CONSELHO REGIONAL DE CONTABILIDADE DE MATO GROSSO DO SUL
Rua Euclides da Cunha, 994, - Bairro Jardim dos Estados, @cidade_unidade@/, CEP 79020-230
Telefone: (67) 3326-0750 - www.crcms.org.br

TERMO DE REFERÊNCIA

Processo nº 9079621110000930.000010/2024-63

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Referente a necessidade de contratação de pessoa jurídica para fornecimento de Licenças de Uso de solução de Antivírus (Renovação) para o CRCMS pelo período de 36 meses.

ITEM	DESCRIÇÃO DO ITEM	CATMAT/ CATSERV	UNIDADE	QTDE	PERÍODO/ VIGÊNCIA	VALOR UNIT (PREÇO MÉDIO	VALOR TOTAL DO ITEM (R$)
1	Aquisição/Renovação de licenças de uso de solução de antivírus (Kaspersky Next EDR Optimum).	27502	un	40	36 meses	R$ 484,67	R$ 19.386,80
						Custo estimado total	**R$ 19.386,80**

1.2. Os bens objeto desta contratação são caracterizados como comuns, conforme justificativa constante do Estudo Técnico Preliminar.

1.3. O objeto desta contratação não se enquadra como sendo de bem de luxo, conforme Decreto nº 10.818, de 27 de setembro de 2021.

1.4. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à vigência da contratação.

2. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

2.1. A Fundamentação da Contratação e de seus quantitativos encontra-se pormenorizada em Tópico específico dos Estudos Técnicos Preliminares, apêndice deste Termo de Referência.

2.2. O objeto da contratação está alinhado com os seguintes documentos:

a) Planejamento Estratégico - Resolução CFC n.º 1.543, de 16 de agosto de 2018 - Aprova o Planejamento Estratégico do Sistema CFC/CRCs para 2018/2027, com alinhamento aos objetivos constantes no Plano Estratégico por meio do Objetivo n.º 12 "Ampliar e integrar o uso da Tecnologia da Informação no Sistema CFC/CRCs".

b) Orçamento - Resolução CRCMS n.º 249 de 1 de dezembro de 2023 – Dispõe sobre a Proposta Orçamentária para o Exercício Financeiro de 2024 do CRCMS e dá outras providências.

c) Plano de Trabalho do CRCMS no projeto 5010 Modernização do Parque de Informática (Hardware e Software), que dispõe de recurso orçamentário para despesa na rubrica 6.3.2.1.05.01.002 (Softwares).

d) Plano Anual de Contratação, aprovado por meio da Portaria CRCMS n.º 02, de 12 de janeiro de 2024, que institui prazos para elaboração e execução das contratações no âmbito do CRCMS.

e) Plano Diretor de Tecnologia da Informação, aprovado por meio da Resolução CRCMS nº250, de 1 de dezembro de 2023.

2.3. Justificativa

2.3.1. Visando a segurança dos computadores e servidores do CRCMS e também oferecer maior liberdade de uso da infraestrutura de TI por parte dos usuários da rede, a solução de antivírus garante que a organização não corra riscos de invasões, código malicioso, como vírus, spywares, ransowares, infecções ou descuidos por parte de todos que operam computadores no Conselho.

2.3.2. A solução de antivírus visa a manutenção da integridade, da disponibilidade e da confiabilidade dos dados, essencial para o cumprimento das atividades do CRCMS.

2.3.3. Para atendimento do exposto, será contratada pessoa jurídica para renovação das 40 licenças atuais por mais 36 meses do antivírus Kaspersky Next EDR Optimum. A contratação de outro antivírus ou versão iria descaracterizar o modelo atual de proteção ao qual a infraestrutura já conta com garantias de qualidade e confiança, mantendo o parque homogêneo.

3. DESCRIÇÃO DA SOLUÇÃO

3.1. Analisando as alternativas disponíveis e que atendam à necessidade da área requisitante, considerando a viabilidade técnica e econômica, a solução indicada pela Equipe de Planejamento da Contratação é a realização de procedimento licitatório para aquisição do item, de acordo com especificações comuns de mercado capazes de atender aos requisitos de negócio.

ITEM	Nº UNIDADES /MESES	CATMAT/ CATSERV	ESPECIFICAÇÃO MÍNIMA
			1. DO MÓDULO DE PROTEÇÃO DE ENDPOINT 1.1. A solução proposta deverá proteger os sistemas operacionais abaixo: Windows 7 Windows 8 Windows 8.1

Windows 10

Windows 11

1.2. Servidores

Windows Small Business Server 2011

Windows MultiPoint Server 2011

Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022

1.3. Servidores de terminal Microsoft

Serviços de Área de Trabalho Remota da Microsoft baseados no Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022

1.4. Sistemas operacionais Linux de 32 bits:

CentOS 6.7 e posterior

Debian GNU/Linux 11.0 e posterior

Debian GNU/Linux 12.0 e posterior

Red Hat Enterprise Linux 6.7 e posterior

1.5. Sistemas operacionais Linux de 64 bits:

Amazon Linux 2.

CentOS 6.7 e mais tarde

CentOS 7.2 e posterior.

CentOS Stream 8.

CentOS Stream 9.

Debian GNU/Linux 11.0 e posterior.

Debian GNU/Linux 12.0 e posterior.

Linux Mint 20.3 e superior.

Linux Mint 21.1 e posterior.

openSUSE Leap 15.0 e posterior.

Oracle Linux 7.3 e posterior.

Oracle Linux 8.0 e posterior.

Oracle Linux 9.0 e posterior.

Red Hat Enterprise Linux 6.7 e posterior

Red Hat Enterprise Linux 7.2 e posterior.

Red Hat Enterprise Linux 8.0 e posterior.

Red Hat Enterprise Linux 9.0 e posterior.

Rocky Linux 8.5 e posterior.

Rocky Linux 9.1.

SUSE Linux Enterprise Server 12.5 ou posterior.

SUSE Linux Enterprise Server 15 ou posterior.

Ubuntu 20.04 LTS.

Ubuntu 22.04 LTS.

Sistemas operacionais Arm de 64 bits:

CentOS Stream 9.

SUSE Linux Enterprise Server 15.

Ubuntu 22.04 LTS.

1.6. Sistemas operacionais MAC OS:

MacOS 12 – 14

1.7. Ferramentas de virtualização MAC OS:

Parallels Desktop 16 para Mac Business Edition

VMware Fusion 11.5 Professional

VMware Fusion 12 Professional

1.8. A solução proposta deverá suportar as seguintes plataformas virtuais:

VMware Workstation 17.0.2 Pro

VMware ESXi 8.0 Update 2

Microsoft Hyper-V Server 2019

Citrix Virtual Apps e Desktop 7 2308

Citrix Provisioning 2308

Citrix Hypervisor 8.2 Update 1

2. DO MÓDULO DE GERENCIAMENTO AVANÇADO

2.1. A solução proposta deve suportar arquitetura cloud-native e on-premisse;

2.2. A solução proposta deve incluir suporte para implantação baseada em nuvem por meio de:

Amazon Web Services

Microsoft Azure

2.3. A solução proposta deve incluir as seguintes opções de integração SIEM:

HP (Microfoco) ArcSight

IBM QRadar

Splunk

Kaspersky KUMA

2.4. A solução proposta deve fornecer a capacidade de integração com as soluções Managed Endpoint Detection and Response (MDR) e Anti-APT do próprio fornecedor, para caça ativa a ameaças e resposta automatizada a incidentes.

2.5. A solução proposta deve ter a capacidade de permitir aplicações baseadas em seus certificados de assinatura digital, MD5, SHA256, metadados, caminho do arquivo e categorias de segurança pré-definidas;

2.6. A solução proposta deve suportar Single Sign On (SSO) usando NTLM e Kerberos.

2.7. O administrador deve ser capaz de adicionar manualmente novos dispositivos à lista de equipamentos ou editar informações sobre equipamentos já existentes na rede.

2.8. A solução proposta deve suportar API OPEN e incluir diretrizes para integração com sistemas externos de terceiros.

2.9. A solução proposta deve incluir uma ferramenta integrada para realizar diagnósticos remotos e coletar logs de solução de problemas sem exigir acesso físico ao computador.

2.10. A solução proposta deve incorporar no sensor de endpoint distribuição/retransmissão para transferir ou fazer proxy de solicitações de reputação de ameaças dos terminais para o servidor de gerenciamento.

2.11. A solução proposta deve suportar o download de arquivos diferenciais em vez de pacotes completos de atualização.

2.12. A solução proposta deve incluir Role Based Access Control (RBAC) com funções predefinidas personalizáveis.

2.13. O servidor de gerenciamento primário da solução proposta deve ser capaz de retransmitir atualizações e serviços de reputação em nuvem.

2.14. O servidor de gerenciamento da solução proposta deve ter funcionalidade para criar múltiplos perfis dentro de uma política de proteção com diferentes configurações de proteção que possam estar simultaneamente ativas em uns único/múltiplos dispositivos com base nas seguintes regras de ativação:

Status do dispositivo

Tag

Diretório ativo

Proprietários de dispositivos

Hardware

2.15. A solução proposta deve suportar os seguintes canais de entrega de notificação:

E-mail

Registro de sistema

SMS

2.16. A solução proposta deve ter a capacidade de etiquetar/marcar computadores com base em:

Atributos de rede

Nome

Domínio e/ou Sufixo de Domínio

Endereço de IP

Endereço IP para servidor de gerenciamento

Localização no Active Directory

Unidade organizacional

Grupo

Sistema operacional

Número do pacote de serviço

Arquitetura Virtual

Registro de aplicativos

Nome da Aplicação

Versão do aplicativo

Fabricante

Tipo e versão

Arquitetura

2.17. A solução proposta deve ter a capacidade de criar/definir configurações com base na localização de um computador na rede, e não no grupo ao qual pertence no servidor de gestão.

2.18. A solução proposta deve ter a funcionalidade de adicionar um mediador de conexão unidirecional entre o servidor de gerenciamento e o endpoint conectado pela internet/rede pública.

2.19. As informações sobre o equipamento deverão ser atualizadas após cada nova pesquisa na rede. A lista de equipamentos detectados deve abranger o seguinte:

Dispositivos Desktop/Servidores

Dispositivos móveis

Dispositivos de rede

Dispositivos virtuais

Componentes OEM

Periféricos de computador

Dispositivos IoT conectados

Telefones VoIP

Repositórios de rede

2.20. A solução proposta deve permitir ao administrador criar categorias/grupos de aplicação com base em:

Nome da Aplicação

Caminho do aplicativo

Metadados do aplicativo

Aplicativo Certificado digital

Categorias de aplicativos predefinidas pelo fornecedor

SHA256 e MD5

2.21. A solução proposta deverá permitir especificamente o bloqueio dos seguintes dispositivos:

Bluetooth

Dispositivos móveis

Modems externos

CD/DVD

Câmeras e scanners

MTPs

E a transferência de dados para dispositivos móveis

2.22. A solução proposta deve ter capacidade de ler informações do Active Directory para obter dados sobre contas de computadores na organização.

2.23. A solução proposta deve ter funcionalidade integrada para conectar-se remotamente ao endpoint usando a tecnologia Windows Desktop Sharing. Além disso, a solução deve ser capaz de manter a auditoria das ações do administrador durante a sessão.

2.24. A solução proposta deverá possuir a funcionalidade de criar uma estrutura de grupos de administração utilizando a hierarquia de Grupos, com base nos seguintes dados:

Estruturas de domínios e grupos de trabalho do Windows

Estruturas de grupos do Active Directory

Conteúdo de um arquivo de texto criado manualmente pelo administrador

2.25. A solução proposta deve ser capaz de recuperar informações sobre os equipamentos detectados durante uma pesquisa na rede. O inventário resultante deverá abranger todos os equipamentos conectados à rede da organização.

2.26. A solução proposta deve permitir realizar as seguintes ações para endpoints:

Verificação manual;

Verificação no acesso;

Verificação por demanda;

Verificação de arquivos compactados

Verificação de arquivos individuais, pastas e unidades;

Bloqueio e verificação de scripts

Proteção contra alteração de registros;

Proteção contra estouro de buffer;

Verificação em segundo plano/inativa

2.27. Verificação de unidade removível na conexão com o sistema;

2.28. A solução proposta deve suportar a instalação do sensor de endpoint juntamente com soluções de terceiros, seja utilizando somente o módulo de EDR ou anti-malware.

2.29. O servidor de gerenciamento da solução proposta deve manter um histórico de revisões das políticas, tarefas, pacotes, grupos de gerenciamento criados, para que modificações em uma determinada política/tarefa possam ser revisadas.

2.30. A solução proposta deve ter a capacidade de definir um

			intervalo de endereços IP, de forma a limitar o tráfego do cliente para o servidor de gestão com base no tempo e na velocidade. 2.31. A solução proposta deve ter a capacidade de realizar inventário em scripts e arquivos, tais como: dll, exe, bat e etc. 2.32. A solução proposta deve prever a criação de uma cópia de segurança do sistema de administração com o auxílio de ferramentas integradas do sistema de administração. 2.33. A solução proposta deve suportar Windows Failover Cluster. 2.34. A solução proposta deve ter um recurso de clustering integrado. 2.35. A solução proposta deve incluir alguma forma de sistema para controlar epidemias de vírus. 2.36. A solução proposta deve incluir Role Based Access Control (RBAC), e isso deve permitir que as restrições sejam replicadas em todos os servidores de gerenciamento na hierarquia. 2.37. O servidor de gestão da solução proposta deverá incluir funções de segurança pré-definidas para o Auditor, Supervisor e Oficial de Segurança. 2.38. A solução proposta deve permitir ao administrador criar um túnel de conexão entre um dispositivo cliente remoto e o servidor de gerenciamento caso a porta usada para conexão ao servidor de gerenciamento não esteja disponível no dispositivo. 2.39. A solução proposta deve ter a capacidade de priorizar rotinas de varredura personalizadas e sob demanda para estações de trabalho Linux. 2.40. A solução proposta deve ser capaz de registrar operações de arquivos (Escrita e Exclusão) em dispositivos de armazenamento USB. 2.41. A solução proposta deve ter capacidade de bloquear a execução de qualquer executável do dispositivo de armazenamento USB. 2.42. A solução proposta deve contar com filtragem de firewall por endereço local, interface física e Time-To-Live (TTL) de pacotes. 2.43. A solução proposta deverá possuir controles para download de DLL e drivers. 2.44. A solução proposta deve ter a capacidade de restringir as atividades do aplicativo dentro do sistema de acordo com o nível de confiança atribuído ao aplicativo e de limitar os direitos dos aplicativos de acessar determinados recursos, incluindo arquivos do sistema e do usuário utilizando de módulo especifico de prevenção de intrusão. 2.45. A solução proposta deve ter a capacidade de excluir automaticamente as regras de controle de aplicativos se um aplicativo não for iniciado durante um intervalo especificado. O intervalo deve ser configurável. 2.46. A solução proposta deve incluir múltiplas formas de

			notificar o administrador sobre eventos importantes que ocorreram (notificação por e-mail, anúncio sonoro, janela pop-up, entrada de log). 2.47. A solução proposta deve incluir Controle de inicialização de aplicativos para o sistema operacional Windows Server. 2.48. A solução proposta deve distribuir automaticamente as contas de computador por grupo de gerenciamento caso novos computadores apareçam na rede. Deve fornecer a capacidade de definir as regras de transferência de acordo com o endereço IP, tipo de sistema operacional e localização nas Unidades Organizacionais do Active Directory. 2.49. A solução proposta deve permitir o teste de atualizações baixadas por meio do software de administração centralizado antes de distribuí-las às máquinas dos clientes e a entrega das atualizações aos locais de trabalho dos usuários imediatamente após recebê-las. 2.50. A solução proposta deve permitir a criação de uma hierarquia de servidores de administração a um nível arbitrário e a capacidade de gerir centralmente toda a hierarquia a partir do nível superior. 2.51. A solução proposta deve suportar o Modo de Serviços Gerenciados para servidores de administração, para que instâncias de servidores de administração isoladas logicamente possam ser configuradas para diferentes usuários e grupos de usuários. 2.52. A solução proposta deve dar acesso aos serviços em nuvem do fornecedor de segurança anti-malware através do servidor de administração. 2.53. A solução proposta deve ser capaz de realizar inventários de software e hardware instalados nos computadores dos usuários. 2.54. A solução proposta deve ter um mecanismo de notificação para informar os usuários sobre eventos no software e nas configurações anti-malware instalados, e para distribuir notificações sobre eventos por e-mail. 2.55. A solução proposta deve permitir a instalação centralizada de aplicativos de terceiros em todos ou em computadores selecionados. 2.56. A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de retransmissão de atualizações e pacotes de instalação, a fim de reduzir a carga da rede no sistema principal do servidor de administração. 2.57. A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de encaminhamento de eventos do sensor de endpoint do grupo selecionado de computadores clientes para o servidor de administração centralizado, a fim de reduzir a carga da rede no sistema do servidor de administração principal. .

2.58. A solução proposta deve ser capaz de gerar relatórios gráficos para eventos de software anti-malware e dados sobre inventário de hardware e software, licenciamento, etc.

2.59. A solução proposta deve permitir que o administrador defina configurações restritas nas configurações de política/perfil, para que uma tarefa de verificação de vírus possa ser acionada automaticamente quando um determinado número de vírus for detectado durante um período de tempo definido. Os valores para o número de vírus e escala de tempo devem ser configuráveis.

2.60. A solução proposta deve permitir ao administrador personalizar relatórios.

2.61. A solução proposta deve ter a funcionalidade de detectar máquinas virtuais não persistentes e excluí-las automaticamente e seus dados relacionados do servidor de gerenciamento quando desligado.

2.62. A solução proposta deve permitir ao administrador definir um período de tempo após o qual um computador não conectado ao servidor de gerenciamento e seus dados relacionados serão automaticamente excluídos do servidor.

2.63. A solução proposta deve permitir ao administrador definir diferentes condições de mudança de status para grupos de endpoint no servidor de gerenciamento.

2.64. A solução proposta deve permitir que o administrador adicione ferramentas de gerenciamento de endpoint personalizadas/de terceiros ao servidor de gerenciamento.

2.65. A solução proposta deve ter um recurso/módulo integrado para coletar remotamente os dados necessários para solução de problemas dos endpoint, sem exigir acesso físico.

2.66. A funcionalidade 'Dispositivo desativado' deve estar disponível, para que tais dispositivos não sejam exibidos na lista de equipamentos.

2.67. O relatório da solução proposta deve incluir detalhes sobre quais componentes de proteção de endpoint estão ou não instalados em dispositivos clientes, independentemente do perfil de proteção aplicado/existente para esses dispositivos;

2.68. O servidor de gerenciamento primário da solução proposta deve ser capaz de recuperar relatórios de informações detalhadas sobre o status de integridade, etc., dos terminais gerenciados dos servidores de gerenciamento secundários.

2.69. A solução proposta deve suportar integração com solução APT.

2.70. A solução proposta deve suportar a integração com o serviço Managed Detection and Response.

2.71. A solução proposta deve permitir instalar o modulo de gerenciamento on-premisse nos seguintes sistemas operacionais:

Windows

Linux

2.72. A solução proposta deverá suportar os seguintes servidores de banco de dados:

Windows:

Microsoft SQL Server

Microsoft Banco de dados SQL do Azure

MySQL Standard e Enterprise

MariaDB

PostgreSQL

Linux:

MySQL

MariaDB

PostgreSQL

2.73. A solução proposta deverá suportar as seguintes plataformas virtuais:

Windows:

VMware vSphere 6.7 e 7.0

Estação de trabalho VMware 16 Pro

Servidor Microsoft Hyper-V 2012 de 64 bits

Servidor Microsoft Hyper-V 2012 R2 de 64 bits

Microsoft Servidor Hyper -V 2016 de 64 bits

Servidor Microsoft Hyper-V 2019 de 64 bits

Servidor Microsoft Hyper-V 2022 de 64 bits

Citrix XenServer 7.1 LTSR

Citrix XenServer 8.x

Oracle VM VirtualBox 6.x

Linux:

VMware vSphere 6.7, 7.0 e 8.0

VMware Desktop 16 Pro e 17 Pro

Servidor Microsoft Hyper-V 2012 de 64 bits

Servidor Microsoft Hyper-V 2012 R2 de 64 bits

Microsoft Servidor Hyper -V 2016 de 64 bits

Servidor Microsoft Hyper-V 2019 de 64 bits

Servidor Microsoft Hyper-V 2022 de 64 bits

Citrix XenServer 7.1 e 8.x

Oracle VM VirtualBox 6.x e7.x

2.74. A solução proposta deve suportar criptografia em vários níveis:

Criptografia completa do disco – incluindo disco do sistema

Criptografia de arquivos e pastas

Criptografia de mídia removível

Gerenciamento de criptografia BitLocker e MacOS Filevault2

2.75. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita:

A criptografia de arquivos em unidades de computador locais.

A criação de listas de criptografia de arquivos por extensão ou grupo de extensões.

A criação de listas criptografadas de pastas em unidades de computador locais.

2.76. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita a criptografia de arquivos em unidades removíveis. Isto deve incluir a capacidade de:

Especifique uma regra de criptografia padrão pela qual o aplicativo aplique a mesma ação a todas as unidades removíveis.

Configure regras de criptografia para arquivos armazenados em unidades removíveis individuais.

2.77. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que suporte vários modos de criptografia de arquivos para unidades removíveis:

A criptografia de todos os arquivos armazenados em unidades removíveis.

A criptografia de novos arquivos somente quando eles são salvos ou criados em unidades removíveis.

2.78. A solução proposta deve oferecer a funcionalidade Integrated File Level Encryption (FLE) que permite que os arquivos em unidades removíveis sejam criptografados em modo portátil. Deve permitir o acesso a arquivos criptografados em unidades removíveis conectadas a computadores sem funcionalidade de criptografia

2.79. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita a criptografia de todos os arquivos que aplicativos específicos possam criar ou modificar, tanto em discos rígidos quanto em unidades removíveis.

2.80. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita o gerenciamento de regras de acesso de aplicativos a arquivos criptografados, incluindo a definição de uma regra de acesso a arquivos criptografados para qualquer aplicativo. Deve permitir o bloqueio do acesso a arquivos criptografados ou permitir o acesso a arquivos criptografados apenas como texto cifrado.

2.81. A solução proposta deve oferecer a capacidade de

			restaurar dispositivos criptografados se um disco rígido ou unidade removível criptografado estiver corrompido. 2.82. A solução proposta deve oferecer a funcionalidade Integrated Full Disk Encryption (FDE) para discos rígidos e unidades removíveis. Tal como acontece com o FLE, deve haver a capacidade de especificar uma regra de criptografia padrão pela qual o aplicativo aplica a mesma ação a todas as unidades removíveis ou de configurar regras de criptografia para unidades removíveis individuais. 2.83. A solução proposta deve oferecer um módulo de criptografia gerenciado centralmente em todos os computadores, com capacidade de impor políticas de criptografia e modificar/interromper configurações de criptografia. 2.84. A solução proposta deve oferecer a capacidade de monitorar centralmente o status da criptografia e gerar relatórios sobre computadores/dispositivos criptografados. 2.85. A solução proposta deve oferecer criptografia totalmente transparente para os usuários finais e que não tenha impacto adverso no desempenho e na utilização do sistema. 2.86. A solução proposta deve oferecer criptografia completa de disco que suporte o gerenciamento centralizado de usuários autorizados, incluindo adição, remoção e redefinição de senha. Somente usuários autorizados devem ter permissão para inicializar o disco criptografado. 2.87. A solução proposta deve ter a capacidade de bloquear o acesso de aplicativos a dados criptografados, se necessário. 2.88. A solução proposta deverá suportar a encriptação automática de dispositivos de armazenamento amovíveis e deverá ser capaz de impedir a cópia de dados para suportes não encriptados. 2.89. A solução proposta deve proporcionar a possibilidade de criação de contentores protegidos por palavra-passe que possam ser utilizados para o intercâmbio de dados com utilizadores externos. 2.90. A solução proposta deve fornecer um local central para armazenamento de chaves de criptografia e múltiplas opções de recuperação. 2.91. O servidor administrador/gerenciador da solução proposta deve ter a capacidade de descriptografar todos os dados criptografados. independentemente da localização e/ou usuário. 2.92. A solução proposta deve suportar layouts de teclado QWERTY e AZERTY para autorização de pré-inicialização. 2.93. A solução proposta deve fornecer a funcionalidade para gerenciar/aplicar a criptografia do Microsoft Bit Locker. 2.94. A solução proposta deve fornecer a funcionalidade para personalizar as configurações de criptografia do Microsoft BitLocker, incluindo:

Uso do Trusted Platform Module e configurações de senha.

Uso de criptografia de hardware para estações de trabalho e criptografia de software se a criptografia de hardware não estiver disponível.

2.95. Uso de autenticação que exige entrada de dados em um ambiente de pré-inicialização, mesmo que a plataforma não tenha capacidade para entrada de pré-inicialização (por exemplo, com teclados touchscreen em tablets).

2.96. A solução proposta deve suportar criptografia em Microsoft Surface Tablets.

2.97. A solução proposta deverá incluir recursos para gerenciar computadores remotamente, incluindo:

Instalação remota de software de terceiros

Relatórios sobre software e hardware existentes

Monitoramento para instalação de software não autorizado

Remoção de software não autorizado

2.98. A solução proposta deverá incluir recursos de gerenciamento de patches para sistemas operacionais Windows e para aplicativos de terceiros instalados.

2.99. A funcionalidade de gerenciamento de patches da solução proposta deve ser totalmente automatizada, com capacidade de detectar, baixar e enviar patches ausentes para endpoints.

2.100. A solução proposta deve fornecer a possibilidade de selecionar quais patches serão baixados/enviados para os endpoints, com base em sua criticidade.

2.101. A solução proposta deve ser capaz de detectar vulnerabilidades existentes em sistemas operacionais e outros aplicativos instalados e, em seguida, responder baixando/enviando automaticamente os patches necessários para os terminais.

2.102. A solução proposta deve fornecer relatórios abrangentes sobre vulnerabilidades descobertas e patches ausentes, bem como sobre endpoints e status de implantação de patches.

2.103. A solução proposta deve ter a capacidade de aplicar patches específicos com base na criticidade ou gravidade.

2.104. O servidor de gerenciamento da solução proposta deve ser configurável como uma fonte de atualizações para Microsoft Updates e aplicativos de terceiros.

2.105. A solução proposta deve incluir o aconselhamento sobre vulnerabilidade do fornecedor de aplicativos, bem como do fornecedor de segurança

2.106. A solução proposta deve permitir ao administrador aprovar atualizações.

2.107. A solução proposta deve ser capaz de identificar automaticamente patches ausentes em endpoints individuais e

			enviar apenas os que são necessários/ausentes. 2.108. A solução proposta deve suportar a agregação de patches para minimizar o número de atualizações necessárias. 2.109. A solução proposta deve notificar o administrador sobre quaisquer patches ausentes nos terminais assim que as informações relevantes estiverem disponíveis. 2.110. A solução proposta deverá proporcionar a possibilidade de gerir separadamente a aplicação de patches para sistemas operativos e para aplicações de terceiros. 2.111. A solução proposta deverá proporcionar a possibilidade de corrigir vulnerabilidades existentes em qualquer ponto final ou apenas em pontos específicos. 2.112. A solução proposta deve fornecer a facilidade de detectar/instalar automaticamente todos os patches perdidos anteriormente que são necessários para aplicar o patch selecionado (dependências). 2.113. A solução proposta deve suportar a distribuição automatizada de patches e atualizações para mais de 150 aplicações. 2.114. A solução proposta deve ter funcionalidade de suporte ao modo de teste de patch. 2.115. A solução proposta deve incluir campos dedicados que contenham informações sobre 'Exploração encontrada para a vulnerabilidade'. 2.116. A solução proposta deve incluir campos dedicados que contenham informações sobre "Ameaça encontrada para a vulnerabilidade". 2.117. A solução proposta deve permitir que o administrador restrinja a capacidade dos usuários do dispositivo de aplicar eles próprios as atualizações da Microsoft. 2.118. A solução proposta deve permitir ao administrador especificar quais atualizações podem ser instaladas pelos usuários. 2.119. A solução proposta deve permitir ao administrador visualizar uma lista de atualizações e patches não relacionados aos dispositivos clientes. 2.120. A solução proposta deve apoiar a implantação do sistema operacional. 2.121. A solução proposta deve suportar Wake-on LAN e UEFI. 2.122. A solução proposta deve ter funcionalidade integrada de compartilhamento remoto de área de trabalho. Todas as operações de arquivo executadas no endpoint remoto durante a sessão devem ser registradas no Management Server. 2.123. A solução proposta deve ser capaz de fornecer correções de vulnerabilidades aos computadores clientes sem instalar as atualizações. 2.124. A solução proposta deve permitir que o administrador

escolha as atualizações do Windows a serem instaladas, após o que o usuário do dispositivo cliente poderá instalar apenas as atualizações permitidas/selecionadas pelo administrador.

2.125. A solução proposta deve informar o administrador sobre atualizações e patches não relacionados no dispositivo cliente.

2.126. A solução proposta deve ser configurável/atribuível como fonte de atualização para atualizações da Microsoft e de terceiros.

2.127. A solução proposta deve permitir ao administrador selecionar o produto Microsoft e os idiomas para os quais as atualizações serão baixadas.

2.128. A solução proposta deve ser capaz de enviar/implantar remotamente arquivos EXE, MSI, bat, cmd, MSP e permitir que o administrador defina o parâmetro de linha de comando para a instalação remota.

2.129. A solução proposta deve ser capaz de desinstalar aplicativos remotamente, não se limitando a programas antivírus incompatíveis.

2.130. A solução proposta deve permitir ao administrador utilizar uma única tarefa/trabalho e definir diferentes regras ou critérios de correção de vulnerabilidades para atualizações de aplicações da Microsoft e de terceiros.

2.131. A solução proposta deve permitir que o administrador configure regras para instalação de patches/atualizações da Microsoft e de terceiros:

Inicie a instalação ao reiniciar ou desligar o computador.

Instale o gerador necessário todos os pré-requisitos do sistema.

Permitir a instalação de novas versões de aplicativos durante as atualizações.

Baixe atualizações para o dispositivo sem instalá-las.

2.132. A solução proposta deve ter a capacidade de testar a instalação de atualizações em uma porcentagem de computadores antes de aplicá-la a todos os computadores de destino. O administrador deve ser capaz de configurar o número de computadores de teste como uma porcentagem e o tempo alocado antes da implementação completa em termos de horas.

2.133. A solução proposta deve permitir a remoção/desinstalação de atualizações específicas de aplicativos e sistemas operacionais.

2.134. O servidor de gerenciamento da solução proposta deve ser capaz de enviar logs para servidores SIEMs e SYSLOG nos seguintes formatos:

CEF;

LEEF;

2.135. A solução proposta deve ser capaz de rastrear licenças de aplicações de terceiros e gerar notificações de quaisquer violações potenciais.

			2.136. O relatório da solução proposta deve conter informações CVE. 2.137. A solução proposta deve suportar instalação de aplicações e software de terceiros; **3. DO MÓDULO DE GERENCIAMENTO SIMPLIFICADO** 3.1. A solução proposta deve suportar arquitetura cloud; 3.2. A solução proposta deve incluir um console web integrado para o gerenciamento dos endpoint, que não deve exigir nenhuma instalação adicional. 3.3. O console de gerenciamento web da solução proposta deve ser simples de usar e deve suportar dispositivos com tela sensível ao toque. 3.4. A solução proposta deve permitir ao administrador gerar relatórios pré-definidos. 3.5. A solução proposta deve suportar a descoberta de uso por parte do usuário de aplicações e exibir informações detalhadas de uso de aplicações utilizadas por meios de navegadores e aplicações instaladas no endpoint. 3.6. A solução proposta deve atender as condições apontadas no item e subintes 6. 3.7. A solução proposta deve suportar sistemas operacionais Windows, Mac, Android e iOS. 3.8. A solução proposta deve incluir informações do endpoint: IP público de internet; IP interno do dispositivo; Versão do agente de proteção; Última comunicação com a console, contendo data e hora; Informações do sistema operacional; 3.9. A solução proposta deve permitir proteger as caixas de correio do Exchange Online, os utilizadores do OneDrive e os sites do SharePoint Online geridos através do Office 365. 3.10. A solução proposta deve permitir detectar informações críticas em arquivos localizados nos armazenamentos em nuvem do Office 365. 3.11. A solução proposta deve incluir treinamento em segurança cibernética. **4. REQUISITOS GERAIS** 4.1. A solução proposta deve ser capaz de detectar os seguintes tipos de ameaças:
1	36	27502	Malwares, Worms, Trojans, Backdoors, Rootkits, Spyware, Adware, Ransomware, Keyloggers, Crimeware, sites e links de phishing, vulnerabilidades do tipo ZeroDay e outros softwares maliciosos e indesejados.

4.2. A solução proposta deve ser de um único fornecedor e suportar todos módulos descritos neste termo de referência.

4.3. A solução proposta deve suportar integração com Anti-malware Scan Interface (AMSI).

4.4. A solução proposta deve ter capacidade de integração com a central de segurança do Windows Defender.

4.5. A solução proposta deve suportar o subsistema Linux no Windows.

4.6. A solução proposta deve fornecer tecnologias de proteção da próxima geração. Sendo no mínimo:

Proteção contra ameaças sem arquivos (Fileless);

Fornecimento de proteção baseada em machine leaning em várias camadas e análise comportamental durante diferentes estágios da cadeia de ataque;

4.7. A solução proposta deve fornecer varredura de memória para estações de trabalho Windows;

4.8. A solução proposta deve fornecer varredura de memória do kernel para estações de trabalho Linux.

4.9. A solução proposta deve fornecer a capacidade de alternar para o modo nuvem para proteção contra ameaças, diminuindo o uso de RAM e disco rígido em máquinas com recursos limitados.

4.10. A solução proposta deve ter componentes dedicados para monitorar, detectar e bloquear atividades em endpoint: Windows, Linux e Mac. Servidores: Windows e Linux, para proteção contra ataques remotos de criptografia.

4.11. A solução proposta deve incluir componentes sem assinatura para detectar ameaças mesmo sem atualizações frequentes. A proteção deve ser alimentada por machine learning estático para pré-execução e machine learning dinâmico para estágios pós-execução da cadeia de eliminação em endpoints e na nuvem para servidores e estações de trabalho Windows.

4.12. A solução proposta deve fornecer análise comportamental baseada em machine learning.

4.13. A solução proposta deve incluir a capacidade de configurar e gerenciar configurações de firewall integradas aos sistemas operacionais Windows Server e Linux, através de seu console de gerenciamento.

4.14. A solução proposta deve incluir os seguintes componentes no sensor instalado no endpoint:

Controles de aplicativos,

Controle web e dispositivos

HIPS e Firewall

Descoberta de patches e vulnerabilidades de sistemas operacionais Windows;

Gerenciamento de criptografia de arquivos e discos;

Controle adaptativo para detecção de anomalias;

4.15. A capacidade de detectar e bloquear hosts não confiáveis na detecção de atividades semelhantes à criptografia em recursos compartilhados do servidor.

4.16. A solução proposta deve ser protegida por senha para evitar que o processo do anti-malware seja interrompido sendo a autoproteção, independentemente do nível de autorização do usuário no sistema.

4.17. A solução proposta deve ter bancos de dados de reputação locais e globais.

4.18. A solução proposta deve ser capaz de verificar o tráfego HTTPS, HTTP, SMTP e FTP contra malwares.

4.19. A solução proposta deve incluir um módulo capaz, no mínimo, de:

Bloqueio de aplicativos com base em sua categorização.

Bloqueio/permissão de pacotes, protocolos, endereços IP, portas e direção de tráfego específicos.

A adição de sub-redes e a modificação de permissões de atividade.

4.20. A solução proposta deve impedir a conexão de dispositivos USB reprogramados emulando teclados e permitir o controle do uso de teclados na tela mediante autorização.

4.21. A solução proposta deve ser capaz de bloquear ataques à rede e reportar a origem da infecção.

4.22. A solução proposta deve ter armazenamento local nos endpoint para manter cópias dos arquivos que foram excluídos ou modificados durante a desinfecção. Esses arquivos devem ser armazenados em um formato específico que garanta que não representem qualquer ameaça.

4.23. A solução proposta deve incluir limpeza remota dos dispositivos com as seguintes funcionalidades:

Modo silencioso;

Discos rígidos e dispositivos removíveis;

De todos as contas de usuários do dispositivo.

4.24. A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes modos:

Exclusão imediata de dados;

Exclusão de dados adiada.

4.25. A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes métodos de exclusão de dados:

Excluir usando os recursos do sistema operacional - os arquivos são excluídos;

Excluir completamente, sem recuperação - tornando

praticamente impossível restaurar os dados após a exclusão.

4.26. A solução proposta deve ter uma abordagem proativa para impedir que malware explore vulnerabilidades existentes em servidores e estações de trabalho.

4.27. A solução proposta deve suportar a tecnologia AM-PPL (Anti-Malware Protected Process Light) para proteção contra ações maliciosas.

4.28. A solução proposta deve incluir proteção contra ataques que explorem vulnerabilidades no protocolo ARP para falsificar o endereço MAC do dispositivo.

4.29. A solução proposta deve incluir um componente de controle capaz de aprender a reconhecer o comportamento típico do usuário em um indivíduo ou grupo específico de computadores protegidos e, em seguida, identificar e bloquear ações anômalas e potencialmente prejudiciais realizadas por esse terminal ou usuário.

4.30. A solução proposta deve fornecer funcionalidade Anti-Bridging para estações de trabalho Windows para evitar pontes não autorizadas para a rede interna que contornem as ferramentas de proteção de perímetro. Os administradores devem ser capazes de proibir o estabelecimento simultâneo de conexões com fio, Wi-Fi e modem.

4.31. A solução proposta deve incluir um componente dedicado para verificação de conexões criptografadas.

4.32. A solução proposta deve ser capaz de descriptografar e verificar o tráfego de rede transmitido por conexões criptografadas.

4.33. A solução proposta deve ter a capacidade de excluir automaticamente recursos da web quando ocorre um erro de verificação durante a execução de uma verificação de conexão criptografada. Esta exclusão deve ser exclusiva do host e não deve ser compartilhada com outros endpoint;

4.34. A solução proposta deve incluir funcionalidade para apagar dados remotamente das estações de trabalho;

4.35. A solução proposta deve incluir funcionalidade para excluir automaticamente os dados caso não haja conexão com o servidor de gerenciamento de endpoint.

4.36. A solução proposta deve suportar detecção baseadas em multicamadas sendo no mínimo: Assinatura, heurística, machine learning ou assistida por nuvem.

4.37. A solução proposta deve ter a capacidade de gerar um alerta, limpar e excluir uma ameaça detectada.

4.38. A solução proposta deve ser capaz de monitorar e bloquear ações que não são típicas dos computadores da rede de uma empresa.

4.39. A solução proposta deve ter a capacidade de acelerar as verificações ignorando os objetos que não foram alterados

			desde a verificação anterior. 4.40. A solução proposta deve permitir que o administrador exclua arquivos/pastas/aplicativos/certificados digitais específicos da verificação, seja no acesso (proteção em tempo real) ou durante verificações sob demanda. 4.41. A solução proposta deve verificar automaticamente as unidades removíveis em busca de malware quando elas estiverem conectadas a qualquer endpoint. 4.42. A solução proposta deve ser capaz de bloquear o uso de dispositivos de armazenamento USB ou permitir o acesso apenas aos dispositivos permitidos. 4.43. A solução proposta deve ser capaz de diferenciar dispositivos de armazenamento USB, impressoras, celulares e outros periféricos. 4.44. A solução proposta deve ter a capacidade de bloquear/permitir o acesso do usuário aos recursos da web com base nos sites e tipo de conteúdo. 4.45. A solução proposta deve ter categoria de detecção para bloquear banners de sites. 4.46. A solução proposta deve fornecer a capacidade de configurar redes Wi-Fi com base no nome da rede, tipo de autenticação e tipo de criptografia em dispositivos móveis; 4.47. A solução proposta deve suportar políticas baseadas no usuário para controle de dispositivos, web e aplicativos. 4.48. A solução proposta deve apresentar integração na nuvem, para fornecer atualizações mais rápidas possíveis sobre malware e ameaças potenciais. 4.49. A solução proposta deve ter capacidade de gerenciar direitos de acesso de usuários para operações de leitura e gravação em CDs/DVDs, dispositivos de armazenamento removíveis e dispositivos MTP. 4.50. A solução proposta deve permitir que o administrador monitore o uso de portas personalizadas/aleatórias pelo aplicativo; 4.51. A solução proposta deve suportar o bloqueio de aplicativos proibidos (lista de negações) de serem lançados no endpoint e o bloqueio de todos os aplicativos que não sejam aqueles incluídos nas listas de permissões. 4.52. A solução proposta deve ter um componente de controle de aplicativos integrado à nuvem para acesso imediato às atualizações mais recentes sobre classificações e categorias de aplicativos. 4.53. A solução proposta deve incluir filtragem de malware de tráfego, verificação de links da web e controle de recursos da web com base em categorias de nuvem. 4.54. O componente de controle web da solução proposta deve incluir uma categoria criptomoedas e mineração. 4.55. O componente de controle de aplicações da solução

proposta deve incluir os modos operacionais lista de negações e lista de permissões.

4.56. A solução proposta deve suportar o controle de scripts executados em PowerShell.

4.57. A solução proposta deve suportar modo teste com geração de relatórios sobre execução de aplicativos bloqueados.

4.58. A solução proposta deve ter a capacidade de controlar o acesso do sistema/aplicativo do usuário a dispositivos de gravação de áudio e vídeo.

4.59. A solução proposta deve fornecer um recurso para verificar os aplicativos listados em cada categoria baseada em nuvem.

4.60. A solução proposta deve ter capacidade de integração com um sistema avançado de proteção contra ameaças específico do fornecedor.

4.61. A solução proposta deve ter a capacidade de regular automaticamente a atividade dos programas em execução, incluindo o acesso ao sistema de arquivos e ao registro, bem como a interação com outros programas.

4.62. A solução proposta deve ter a capacidade de categorizar automaticamente os aplicativos iniciados antes da instalação da proteção de endpoint.

4.63. A solução proposta deve ter proteção contra ameaças de e-mail de endpoint com:

Filtro de anexos.

Verificação de mensagens de e-mail ao receber, ler e enviar.

4.64. A solução proposta deve ter a capacidade de verificar vários redirecionamentos, URLs encurtados, URLs sequestrados e atrasos baseados em tempo.

4.65. A solução proposta deve permitir que o usuário do computador verifique a reputação de um arquivo;

4.66. A solução proposta deve incluir a verificação de todos os scripts, incluindo quaisquer scripts WSH (JavaScript, Visual Basic Script Scripts WSH (JavaScript, Visual Basic Script etc.);

4.67. A solução proposta deve fornecer proteção contra malware ainda desconhecido com base na análise do seu comportamento e verificação de alterações no registo do sistema, juntamente com mecanismo de remediação para restaurar automaticamente quaisquer alterações no sistema feitas pelo malware.

4.68. A solução proposta deve fornecer proteção contra ataques de hackers por meio de um firewall com sistema de prevenção de intrusões e regras de atividade de rede para aplicações mais populares ao trabalhar em redes de computadores de qualquer tipo, incluindo redes sem fio.

4.69. A solução proposta deve incluir suporte ao protocolo IPv6.

4.70. A solução proposta deve oferecer a verificação de seções

críticas do computador como uma tarefa independente.

4.71. A solução proposta deve incorporar a tecnologia de autoproteção de aplicação:

4.72. Protegendo contra o gerenciamento remoto não autorizado de um serviço de aplicativo.

4.73. Protegendo o acesso aos parâmetros do aplicativo definindo uma senha. Evitando a desativação da proteção por malware, criminosos ou usuários.

4.74. A solução proposta deve oferecer a capacidade de escolher quais componentes de proteção contra ameaças instalar.

4.75. A solução proposta deve incluir a verificação anti-malware e desinfecção de arquivos em arquivos nos formatos RAR, ARJ, ZIP, CAB, LHA, JAR, ICE, incluindo arquivos protegidos por senha.

4.76. A solução proposta deve proteger contra malware ainda desconhecido pertencente a famílias cadastradas, com base em análise heurística.

4.77. A solução proposta deve notificar o administrador sobre eventos importantes que ocorreram através de notificação por e-mail.

4.78. A solução proposta deve permitir ao administrador criar um único pacote de instalação do sensor de proteção com a configuração necessária.

4.79. A solução proposta deve fornecer controles de aplicativos e dispositivos para estações de trabalho Windows.

4.80. A proteção da solução proposta para servidores e estações de trabalho deve incluir um componente dedicado para proteção contra atividades de ransomware/malwares que criptografa os recursos compartilhados.

4.81. A solução proposta deve, ao detectar atividades semelhantes a ransomware/criptografia , bloquear automaticamente o computador atacante por um intervalo especificado e listar informações sobre o IP e carimbo de data/hora do computador atacante e o tipo de ameaça.

4.82. A solução proposta deve fornecer uma lista predefinida de exclusões de verificação para aplicativos e serviços Microsoft.

4.83. A solução proposta deve suportar a instalação de proteção de endpoint em servidores sem a necessidade de reinicialização.

4.84. A solução proposta deve permitir a instalação de software com funcionalidades de anti-malware e detecção e resposta de incidente a partir de um único pacote de distribuição.

4.85. A solução proposta deve suportar endereços IPv6.

4.86. A solução proposta deve suportar verificação em duas etapas (autenticação).

4.87. A solução proposta deve prever a instalação, atualização e remoção centralizada de software antimalware, juntamente com configuração, administração centralizada e visualização de relatórios e informações estatísticas sobre o seu funcionamento.

			4.88. A solução proposta deverá contar com a remoção centralizada (manual e automática) de aplicações incompatíveis do centro de administração. 4.89. A solução proposta deve fornecer métodos flexíveis para instalação do sensor de endpoint via: RPC, GPO e um agente de administração para instalação remota e a opção de criar um pacote de instalação independente para instalação do endpoint de segurança localmente. 4.90. A solução proposta deve permitir a instalação remota do sensor de endpoint com os bancos de dados anti-malware mais recentes. 4.91. A solução proposta deve permitir a atualização automática do sensor de endpoint e de bases de dados de anti-malware. 4.92. A solução proposta deve contar com recursos de busca automática de vulnerabilidades em aplicações e no sistema operacional em máquinas protegidas. 4.93. A solução proposta deve permitir a gestão de um componente que proíba a instalação e/ou execução de programas. 4.94. A solução proposta deve permitir a gestão de um componente que controla o trabalho com dispositivos de E/S externos. 4.95. A solução proposta deve permitir o gerenciamento de componente que controle a atividade do usuário na internet. 4.96. A solução proposta deve ser capaz de implantar automaticamente proteção para infraestruturas virtuais baseadas em VMware ESXi , Microsoft Hyper-V, plataforma de virtualização Citrix XenServer ou hipervisor. 4.97. A solução proposta deve incluir a distribuição automática de licenças nos computadores clientes. 4.98. A solução proposta deverá ser capaz de exportar relatórios para arquivos PDF, CSV ou XLS. 4.99. A solução proposta deve proporcionar a administração centralizada de armazenamentos de backup e quarentena em todos os recursos da rede onde o sensor de endpoint está instalado. 4.100. A solução proposta deve prever a criação de contas internas para autenticar administradores no servidor de administração. 4.101. A solução proposta deverá ter capacidade de gerenciar dispositivos móveis através de comandos remotos. 4.102. A solução proposta deve ter a capacidade de excluir atualizações baixadas. 4.103. A solução proposta deve mostrar claramente informações sobre a distribuição de vulnerabilidades entre computadores gerenciados. 4.104. A interface do servidor de gerenciamento da solução proposta deverá suportar o idioma Inglês e português.

4.105. A solução proposta deve ter um painel customizável gerando e exibindo estatísticas em tempo real dos sensores de endpoints.

4.106. A solução proposta deve incorporar funcionalidade de distribuição/retransmissão para suportar a entrega de proteção, atualizações, patches e pacotes de instalação para locais e remotos.

4.107. Os relatórios da solução proposta devem incluir informações sobre cada ameaça e a tecnologia que a detectou.

4.108. A solução proposta deve incluir a opção para implantar uma console de gerenciamento local ou usar o console de gerenciamento baseado em nuvem fornecido pelo fornecedor.

4.109. A solução proposta deve ser capaz de se integrar ao console de gerenciamento baseado em nuvem do fornecedor para gerenciamento de endpoint sem custo adicional.

4.110. A solução proposta deve permitir a migração rápida do console de gerenciamento local para o console de gerenciamento baseado em nuvem do fornecedor.

4.111. A solução proposta deve fornecer mecanismos de atualização de banco de dados, incluindo:

Múltiplas formas de atualização, incluindo canais de comunicação globais através do protocolo HTTPS, recursos compartilhados em rede local e mídia removível.

Verificação da integridade e autenticidade das atualizações por meio de assinatura digital eletrônica.

4.112. A solução proposta deve permitir monitorar vulnerabilidades existentes em dispositivos gerenciados.

4.113. A solução proposta deve gerar relatórios de vulnerabilidades encontradas nos dispositivos com sensor de endpoint instalado.

5. DO MÓDULO DE GERENCIAMENTO DE DISPOSITIVOS MÓVEIS

5.1. O modulo deve ser integrado a console de gerenciamento;

5.2. A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis, incluindo Android:

Android 5.0 ou posterior (incluindo Android 12L, excluindo Go Edition)

5.3. A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis iOS:

iOS 10–17 ou iPadOS 13–17

5.4. A solução proposta deve oferecer suporte a dispositivos Android Device Owner.

5.5. A solução proposta deve suportar dispositivos iOS supervisionados.

5.6. A solução proposta deve permitir a proteção do sistema de

arquivos do smartphone e a interceptação e varredura de todos os objetos recebidos transferidos através de conexões sem fio (porta infravermelha, Bluetooth), EMS e MMS, ao mesmo tempo em que sincroniza com o computador pessoal e carrega arquivos através de um navegador.

5.7. A solução proposta deve ter a capacidade de bloquear sites maliciosos projetados para espalhar códigos maliciosos e sites de phishing projetados para roubar dados confidenciais do usuário e acessar suas informações financeiras.

5.8. A solução proposta deve ter a funcionalidade de adicionar um site excluído da verificação a uma lista de permissões.

5.9. A solução proposta deve incluir a filtragem de websites por categorias e permitir ao administrador restringir o acesso dos utilizadores a categorias específicas (por exemplo, websites relacionados com jogos de azar ou categorias de redes sociais).

5.10. A solução proposta deve permitir ao administrador obter informações sobre o funcionamento do sensor de endpoint e da proteção web no dispositivo móvel do usuário.

5.11. A solução proposta deverá ter a funcionalidade de detectar a localização do dispositivo móvel via GPS, e mostrá-la no Google Maps.

5.12. A solução proposta deve permitir ao administrador tirar uma foto da câmera frontal do celular quando ele estiver bloqueado.

5.13. A solução proposta deve ter recursos de conteinerização para dispositivos Android.

5.14. A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos Android:

Dados em contêineres

Contas de e-mail corporativo

Configurações para conexão à rede Wi-Fi corporativa e VPN

Nome do ponto de acesso (APN)

Perfil do Android for Work

Recipiente KNOX

Chave do gerenciador de licença KNOX

5.15. A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos iOS:

Todos os perfis de configuração instalados

Todos os perfis de provisionamento

O perfil iOS MDM

5.16. Aplicativos para os quais a caixa de seleção remover e o perfil iOS MDM foram marcadas

5.17. A solução proposta deve permitir a criptografia de todos os dados do dispositivo (incluindo dados de contas de usuários,

unidades removíveis e aplicativos, bem como mensagens de e-mail, mensagens SMS, contatos, fotos e outros arquivos). O acesso aos dados criptografados só deve ser possível em um dispositivo desbloqueado por meio de uma chave especial ou senha de desbloqueio do dispositivo .

5.18. A solução proposta deve oferecer controles para garantir que todos os dispositivos cumpram os requisitos de segurança corporativa. O controlo de conformidade deverá basear-se num conjunto de regras que deverá incluir as seguintes componentes:

Critérios de verificação do dispositivo;

Prazo alocado para o usuário corrigir a não conformidade configurando ação que será tomada no dispositivo caso o usuário não corrija a não conformidade dentro do prazo definido;

5.19. A solução proposta deve ter a funcionalidade de detectar e notificar o administrador sobre hacks de dispositivos, por exemplo, root, Jailbreak e etc.

5.20. A solução proposta deverá permitir a gestão de pelo menos as seguintes características do dispositivo:

Cartões de memória e outras unidades removíveis

Câmera do dispositivo

Conexões Wi-Fi

Conexões Bluetooth

Porta de conexão infravermelha

Ativação do ponto de acesso Wi-Fi

Conexão de área de trabalho remota

Sincronização de área de trabalho

Definir configurações da caixa de correio do Exchange

Configurar caixa de e-mail em dispositivos iOS MDM

Configure contêineres Samsung KNOX.

Definir as configurações do perfil do Android for Work

Configurar e-mail/calendário/contatos

Defina as configurações de restrição de conteúdo de mídia.

Definir configurações de proxy no dispositivo móvel

Configurar certificados e SCEP

5.21. A solução proposta deverá permitir a configuração de uma conexão com dispositivos AirPlay para permitir o streaming de músicas, fotos e vídeos do dispositivo iOS MDM para dispositivos AirPlay .

5.22. A solução proposta deve suportar todos os métodos de implantação abaixo para o sensor móvel:

Google Play, Huawei App Gallery e Apple App Store

Portal de inscrição móvel KNOX

Pacotes de instalação pré-configurados independentes

5.23. A solução proposta deverá permitir a configuração de Nomes de Pontos de Acesso (APN) para conectar um dispositivo móvel a serviços de transferência de dados em uma rede móvel.

5.24. A solução proposta deve permitir que o PIN de um dispositivo móvel seja redefinido remotamente.

5.25. A solução proposta deve incluir a opção de registrar dispositivos Android usando sistemas EMM de terceiros:

VMware AirWatch 9.3 ou posterior

MobileIron 10.0 ou posterior

IBM MaaS360 10.68 ou posterior

Microsoft Intune 1908 ou posterior

SOTI MobiControl 14.1.4 (1693) ou posterior

5.26. A solução proposta deve ter funcionalidade para forçar a instalação de um aplicativo no dispositivo.

5.27. A solução proposta deve suportar a implantação de sensor de endpoint iniciada pelo usuário através de:

Google Play

Galeria de aplicativos Huawei

Loja de aplicativos da Apple

5.28. A solução proposta deve ser capaz de escanear arquivos abertos no dispositivo.

5.29. A solução proposta deve ser capaz de verificar programas instalados a partir da interface do dispositivo.

5.30. A solução proposta deve ser capaz de verificar objetos do sistema de arquivos no dispositivo ou em placas de extensão de memória conectadas, mediante solicitação do usuário ou de acordo com um agendamento.

5.31. A solução proposta deve proporcionar o isolamento confiável de objetos infectados em um local de armazenamento de quarentena.

5.32. A solução proposta deve contar com a atualização dos bancos de dados de antivírus utilizados para busca de programas maliciosos e exclusão de objetos perigosos.

5.33. A solução proposta deve ser capaz de verificar dispositivos móveis em busca de malware e outros objetos indesejados sob demanda e dentro do cronograma e lidar com eles automaticamente.

5.34. A solução proposta deve ser capaz de gerenciar e monitorar dispositivos móveis a partir do mesmo console usado para gerenciar computadores e servidores.

5.35. A solução proposta deve fornecer funcionalidade Anti-Roubo, para que dispositivos perdidos e/ou deslocados possam ser localizados, bloqueados e apagados remotamente.

5.36. A solução proposta deve fornecer a possibilidade de bloquear o lançamento de aplicativos proibidos no dispositivo móvel.

5.37. A solução proposta deve ser capaz de impor configurações de segurança, como restrições de senha e criptografia, em dispositivos móveis.

5.38. A solução proposta deve ter a capacidade de enviar aplicações recomendadas/exigidas pelo administrador para o dispositivo móvel.

5.39. A solução proposta deverá possuir Controle de Aplicativos com os modos de aplicação Proibido/Permitido.

5.40. A solução proposta deve incluir um modelo de assinatura integrado a nuvem do fabricante para proteção de ataques mais recentes;

5.41. A solução proposta deve proteger contra ameaças online em dispositivos iOS.

6. DO MÓDULO DE EDR

6.1. Deve apresentar um gráfico de propagação de ameaças com os principais processos. conexões de rede, DLLs, seções de registro afetado ou envolvido no alerta.

6.2. Todas as detecções são destacadas no gráfico, fornecendo ao analista o contexto completo para o incidente e facilitando o processo de revelação dos componentes afetados.

6.3. A solução proposta deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um gráfico visualizado da cadeia de desenvolvimento de ameaças;

6.4. Dever ser integrado ao portal de inteligência do fornecedor para enriquecimento dos detalhes da análise;

6.5. Deve apresentar informações detalhadas contendo:

Usuário que executou a ação;

Informações acesso privilegiado;

6.6. A solução proposta deve ter sandbox em nuvem do fabricante integrada para verificar automaticamente arquivos e aplicar respostas caso atividades suspeitas sejam detectadas.

6.7. A solução proposta deve suportar integração com serviço de reputação em nuvem.

6.8. A solução proposta deve oferecer suporte ao gerenciamento central e à análise por meio do console Web local e do console de gerenciamento em nuvem avançado. (Dados relacionados ao incidente, status do sistema e dados de verificação de integridade, configurações, etc.)

6.9. O agente EDR deve ter integração com o aplicativo de proteção de endpoint(agente único).

6.10. Soluções EDR e proteção de endpoint devem ter console unificado para administradores e analistas;

6.11. A solução proposta deve suportar a detecção automatizada de atividades maliciosas usando a solução Endpoint Protection e a tecnologia de sandbox na nuvem.

6.12. A solução proposta deve complementar as informações do veredicto da solução Endpoint Protection com artefatos do sistema sobre a detecção.

6.13. A solução proposta deve suportar a geração automática de indicadores de ameaça (IoC) após a detecção ocorrer com capacidade de aplicar ações de resposta.

6.14. A solução deve ter a capacidade de forçar a execução da varredura IoC em todos os endpoints com agentes EDR instalados.

6.15. A solução proposta deve suportar a execução de varredura IoC de acordo com um agendador.

6.16. A solução proposta deve suportar a importação de IoC de terceiros no formato OpenIoC para uso em digitalização em rede.

6.17. A solução proposta deve oferecer suporte à verificação usando conjuntos de IoCs gerados automaticamente, carregados ou externos (de terceiros) para detectar ameaças anteriores não detectadas.

6.18. A solução proposta deve permitir suportar a exportação do IoC gerado pela solução para monitorar vulnerabilidades existentes nos dispositivos gerenciados, um arquivo no formato OpenIoC.

6.19. A solução proposta deve gerar um cartão de incidente detalhado relacionado à ameaça detectada em um endpoint.

6.20. A solução proposta deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um cartão de incidente visualizado. Um cartão de incidente deve incluir pelo menos as seguintes informações sobre a ameaça detectada:

6.21. Gráfico da cadeia de desenvolvimento de ameaças e detalhamento para análise posterior (cadeia de ataque).

6.22. Informações sobre o dispositivo no qual a ameaça foi detectada, contendo: nome, endereço IP, endereço MAC, lista de usuários, sistema operacional.

6.23. Informações gerais sobre a detecção, incluindo modo de detecção.

6.24. Alterações no registro associadas à detecção.

6.25. Histórico da presença de arquivos no dispositivo.

6.26. Ações de resposta executadas pela aplicação.

6.27. O gráfico da cadeia de desenvolvimento de ameaças (kill chain) deve fornecer informações visuais sobre os objetos envolvidos no incidente, por exemplo, sobre os principais processos no dispositivo, conexões de rede, bibliotecas, registro, etc.

6.28. A visualização de incidente deve apresentar uma visão detalhada dos artefatos do sistema e dos dados relacionados ao incidente para análise da causa raiz:

6.29. Processo

6.30. Conexões de rede

6.31. Alterações no registro

6.32. Detalhes do download de objeto

6.33. A solução proposta deve fornecer orientação de resposta (resposta guiada).

6.34. A solução proposta deve suportar “clique único” no console de gerenciamento avançado para resposta a um incidente

6.35. A solução proposta deve suportar pelo menos as seguintes ações de resposta que um administrador pode executar quando ameaças são detectadas:

6.36. Impedir a execução de objetos

6.37. Isolamento de host

6.38. Excluir objeto do host ou grupo de hosts

6.39. Encerrar um processo no dispositivo

6.40. Colocar um objeto em quarentena

6.41. Execute a verificação do sistema

6.42. Execução remota de programa/processo/comando

6.43. Iniciar a varredura IoC para um grupo de hosts.

7. REQUISITOS PARA DOCUMENTAÇÃO DA SOLUÇÃO

7.1. A documentação da solução de proteção de endpoint incluindo ferramentas de administração, deve incluir os seguintes documentos:

7.2. Ajuda on-line para administradores

7.3. Ajuda on-line para melhores práticas de implementação

7.4. Ajuda on-line para proteção de servidores de administração

7.5. A documentação do software anti-malware fornecida deve descrever detalhadamente os processos de instalação, configuração e uso do software anti-malware.

7.6. Deve estar disponível página com informações de ciclo de vida das soluções e módulos;

8. IMPLANTAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO DE SEGURANÇA

8.1.Fornecer serviço de implantação e configuração inicial da solução de software de segurança contratada.

8.2. A implantação da solução de segurança deverá ser

presencial, realizada na infraestrutura do datacenter localizado na sede do CONTRATANTE.

8.2.1. A critério exclusivo da CONTRATANTE a implantação poderá ser realizada remotamente;

8.3. Programar os procedimentos de implantação e repasse de conhecimento, devendo observar as seguintes fases:

8.3.1. Planejamento do ambiente e validação dos parâmetros e requisitos técnicos;

8.3.2. Planejamento da estratégia de distribuição da solução de segurança para as máquinas clientes;

8.3.3. Instalação e configuração da Interface de Gerenciamento Centralizado, bem como em um grupo de amostragem das estações clientes;

8.3.4. Validação e testes do novo ambiente e realização de ajustes conforme a necessidade;

8.3.5. Acompanhamento do ambiente após a conclusão da instalação, até que este ambiente esteja apto à plena entrada em produção;

8.3.6. Apresentação da documentação técnica do ambiente.

8.4. A implantação da solução de segurança deverá ser realizada pela CONTRATANTE com nível de parceria mínimo (Platinum Kaspersky), e por profissional certificado pelo fabricante (Certified Professional: Kaspersky EDR Optimum) da solução ofertada na proposta, com apresentação do correspondente documento de certificação, em versão original ou cópia autenticada.

8.5. A instalação e configuração dos componentes da solução de segurança deverão ocorrer nas datas e horários definidos pela equipe técnica do CONTRATANTE, no ambiente de datacenter do CRCMS, que supervisionará os trabalhos.

8.6. A solução deverá ter a capacidade de remoção do atual antivírus instalado e ser capaz de instalar de forma remota o agente do antivírus pela console de gerenciamento, e caso não tenha a capacidade de realização da remoção completa, a CONTRATADA deverá remover a atual solução utilizando scripts, softwares de terceiros, ou mesmo de forma manual, e prover a instalação da nova solução de segurança;

8.7. Atividades que exijam a paralisação ou que causem o comprometimento de serviços de informática em produção deverão ser executados fora do horário de expediente e deverão ser agendados e aprovados pela CONTRATANTE.

8.8. Deverá ser gerado um relatório pela CONTRATADA comprovando a instalação e configuração da solução, sendo que deverá estar em pleno funcionamento local e integrada ao console de gerenciamento.

8.9. Deve haver o repasse de conhecimento hands-on com relação às configurações realizadas.

4. REQUISITOS DA CONTRATAÇÃO

4.1. Requisitos de negócio

4.1.1. As quantidades deverão obedecer às definições do item 3, deste Termo de Referência.

4.1.2. A solução deverá estar acompanhada de sua documentação técnica completa e atualizada, preferencialmente, no idioma português, falado e escrito no Brasil, compreendendo manuais, guias de instalação e outros pertinentes.

4.1.3. A documentação deverá ser fornecida em sua forma original, impressa ou em mídia digital, não sendo aceitas cópias de qualquer tipo, mesmo que autenticadas, e deverá ser disponibilizada no site do fabricante para download.

4.2. Requisitos de Capacitação

4.2.1. Não faz parte do escopo da contratação a realização de capacitação técnica na utilização dos recursos relacionados ao objeto da presente contratação.

4.3. Requisitos Legais

4.3.1. O presente processo de contratação deve estar aderente à Constituição Federal, à Lei nº 14.133/2021, à Instrução Normativa SGD/ME nº 94, de 2022, Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021, Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), Lei n° 10.520, de 17 de julho de 2001, Decreto 10.024, de 20 de setembro de 2019, e a outras legislações aplicáveis;

4.3. Requisitos de Manutenção

4.3.1. A Contratada deverá disponibilizar suporte técnico via Help Desk, telefone e/ou E-mail.

4.3.2. A manutenção será oferecida por meio da garantia, vinculada aos produtos adquiridos. Demais requisitos sobre a manutenção dos produtos licitados, poderão ser analisados no contrato a ser formalizado com a empresa vencedora do certame. Será verificada a necessidade de aplicação de manutenção preventiva, corretiva, evolutiva e adaptativa em momento oportuno, porém a garantia deverá compreender 36 meses no mínimo conforme descrição técnica no item 3.1. A necessidade de tempo de resposta e de solução de problemas, constará no contrato formalizado com a vencedora do certame, onde os níveis mínimos de garantia serão exigidos. Porém, desde já informamos que o tempo de resposta quando da necessidade dos usuários em face ao problema com o equipamento deverá ser de no máximo 48 horas para a solução do problema.

4.4. Requisitos Temporais

4.4.1. Rotinas de Execução

Prazos

O serviço, deverá ser entregue, no máximo 30 (trinta) dias corridos, contado a partir da data de assinatura do contrato. Dentro desse mesmo prazo, também, deverão estar em operação a implementação das soluções.

Horários

Dia útil, das 7h30 às 11:30h e das 13h00 às 17h.

Locais de Entrega

Sede do CRCMS, situado à Rua Euclides da Cunha, 994 – Bairro Jardim dos Estados, CEP 79020-230 – Campo Grande – MS.

4.5. Requisitos de Segurança e Privacidade

4.5.1. No que couber, o "Requisitos e Obrigações quanto a Segurança da Informação e Privacidade" com a finalidade de garantir a disponibilidade, integridade, confidencialidade e autenticidade das informações e a privacidade dos dados. Deverá ser observado na IN SGD/ME nº 94/2022.

4.6. Requisitos Sociais, Ambientais e Culturais

4.6.1. As aquisições dos itens 3.1 deverão estar no idioma Português Brasileiro, atendendo as especificações técnicas do item. A Contratada deverá adotar práticas de sustentabilidade ambiental na execução do objeto, quando couber, conforme disposto na Instrução Normativa nº 1/2010 - SLTI/MPOG.

4.7. Requisitos da Arquitetura Tecnológica

4.7.1. Os serviços deverão ser executados observando-se as diretrizes de arquitetura tecnológica estabelecidas pela área técnica da Contratante.

4.7.2. A adoção de tecnologia ou arquitetura diversa deverá ser autorizada previamente pela Contratante. Caso não seja autorizada, é vedado à Contratada adotar arquitetura, componentes ou tecnologias diferentes daquelas definidas pela Contratante.

4.8. Requisitos de Projeto e de Implementação

4.8.1. Os serviços deverão observar integralmente os requisitos de projeto e de implementação descrito no item 3.1, atendendo as especificações técnicas do item.

4.9. Requisitos de Implantação

4.9.1. Os serviços deverão observar integralmente os requisitos de implantação, instalação e fornecimento descrito no item 3.1, atendendo as especificações técnicas do item.

4.10. Requisitos de Metodologia de Trabalho

4.10.1. Na execução das demandas a CONTRATADA deve zelar pela observância às políticas, diretrizes, procedimentos, padrões e modelos para as atividades de gestão e fiscalização de contratos e planejamento de contratações – dentre esses, destacadamente, a Metodologia de Desenvolvimento de Sistemas (MDSMEC), a Metodologia de Gerenciamento de Projetos (MGP-MEC) o Guia de Métricas do MEC e a Política de Gerenciamento de Configuração.

No que couber, quando não especificado de outra forma, o processo de trabalho é aquele descrito no Modelo de Execução para cada ITEM de serviço, conforme detalhado nos requisitos específicos no item 3.1 do TR. Também, no que couber, na execução dos serviços a CONTRATADA deve manter observância às políticas, regulamentações, especificações técnicas e orientações definidos pelos seguintes padrões de GOVERNO:

a) Padrões de Interoperabilidade de Governo Eletrônico (e-PING) e Modelo de Acessibilidade em

Governo Eletrônico (e-MAG), conforme as Portarias Normativas SLTI nº 5, de 14 de julho de 2005 e nº 3, de 7 de maio de 2007 e suas atualizações;

b) Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), conforme a Medida Provisória nº 2.200-2, de 24 de agosto de 2001, e suas atualizações, quando houver necessidade de utilização de certificação digital; e

c) Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos (e-ARQ Brasil), quando a solução abranger a gestão de documentos arquivísticos digitais e não digitais, conforme Resolução do CONARQ nº 32, de 17 de maio de 2010 e suas atualizações. Ainda, nos termos do Decreto n° 8.936, de 19 de dezembro de 2016, e da Instrução Normativa SGD/ME n° 94/2022, as demandas que produzirem software/sistema que se consubstancie em serviço público digital devem ser integradas à Plataforma de Cidadania Digital.

A metodologia aplicada no trabalho de desenvolvimento será a ágil, visando a realização de melhorias e alterações constantes, baseadas no feedback dos usuários, dos próprios clientes e até do time interno de criação.

4.11. Requisitos de Segurança da Informação e Privacidade

4.11.1. Os serviços contratados deverão ser prestados em conformidade com leis, normas e diretrizes vigentes no âmbito da Administração Pública Federal, relacionadas à Segurança da Informação e Comunicações (SIC); em especial atenção ao "Requisitos e Obrigações quanto a Segurança da Informação e Privacidade" Com a finalidade de garantir a disponibilidade, integridade, confidencialidade e autenticidade das informações e a privacidade dos dados. Deverá ser observado na IN SGD/ME nº 94/2022.

4.11.2. A CONTRATADA deverá credenciar junto ao CONTRATANTE seus profissionais que venham a ser designados para prestar serviços de forma presencial, bem como aqueles autorizados a retirar e/ou entregar documentos junto ao CONTRATANTE. Assim como deverá identificar qualquer equipamento de sua propriedade que venha a ser instalado nas dependências do CONTRATANTE, utilizando placas de controle patrimonial, selos de segurança etc. A CONTRATADA deverá comprometer-se, por si e por seus funcionários, em documento formal, a aceitar e aplicar rigorosamente todas as normas e procedimentos de segurança implementados no ambiente de Tecnologia da Informação do CONTRATANTE – inclusive com a assinatura de TERMO de responsabilidade e manutenção de sigilo. A CONTRATADA deverá adotar critérios adequados para o processo seletivo de profissionais que irão atuar diretamente na execução do OBJETO, com o propósito de evitar a incorporação de perfis que possam comprometer a segurança ou credibilidade do CONTRATANTE.

4.11.3. A CONTRATADA deverá comunicar ao CONTRATANTE, com a antecedência mínima necessária, qualquer ocorrência de transferência, remanejamento ou demissão de funcionários envolvidos diretamente na execução do CONTRATO, para que seja providenciada a revogação de todos os privilégios de acesso aos sistemas, informações e recursos do CONTRATANTE porventura colocados à disposição para realização dos serviços contratados.

4.12. Sustentabilidade

4.12.1. A empresa contratada deverá adotar os critérios e práticas de sustentabilidade ambiental na execução do objeto, naquilo que couber, em consonância com o art. 6º da Instrução Normativa SLTI/MPOG n.º 01, de 19/01/2010 e demais ordenamentos jurídicos vigentes.

4.13. Subcontratação

4.13.1. Não é admitida a subcontratação do objeto contratual.

4.14. Garantia da Contratação

4.14.1. Será exigida a garantia da contratação de que tratam os arts. 96 e seguintes da Lei nº 14.133, de 2021, no percentual e condições descritas nas cláusulas do contrato.

4.15. Informações relevantes para o [dimensionamento E/OU apresentação] da proposta

4.15.1. A demanda do órgão tem como base as seguintes características:

4.15.2. Para dimensionamento da Proposta, o Licitante deverá incluir os custos para fornecimento dos produtos, além das obrigações estabelecidas no momento da apresentação da proposta, conforme Anexos.

5. INFORMAÇÕES RELEVANTES PARA A PROPOSTA

5.1. Parcelamento da solução

5.1.1. Recomenda-se a contratação por itens com vistas a estimular uma maior disputa com potencial impacto na redução do preço final de cada item, com fundamento na Súmula nº 247 do Tribunal de Contas da União, no que tange à obrigatoriedade da adjudicação por item e não por preço global.

5.1.2. Foi realizada uma pesquisa dos serviços no mercado, chegando-se à conclusão de que existem no mercado diversas empresas que atendem ao objeto especificado neste Estudo Técnico Preliminar.

6. PÁPEIS E RESPONSABILIDADES

6.1. São obrigações da CONTRATANTE

6.1.1. Nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contato para acompanhar e fiscalizar a execução dos contratos;

6.1.2. Proporcionar as condições necessárias à execução dos serviços ora contratados, assim como prestar, prontamente, as informações e esclarecimentos que venham a ser solicitados pela Contratada.

6.1.3. Transmitir ao preposto da Contratada toda e qualquer demanda.

6.1.4. Efetuar o pagamento à Contratada, após o devido atesto da nota fiscal/fatura.

6.1.5. Aplicar à Contratada as penalidades regulamentares e contratuais.

6.1.6. Comunicar à Contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC.

6.1.7. Rejeitar, no todo ou em parte, o serviço que a Contratada executar fora das especificações fornecidas pelo CRCMS.

6.1.8. Comunicar, por escrito, à Contratada, toda e qualquer orientação sobre os serviços, excetuados os entendimentos orais determinados pela urgência, que deverão ser confirmados, por escrito, no prazo de 24 (vinte quatro) horas úteis.

6.1.9. Notificar a Contratada, por escrito e com antecedência, sobre multas, penalidades e quaisquer débitos de sua responsabilidade.

6.1.10. Fazer cumprir fielmente as cláusulas integrantes do Edital de Licitação e seus anexos.

6.1.11. Zelar pelo cumprimento dos padrões definidos entre as partes, determinando a proponente

refazer os serviços, sem ônus à Contratada, tantas vezes quanto necessárias, sempre que apresentarem incompatibilidade com o serviço contratado.

6.1.12. Receber os serviços prestados pela Contratada, os respectivos documentos legais e descritivos, identificando a quantidade, a qualidade e as não conformidades destes com o Edital de Licitação, registrando essas informações em documento apropriado.

6.1.13. Fiscalizar, realizar testes, inspeções, perícias ou os meios necessários que permitam verificar a qualidade e a confiabilidade.

6.1.14. Informar à Contratada o aceite dos serviços adquiridos ou a recusa deles, por escrito, descrevendo os fatos que motivaram.

6.1.15. Notificar a Contratada quanto ao não atendimento de cláusulas contratuais por ela firmadas com a Contratante, quanto a providências técnicas e/ou administrativas anteriormente informadas e não atendidas prontamente por ela, quanto a responsabilidade por descumprimento do Contrato e respectivas penalidades, quanto a irregularidades constatadas na prestação dos serviços.

6.1.16. Avaliar os relatórios de entrega, total ou parcial, dos serviços prestados, emitidos pela Contratada ou, quando houver, os relatórios técnicos que descrevam a implantação, a metodologia, as alterações, as técnicas adotadas, as adequações ou que levantem questionamento técnico, respondendo-os com aceite ou recusa e /ou naquilo que for pertinente.

6.1.17. Fiscalizar os documentos que comprovem as regularidades jurídicas, fiscais e trabalhistas da Contratada e a qualificação de sua equipe técnica, solicitando os originais quando julgar necessário.

6.1.18. Quando necessário, autorizar formalmente a entrada dos funcionários da Contratada, devidamente identificados, garantindo a execução plena do objeto do Contrato.

6.2. São obrigações da CONTRATADA

6.2.1. Indicar formalmente preposto apto a representá-la junto à contratante, que deverá responder pela fiel execução do contrato.

6.2.2. Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual.

6.2.3. Reparar quaisquer danos diretamente causados à contratante ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pela contratante.

6.2.4. Propiciar todos os meios necessários à fiscalização do contrato pela contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, desde que motivadas as causas e justificativas desta decisão.

6.2.5. Manter, durante toda a execução do contrato, as mesmas condições da habilitação.

6.2.6. Quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC.

6.2.7. Quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato.

6.2.8. Fazer a transição contratual, quando for o caso. Prestar garantia na forma e condições estabelecidas.

6.2.9. Arcar com todos os encargos diretos e indiretos que incidir sobre o fornecimento, instalação, manutenção, garantia técnica integral, suporte e treinamentos em face dos serviços contratados, inclusive sob eventuais substituições e reposições.

6.2.10. Abster-se de quaisquer iniciativas que impliquem ônus para o Conselho Regional de

Contabilidade do Mato Grosso do Sul (CRCMS), se não previstas neste instrumento ou expressamente autorizadas pelo CRCMS.

6.2.11. Respeitar o sistema de segurança do CRCMS e fornecer todas as informações por ele solicitadas, relativas ao cumprimento do objeto.

6.2.12. Guardar inteiro sigilo dos serviços contratados e dos dados processados, bem como de toda e qualquer documentação gerada, reconhecendo serem esses de propriedade e uso exclusivo do CRCMS, sendo vedada, à Contratada, sua cessão, locação ou venda a terceiros.

6.2.13. Garantir a segurança das informações do CRCMS e se comprometer em não divulgar ou fornecer a terceiros quaisquer dados e informações que tenha recebido do CRCMS no curso da prestação dos serviços, a menos que autorizado formalmente e por escrito para tal.

6.2.14. Propiciar todos os meios e facilidades necessárias à fiscalização da Solução de Tecnologia da Informação pela Contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcialmente, em qualquer tempo, sempre que considerar a medida necessária.

6.2.15. Responsabilizar-se pelo total controle dos serviços, coibindo tentativas de fraude e quaisquer danos ao Contratante.

6.2.16. Não transferir a terceiros o Contrato, por qualquer forma e nem mesmo parcialmente.

6.2.17. Comunicar ao Fiscal do contrato, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal relacionada ao serviço prestado.

6.2.18. Cumprir os prazos estabelecidos no Termo de Referência e seus anexos, sob pena de aplicação de multa e demais cominações pelo Contratante.

6.2.19. Reproduzir quaisquer manuais e demais documentos técnicos e informativos escritos que descrevam os serviços prestados e disponibilizá-los ao Contratante.

6.2.20. Submeter previamente, por escrito, à Contratante, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações do Termo de Referência.

6.2.21. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato;

6.2.22. Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança da Contratante.

6.2.23. Apresentar nota fiscal, licenciamento ou documento equivalente sobre todos os produtos e serviços utilizados para a execução do objeto desse Termo de Referência e anexos que confiram à Contratada o seu direito de uso.

6.2.24. Substituir, às suas expensas, o equipamento ou material em que verificar defeitos ou incorreções.

6.2.25. Não atribuir ao Contratante qualquer ônus ou responsabilidade, quer pela via administrativa ou judicial, pelas obrigações oriundas da execução do objeto do presente Contrato.

6.2.26. Abster-se, qualquer que seja a hipótese, de veicular publicidade acerca das atividades, objeto da contratação, sem prévia autorização da Contratante.

6.2.27. Diante de situações de irregularidades de caráter urgente deverá comunicar, por escrito, o CRCMS com os esclarecimentos julgados necessários e, as informações sobre possíveis paralisações de serviços, a apresentação de relatório técnico ou razões justificadoras a serem apreciadas e decididas pelo agente designado.

7. MODELO DE EXECUÇÃO DO CONTRATO

7.1. Rotinas de Execução | Encaminhamento formal de demandas

7.1.1. Os serviços deverão ser entregues na sede do CRCMS, situado à Rua Euclides da Cunha, 994 – Bairro Jardim dos Estados, CEP 79020-230 – Campo Grande - MS em dias úteis (segunda a sexta-feira), no horário das 7h30 às 11h30 e das 13h às 17h.

7.1.2. Deverá ser oferecido o suporte técnico, atualizações, correções de problemas.

7.1.3. A Contratada deverá realizar o Suporte Técnico, via web ou telefone, pelo período de 36 (trinta e seis) meses, a contar da data de emissão do Termo de Recebimento Definitivo e funcionamento dos serviços, devendo realizar ainda a atualização de versão necessárias.

7.1.4. A Contratada deverá disponibilizar canais de acesso através de número de telefone e Internet, para abertura de chamados técnicos objetivando respostas de problemas e dúvidas quanto ao funcionamento dos hardwares e softwares.

7.1.5. A abertura de chamados técnicos deverá ser registrada e constar, explícito e claramente a data, horário, descrição do problema e o respectivo grau de criticidade.

7.2. Condições de Entrega

7.2.1. O prazo de entrega dos serviços é de 30 (trinta) dias corridos, contados da data de assinatura do contrato.

7.2.2. Caso não seja possível a entrega na data assinalada, a empresa deverá comunicar as razões respectivas com pelo menos 10 (dez) dias corridos de antecedência para que qualquer pleito de prorrogação de prazo seja analisado, ressalvadas situações de caso fortuito e força maior. Quantidade mínima de bens ou serviços para comparação e controle

7.3. Mecanismos formais de comunicação

7.3.1. Ata de reunião;

7.3.2. Ofício;

7.3.3. Sistema de abertura de chamados;

7.3.4. E-mails.

7.4. Formas de Pagamento

7.4.1. Os critérios de medição e pagamento dos serviços prestados são tratados no item 8 - Modelo de Gestão do Contrato.

7.5. Documentação da solução

7.5.1. A Contratada deverá disponibilizar documentação descrevendo os procedimentos de administração da solução (manual da ferramenta de administração) no idioma português do Brasil.

7.5.2. A Contratada deverá disponibilizar manual de utilização da solução (Manual do Usuário) no idioma português do Brasil.

8. MODELO DE GESTÃO DO CONTRATO

8.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

8.2. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de

execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

8.3. As comunicações entre o CRCMS e o contratado devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

8.4. O CRCMS poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

8.5. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos (Lei nº 14.133, de 2021, art. 117, caput), nos termos do art. 33 da IN SGD nº 94, de 2022, observando-se, em especial, as rotinas a seguir.

8.6. O fiscal técnico do contrato, além de exercer as atribuições previstas no art. 33, II, da IN SGD nº 94, de 2022, acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração;

8.6.1. O fiscal técnico do contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados;

8.6.2. Identificada qualquer inexatidão ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção;

8.6.3. O fiscal técnico do contrato informará ao gestor do contrato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso;

8.6.4. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato;

8.6.5. O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual;

8.7. O fiscal administrativo do contrato, além de exercer as atribuições previstas no art. 33, IV, da IN SGD nº 94, de 2022, verificará a manutenção das condições de habilitação do contratado, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário;

8.7.1. Caso ocorram descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência;

8.8. O gestor do contrato, além de exercer as atribuições previstas no art. 33, I, da IN SGD nº 94, de 2022, coordenará a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração;

8.8.1. O gestor do contrato acompanhará a manutenção das condições de habilitação do Contratado, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais;

8.8.2. O gestor do contrato acompanhará os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência;

8.8.3. O gestor do contrato emitirá documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações.

8.8.4. O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso.

8.8.5. O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à tempestiva renovação ou prorrogação contratual.

8.9. O gestor do contrato deverá elaborará relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração.

8.10. O gestor do contrato deverá enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão nos termos do contrato

8.11. Do recebimento

8.11.1. Os bens serão recebidos provisoriamente, no prazo de 10 (dez) dias, pelos fiscais técnico e administrativo, mediante termos detalhados, quando verificado o cumprimento das exigências de caráter técnico e administrativo.

8.11.2. O prazo da disposição acima será contado do recebimento de comunicação de cobrança oriunda do Contratado com a comprovação da prestação dos serviços a que se referem a parcela a ser paga.

8.11.3. O fiscal técnico do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter técnico.

8.11.4. O fiscal administrativo do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter administrativo.

8.11.5. O fiscal do contrato, quando houver, realizará o recebimento provisório sob o ponto de vista técnico e administrativo.

8.11.6. Para efeito de recebimento provisório, ao final de cada período de faturamento, o fiscal técnico do contrato irá apurar o resultado das avaliações da execução do objeto e, se for o caso, a análise do desempenho e qualidade da prestação dos serviços realizados em consonância com os indicadores previstos, que poderá resultar no redimensionamento de valores a serem pagos à contratada, registrando em relatório a ser encaminhado ao gestor do contrato.

8.11.7. O Contratado fica obrigado a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não atestar a última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.

8.11.8. A fiscalização não efetuará o ateste da última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.

8.11.9. Os bens poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, sem prejuízo da aplicação das penalidades.

8.11.10. Quando a fiscalização for exercida por um único servidor, o Termo Detalhado deverá conter o registro, a análise e a conclusão acerca das ocorrências na execução do contrato, em relação à fiscalização técnica e administrativa e demais documentos que julgar necessários, devendo encaminhá-los ao gestor do contrato para recebimento definitivo.

8.11.11. Os bens serão recebidos definitivamente no prazo de 15 (quinze) dias, contados do recebimento provisório, por servidor ou comissão designada pela autoridade competente, após a

verificação da qualidade e quantidade do serviço e consequente aceitação mediante termo detalhado, obedecendo os seguintes procedimentos:

8.11.12. Emitir documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial, quando houver, no cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado em indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações, conforme regulamento.

8.11.13. Realizar a análise dos relatórios e de toda a documentação apresentada pela fiscalização e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicar as cláusulas contratuais pertinentes, solicitando à Contratada, por escrito, as respectivas correções;

8.11.14. Emitir Termo de recebimento definitivo com base nos equipamentos recebidos.

8.11.15. Comunicar a empresa para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pela fiscalização.

8.11.16. Enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão.

8.11.17. No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, deverá ser observado o teor do art. 143 da Lei nº 14.133, de 2021, comunicando-se à empresa para emissão de Nota Fiscal no que concerne à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

8.11.18. Nenhum prazo de recebimento ocorrerá enquanto pendente a solução, pelo contratado, de inconsistências verificadas na execução do objeto ou no instrumento de cobrança.

8.11.19. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético profissional pela perfeita execução do contrato.

8.12. Sanções Administrativas e Procedimentos para retenção ou glosa no pagamento

8.12.1. Nos casos de inadimplemento na execução do objeto, as ocorrências serão registradas pela Contratante, conforme a tabela abaixo:

ID	OCORRÊNCIA	GLOSA/SANÇÃO
1	Recusa em assinar o contrato, no prazo máximo de 05 (cinco) dias úteis, após regularmente convocado, sem prejuízo da aplicação de outras sanções	Multa no percentual de até 10% (dez por cento), calculada sobre o valor total do contrato,
2	Atraso, sem justificativa, acima de 20 (vinte) dias, na entrega dos bens	Multa no percentual de até 0,5% (meio por cento) do valor do contrato.
3	Atraso na configuração dos serviços rejeitados no recebimento provisório	Multa no percentual de até 0,5% (meio por cento) do valor do contrato.

4	Deixar de cumprir os prazos determinados para atendimento dos chamados de suporte técnico.	Multa no percentual de até 0,5% (meio por cento) do valor do contrato.
5	Atraso injustificado na entrega dos bens no início da execução do contrato, de acordo com os prazos estabelecidos.	Multa no percentual correspondente a 1% (meio por cento), calculada sobre o valor total do contrato, por dia de inadimplência, constatada a falta gravíssima, até o limite máximo de 5% (cinco por cento), ou seja, por 20 (vinte) dias, o que poderá ensejar a rescisão do contrato.
6	Deixar de efetuar os atendimentos referentes aos requisitos de suporte técnico da solução, conforme os prazos estabelecidos neste Termo de Referência	Multa no percentual correspondente a 5% (cinco por cento), calculada sobre o valor total do contrato, por dia de inadimplência, constatada a falta gravíssima, até o limite máximo de 10% (dez por cento), ou seja, por 20 (vinte) dias, o que poderá ensejar a rescisão do contrato.

8.12.2. Nos termos do art. 19, inciso III da Instrução Normativa SGD/ME nº 94, de 2022, será efetuada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, nos casos em que o contratado:

a) não atingir os valores mínimos aceitáveis fixados nos critérios de aceitação, não produzir os resultados ou deixar de executar as atividades contratadas; ou

b) deixar de utilizar materiais e recursos humanos exigidos para fornecimento da solução de TIC, ou utilizá-los com qualidade ou quantidade inferior à demandada;

8.13. Liquidação

8.13.1. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de dez dias úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período, nos termos do art. 7º, §2º da Instrução Normativa SEGES/ME nº 77/2022.

8.13.2. O prazo de que trata o item anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação, no caso de contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021.

8.13.3. Para fins de liquidação, o setor competente deverá verificar se a nota fiscal ou instrumento de cobrança equivalente apresentado expressa os elementos necessários e essenciais do documento, tais como:

a) o prazo de validade;

b) a data da emissão;

c) os dados do contrato e do órgão contratante;

d) o período respectivo de execução do contrato;

e) o valor a pagar; e

f) eventual destaque do valor de retenções tributárias cabíveis.

8.13.4. Havendo erro na apresentação da nota fiscal ou instrumento de cobrança equivalente, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da

situação, sem ônus ao contratante;

8.13.5. A nota fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhado da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 da Lei nº 14.133, de 2021.

8.13.6. A Administração deverá realizar consulta ao SICAF para:

a) verificar a manutenção das condições de habilitação exigidas no edital;

b) identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, que implique proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas.

8.13.7. Constatando-se, junto ao SICAF, a situação de irregularidade do contratado, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do contratante.

8.13.8. Não havendo regularização ou sendo a defesa considerada improcedente, o contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do contratado, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

8.13.9. Persistindo a irregularidade, o contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao contratado a ampla defesa.

8.13.10. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso o contratado não regularize sua situação junto ao SICAF.

8.14. Prazo de pagamento

8.14.1. O pagamento será efetuado no prazo de até 10 (dez) dias úteis contados da finalização da liquidação da despesa, conforme subitem 8.15, nos termos da Instrução Normativa SEGES/ME nº 77, de 2022.

8.14.2. No caso de atraso pelo Contratante, os valores devidos ao contratado serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação do Índice de Custo da Tecnologia da Informação (ICTI) de correção monetária.

8.15. Forma de pagamento

8.15.1. O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado.

8.15.2. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

8.15.3. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

8.15.4. Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.

8.15.5. O contratado regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação,

por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

8.16. Obrigações pertinentes à LGPD

8.16.1. As partes deverão cumprir a Lei n° 13.709, de 14 de agosto de 2018 (LGPD), quanto a todos os dados pessoais a que tenham acesso em razão do certame ou do contrato administrativo que eventualmente venha a ser firmado, a partir da apresentação da proposta no procedimento de contratação, independentemente de declaração ou de aceitação expressa.

8.16.2. Os dados obtidos somente poderão ser utilizados para as finalidades que justificaram seu acesso e de acordo com a boa-fé e com os princípios do art. 6° da LGPD.

8.16.3. É vedado o compartilhamento com terceiros dos dados obtidos fora das hipóteses permitidas em Lei.

8.16.4. A Administração deverá ser informada no prazo de 5 (cinco) dias úteis sobre todos os contratos de suboperação firmados ou que venham a ser celebrados pelo Contratado.

8.16.5. Terminado o tratamento dos dados nos termos do art. 15 da LGPD, é dever do contratado eliminá-los, com exceção das hipóteses do art. 16 da LGPD, incluindo aquelas em que houver necessidade de guarda de documentação para fins de comprovação do cumprimento de obrigações legais ou contratuais e somente enquanto não prescritas essas obrigações.

8.16.6. É dever do contratado orientar e treinar seus empregados sobre os deveres, requisitos e responsabilidades decorrentes da LGPD.

8.16.7. O Contratado deverá exigir de suboperadores e subcontratados o cumprimento dos deveres da presente cláusula, permanecendo integralmente responsável por garantir sua observância.

8.16.8. O Contratante poderá realizar diligência para aferir o cumprimento dessa cláusula, devendo o Contratado atender prontamente eventuais pedidos de comprovação formulados.

8.16.9. O Contratado deverá prestar, no prazo fixado pelo Contratante, prorrogável justificadamente, quaisquer informações acerca dos dados pessoais para cumprimento da LGPD, inclusive quanto a eventual descarte realizado.

8.16.10. Bancos de dados formados a partir de contratos administrativos, notadamente aqueles que se proponham a armazenar dados pessoais, devem ser mantidos em ambiente virtual controlado, com registro individual rastreável de tratamentos realizados (LGPD, art. 37), com cada acesso, data, horário e registro da finalidade, para efeito de responsabilização, em caso de eventuais omissões, desvios ou abusos.

8.16.11. O contrato está sujeito a ser alterado nos procedimentos pertinentes ao tratamento de dados pessoais, quando indicado pela autoridade competente, em especial a ANPD por meio de opiniões técnicas ou recomendações, editadas na forma da LGPD.

8.16.12. Os contratos e convênios de que trata o § 1° do art. 26 da LGPD deverão ser comunicados à autoridade nacional.

9. DO REAJUSTE

9.1. Será adotado como índice de reajuste do Contrato o Índice de Custos de Tecnologia da Informação - ICTI.

10. CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

10.1. Forma de seleção e critério de julgamento da proposta

10.1.1. O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO ELETRÔNICO, com adoção do critério de julgamento pelo menor preço global.

10.2. Exigências de habilitação

10.2.1. Para fins de habilitação, deverá o licitante comprovar os seguintes requisitos:

10.3. Habilitação jurídica

10.3.1. Pessoa física: cédula de identidade (RG) ou documento equivalente que, por força de lei, tenha validade para fins de identificação em todo o território nacional;

10.3.2. Empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

10.3.3. Microempreendedor Individual - MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio https://www.gov.br/empresas-e-negocios/ptbr/empreendedor;

10.3.4. Sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada - EIRELI: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

10.3.5. Sociedade empresária estrangeira: portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME n.º 77, de 18 de março de 2020.

10.3.6. Sociedade simples: inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

10.3.7. Filial, sucursal ou agência de sociedade simples ou empresária: inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz;

10.3.8. Sociedade cooperativa: ata de fundação e estatuto social, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, além do registro de que trata o art. 107 da Lei nº 5.764, de 16 de dezembro 1971.

10.3.9. Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

10.4. Habilitação fiscal, social e trabalhista

10.4.1. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;

10.4.2. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02 de outubro de 2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

10.4.3. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

10.4.4. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de 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;

10.4.5. Prova de inscrição no cadastro de contribuintes Estadual/Distrital ou Municipal/Distrital relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

10.4.6. Prova de regularidade com a Fazenda Estadual/Distrital ou Municipal/Distrital do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;

10.4.7. Caso o fornecedor seja considerado isento dos tributos Estadual/Distrital ou Municipal/Distrital relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.

10.4.8. O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal.

10.5. Qualificação técnica

10.5.1. Para aferir a qualificação técnica das licitantes participantes, será solicitado atestado de capacidade técnica que comprove a aptidão da licitante para o desempenho de atividades pertinentes e compatíveis em características, quantidades e prazos com o objeto em questão, contendo, no mínimo, as seguintes informações:

a) Nome ou razão social, CNPJ e endereço completo do emitente;

b) Descrição do escopo dos serviços prestados;

c) Nome ou razão social da empresa que prestou o serviço ao emitente;

d) Data de emissão do atestado ou da certidão;

e) Assinatura e identificação do signatário (nome, telefone, cargo e função que exerce junto à empresa emitente).

10.5.2. Ficará a cargo do CRCMS, caso julgue necessário, realizar diligências para averiguação dos mesmos.

10.5.3. Os atestados que comprovem a aptidão descrita acima deverão ser emitidos por pessoas jurídicas de direito público ou privado.

10.5.4. No caso de atestados emitidos por pessoas jurídicas de direito privado, não serão considerados aqueles emitidos por empresas pertencentes ao mesmo grupo empresarial da empresa licitante vencedora.

10.5.5. Serão considerados como pertencentes ao mesmo grupo empresarial da empresa licitante, empresas controladas ou controladoras da empresa licitante ou que tenha pelo menos uma mesma pessoa física ou jurídica que seja sócio da empresa emitente e da empresa licitante.

10.5.6. Os atestados deverão referir-se a serviços prestados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente.

10.5.7. O licitante disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados apresentados, apresentando, dentre outros documentos, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em foram prestados os serviços.

11. ESTIMATIVA DO VALOR DA CONTRATAÇÃO

11.1. Para estimativa do custo para a aquisição dos itens, realizou-se pesquisa de preços registrados em contratações similares no âmbito de pregões e contratações públicas através do site https://paineldeprecos.planejamento.gov.br/. A análise dos custos totais da demanda se encontra detalhada a seguir:

ITEM	DESCRIÇÃO DO ITEM	PREÇO 1	PREÇO 2	PREÇO PÚBLICO	QTDE	PERÍODO/ VIGÊNCIA	VALOR UNIT (PREÇO MÉDIO)	VALOR TOTAL DO ITEM (R$)
1	Aquisição/Renovação de licenças de uso de solução de antivírus (Kaspersky Next EDR Optimum).	R$ 450,02	R$ 492,50	R$ 511,50	40	36 meses	R$ 484,67	**R$ 19.386,80**

11.2. A pesquisa de mercado contendo a previsão de preços referenciais como estimativa para a contratação, decorrerá junto ao mercado e será inserido no Termo de Referência. Realizar-se-á junto aos fornecedores, sendo apurados aquisições pela Administração Pública para uma eventual Carona.

11.3. Estimativa calculada com base na MÉDIA dos preços.

11.4. Detalhamento no Estudo Técnico Preliminar, Anexo a este Termo de Referência.

12. ADEQUAÇÃO ORÇAMENTÁRIA

12.1. A contratação e o planejamento estão contidos nos projetos 5002 Tecnologia da Informação, que dispõe de recurso orçamentário para despesa na rubrica 6.3.1.3.02.01.005 (Serviços de Informática).

12.2. A contratação está alinhada com o Plano de Trabalho 2024, e com o inventário de necessidade número 03 do PDTI 2024/2025 do CRCMS.

13. ÍNDICE DE CORREÇÃO MONETÁRIA

13.1. Os preços são fixos e irreajustáveis no prazo de um ano contado da data do orçamento estimado.

13.2. Dentro do prazo de vigência do contrato, os preços contratados poderão sofrer reajuste após o interregno de um ano, aplicando-se o índice de reajustamento ICTI (Índice de Custos de Tecnologia da Informação), mantido pela Fundação Instituto de Pesquisa Econômica Aplicada (IPEA), exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade:

R = V (I – Iº) / Iº, onde:

R = Valor do reajuste procurado;

V = Valor contratual do serviço a ser reajustado;

Iº = índice inicial - refere-se ao índice de custos ou de preços correspondente à data fixada para entrega da proposta da licitação;

I = Índice relativo ao mês do reajustamento;

13.3. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

13.4. No caso de atraso ou não divulgação do índice de reajustamento, o CRCMS pagará à Contratada a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo. Fica a Contratada obrigada a apresentar memória de cálculo referente ao reajustamento de preços do valor remanescente, sempre que este ocorrer.

13.5. Nas aferições finais, o índice utilizado para reajuste será, obrigatoriamente, o definitivo.

13.6. Caso o índice estabelecido para reajustamento venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado, em substituição, o que vier a ser determinado pela legislação em vigor.

13.7. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial para reajustamento do preço do valor remanescente, por meio de termo aditivo.

13.8. O reajuste será realizado por apostilamento.

14. CONSIDERAÇÕES FINAIS

14.1. O presente Termo de Referência foi elaborado com base no pedido de aquisição feito pelo setor de Informática do CRCMS (área demandante), sendo que o "de acordo" do representante da referida área neste Termo implica a integral concordância, sem restrições, com todas as condições e especificações aqui definidas, o qual, inclusive, assume como se fossem suas quaisquer alterações feitas neste documento em relação ao citado pedido de aquisição.

Campo Grande/MS, 12 de agosto de 2024

Wesley de Araujo Vieira
Encarregado do Setor de Informática

De acordo.

Face o exposto acima, aprovo o presente termo de referência.

Contador Otacílio dos Santos Nunes
Presidente do CRCMS

Documento assinado eletronicamente por **Wesley De Araujo Vieira**, **Encarregado**, em 12/08/2024, às 16:52, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Otacílio dos Santos Nunes**, **Presidente**, em 13/08/2024, às 09:43, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.cfc.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0452271** e o código CRC **30DFF9B1**.