.	Todos os leitos da SESAU
E-REFEIÇÃO	Unidades Hospitalares	Realizar a Gestão e controle das Refeições nas Unidades Hospitalares dos servidores que estão de Plantão.	Cemetron - Centro de Medicina Tropical de Rondônia HB - Hospital de Base Ary Pinheiro HICD - Hospital Infantil Cosme Damião JP II - Hospital e Pronto Socorro João Paulo II HRC - Hospital Regional de Cacoal HEURO - Hospital de Urgência e Emergência Regional de Cacoal Cemetron - Centro de Medicina Tropical de Rondônia Hospital Regional de Buritis
NACSUS	NAC-NMJ	Auxiliar e ajudar os processos internos do NAC - Núcleo de Apoio e Conciliação, evitando que os pacientes entrem com uma Ação Judicial contra o Estado de Rondônia.	Núcleo de Apoio a Conciliação

Tabela 8 - Sistemas Desenvolvidos e/ou Mantidos pela SESAU (Abrangência)			
PROCESSO SELETIVO	RH	Realizar o Cadastro dos Candidatos as vagas em Aberto no Processo Seletivo da SESAU, assim como, definir os critérios de Pontuação e deferir ou indeferir algum certificado ou experiência profissional.	RH

LEIA-SE:

Tabela 8 - Sistemas Desenvolvidos e/ou Mantidos pela SESAU (Abrangência)			
Sistema	**Unidade demandante**	**Função**	**Amplitude de atuação**
GERADOR SENHA	POC-CGAF-BARCO	Gerar senhas para Gerenciar a Fila de Atendimento de Pacientes	POC - Policlinica Osvaldo Cruz CGAF - Gerência Farmaceutica
PAINEL CHAMADOR	POC-CGAF-BARCO	Realizar a Chamada da Senha no Painel em Voz, chamando o nome Social do Paciente, juntamente com o número da Senha e Consultório Médico.	POC - Policlinica Osvaldo Cruz CGAF - Gerência Farmaceutica
SAÚDE POC	POC	Realizar a Gestão de Atendimento Administrativo, Atendimento Médico, Prontuário Eletrônico, Configurações de Painéis de Chamada, Configurações de Áreas de Atendimento.	POC - Policlinica Osvaldo Cruz
EPEP POC	POC	Sistema para Estatísticas de Atendimentos da POC, Retirar Relatórios Estratégicos de Atendimento, assim como Dashboard em Tempo Real do Cenário da POC	POC - Policlinica Osvaldo Cruz

Tabela 8 - Sistemas Desenvolvidos e/ou Mantidos pela SESAU (Abrangência)			
ADMINISTRATIVO CGAF	CGAF	Realizar a Gestão de Agendamentos de Pacientes para retirar Medicamentos na Farmácia	CGAF - Gerência Farmaceutica
E-CONSUMO	CAP	Realizar a Gestão de Estoque de Materiais de Consumo	CAP - Coordenadoria de Almoxarifado e Patrimonio HEURO - Hospital de Urgência e Emergência Regional de Cacoal HRC - Hospital Regional de Cacoal Hospital Regional De Buritis JP II - Hospital e Pronto Socorro João Paulo II Cemetron - Centro de Medicina Tropical de Rondônia HB - Hospital de Base Ary Pinheiro HICD - Hospital Infantil Cosme Damião AMI - Assistencia Médica Intensiva HCAMP - Hospital de Campanha de Rondônia HRE - Hospital Regional de Extrema HEURO - Hospital de Urgência e Emergência Regional de Cacoal HRC - Hospital Regional de Cacoal Hospital Regional De São Francisco do Guaporé Hospital Regional De Buritis
E-CONSUMO GASES	Unidades Hospitalares	Realizar a Gestão de Estoque e Solicitação de Medicinais das Unidades Hospitalares	CAP - Coordenadoria de Almoxarifado e Patrimonio HEURO - Hospital de Urgência e Emergência Regional de Cacoal HRC - Hospital Regional de Cacoal Hospital Regional De Buritis JP II - Hospital e Pronto Socorro João Paulo II Cemetron - Centro de Medicina Tropical de Rondônia HB - Hospital de Base Ary Pinheiro HICD - Hospital Infantil Cosme Damião Ami - Assistencia Médica Intensiva HCAMP - Hospital de Campanha de Rondônia HRE - Hospital Regional de Extrema HEURO - Hospital de Urgência e Emergência Regional de Cacoal HRC - Hospital Regional de Cacoal Hospital Regional De São Francisco do Guaporé Hospital Regional De Buritis
HOSPUB	Unidades Hospitalares	Realizar a Gestão de Prontuário Eletrônico	HB - Hospital de Base Ary Pinheiro HICD - Hospital Infantil Cosme Damião JP II - Hospital e Pronto Socorro João Paulo II Cemetron - Centro de Medicina Tropical de Rondônia Ami - Assistencia Médica Intensiva HCAMP - Hospital de Campanha de Rondônia HEURO - Hospital de Urgência e Emergência Regional de Cacoal HRC - Hospital Regional de Cacoal Hospital Regional De São Francisco do Guaporé Hospital Regional de Buritis CAFI NMJ - Nucleo de Mandados Judiciais CDA - Centro de Diálise de Ariquemes POC - Policlinica Osvaldo Cruz

Tabela 8 - Sistemas Desenvolvidos e/ou Mantidos pela SESAU (Abrangência)			
E-LEITOS	Regulação	Painel Dashboard da Taxa de Ocupação dos Leitos de Acordo com as Informações do Hospub, assim como Realizar Pareceres para Solicitação de Leitos para as Unidades.	Todos os leitos da SESAU
E-REFEIÇÃO	Unidades Hospitalares	Realizar a Gestão e controle das Refeições nas Unidades Hospitalares dos servidores que estão de Plantão.	Cemetron - Centro de Medicina Tropical de Rondônia HB - Hospital de Base Ary Pinheiro HICD - Hospital Infantil Cosme Damião JP II - Hospital e Pronto Socorro João Paulo II HRC - Hospital Regional de Cacoal HEURO - Hospital de Urgência e Emergência Regional de Cacoal Cemetron - Centro de Medicina Tropical de Rondônia Hospital Regional de Buritis
NACSUS	NAC-NMJ	Auxiliar e ajudar os processos internos do NAC - Núcleo de Apoio e Conciliação, evitando que os pacientes entrem com uma Ação Judicial contra o Estado de Rondônia.	Núcleo de Apoio a Conciliação
PROCESSO SELETIVO	RH	Realizar o Cadastro dos Candidatos as vagas em Aberto no Processo Seletivo da SESAU, assim como, definir os critérios de Pontuação e deferir ou indeferir algum certificado ou experiência profissional.	RH

2. CONCLUSÃO

Em atenção ao Art. 55, §1º, da Lei Federal 14.133 de 2021, a qual se aplica subsidiariamente a modalidade Pregão e, considerando que as modificações afetam a formulação das propostas de preços, informamos que o prazo de abertura do certame fica **reagendado:**

As alterações sofridas no Instrumento Convocatório e seus anexos não impactaram a cotação de preços:

DATA: 08 de Setembro de 2026

HORÁRIO: 10h30 min (horário de Brasília – DF).

ENDEREÇO ELETRÔNICO: https://www.gov.br/compras/pt-br

Eventuais dúvidas poderão ser sanadas junto ao Pregoeiro e à Equipe de Apoio através do telefone (69) 3212-9243 ou pelo e-mail: supelcotec@gmail.com

Publique-se.

Porto Velho/RO, data e hora do sistema.

GABRIEL ALVES DA SILVA GAMA
Matrícula nº ******238
Pregoeiro da Comissão de Tecnologia - COTEC
Superintendência Estadual de Compras e Licitações - SUPEL|RO

Documento assinado eletronicamente por **Gabriel Alves Da Silva Gama**, **Pregoeiro(a)**, em 21/08/2026, às 09:45, conforme horário oficial de Brasília, com fundamento no artigo 18 caput e seus §§ 1º e 2º, do Decreto nº 21.794, de 5 Abril de 2017.

A autenticidade deste documento pode ser conferida no site portal do SEI, informando o código verificador **75351847** e o código CRC **81C324FD**.

Referência: Caso responda este(a) Adendo, indicar expressamente o Processo nº 0036.028242/2024-36 SEI nº 75351847