

***TERMO DE REFERÊNCIA PARA
CONTRATAÇÃO DE LICENÇAS DE
SOFTWARE ANTIVIRUS***

1. DO OBJETO:

- 1.1. Contratação de empresa especializada para fornecimento de licenças de software de Antivírus, afim de atender às demandas do Conselho Regional de Enfermagem do Amazonas.

2. JUSTIFICATIVA:

- 2.1. O Setor de Tecnologia da Informação tem missão suportar todo o aparato tecnológico necessário ao bom funcionamento do COREM-AM, ampliando a integração com a população e melhorando os serviços disponibilizados a seus usuários, pois todos os serviços são oferecidos por meio de sistemas e portais de acesso, incluindo também, os sistemas internos de apoio à atividade-meio, atividades finalísticas. Com esta responsabilidade, o STI deve garantir a segurança, disponibilidade, desempenho e continuidade dos serviços por meio de estratégias bem definidas de Gestão da Informação, além de assegurar, com eficiência e eficácia, as rotinas operacionais que suportam os processos de negócio dessa Autarquia. Neste contexto, o cuidado com dados e informações que circulam na rede corporativa é um dos nossos principais objetivos.
- 2.2. A motivação para a realização desta pretensa contratação se deve ao fato de o contrato de utilização de licenças de antivírus corporativo, atualmente em uso está se encerrando no dia 30/08/2019 por tanto, a necessidade da contratação de novas licenças que incluam o uso de software de antivírus corporativo e treinamento, bem com atualização continua da versão.
- 2.3. O Antivírus é um programa ou software especificamente desenvolvido para detectar, anular e eliminar, de um computador, vírus e outros tipos de códigos maliciosos que ameaçam o sigilo e a integridade dos dados e informações por tanto, software indispensável para segurança da informação desta autarquia.

3. FUNDAMENTO LEGAL

- 3.1. A prestação dos serviços objeto deste Termo de Referência obedecerá, integralmente, às disposições da Lei nº 10.520 de 17/07/2002, da Lei Complementar nº 123 de 14/12/2006, dos Decretos nº 3.555 de 08/08/2000, nº 5.450 de 31/05/2005, nº 8.538 de 06/10/15 e nº 2.271 de 07/07/97, Instrução Normativa MPOG nº 05/2017, aplicando-se, subsidiariamente, a Lei nº 8.666 de 21/06/93, e suas alterações.
- 3.2. De outras legislações aplicadas a contratações de TI como a Lei nº 8.248/91, Lei nº 7.174/10, IN SLTI MP 04/2010, IN Nº 01, Orientação Normativa SLTI , Nº 01/2015.

4. DA DESCRIÇÃO DOS SERVIÇOS

4.1. Necessidade de Negócio

4.1.1. Necessidade 1:

Programas desenvolvidos para prevenir, detectar e eliminar vírus de computador e outros tipos de softwares nocivos ao sistema operacional.

4.1.2. Funcionalidade:

Disponibilizar os recursos tecnológicos necessários para utilização do programa/aplicativo com licença para os equipamentos do Conselho Regional de Enfermagem do Amazonas – Coren-AM.

4.2. Requisitos do Negocio

Tabela 1 – Requisito do Software

1	Programa/aplicativo de Antivírus com licença
---	--

4.2.1. Especificação Técnica do Negocio

4.2.1.1. Da Solução de ANTIVÍRUS:

4.2.1.1.1. SERVIDOR DE ADMINISTRAÇÃO E CONSOLE ADMINISTRATIVA:

4.2.1.1.1.1. Compatibilidade:

Microsoft Windows Server 2003 ou superior (Todas edições);
Microsoft Windows Server 2003 x64 ou superior (Todas edições);
Microsoft Windows Server 2008 (Todas edições) Microsoft Windows Server 2008 (Todas edições);
Microsoft Windows Server 2008 x64 SP1 (Todas edições);
Microsoft Windows Server 2008 R2 (Todas edições);
Microsoft Windows Server 2008 R2 Core (Todas edições);
Microsoft Windows Server 2012 (Todas edições);
Microsoft Windows Server 2012 R2 (Todas edições);
Microsoft Windows Server 2016(Todas edições);
Microsoft Windows XP Professional SP2 e superior;
Microsoft Windows XP Professional x64 e superior;
Microsoft Windows Vista SP1;
Microsoft Windows Vista x64 SP1;
Microsoft Windows 7;
Microsoft Windows 7 x64;
Microsoft Windows 8;
Microsoft Windows 8 x64;
Microsoft Windows 8.1 Professional / Enterprise;
Microsoft Windows 8.1 Professional / Enterprise x64;
Microsoft Windows 10 x86 e x64.

4.2.1.1.1.2. Suporta as seguintes plataformas virtuais:

VMware: Workstation 9.x, Workstation 10.x, ESX 4.x, ESXi 4.x, ESXi 5.1, 5.5 e 6.0;
Microsoft Hyper-V: 2008, 2008 R2, 2012, 2012 R2;
KVM integrado com: RHEL 5.4 e 5.x acima, SLES 11 SPx, Ubuntu 10.10 LTS;
Microsoft VirtualPC 6.0.156.0;
Parallels Desktop 7 e superior;
Oracle VM VirtualBox 4.0.4-70112 (Somente logon como convidado);

4.2.1.1.1.3. Características:

A console deve ser acessada via WEB (HTTPS) ou MMC;

Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade;

Capacidade de remover remotamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores, sem a necessidade da senha de remoção do atual antivírus;

Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, login script e/ou GPO de Active Directory;

Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac), protegidos pela solução antivírus;

Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas;

Capacidade de monitorar diferentes subnets de rede, grupos de trabalhos já existentes ou que forem criados na rede, a fim de encontrar máquinas novas para serem adicionadas a proteção;

Capacidade de, assim que detectar máquinas novas no Active Directory, subnets ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado.

Capacidade de agrupamento de máquina por características comuns entre as mesmas, por exemplo: agrupar todas as máquinas que não tenham o antivírus instalado, etc;

Capacidade de definir políticas de configurações diferentes por grupos de estações, permitindo que criados subgrupos e com função de herança de políticas entre grupos e subgrupos;

Deve fornecer as seguintes informações dos computadores:

1. Se o antivírus está instalado, iniciado e atualizado;
2. Minutos/horas desde a última: atualização de vacinas, conexão da máquina com o servidor administrativo;
3. Data e horário da última verificação executada na máquina;
4. Versão do antivírus instalado na máquina;
5. Se é necessário reiniciar o computador para aplicar mudanças;
6. Data e horário de quando a máquina foi ligada;
7. Nome do computador;
8. Domínio ou grupo de trabalho do computador;
9. Data e horário da última atualização de vacinas;
10. Sistema operacional;
11. Endereço IP;
12. Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;
13. Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;
14. Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas

clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede;

15. Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo.

16. Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF.

17. Capacidade de enviar e-mails para contas específicas em caso de algum evento;

18. Capacidade de realizar atualização incremental de vacinas nos computadores clientes;

19. Capacidade de diferenciar máquinas virtuais de máquinas físicas.

4.2.1.2. ESTAÇÕES WINDOWS:

4.2.1.2.1. Compatibilidade

Microsoft Windows 7 Professional/Enterprise/Ultimate

Microsoft Windows 7 Professional/Enterprise/Ultimate x64

Microsoft Windows 7 Professional/Enterprise/Ultimate SP1 e superior

Microsoft Windows 7 Professional/Enterprise/Ultimate x64 SP1 e superior

Microsoft Windows 8 Professional/Enterprise

Microsoft Windows 8 Professional/Enterprise x64

Microsoft Windows 8.1 Professional/Enterprise

Microsoft Windows 8.1 Professional/Enterprise x64

Microsoft Windows 10 x86 e x64

4.2.1.2.2. Características:

Deve prover as seguintes proteções:

1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado, Web (módulo para verificação de sites e downloads contra vírus), E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos) e Mensagens Instantâneas (módulo para verificação de mensagens instantâneas, como ICQ, MSN, IRC, etc);

2. Firewall com IDS;

3. Autoproteção (contra-ataques aos serviços/processos do antivírus);

4. Controle de dispositivos externos; de acesso a sites por categoria; de execução de aplicativos e de vulnerabilidades do Windows e dos aplicativos instalados.

5. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

6. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa).

7. Capacidade de automaticamente desabilitar o Firewall do Windows (caso exista) e de antivírus de outro fabricante, para evitar incompatibilidade com a solução;

8. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação;

9. Capacidade de verificar somente arquivos novos e alterados, de verificar objetos usando heurística; arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomá-la a partir da extensão do arquivo e agendar uma pausa na verificação;

10. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;

O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

1. Perguntar o que fazer, ou;

2. Bloquear acesso ao objeto:

1. Apagar o objeto ou tentar desinfetá-lo (de acordo com a configuração preestabelecida pelo administrador);

3. Caso positivo de desinfecção:

1. Restaurar o objeto para uso;

4. Caso negativo de desinfecção:

1. Mover para quarentena ou apagar (de acordo com a configuração preestabelecida pelo administrador);

11. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;

12. Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3 e SMTP, assim como conexões criptografadas (SSL) para POP3;

13. Capacidade de verificar tráfego de ICQ, MSN, AIM e IRC contra vírus e links phishings, links inseridos em e-mails contra phishings e tráfego SSL nos browsers: Internet Explorer, Firefox e Opera;

14. Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados.

15. Capacidade de verificação de tráfego HTTP e qualquer script do Windows Script Host (Java Script, Visual Basic Script, etc), usando heurísticas;

16. Deve ter suporte total ao protocolo IPv6;

17. Na verificação de tráfego web, caso encontrado código malicioso o programa deve:

1. Perguntar o que fazer, ou;

2. Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;

3. Permitir acesso ao objeto.

4. O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador;

5. Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em tempo real, ou;

6. Verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação.

18. Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web.

19. Deve possuir módulo que analise as ações de cada aplicação em execução no computador, gravando as ações executadas e comparando-as com sequências características de atividades perigosas. Tais registros de sequências devem ser atualizados juntamente com as vacinas.

20. Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa.
21. Deve possuir módulo que analise qualquer tentativa de edição, exclusão ou gravação do registro, de forma que seja possível escolher chaves específicas para serem monitoradas e/ou bloqueadas.
22. Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica;
23. Deve possuir módulo IDS (Intrusion Detection System) para proteção contra port scans. A base de dados de análise deve ser atualizada juntamente com as vacinas.
24. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
 1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
 2. Filtragem por aplicativo: onde o administrador poderá escolher o nome de aplicativo terá acesso à rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.
25. Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:
 1. Discos de armazenamento locais
 2. Armazenamento removível
 3. Impressoras
 4. CD/DVD
 5. Drives de disquete
 6. Modems
 7. Dispositivos de fita
 8. Dispositivos multifuncionais
 9. Leitores de smart card
 10. Wi-Fi
 11. Adaptadores de rede externos
 12. Dispositivos Bluetooth
26. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário e agendamento.
27. Capacidade de configurar novos dispositivos por Class ID/Hardware ID
28. Capacidade de limitar o acesso a sites da internet por categoria, por conteúdo (vídeo, áudio, etc), com possibilidade de configuração por usuário ou grupos de usuários e agendamento.
29. Capacidade de bloquear execução de aplicativo que está em armazenamento externo.

4.2.1.3. ESTAÇÕES DE TRABALHO LINUX:

4.2.1.3.1. Compatibilidade Plataforma 32-bits e 64-bits:

1. CentOS 7 ou superior;
2. Debian 7 ou superior;
3. Fedora 15 ou superior;
4. OpenSUSE 11 ou superior;
5. Red Hat Enterprise Linux 6.2 Desktop ou superior;
6. SUSE Linux Enterprise Desktop 11 ou superior;
7. Ubuntu 10.04 LTS ou superior;

4.2.1.3.2. Características:

1. Deve prover as seguintes proteções:

2. Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware, etc.) que verifique qualquer arquivo criado, acessado ou modificado;
3. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora
4. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.
5. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;
6. Capacidade de verificar objetos usando heurística e arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomá-la a partir da extensão do arquivo;
7. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

4.2.1.4. SERVIDORES WINDOWS:

4.2.1.4.1. Compatibilidade

Microsoft Windows Small Business Server 2011 Essentials/Standard x64
Microsoft Windows Server 2003 Standard/Enterprise SP2 x86/x64
Microsoft Windows Server 2003 R2 Standard/Enterprise SP2 x86/x64
Microsoft Windows Server 2008 Standard/Enterprise/Datacenter SP1 x86/x64
Microsoft Windows Server 2008 Core Standard/Enterprise/Datacenter SP1 x86/x64
Microsoft Windows Server 2008 R2 Core Standard/Enterprise/Datacenter SP1
Microsoft Windows Server 2012 Foundation/Essentials/Standard x64
Microsoft Windows Hyper-V Server 2008 R2 SP1
Microsoft Terminal baseado em Windows Server 2003
Microsoft Terminal baseado em Windows Server 2008
Microsoft Terminal baseado em Windows Server 2008 R2
Citrix Presentation Server 4.0 e 4.5
Citrix XenApp 4.5, 5.0 e 6.0

4.2.1.4.2. Características:

1. Deve prover as seguintes proteções:

- Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc.) que verifique qualquer arquivo criado, acessado ou modificado;
Autoproteção contra-ataques aos serviços/processos do antivírus
2. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota.
 3. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.
 4. Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros, etc);
 5. Em caso erros, deve ter capacidade de criar logs e traces automaticamente, sem necessidade de outros softwares;

6. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
7. Capacidade de acrescentar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação;
8. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomá-la a partir da extensão do arquivo;
9. Capacidade de verificar somente arquivos novos e alterados;
10. Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários, etc);
11. Capacidade de verificar objetos usando heurística;
12. Capacidade de configurar diferentes ações para diferentes tipos de ameaças;
- 13. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:**
 1. Perguntar o que fazer, ou;
 2. Bloquear acesso ao objeto;
 1. Apagar o objeto ou tentar desinfetá-lo (de acordo com a configuração preestabelecida pelo administrador)
 2. Caso positivo de desinfecção:
 1. Restaurar o objeto para uso
 3. Caso negativo de desinfecção:
 1. Mover para quarentena ou apagar (de acordo com a configuração preestabelecida pelo administrador);
 14. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
 15. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
 16. Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa

4.2.1.5. SERVIDORES LINUX:

4.2.1.5.1. Compatibilidade Plataforma 32-bits e 64-bits:

1. CentOS 7 ou superior;
2. Debian 7 ou superior;
3. Fedora 15 ou superior;
4. OpenSUSE 11 ou superior;
5. Red Hat Enterprise Linux 6.2 Server ou superior;
6. SUSE Linux Enterprise Server 11 ou superior;
7. Ubuntu Server 10.04 LTS ou superior;

4.2.1.5.2. Características

1. Deve prover as seguintes proteções:

Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;

2. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.
3. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;
4. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomá-la a partir da extensão do arquivo;
5. Capacidade de verificar objetos usando heurística;
6. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
7. Deve possuir módulo de administração remoto através de ferramenta na nuvem ou Webmin (ferramenta nativa GNU-Linux).

4.3. Requisitos de Capacitação

Um treinamento rápido executado pelo Setor de Tecnologia da Informação do Coren-AM é suficiente para utilização da ferramenta.

4.4. Requisitos de Manutenção

Garantia de 36 (trinta e seis) meses contados do recebimento definitivo.

4.5. Requisitos Temporais

O prazo para o fornecimento do objeto será de 5 (cinco) dias úteis, a partir do recebimento da ordem de fornecimento.

4.6. Requisitos Legais

A presente contratação deve observar as seguintes leis e normas:

- a) Lei nº 8.666, de 21 de junho de 1993, que institui normas para licitações e contratos da Administração Pública.
- b) Lei nº 10.520, de 17 de julho de 2002, que institui modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns.
- c) Decreto nº 5.450, de 31 de maio de 2005, que regulamenta o pregão na forma eletrônica, para aquisição de bens e serviços comuns.
- d) Portaria Nº 306, de 13 de dezembro de 2001, do Ministério do Planejamento, Orçamento e Gestão.

5. DA NATUREZA E CLASSIFICAÇÃO DOS SERVIÇOS

- 5.1. Trata-se de aquisição de bens comuns, cujos padrões de desempenho e qualidade podem ser objetivamente definidos pelo edital, por meio de especificações usuais de mercado, nos termos do parágrafo único do art. 1º da Lei n. 10.520/2012, assim como no parágrafo 2º do art. 3º do ANEXO I do Decreto n. 3.555/2000 e no parágrafo 1º do art. 2º do Decreto 5.450/2005. Nos termos do art. 16, inciso IV do Decreto n. 8.248/1991, tratam-se ainda de bens de informática.

6. DA QUANTIDADE E VALOR ESTIMADO

- 6.1.** A demanda prevista para atender o Conselho Regional de Enfermagem do Amazonas é de 83 (oitenta e três) licenças de antivírus, sendo 81 (oitenta e um) para as estações de trabalho e 2 (dois) para servidores.
- 6.2.** A relação de equipamentos do COREN-AM atualmente dispõe é a seguinte:

ITEM	EQUIPAMENTOS DO COREN-AM	OBSERVAÇÃO
Sector de Licitação e Contrato – SELIC		
1	Notebook Samsung - Patrimônio de n.º 320.	-
Comunicação		
2	Notebook Positivo - Patrimônio de n.º 441.	-
3	CPU – Megaware – Patrimônio de n.º 425.	-
Sector de Tecnologia e Informação – STI		
4	Notebook Samsung - Patrimônio de n.º 382.	-
5	Notebook Samsung - Patrimônio de n.º 383.	-
6	Notebook HP - Patrimônio de n.º 670.	-
7	CPU Servidor - Intel – Patrimônio de n.º 384.	-
8	CPU – Intel - Patrimônio de n.º 355.	-
9	CPU HP – Patrimônio de n.º 651.	-
10	CPU HP – Patrimônio de n.º 653.	-
Secretaria Executiva – SECEX		
11	Notebook Positivo - Patrimônio de n.º 433.	-
12	CPU – Megaware – Patrimônio de n.º 473.	-
13	Notebook HP - Patrimônio de n.º 667.	-
Gabinete da Presidência		
14	Notebook HP - Patrimônio de n.º 665.	-
Controladoria Geral – CONTROL		
15	Notebook HP - Patrimônio de n.º 664.	-
16	Notebook Positivo - Patrimônio de n.º 445.	-
17	CPU – Megaware – Patrimônio de n.º 423.	-
18	CPU – Intel - Patrimônio de n.º 321.	-
19	CPU – Megaware – Patrimônio de n.º 458.	-

Procuradoria Geral – PROGER		
20	Notebook Positivo - Patrimônio de n.º 435.	-
21	CPU HP – Patrimônio de n.º 650.	-
22	CPU – Megaware – Patrimônio de n.º 438.	-
Departamento de Administração e Gestão de Pessoal – DAGEPE		
23	CPU HP – Patrimônio de n.º 646.	-
24	CPU – Megaware – Patrimônio de n.º 443.	-
25	CPU – Intel - Patrimônio de n.º 298.	-
26	Notebook Positivo - Patrimônio de n.º 452.	-
Departamento Contábil – DECON		
27	CPU HP – Patrimônio de n.º 652.	-
28	CPU – Megaware – Patrimônio de n.º 446.	-
Departamento Financeiro – DEFIN		
29	Notebook HP - Patrimônio de n.º 666.	-
30	CPU – Megaware – Patrimônio de n.º 462.	-
Departamento de Fiscalização – DEFIS		
31	CPU – Megaware – Patrimônio de n.º 430.	-
32	CPU HP – Patrimônio de n.º 645.	-
33	CPU HP – Patrimônio de n.º 647.	-
34	CPU HP – Patrimônio de n.º 648.	-
Corregedoria e Processos Éticos – COPET		
35	CPU – Intel - Patrimônio de n.º 335.	-
36	Notebook Positivo - Patrimônio de n.º 455.	-
Câmara Técnica – CT		
37	Notebook Positivo - Patrimônio de n.º 432.	-
Departamento de Registro e Cadastro – DRC		
38	CPU HP – Patrimônio de n.º 644.	-
39	CPU – Intel - Patrimônio de n.º 499.	-
40	CPU – Intel - Patrimônio de n.º 330.	-
41	CPU – Intel - Patrimônio de n.º 352.	-

Setor de Negociação		
42	CPU – Megaware – Patrimônio de n.º 436.	-
43	CPU – Megaware – Patrimônio de n.º 421.	-
Setor de Dívida Ativa		
44	Notebook Positivo - Patrimônio de n.º 453.	-
45	CPU – Intel - Patrimônio de n.º 504.	-
46	CPU HP – Patrimônio de n.º 649.	-
Protocolo e Arquivo		
47	Notebook Positivo - Patrimônio de n.º 434.	-
48	CPU – Intel - Patrimônio de n.º 314.	-
49	Notebook Positivo - Patrimônio de n.º 460.	-
50	CPU – Megaware – Patrimônio de n.º 468.	-
Ouvidoria		
Recepção		
51	CPU – Intel - Patrimônio de n.º 297.	-
Estoque		
52	Notebook Positivo - Patrimônio de n.º 445.	-
53	Notebook Positivo - Patrimônio de n.º 456.	-
54	Notebook HP - Patrimônio de n.º 671.	-
55	Notebook HP - Patrimônio de n.º 669.	-
56	Notebook HP - Patrimônio de n.º 668.	-

6.3. Os equipamentos a serem adquiridos pelo COREN-AM são os seguintes:

ORIGEM	DESCRIÇÃO	Q T D E	OBSERVAÇÃO
Processo Administrativo do Coren-AM – PAD/Coren-AM de n.º 156/2019	Servidor	01	Em processamento
	Estação de Trabalho	05	
	Totem de Autoatendimento	01	
Processo Administrativo do Cofen PAD/Cofen	Notebook	20	Em processamento

6.4. Conforme estudo técnico preliminar o valor referencial estimado é o seguinte:

ITEM	DESCRIÇÃO	Q T D E	VLR. UNITÁRIO (R\$)	VLR. TOTAL (R\$)
01	Aquisição de Software Pronto, Descrição: Solução de antivírus, com antispymware, gerenciamento centralizado, licença de uso de software, serviço de entrega, instalação e configuração, garantia de atualização contínua, suporte técnico on-site e a transferência de conhecimento técnico, operacional e administrativo, para segurança e proteção para os equipamentos como estação de trabalho, notebooks, tablets e smartphones, por 36 meses. Estação de Trabalho.	81	26,17	2.119,77
02	Aquisição de Software Pronto, Descrição: Solução de antivírus, com antispymware, gerenciamento centralizado, licença de uso de software, serviço de entrega, instalação e configuração, garantia de atualização contínua, suporte técnico on-site e a transferência de conhecimento técnico, operacional e administrativo, para segurança e proteção para os equipamentos como servidores, por 36 meses. Servidor.	02	26,17	52,34
TOTAL GERAL (R\$) →				2.172,11

- 6.5. Os valores referentes aos pagamentos das licenças serão estabelecidos em moeda corrente nacional.
- 6.6. Não serão aceitos valores globais superiores ao valor global anual referencial.
- 6.7. Nos valores a serem apresentados deverão estar compreendidos, além dos tributos, todos e quaisquer encargos que, direta ou indiretamente, decorram da execução do objeto licitado.

7. DAS OBRIGAÇÕES DA CONTRATADA

- 7.1. Fornecer a solução corporativa de antivírus cumprindo todas as obrigações constantes no Termo de Referência, seus anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto e, ainda;
- 7.2. Responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com os artigos 14 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990);
- 7.3. Reparar ou corrigir, às suas expensas os defeitos quanto ao licenciamento;
- 7.4. Manter, durante toda a execução do objeto contratado, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas neste termo;
- 7.5. Indicar preposto para representá-la durante a execução do objeto contratado.
- 7.6. Prover todos os meios necessários para garantir a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações do Contratante hospedadas na solução contratada.

8. DA OBRIGAÇÕES DA CONTRATANTE

- 8.1. Proporcionar todas as facilidades indispensáveis à boa execução das obrigações contratuais.
- 8.2. Permitir acesso às suas dependências aos empregados da Contratada para a entrega do objeto contratado.
- 8.3. Acompanhar e fiscalizar toda a execução do objeto, assegurando assim, o cumprimento de todas as condições estabelecidas neste termo de referência;
- 8.4. Efetuar o pagamento à Contratada, conforme prazo e forma prevista neste termo de referência.
- 8.5. Solicitar, sempre que necessário, esclarecimentos à Contratada quanto ao fornecimento do objeto, notificando-a por escrito quando identificadas irregularidades na sua execução ou quando apresentados problemas durante a vigência do período de garantia do produto.
- 8.6. Rejeitar, no todo ou em parte, objeto entregue fora das especificações técnicas exigidas.
- 8.7. Fornecer atestados de capacidade técnica, quando solicitados, desde que atendidas as obrigações contratuais.
- 8.8. Aplicar à Contratada, quando necessário, as sanções legais cabíveis, garantida a ampla defesa.

9. ACOMPANHAMENTO E FISCALIZAÇÃO

- 9.1. Nos termos do art. 67 Lei nº 8.666, de 1993, será designado representante para acompanhar e fiscalizar a entrega do Objeto, anotando em registro próprio todas as ocorrências relacionadas com a execução e determinando o que for necessário à regularização de falhas ou defeitos observados.
- 9.2. A fiscalização de que trata este item não exclui nem reduz a responsabilidade da Contratada, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas ou vícios redibitórios, e, na ocorrência desta, não implica em corresponsabilidade do COREN-AM ou de seus agentes e prepostos, de conformidade com o art. 70 da Lei nº 8.666, de 1993.
- 9.3. O representante do COREN-AM anotar em registro próprio todas as ocorrências relacionadas com a execução do contrato, indicando dia, mês e ano, bem como o nome dos funcionários eventualmente envolvidos, determinando o que for necessário à

regularização das falhas ou defeitos observados e encaminhando os apontamentos à autoridade competente para as providências cabíveis.

10. SANÇÕES ADMINISTRATIVAS

10.1. Com fundamento no artigo 7º da Lei n.º 10.520/2002 e no art. 28 do Decreto n.º 5.450/2005, ficará impedida de licitar e contratar com a União, Estados, Amazonas e Municípios, Distrito Federal e Municípios e será descredenciada do Sicaf e do cadastro de fornecedores da Contratante, pelo prazo de até 5 (cinco) anos, garantida a ampla defesa, sem prejuízo das demais cominações legais e de multa de até 30% (trinta por cento) sobre o valor da contratação, sem prejuízo da rescisão unilateral do contrato (art. 78 da Lei 8.666, de 1993), a Contratada que:

- a) não assinar o termo de contrato ou aceitar/retirar o instrumento equivalente, quando convocado dentro do prazo de validade da proposta;
- b) apresentar documentação falsa;
- c) deixar de entregar os documentos exigidos no certame;
- d) ensejar o retardamento da execução do objeto;
- e) não manter a proposta;
- f) cometer fraude fiscal;
- g) comportar-se de modo inidôneo;

10.2. Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os licitantes, em qualquer momento da licitação, mesmo após o encerramento da fase de lances.

10.3. O licitante/adjudicatário que cometer qualquer das infrações discriminadas no subitem anterior ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

10.3.1. Multa de 5% (cinco por cento) sobre o valor estimado do(s) item(s) prejudicado(s) pela conduta do licitante;

10.3.2. Impedimento de licitar e de contratar com a União e descredenciamento no SICAF, pelo prazo de até cinco anos;

10.4. A penalidade de multa pode ser aplicada cumulativamente com a sanção de impedimento.

10.5. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa ao licitante/adjudicatário, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente na Lei nº 9.784, de 1999.

10.6. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

11. DO PRAZO E LOCAL DE ENTREGA DO MATERIAL

11.1. Os itens deverão ser entregues através do e-mail ti@corenam.gov.br, no horário das 08h às 16h, de segunda à sexta-feira, exceto feriados, Sede do Conselho Regional de Enfermagem do Amazonas – COREN/AM.

11.2. Realizada a contratação, a Contratada terá o prazo máximo de entrega de 05 (cinco) dias, contados do recebimento da Nota de Empenho e Requisição de Materiais;

11.3. O objeto licitado será recebido:

11.3.1. Provisoriamente, pelo Setor de Tecnologia da Informação – STI/COREN-AM para posterior verificação da conformidade e quantidade do produto com as especificações constantes no Termo de Referência e da proposta da empresa vencedora, o qual emitirá relatório para o fiscal de contrato, sendo este o responsável para emitir o atesto de recebimento provisório.

11.3.2. Definitivamente, pelo Gestor/fiscal do contrato auxiliado pelo Setor de Tecnologia da Informação – STI/COREN-AM, após verificação da qualidade e quantidade do produto e consequente aceitação, no prazo de até 10 (dez) dias corridos, contados da data da entrega.

11.4. Caso seja detectado, quando da entrega, que o produto não atende às especificações técnicas previstas, poderá o COREN-AM, rejeitá-lo integralmente ou em parte, obrigando-se o fornecedor a providenciar a sua substituição no prazo de até 5 (cinco) dias úteis, contados da notificação;

11.4.1. Caso haja recusa de mais de 10% (dez por cento) dos itens, estes serão devolvidos.

11.5. Todos os materiais deverão ser novos, a fim de permitir completa segurança durante o envio, além disso, devem estar em perfeitas condições quando da recepção pelo COREN-AM e identificados externamente com os dados constantes da Nota Fiscal;

11.6. O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da Contratada pelos prejuízos resultantes da incorreta execução do contrato;

11.8. A Contratada será responsável pela troca do produto que apresentar falha no seu funcionamento ou defeito de fabricação, durante o prazo de validade deste;

12. DO PAGAMENTO

12.1. As Notas Fiscais/Faturas deverão ser emitidas em 02(duas) vias, corretamente preenchidas e sem rasuras, acompanhadas dos respectivos comprovantes de recolhimento dos encargos sociais, devendo conter a descrição do objeto e do número do CONTRATO/EMPENHO.

12.2. O CNPJ constante da Nota Fiscal/Fatura deverá ser o mesmo indicado na Proposta apresentada pela CONTRATADA e da nota de empenho emitida pelo CONTRATANTE, mesmo que sejam empresas consideradas matriz e filial ou vice-versa, ou pertencente ao mesmo grupo ou conglomerado, sob pena de não ser efetuado o pagamento.

12.3. Na hipótese de Nota Fiscal/Fatura apresentar erros ou dúvidas quanto à exatidão ou documentação, o Contratante poderá pagar apenas a parcela não controvertida no prazo fixado para pagamento, de acordo com o relatório emitido pela Tesouraria, ressalvado o direito da Contratada de reapresentar para cobrança as partes controvertidas com as devidas justificativas (nestes casos o Contratante terá o prazo de cinco (5) dias úteis, a partir do recebimento, para efetuar uma análise e o pagamento).

12.4. O pagamento somente poderá ser efetuado se a licitante estiver em situação fiscal regular, isto é, desde que apresente as certidões elencadas abaixo:

- a)** Certidão conjunta negativa de débitos relativos a tributos federais e à dívida ativa da União expedida pela Secretaria da Receita Federal.

- b) Certidão de regularidade de débito com a Fazenda Estadual e Municipal da localidade da Licitante, pertinente ao seu ramo de atividade e relativa aos tributos relacionados com o objeto ou outra prova equivalente na forma da lei;
- c) Certidão de regularidade de débito com o Sistema de Seguridade Social (INSS);
- d) Certificado de regularidade de situação com o Fundo de Garantia por Tempo de Serviço (FGTS);
- e) Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de Maio de 1943.

12.5. Os pagamentos serão efetuados, por meio de ordem bancária a ser creditada na conta corrente do CONTRATADO, até 5º (quinto) dia útil após o recebimento dos materiais e nota fiscal, após verificação e emissão de atestado pelo servidor da contratante responsável pela fiscalização do contrato.

12.6. O CONTRATANTE poderá deduzir do montante a pagar os valores correspondentes a multas, ressarcimentos ou indenizações devidas pelo CONTRATADO.

13. PRAZO DE VIGÊNCIA DO CONTRATO

13.1. Prazo de validade do instrumento de contrato será de 30 (trinta) dias a contar da sua assinatura.

13.2. O instrumento poderá ser extinto ocorrendo o pagamento total do objeto.

13.3. Ocorrendo a extinção do contrato, este não anula a garantia do objeto.

14. GARANTIA

14.1. Não será exigida garantia da execução do contrato, mas a Contratante poderá reter, do montante a pagar, valores para assegurar o pagamento de multas, indenizações e ressarcimentos devidos pela Contratada.

15. RECURSOS ORÇAMENTARIOS

15.1. Conforme Nota Orçamentaria e Disponibilidade Orçamentaria do Departamento Contábil do Coren-AM – DECON/COREN-AM, os recursos orçamentários necessários ao atendimento do objeto correrão pelo Orçamento do COREN-AM no exercício de 2019/2020, e serão alocados pelo Departamento Financeiro deste Conselho 6.2.2.1.1.01.33.90.039.002.012.003 – Locação De Software.

16. QUALIFICAÇÃO MÍNIMA EXIGIDA

16.1. Entre outros documentos a serem solicitados pela área responsável pela Licitação, é necessário que a empresa a ser CONTRATADA como Agente de Integração, para efeito de habilitação, apresente os seguintes documentos:

- a) Declaração informando que, caso seja declarada vencedora, comprovará, na data de assinatura do Contrato, possuir representação dotada de infraestrutura técnica e operacional adequada, com recursos humanos qualificados, necessários e suficientes para a prestação dos serviços a serem contratados na cidade de Manaus/AM;
- b) Atestado (s) de capacidade técnica, expedido (s) por pessoa jurídica de direito público ou privado, comprovando as condições, a qualidade, a presteza e a agilidade dos serviços

que prestou ou vem prestando, pertinentes e compatíveis com o objeto deste Termo de Referência, em características, quantidades e prazos; e,

- c) Relação nominal da equipe técnica da (s) instituição (ões) que apresentou (aram) o (s) atestado (s) de capacidade técnica, contendo nome, endereço, telefone e e-mail para possível agendamento de entrevista.

17. DISPOSIÇÕES GERAIS

- 17.1.** O valor final para o cumprimento do objeto do presente Termo de Referência será definido após a Cotação Prévia de Preços, que será realizada pelo Setor de Licitações e Contratos.
- 17.2.** O Contratante poderá realizar acréscimos ou supressões nas quantidades inicialmente previstas, respeitados os limites do artigo 65 da Lei 8.666/93 e suas alterações, tendo como base os preços constantes da proposta da Contratada.
- 17.3.** O Contratante se reserva o direito de paralisar ou suspender, a qualquer tempo, a execução dos serviços, mediante pagamento único e exclusivo dos trabalhos já executados, por ajuste entre as partes interessadas, dos materiais existentes no local dos serviços, e a ele destinados.

Manaus, 17 de junho de 2019.

Elaborado pelo DAGEPE/COREN-AM.