CONTRATO Nº 05/2023-UA IMBEL

O ORIGINAL DESTE CONTRATO ENCONTRA-SE ARQUIVADO NA SALCP/UA IMBEL

PROCESSO ADMINISTRATIVO N° 128/2023-UA IMBEL

REFERÊNCIA: PREGÃO ELETRÔNICO N° 01/2023-SRP/UA IMBEL

VALOR GLOBAL: R$ 29.736,00

VIGÊNCIA: 03/05/2023 A 02/05/2026

CONTRATO CELEBRADO ENTRE A INDÚSTRIA DE MATERIAL BÉLICO DO BRASIL – IMBEL/SEDE E A EMPRESA E-SEC TECNOLOGIA EM SEGURANÇA DE DADOS LTDA, PARA O FORNECIMENTO DE LICENÇA DE DIREITOS DE USO DO SOFTWARE KASPERSKY ENDPOINT SECURITY – ADVANCED, COM GARANTIA E SUPORTE PARA 36 (TRINTA E SEIS) MESES.

A **INDÚSTRIA DE MATERIAL BÉLICO DO BRASIL - IMBEL,** Empresa Pública Federal, vinculada ao Ministério da Defesa, por intermédio do Comando do Exército, constituída pela Lei nº 6.227, de 14/07/1975, com seu Estatuto Social aprovado pela Assembleia Geral Extraordinária nº 04/2020, realizada em 14/12/2020, registrada perante a Junta Comercial, Industrial e Serviços do Distrito Federal - JUCISDF, em 15/01/2021, conforme NIRE 53500000275 e sob nº 1646051, publicado no Diário Oficial da União - DOU, Seção I, página 23 a 28, de 19/01/2021, arquivado e publicado na JUCISDF sob nº 1650189, em 27/01/2021, regida pela Lei nº 13.303, de 30/06/2016, Lei nº 6.404, de 15/12/1976, Decreto nº 8.945, de 27/12/2016, e demais legislações aplicáveis, classificada como Empresa Pública Dependente, nos termos do art. 2º, III, da Lei Complementar nº 101, de 04/05/2000 e da Portaria nº 289, de 29/05/2008, da Secretaria do Tesouro Nacional - STN, publicada no DOU, Seção I, de 30/05/2008, com capital integralmente subscrito pela UNIÃO, inscrita no CNPJ/MF sob n° 00.444.232/0001-39, com SEDE e foro na cidade de Brasília - Distrito Federal, localizada no Quartel General do Exército, Bloco “H”, 3°

Pavimento, Setor Militar Urbano - SMU, Brasília - Distrito Federal, CEP 70630-901, denominada **CONTRATANTE,** ou simplesmente **IMBEL**, neste ato representada, na forma do seu Estatuto, pelo Sr **E.X.C**, Ordenador de Despesas, brasileiro, portador da Carteira de Identidade nº **568** SSP/DF, inscrito no CPF sob o nº ***.178.581-**, que no final assina, e de outro lado a Empresa **E-SEC TECNOLOGIA EM SEGURANÇA DE DADOS LTDA**, pessoa jurídica de direito privado, inscrita no CNPJ sob o nº 03.242.841/0001-01, localizada no SHS, Quadra 06, Brasil 21, Bloco A, Sala 501, Asa Sul, Brasília-DF, CEP 90316-12, denominada **CONTRATADA**, neste ato representada pelo Sr **L. DA S. C.**, Diretor de Tecnologia, brasileiro, portador da Carteira de Identidade nº *.377.*** SSP/DF, inscrito no CPF sob o n° ***.892.271-** e pelo Sr **R. DE A. S.**, Diretor Executivo, brasileiro, portador da Carteira de Identidade nº *.191.0** SSP/DF, inscrito no CPF sob o n° ***.171.621-**, consoante o que consta o Processo Administrativo n° 000128/2023-UA **IMBEL**, referente Pregão Eletrônico nº 01/2023-SRP/UA **IMBEL**, resolvem celebrar o presente contrato, que será regido pelo Termo de Referência e pela proposta da **CONTRATADA**, no que couber, independentemente de suas expressas transcrições, pelo Decreto nº 8.945/2016, de 27 de dezembro de 2016, pela Lei nº 13.303/2016, pelo Regulamento de Licitações e Contratos da **IMBEL**, aprovado na 305ª Reunião do Conselho de Administração da **IMBEL**, ocorrida em 22/05/2018, conforme Resolução nº 06/2018-CA-**IMBEL, de 22/05/2018,** e pelas cláusulas e condições a seguir dispostas:

CLÁUSULA PRIMEIRA - DO OBJETO

Licença de direitos de uso do Software Kaspersky Endpoint Security – Advanced, com garantia e suporte para 36 (trinta e seis) meses, conforme condições, quantidades e exigências estabelecidas no Termo de Referência e na Proposta da **CONTRATADA**.

CLÁUSULA SEGUNDA - DO PRAZO DE ENTREGA DO OBJETO

O prazo de entrega do objeto será de até 30 (trinta) dias corridos a partir do dia útil imediato ao da assinatura deste contrato.

CLÁUSULA TERCEIRA - DA FORMA DE PAGAMENTO

3.1. O pagamento pelo serviço efetivamente prestado será efetuado em até 30 (trinta) dias após a entrega da Nota Fiscal/Fatura correspondente.

3.2. Na ocorrência de erros na(s) Nota(s) Fiscal(is) do(s) Serviço(s)/Fatura(s) ou situação que impeça a liquidação da despesa, aquela(s) será(ão) devolvidas(s) e o pagamento ficará pendente até que as medidas saneadoras sejam providenciadas pela **CONTRATADA**.

3.3. Na hipótese acima mencionada, a contagem do prazo para pagamento será iniciada após a correção dos erros identificados e reapresentação da(s) Nota(s) Fiscal(is) do(s) Serviço(s)/Fatura(s), não acarretando qualquer ônus para a **CONTRATANTE**.

3.4. O pagamento será efetuado em favor da **CONTRATADA** através de ordem bancária, devendo para isso ficar explicitado o nome da instituição financeira recebedora, agência, localidade, número da operação, quando for o caso, e número da conta corrente na qual deverá ser depositado o crédito, que ocorrerá após mediante a aceitação e atesto na(s) Nota(s) Fiscal(is) do(s) Serviço(s)/Fatura(s), pelo fiscal do contrato em até 3 (três) dias úteis.

3.5. Será realizada consulta "*ON LINE*" ao Sistema de Cadastro de Fornecedores - SICAF antes do pagamento a ser efetuado a **CONTRATADA**, para a verificação de sua situação, no que diz respeito às condições exigidas para contratação, cujo resultado será impresso e juntado aos autos processuais próprios.

3.6. Constada a não regularidade junto ao SICAF, a **CONTRATADA** será acionada para que no prazo de 5 (cinco) dias úteis regularize a sua situação, contados da data da notificação.

3.7. Não sendo regularizada a situação no prazo acima estabelecido, o contrato poderá ser rescindido e a **CONTRATADA** sujeita às multas estabelecidas.

3.8. Dos pagamentos devidos à **CONTRATADA** serão descontados os impostos e contribuições de acordo com os ditames estabelecidos na legislação de regência.

3.9. O pagamento somente será efetuado quando do recolhimento de eventuais multas que tenham sido impostos à **CONTRATADA** em decorrência de inadimplemento contratual.

3.10. A **IMBEL** reserva-se o direito de suspender o pagamento caso os serviços sejam entregues em desacordo com este contrato.

3.11. No caso de eventuais atrasos de pagamento provocados exclusivamente pela **IMBEL**, o valor devido deverá ser acrescido de atualização financeira e a sua apuração se fará desde a data do vencimento da fatura até a data do efetivo pagamento, em que os juros de mora serão calculados à taxa de 0,5% (meio por cento) ao mês, ou 6% (seis por cento) ao ano, mediante a aplicação da seguinte fórmula:

$$I = \frac{\left(\frac{TX}{100}\right)}{365}$$

EM = I x N x VP, onde:

I = Índice de atualização financeira.

TX = Percentual da taxa de juros de mora anual.

EM = Encargos moratórios.

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento.

VP = Valor da parcela em atraso.

3.12. Em hipótese alguma será admitida antecipação do pagamento.

CLÁUSULA QUARTA - DO REGIME DE EXECUÇÃO

O objeto do presente contrato será executado pela **CONTRATADA** sob o regime de execução da forma indireta de empreitada por preço unitário.

CLÁSULA QUINTA - REQUISITOS TÉCNICOS

5.1. Licença de direitos de uso do software Kaspersky Endpoint Security – Advanced pelo período de 36 (trinta e seis) meses.

5.2. A solução de antivírus deve apresentar o modelo cliente/servidor, com uma gerência centralizada e hierarquizada, dentro da infraestrutura da **IMBEL**, normalmente caracterizada pelo termo on-premise. Não será aceita a administração/gerência do parque computacional da **IMBEL** na nuvem da fabricante.

5.3. Todas as licenças de software da solução de antivírus são perpétuas, ou seja, expirado o período de validade da licença, o software deverá permanecer funcional para a proteção contra códigos maliciosos, excetuando-se as atualizações. Dessa forma, serão aceitas reduções nas funcionalidades após a expiração das licenças, contanto que a proteção contra código maliciosos e o gerenciamento da solução continuem ativos na solução de antivírus, usando os softwares e base de assinaturas que a **IMBEL** possuir ao final do período de validade.

SERVIDOR DE ADMINISTRAÇÃO E CONSOLE DE GERENCIAMENTO COMPATIBILIDADE:

5.4. Microsoft Windows Server 2016 Standard / Core / Datacenter x64.

5.5. Microsoft Windows Server 2019 Standard / Core / Datacenter x64.

5.6. Microsoft Windows Server 2022 Standard / Core / Datacenter x64.

5.7. SUPORTA AS SEGUINTES PLATAFORMAS VIRTUAIS

5.8. Vmware: Workstation 15.x Pro, vSphere 6.5, vSphere 6.7.

5.9. Microsoft Hyper-V: 2012, 2012 R2, 2016 x64, 2019 x64, 2022 x64.

CARACTERÍSTICAS:

5.10. A console deve ser acessada via web (https) ou mmc.

5.11. A console deve suportar arquitetura on-premise e arquitetura cloud-based.

5.12. Console deve ser baseada no modelo cliente/servidor.

5.13. A console deve suportar autênticação de dois fatores.

5.14. Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade.

5.15. Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus.

5.16. Deve permitir incluir usuários do AD para logarem no console de administração.

5.17. Console deve ser totalmente integrada com suas funções e módulos caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, Patch management e MDM.

5.18. As licenças deverão ser perpétuas, ou seja, expirado a validade da mesma o produto deverá permanecer funcional para a proteção contra códigos maliciosos utilizando as definições até o momento da expiração da licença.

5.19. Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores.

5.20. Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, através da console de gerenciamento e GPO de AD.

5.21. Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria.

5.22. Deve armazenar histórico das alterações feitas em políticas.

5.23. Deve permitir voltar para uma configuração antiga da política de acordo com o histórico de alterações efetuadas pelo administrador apenas selecionando a data em que a política foi alterada.

5.24. Deve ter a capacidade de comparar a política atual com a anterior, informando quais configurações foram alteradas.

5.25. A solução de gerencia deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas.

5.26. Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador.

5.27. A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle.

5.28. Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por sub-rede com os seguintes parâmetros: KB/s e horário.

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

5.30. Capacidade de gerenciar smartphones e tablets (Android e iOS) protegidos pela solução de segurança.

5.31. Capacidade de instalar atualizações em computadores de teste antes de instalar nos demais computadores da rede.

5.32. Capacidade de gerar pacotes customizados (auto executáveis) contendo a licença e configurações do produto.

5.33. Capacidade de atualizar os pacotes de instalação com as últimas vacinas.

5.34. Capacidade de fazer distribuição remota de qualquer software, ou seja, deve ser capaz de remotamente enviar qualquer software pela estrutura de gerenciamento de antivírus para que seja instalado nas máquinas clientes.

5.35. A comunicação entre o cliente e o servidor de administração deve ser criptografada.

5.36. Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes.

5.37. Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado utilizando os seguintes parâmetros:

5.38. Nome do computador;

5.39. Nome do domínio;

5.40. Range de IP;

5.41. Sistema Operacional; e

5.42. Máquina virtual.

5.43. Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas.

5.44. Deve ter a capacidade de descobrir novos dispositivos na rede, utilizando as seguintes técnicas:

5.45. Pesquisa de rede (Windows pooling);

5.46. Pesquisa ativa do AD (AD pooling);

5.47. Pesquisa de IP (IP pooling); e

5.48. Pesquisa de rede (Zeroconf pooling).

5.49. Deve permitir, por meio da console de gerenciamento, extrair um artefato em quarentena de um cliente sem a necessidade de um servidor ou console de quarentena adicional.

5.50. Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas à proteção.

5.51. Capacidade de monitorar grupos de trabalhos já existentes e quaisquer grupos de trabalho

que forem criados na rede, a fim de encontrar máquinas novas para serem adicionadas a proteção.

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

5.53. Capacidade de agrupamento de máquina por características comuns entre as mesmas, por exemplo: agrupar todas as máquinas que não tenham o antivírus instalado, agrupar todas as máquinas que não receberam atualização nos últimos 2 dias, etc.

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

5.55. Deve fornecer as seguintes informações dos computadores:

5.56. Se o antivírus está instalado;

5.57. Se o antivírus está iniciado;

5.58. Se o antivírus está atualizado;

5.59. Minutos/horas desde a última conexão da máquina com o servidor administrativo;

5.60. Minutos/horas desde a última atualização de vacinas;

5.61. Data e horário da última verificação executada na máquina;

5.62. Versão do antivírus instalado na máquina;

5.63. Se é necessário reiniciar o computador para aplicar mudanças;

5.64. Data e horário de quando a máquina foi ligada;

5.65. Quantidade de vírus encontrados (contador) na máquina;

5.66. Nome do computador;

5.67. Domínio ou grupo de trabalho do computador;

5.68. Data e horário da última atualização de vacinas;

5.69. Sistema operacional com Service Pack;

5.70. Quantidade de processadores;

5.71. Quantidade de memória RAM;

5.72. Sessões de usuários, com informações de contato (caso disponíveis no Active Directory);

5.73. Endereço IP;

5.74. Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido;

5.75. Informação completa de hardware contendo: processadores, memória, adaptadores de

vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD;

5.76. Vulnerabilidades de aplicativos instalados na máquina; e

5.77. Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las.

5.78. Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:

5.79. Alteração de Gateway Padrão;

5.80. Alteração de sub-rede;

5.81. Alteração de domínio;

5.82. Alteração de servidor DHCP;

5.83. Alteração de servidor DNS;

5.84. Alteração de servidor WINS;

5.85. Alteração de sub-rede;

5.86. Resolução de Nome; e

5.87. Disponibilidade de endereço de conexão SSL.

5.88. Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet.

5.89. Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes.

5.90. Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus.

5.91. A console de gerenciamento deve suportar funções de controle de acesso com base na função (RBAC) para a hierarquia de servidores.

5.92. Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos.

5.93. Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede.

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

5.95. Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML.

5.96. Capacidade de monitoramento do sistema através de um SNMP client.

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

5.98. Listar em um único local, todos os computadores não gerenciados na rede.

5.99. Deve encontrar computadores na rede através de no mínimo três formas: Domínio, Active Directory e sub-rede.

5.100. Deve possuir compatibilidade com Microsoft NAP, quando instalado em um Windows 2008 Server.

5.101. Capacidade de baixar novas versões do antivírus direto pela console de gerenciamento, sem a necessidade de importá-los manualmente.

5.102. Capacidade de ligar máquinas via Wake on Lan para realização de tarefas (varredura, atualização, instalação, etc), inclusive de máquinas que estejam em subnets diferentes do servidor.

5.103. Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo).

5.104. Deve através de opções de optimizações fazer com que o computador gerenciado conceda recursos à outras aplicações, mantendo o antivírus ativo, porém sem comprometer o desempenho do computador.

5.105. Deve permitir a configuração de senha no endpoint e configurar quando que será necessário a utilizá-la, (ex: Solicitar senha quando alguma tarefa de scan for criada localmente no endpoint).

5.106. Deve ser capaz de configurar quais eventos serão armazenados localmente, nos eventos do Windows ou ainda se serão mostrados na tela para o colaborador, sejam estes eventos informativos, de alertas ou de erros.

5.107. Capacidade de realizar atualização incremental de vacinas nos computadores clientes.

5.108. Deve armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo:

5.109. Nome do vírus;

5.110. Nome do arquivo infectado;

5.111. Data e hora da detecção;

5.112. Nome da máquina ou endereço IP; e

5.113. Ação realizada.

5.114. Capacidade de reportar vulnerabilidades de softwares presentes nos computadores.

5.115. Capacidade de listar updates nas máquinas com o respectivo link para download.

5.116. Deve criar um backup de todos arquivos deletados em computadores durante a desinfecção para que possam ser restaurados.

5.117. Deve ter uma quarentena na própria console de gerenciamento, permitindo baixar um artefato ou enviar direto para análise do fabricante.

5.118. Capacidade de realizar resumo de hardware de cada máquina cliente.

5.119. Capacidade de realizar resumo de hardware de cada máquina cliente.

5.120. Capacidade de diferenciar máquinas virtuais de máquinas físicas.

ESTAÇÕES WINDOWS E COMPATIBILIDADE:

5.121. Microsoft Windows 8 Professional/Enterprise x86 / x64;

5.122. Microsoft Windows 8.1 Professional / Enterprise x86 / x64;

5.123. Microsoft Windows 10 Pro / Enterprise / Home / Education x86 / x64;

5.124. Microsoft Windows 11 Pro / Enterprise / Home / Education x86 / x64;

5.125. Microsoft Windows Server 2022 Essentials / Standard / Datacenter;

5.126. Microsoft Windows Server 2019 Essentials / Standard / Datacenter; e

5.127. Microsoft Windows Server 2016 Essentials / Standard / Datacenter;

CARACTERÍSTICAS:

5.128. Deve prover as seguintes proteções:

5.129. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

5.130. Antivírus de Web (módulo para verificação de sites e downloads contra vírus);

5.131. Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos);

5.132. O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza;

5.133. Firewall com IDS;

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

5.135. Controle de dispositivos externos;

5.136. Controle de acesso a sites por categoria, ex: Bloquear conteúdo adulto, sites de jogos, etc;

5.137. Controle de acesso a sites por horário;

5.138. Controle de acesso a sites por usuários;

5.139. Controle de acesso a websites por dados, ex: Bloquear websites com conteúdo de vídeo e áudio;

5.140. Controle de execução de aplicativos;

5.141. Controle de vulnerabilidades do Windows e dos aplicativos instalados;

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

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

5.144. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;

5.145. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado;

5.146. Capacidade de adicionar aplicativos a uma lista de "aplicativos confiáveis", onde as atividades de rede, atividades de disco e acesso ao registro do Windows não serão monitoradas;

5.147. Deverá possuir módulo dedicado para proteção contra port scanning;

5.148. Deverá possuir módulo dedicado para proteção contra network flooding;

5.149. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);

5.150. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

5.151. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo; e

5.152. Ter a capacidade de fazer detecções por comportamento, identificando ameaças avançadas sem a necessidade de assinaturas.

5.153. Ao detectar uma ameaça, a solução deve exibir informações:

5.154. Do objeto SHA256; e

5.155. Do objeto MD5.

5.156. Capacidade de verificar somente arquivos novos e alterados.

5.157. Capacidade de verificar objetos usando heurística.

5.158. Capacidade de agendar uma pausa na verificação.

5.159. Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias.

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

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

5.162. Perguntar o que fazer, ou;

5.163. Bloquear acesso ao objeto.

5.164. Apagar o objeto ou tentar desinfetá-lo (de acordo com a configuração pré-estabelecida pelo administrador).

5.165. Caso positivo de desinfecção:

5.166. Restaurar o objeto para uso.

5.167. Caso negativo de desinfecção:

5.168. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

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

5.170. Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, POP3S, IMAP, NNTP, SMTP e MAPI;

5.171. Capacidade de verificar links inseridos em e-mails contra phishings;

5.172. Capacidade de verificar tráfego nos browsers: Internet Explorer, Firefox, Google Chrome e Opera; e

5.173. Capacidade de verificação de corpo e anexos de e-mails usando heurística.

5.174. O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve:

5.175. Perguntar o que fazer, ou;

5.176. Bloquear o e-mail.

5.177. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador).

5.178. Caso positivo de desinfecção:

5.179. Restaurar o e-mail para o usuário.

5.180. Caso negativo de desinfecção:

5.181. Mover para quarentena ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador);

5.182. Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados;

5.183. Capacidade de filtrar anexos de e-mail, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador;

5.184. Capacidade de verificação de tráfego HTTP/HTTPS e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc), usando heurísticas; e

5.185. Capacidade de alterar as portas monitoradas pelos módulos de Web e E-mail.

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

5.187. Perguntar o que fazer, ou;

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

5.189. Permitir acesso ao objeto.

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

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

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

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

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

5.195. Deve possuir módulo que analise qualquer tentativa de edição, exclusão ou gravação do registro, de forma que seja possível escolher chaves específicas para serem monitoradas e/ou bloqueadas.

5.196. Deve possuir módulo de bloqueio de Phishing, com atualizações incluídas nas vacinas, obtidas pelo Anti-Phishing Working Group (http://www.antiphishing.org/).

5.197. Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica.

5.198. Deve possuir módulo IDS (Intrusion Detection System) para proteção contra port scans e exploração de vulnerabilidades de softwares. A base de dados de análise deve ser atualizada juntamente com as vacinas.

5.199. Deve permitir a importação e exportação de listas de regras e exclusões para as aplicações no formato XML.

5.200. Deve permitir a criação de zonas confiáveis locais independentes por parte do usuário.

5.201. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:

5.202. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas; e

5.203. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de

aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.

5.204. Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:

5.205. Discos de armazenamento locais;

5.206. Armazenamento removível;

5.207. Impressoras;

5.208. CD/DVD;

5.209. Drives de disquete;

5.210. Modems;

5.211. Dispositivos de fita;

5.212. Dispositivos multifuncionais;

5.213. Leitores de smart card;

5.214. Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile, etc);

5.215. Wi-Fi;

5.216. Adaptadores de rede externos;

5.217. Dispositivos MP3 ou smartphones;

5.218. Dispositivos Bluetooth;

5.219. Câmeras e Scanners;

5.220. Capacidade de liberar acesso a um dispositivo e usuários por um período de tempo específico, sem a necessidade de desabilitar a proteção e o gerenciamento central ou de intervenção local do administrador na máquina do usuário;

5.221. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário;

5.222. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento;

5.223. Deve permitir controlar o acesso a dispositivos externos com base em prioridade de regras; e

5.224. Capacidade de habilitar “logging” em dispositivos removíveis tais como Pendrive, Discos externos, etc.

5.225. Capacidade de configurar novos dispositivos por Class ID/Hardware ID.

5.226. Capacidade de limitar a execução de aplicativos por hash MD5, nome do arquivo, versão do arquivo, nome do aplicativo, versão do aplicativo, fabricante/desenvolvedor, categoria (ex: navegadores, gerenciador de download, jogos, aplicação de acesso remoto, etc).

5.227. O controle de aplicações deve ter a capacidade de criar regras seguindo os seguintes modos de operação:

5.228. Black list: Permite a execução de qualquer aplicação, exceto pelas especificadas por regras.

5.229. White list: Impede a execução de qualquer aplicação, exceto pelas especificadas por regras.

5.230. Capacidade de bloquear execução de aplicativo que está em armazenamento externo.

5.231. Capacidade de limitar o acesso dos aplicativos a recursos do sistema, como chaves do registro e pastas/arquivos do sistema, por categoria, fabricante ou nível de confiança do aplicativo.

5.232. Capacidade de, em caso de epidemia, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web.

5.233. Capacidade de, caso o computador cliente saia da rede corporativa, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web.

5.234. Capacidade de voltar ao estado anterior do sistema operacional após um ataque de malware.

5.235. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros.

5.236. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).

5.237. Capacidade de integração com o Windows Defender Security Center.

5.238. Capacidade de integração com a Anti-malware Scan Interface (AMSI).

5.239. Deve permitir sincronização com soluções de terceiros por meio de API.

5.240. Deve permitir o gerenciamento remoto da solução por meio de aplicativos de administração remota.

ESTAÇÕES MAC OS X E COMPATIBILIDADE:

5.241. macOS Catalina 10.15;

5.242. macOS Mojave 10.14;

5.243. masOS High Sierra 10.13;

5.244. macOS Sierra 10.12; e

5.245. macOS 11.0 Big Sur.

CARACTERÍSTICAS:

5.246. Deve prover proteção residente para arquivos (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

5.247. Possuir módulo de web-antivírus para proteger contra ameaças durante navegação na internet com possibilidade de analisar endereços https;

5.248. Possuir módulo de bloqueio á ataques na rede;

5.249. Possibilidade de bloquear a comunicação entre a máquina atacante e os demais computadores por tempo definido pelo administrador;

5.250. Capacidade de criar exclusões para computadores que não devem ser monitorados pelo módulo de bloqueio à ataques na rede;

5.251. Possibilidade de importar uma chave no pacote de instalação;

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

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

5.254. Capacidade de voltar para a base de dados de vacina anterior;

5.255. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;

5.256. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);

5.257. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;

5.258. Capacidade de verificar somente arquivos novos e alterados;

5.259. Capacidade de verificar objetos usando heurística; e

5.260. Capacidade de agendar uma pausa na verificação.

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

5.262. Perguntar o que fazer, ou;

5.263. Bloquear acesso ao objeto; e

5.264. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador).

5.265. Caso positivo de desinfecção:

5.266. Restaurar o objeto para uso.

5.267. Caso negativo de desinfecção:

5.268. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador).

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

5.270. Capacidade de verificar arquivos de formato de e-mail.

5.271. Possibilidade de trabalhar com o produto pela linha de comando, com no mínimo opções para atualizar as vacinas, iniciar uma varredura, para o antivírus e iniciar o antivírus pela linha de comando.

5.272. Capacidade de, através da mesma console central de gerenciamento:

5.273. Ser instalado;

5.274. Ser removido; e

5.275. Ser gerenciado.

ESTAÇÕES DE TRABALHO LINUX E COMPATIBILIDADE:

5.276. PLATAFORMA 32-BITS:

5.277. Ubuntu 22.04 LTS; e

5.278. Debian GNU / Linux 11.6.

5.279. PLATAFORMA 64-BITS:

5.280. Ubuntu 22.04 LTS; e

5.281. Debian GNU / Linux 11.6.

CARACTERÍSTICAS:

5.282. Deve prover as seguintes proteções:

5.283. Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado.

5.284. Deve permitir gerenciamento, no mínimo, das seguintes formas:

5.285. Via linha de comando;

5.286. Via console administrativa;

5.287. Via GUI; e

5.288. Via web (remotamente).

5.289. Deve possuir funcionalidade de scan de drives removíveis, tais como:

5.290. CDs;

5.291. DVDs;

5.292. Discos blu-ray;

5.293. Flash drives (pen drives);

5.294. HDs externos e

5.295. Disquetes.

5.296. Deve fornecer os seguintes controles para dispositivos externos conectados ao computador:

5.297. Por tipo de dispositivo,

5.298. Por barramento de conexão.

5.299. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.

5.300. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

5.301. Capacidade de criar exclusões por local, máscara e nome da ameaça;

5.302. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

5.303. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes; e

5.304. Detectar aplicações que possam ser utilizadas como vetor de ataque por hackers.

5.305. Fazer detecções através de heurística utilizando no mínimo as seguintes opções de nível:

5.306. Alta;

5.307. Média;

5.308. Baixa;

5.309. Recomendado;

5.310. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena; e

5.311. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.

5.312. Em caso erros, deve ter capacidade de criar *logs* automaticamente, sem necessidade de outros softwares.

5.313. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento.

5.314. Capacidade de verificar objetos usando heurística.

5.315. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena.

5.316. Deve fornecer análise de todo o tráfego HTTP/HTTPS/FTP que chegar no computador do usuário.

5.317. O módulo de análise de tráfego deve fornecer os seguintes componentes de proteção:

5.318. Detecção de phishing e sites maliciosos;

5.319. Bloqueio de download de arquivos maliciosos;

5.320. Bloqueio de adware;

5.321. Deve possuir módulo escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados; e

5.322. Deve fornecer a possibilidade de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

5.323. Deve possuir módulo de proteção contra criptografia maliciosa.

SERVIDORES WINDOWS COMPATIBILIDADE:

PLATAFORMA 32-BITS:

5.324. Windows Server 2022 Standard/Enterprise/Datacenter e posterior;

5.325. Windows Server 2019 Standard/Enterprise/Datacenter e posterior; e

5.326. Windows Server 2016 Standard/Enterprise/Datacenter e posterior;

PLATAFORMA 64-BITS:

5.327. Microsoft Windows Server 2016 Standard / Datacenter;

5.328. Microsoft Windows Server 2019 Standard / Datacenter;

5.329. Microsoft Windows Server 2022 Standard / Datacenter;

5.330. Microsoft Windows Storage Server 2012;

5.331. Microsoft Windows Hyper-V Server 2022;

5.332. Microsoft Windows Hyper-V Server 2019;

5.333. Windows Hyper-V Server 2016;

5.334. Windows Hyper-V Server 2019; e

5.335. Windows Hyper-V Server 2022.

CARACTERÍSTICAS:

5.336. Deve prover as seguintes proteções:

5.337. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

5.338. Auto-proteção contra-ataques aos serviços/processos do antivírus;

5.339. Firewall com IDS;

5.340. Controle de vulnerabilidades do Windows e dos aplicativos instalados; e

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

5.342. Deve permitir gerenciamento, no mínimo, das seguintes formas:

5.343. Via console administrativa;

5.344. Via web (remotamente); e

5.345. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.

5.346. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

5.347. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

5.348. Gerenciamento de tarefa (criar ou excluir tarefas de verificação);

5.349. Leitura de configurações;

5.350. Modificação de configurações;

5.351. Gerenciamento de Backup e Quarentena;

5.352. Visualização de logs;

5.353. Gerenciamento de logs;

5.354. Gerenciamento de ativação da aplicação;

5.355. Gerenciamento de permissões (adicionar/excluir permissões acima); e

5.356. Deve possuir bloqueio de inicialização de aplicativos baseado em whitelists.

5.357. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:

5.358. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas; e

5.359. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.

5.360. Capacidade de separadamente selecionar o número de processos que irão executar funções de varredura em tempo real, o número de processos que executarão a varredura sob demanda e o número máximo de processos que podem ser executados no total.

5.361. Bloquear malwares tais como Cryptlockers mesmo quando o ataque vier de um computador sem antivírus na rede.

5.362. Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros, etc).

5.363. Em caso de erros, deve ter capacidade de criar *logs* e *traces* automaticamente, sem necessidade de outros softwares.

5.364. Deve possuir funcionalidade de análise personalizada de logs do Windows.

5.365. Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor.

5.366. Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor.

5.367. Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas.

5.368. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação.

5.369. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado.

5.370. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo.

5.371. Capacidade de verificar somente arquivos novos e alterados.

5.372. Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários, etc.).

5.373. Capacidade de verificar objetos usando heurística.

5.374. Capacidade de configurar diferentes ações para diferentes tipos de ameaças.

5.375. Capacidade de agendar uma pausa na verificação.

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

5.377. Perguntar o que fazer, ou;

5.378. Bloquear acesso ao objeto.

5.379. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador).

5.380. Caso positivo de desinfecção:

5.381. Restaurar o objeto para uso.

5.382. Caso negativo de desinfecção:

5.383. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

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

5.385. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena; e

5.386. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados.

5.387. Em caso de detecção de sinais de uma infecção ativa, deve possuir capacidade de, automaticamente:

5.388. Executar os procedimentos pré-configurados pelo administrador; e

5.389. Em caso de ausência de procedimentos pré-configurados, criar tais procedimentos e executá-los.

5.390. Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa.

5.391. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros.

5.392. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).

5.393. Capacidade de bloquear a criptografia de arquivos em pastas compartilhadas, após a execução de um malware em um dispositivo que possua o mapeamento da pasta.

5.394. Deve possuir controle de dispositivos externos.

SERVIDORES LINUX COMPATIBILIDADE:

PLATAFORMA 32-BITS:

5.395. Ubuntu Server 22.04 LTS;

5.396. Debian GNU / Linux 11.6;

5.397. Debian GNU / Linux 10;

5.398. Debian GNU / Linux 9; e

5.399. Debian GNU / Linux 8.

PLATAFORMA 64-BITS:

5.400. Ubuntu Server 22.04 LTS;

5.401. Debian GNU / Linux 11.6;

5.402. Debian GNU / Linux 10;

5.403. Debian GNU / Linux 9; e

5.404. Debian GNU / Linux 8.

CARACTERÍSTICAS:

5.405. Deve prover as seguintes proteções:

5.406. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que

verifique qualquer arquivo criado, acessado ou modificado.

5.407. Deve permitir gerenciamento, no mínimo, das seguintes formas:

5.408. Via linha de comando;

5.409. Via console administrativa;

5.410. Via GUI;

5.411. Via web;

5.412. Deve possuir funcionalidade de scan de drives removíveis, tais como:

5.413. CDs;

5.414. DVDs;

5.415. Discos Blu-ray;

5.416. Flash drives;

5.417. HDs externos;

5.418. Disquetes;

5.419. Deve fornecer os seguintes controles para dispositivos externos conectados ao computador:

5.420. Por tipo de dispositivo; e

5.421. Por barramento de conexão.

5.422. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.

5.423. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas).

5.424. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes.

5.425. Gerenciamento de Quarentena: Deve bloquear objetos suspeitos.

5.426. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados).

5.427. Em caso erros, deve ter capacidade de criar *logs* automaticamente, sem necessidade de outros softwares.

5.428. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento.

5.429. Capacidade de verificar objetos usando heurística.

5.430. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados.

5.431. Fazer detecções através de heurística utilizando no mínimo as seguintes opções de nível:

5.432. Alta;

5.433. Média;

5.434. Baixa;

5.435. Recomendado; e

5.436. Deve fornecer análise de todo o tráfego HTTP/HTTPS/FTP que chegar no computador do usuário.

5.437. O módulo de análise de tráfego deve fornecer os seguintes componentes de proteção:

5.438. Detecção de phishing e sites maliciosos;

5.439. Bloqueio de download de arquivos maliciosos;

5.440. Bloqueio de adware; e

5.441. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

5.442. Deve possuir módulo de proteção contra criptografia maliciosa.

SMARTPHONES, TABLETS E COMPATIBILIDADE:

5.443. Android 10;

5.444. Android 11;

5.445. Android 12; e

5.446. Android 13.

CARACTERÍSTICAS:

5.447. Deve prover as seguintes proteções:

5.448. Proteção em tempo real do sistema de arquivos do dispositivo – interceptação e verificação de:

5.449. Proteção contra adware e autodialers;

5.450. Todos os objetos transmitidos usando conexões wireless (porta de infravermelho, Bluetooth) e mensagens EMS, durante sincronismo com PC e ao realizar download usando o browser;

5.451. Arquivos abertos no smartphone;

5.452. Programas instalados usando a interface do smartphone;

5.453. Verificação dos objetos na memória interna do smartphone e nos cartões de expansão sob demanda do usuário e de acordo com um agendamento;

5.454. Deverá isolar em área de quarentena os arquivos infectados;

5.455. Deverá atualizar as bases de vacinas de modo agendado; e

5.456. Capacidade de desativar por política: Wi-fi; Câmera; Bluetooth.

5.457. Deverá ter função de limpeza de dados pessoais a distância, em caso de roubo, por

exemplo.

5.458. Capacidade de requerer uma senha para desbloquear o dispositivo e personalizar a quantidade de caracteres para esta senha.

5.459. Deverá ter firewall pessoal (Android).

5.460. Capacidade de tirar fotos quando a senha for inserida incorretamente.

5.461. Capacidade de enviar comandos remotamente de:

5.462. Localizar; e

5.463. Bloquear.

5.464. Capacidade de detectar Root em dispositivos Android.

5.465. Capacidade de bloquear o acesso a site por categoria em dispositivos.

5.466. Capacidade de bloquear o acesso a sites phishing ou maliciosos.

5.467. Capacidade de configurar White e blacklist de aplicativos.

5.468. Capacidade de localizar o dispositivo quando necessário.

5.469. Permitir atualização das definições quando estiver em "roaming".

5.470. Capacidade de selecionar endereço do servidor para buscar a definição de vírus.

5.471. Capacidade de agendar uma verificação (Android).

5.472. Capacidade de enviar URL de instalação por e-mail.

5.473. Capacidade de fazer a instalação através de um link QRCode.

5.474. Capacidade de executar as seguintes ações caso a desinfecção falhe (Android):

5.475. Deletar;

5.476. Ignorar;

5.477. Quarentenar; e

5.478. Perguntar ao usuário.

GERENCIAMENTO DE DISPOSITIVOS MÓVEIS (MDM) – ANDROID COMPATIBILIDADE:

5.479. Android 10;

5.480. Android 11;

5.481. Android 12; e

5.482. Android 13.

5.483. SOFTWARES DE GERÊNCIA DE DISPOSITIVOS:

5.484. VMWare AirWatch 9.3;

5.485. MobileIron 10.0;

5.486. IBM Maas360 10.68;

5.487. Microsoft Intune 1908; e

5.488. SOTI MobiControl 14.1.4 (1693).

CARACTERÍSTICAS:

5.489. Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange;

5.490. Capacidade de ajustar as configurações de:

5.491. Sincronização de e-mail;

5.492. Uso de aplicativos;

5.493. Senha do usuário;

5.494. Criptografia de dados; e

5.495. Conexão de mídia removível.

5.496. Capacidade de instalar certificados digitais em dispositivos móveis.

5.497. Deve permitir configurar horário para sincronização do dispositivo com a console de gerenciamento.

5.498. Capacidade de desinstalar remotamente o antivírus do dispositivo.

5.499. Deve permitir fazer o upgrade do antivírus de forma remota sem a necessidade de desinstalar a versão atual.

5.500. Capacidade de sincronizar com Samsung Knox.

GERENCIAMENTO DE DISPOSITIVOS MÓVEIS (MDM) – IOS:

COMPATIBILIDADE:

5.501. Dispositivos com os sistemas operacionais:

5.502. iOS 13;

5.503. iOS 14;

5.504. iOS 15; e

5.505. iOS 16.

CARACTERÍSTICAS:

5.506. Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange;

5.507. Capacidade de ajustar as configurações de:

5.508. Sincronização de e-mail;

5.509. Senha do usuário;

5.510. Criptografia de dados;

5.511. Capacidade de instalar certificados digitais em dispositivos móveis;

5.512. Capacidade de instalar as ferramentas necessárias para o gerenciamento dos dispositivos

clientes através de:

5.513. Link por e-mail;

5.514. Link por mensagem de texto;

5.515. QR Code;

5.516. Capacidade de, remotamente, apagar todos os dados de dispositivos iOS; e

5.517. Capacidade de, remotamente, bloquear um dispositivo iOS.

CRIPTOGRAFIA E COMPATIBILIDADE

5.518. Microsoft Windows 8 Enterprise x86/x64;

5.519. Microsoft Windows 8 Pro x86/x64;

5.520. Microsoft Windows 8.1 Pro x86/x64;

5.521. Microsoft Windows 8.1 Enterprise x86/x64;

5.522. Microsoft Windows 10 Enterprise/Pro x86/x64; e

5.523. Microsoft Windows 11 Pro x86/x64.

5.524. CARACTERÍSTICAS:

5.525. O acesso ao recurso criptografado (arquivo, pasta ou disco) deve ser garantido mesmo em caso o usuário tenha esquecido a senha, através de procedimentos de recuperação;

5.526. Utilizar, no mínimo, algoritmo AES com chave de 256 bits;

5.527. Capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de pré-boot para autenticação do usuário;

5.528. Capacidade de utilizar *Single Sign-On* para a autenticação de pré-boot;

5.529. Permitir criar vários usuários de autenticação pré-boot;

5.530. Deve permitir que o usuário monitore a criptografia do disco ou o processo de descriptografia em tempo real; e

5.531. Capacidade de criar um usuário de autenticação pré-boot comum com uma senha igual para todas as máquinas a partir da console de gerenciamento.

5.532. Capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções:

5.533. Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes;

5.534. Criptografar todos os arquivos individualmente;

5.535. Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas;

5.536. Criptografar o dispositivo em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha; e

5.537. Capacidade de selecionar pastas e arquivos (por tipo, ou extensão) para serem criptografados automaticamente.

5.538. Capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados.

5.539. Capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados.

5.540. Verifica compatibilidade de hardware antes de aplicar a criptografia.

5.541. Possibilita estabelecer parâmetros para a senha de criptografia.

5.542. Capacidade de permitir o usuário solicitar permissão a determinado arquivo criptografado para o administrador mediante templates customizados.

5.543. Permite criar exclusões para não criptografar determinados "discos rígidos" através de uma busca por nome do computador ou nome do dispositivo.

5.544. Permite criptografar as seguintes pastas pré-definidas: "meus documentos", "Favoritos", "Desktop", "Arquivos temporários" e "Arquivos do Outlook".

5.545. Permite utilizar variáveis de ambiente para criptografar pastas customizadas.

5.546. Capacidade de criptografar arquivos por grupos de extensão, tais como: Documentos do office, Document, arquivos de áudio, etc.

5.547. Permite criar um grupo de extensões de arquivos a serem criptografados.

5.548. Capacidade de criar regra de criptografia para arquivos gerados por aplicações; e

5.549. Permite criptografia de dispositivos móveis mesmo quando o endpoint não possuir comunicação com a console de gerenciamento.

5.550. Capacidade de deletar arquivos de forma segura após a criptografia.

5.551. Capacidade de criptografar somente o espaço em disco utilizado.

5.552. Deve ter a opção de criptografar arquivos criados a partir de aplicações selecionadas pelo administrador.

5.553. Capacidade de bloquear aplicações selecionadas pelo administrador de acessarem arquivos criptografados.

5.554. Deve permitir criptografar somente o espaço utilizado em dispositivos removíveis tais como pendrives, HD externo, etc.

5.555. Capacidade de criptografar discos utilizando a criptografia BitLocker da Microsoft.

5.556. Deve ter a opção de utilização de TPM para criptografia através do BitLocker.

5.557. Capacidade de fazer "Hardware encryption".

GERENCIAMENTO DE SISTEMAS

5.558. Capacidade de criar imagens de sistema operacional remotamente e distribuir essas

imagens para computadores gerenciados pela solução e para computadores *bare-metal*.

5.559. Deve possibilitar a utilização de servidores PXE na rede para deploy de imagens.

5.560. Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares vulneráveis.

5.561. Capacidade de corrigir as vulnerabilidades de softwares, fazendo o download centralizado da correção ou atualização e aplicando essa correção ou atualização nas máquinas gerenciadas de maneira transparente para os usuários.

5.562. Capacidade de gerenciar licenças de softwares de terceiros.

5.563. Capacidade de atualizar informações sobre hardware presente nos relatórios após mudanças de hardware nas máquinas gerenciadas.

5.564. Capacidade de gerenciar um inventário de hardware, com a possibilidade de cadastro de dispositivos (ex: router, switch, projetor, acessório, etc).

5.565. Possibilita fazer distribuição de software de forma manual e agendada.

5.566. Suporta modo de instalação silenciosa.

5.567. Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis.

5.568. Possibilita fazer a distribuição através de agentes de atualização.

5.569. Utiliza tecnologia multicast para evitar tráfego na rede.

5.570. Possibilita criar um inventário centralizado de imagens.

5.571. Capacidade de atualizar o sistema operacional direto da imagem mantendo os dados do usuário.

5.572. Suporte a Wake On Lan para deploy de imagens.

5.573. Capacidade de atuar como servidor de atualização do Windows podendo fazer deploy de patches.

5.574. Suporta modo de teste, podendo atribuir alguns computadores para receberem as atualizações de forma automática para avaliação de alterações no comportamento.

5.575. Capacidade de gerar relatórios de vulnerabilidades e patches.

5.576. Possibilita criar exclusões para aplicação de patch por tipo de sistema operacional, Estação de trabalho e Servidor ou por grupo de administração.

5.577. Permite iniciar instalação de patch e correções de vulnerabilidades ao reiniciar ou desligar o computador.

5.578. Permite baixar atualizações para o computador sem efetuar a instalação.

5.579. Permite o administrador instalar somente atualizações aprovadas, instalar todas as atualizações (exceto as bloqueadas) ou instalar todas as atualizações incluindo as bloqueadas.

5.580. Capacidade de instalar correções de vulnerabilidades de acordo com a severidade.

5.581. Permite selecionar produtos a serem atualizados pela console de gerenciamento.

5.582. Permite selecionar categorias de atualizações para serem baixadas e instaladas, tais como: atualizações de segurança, ferramentas, drivers, etc.

5.583. Capacidade de adicionar caminhos específicos para procura de vulnerabilidades e updates em arquivos.

5.584. Capacidade de instalar atualizações ou correções somente em computadores definidos, em grupos definidos ou em uma porcentagem de computadores conforme selecionado pelo administrador.

5.585. Capacidade de configurar o reinicio do computador após a aplicação das atualizações e correções de vulnerabilidades.

5.586. Deve permitir selecionar o idioma das aplicações que serão atualizadas.

5.587. Permitir agendar o sincronismo entre a console de gerenciamento e os sites da Microsoft para baixar atualizações recentes.

CLÁUSULA SEXTA - DAS CONDIÇÕES DA GARANTIA DE FUNCIONAMENTO

6.1. A garantia de funcionamento da solução é de 36 (trinta e seis) meses, podendo ser prorrogado por igual e sucessivo período, até o limite de 60 (sessenta) meses. A decisão pela escolha de 36 (trinta e seis) meses de vigência teve por base a economicidade em escala, uma vez que os fornecedores reduzem o preço unitário ofertado para demandas/períodos maiores.

6.2. A garantia de funcionamento incluirá serviços de suporte técnico, manutenção e atualização (upgrade e update) da solução de antivírus corporativa, a substituição de quaisquer produtos defeituosos que compõem a solução – tudo sem qualquer ônus adicional para a **IMBEL**.

6.3. A garantia de funcionamento compreenderá, ainda, serviços como correção de erros e falhas no software, o que inclui o recebimento de correções (patches, hotfixes, service packs etc.) de toda a solução, cujas correções serão feitas pela fabricante, sem ônus adicional, conforme Acórdão n.2569/2018 – TCU – Plenário.

6.4. O suporte técnico deverá ser prestado em idioma local (Brasil/português) ou com tradução simultânea.

6.5. O suporte técnico incluirá o acesso, livre de qualquer ônus ou restrição, à base de dados de problema e soluções do fabricante.

6.6. Serão fornecidas as seguintes informações para abertura de chamados de suporte técnico junto ao fabricante:

6.6.1. Identificação do software afetado, incluindo versão;

6.6.2. Problema observado; e

6.6.3. Nome e contato do responsável pela solicitação do serviço, por parte do órgão responsável.

6.7. Nível de severidade do chamado, de acordo com a tabela a seguir:

GRAU DE SEVERIDADE	DESCRIÇÃO
Alta	Incidente urgente. Existe alto impacto no uso da solução no ambiente de produção e há o comprometimento do funcionamento dos trabalhos da organização. Não há solução de contorno.
Média	Incidente em que existe alto impacto no uso da solução no ambiente de produção, mas não há comprometimento do funcionamento por completo dos trabalhos da organização. Pode haver solução de contorno.
Baixa	Incidente em que existe baixo impacto no uso da solução no ambiente de produção e não há comprometimento nos trabalhos da organização. Esclarecimento de dúvidas sobre as funcionalidades do software. Implantação de novas funcionalidades.

6.8. A definição da gravidade do chamado de suporte técnico é prerrogativa da **CONTRATANTE**.

6.9. Cada chamado técnico aberto pela **CONTRATANTE** será registrado pela **CONTRATADA** em relatório específico, denominado Relatório Técnico, visando ao acompanhamento e controle da execução dos serviços.

6.10. Os prazos para início de atendimento dos chamados de suporte técnico serão de:

GRAU DE SEVERIDADE	PRAZO PARA ATENDIMENTO
Alta	4 horas úteis
Média	2 dias úteis
Baixa	5 dias úteis

6.11. Hora útil refere-se ao intervalo de sessenta minutos compreendido entre das 8h às 18h, em dias úteis, podendo começar num dia e terminar no outro (ex.: das 17h30 de uma sexta-feira às 08h30 da segunda-feira seguinte, conta-se apenas uma hora útil).

6.12. O cálculo de dias úteis é realizado com base na diferença entre a data/hora final e a data/hora inicial da contagem de prazo, considerando apenas os dias úteis e o horário de funcionamento da **IMBEL**. São excluídos da contagem sábados, domingos e feriados.

6.13. Excepcionalmente, mediante acordo prévio entre a **IMBEL**, a manutenção corretiva poderá ser realizada durante finais de semana e feriados, mantendo-se os prazos para o serviço

de manutenção.

CLÁUSULA SÉTIMA - DO VALOR DO CONTRATO

O valor global deste contrato, consoante o contido na proposta da **CONTRATADA**, é de R$ 29.736,00 (vinte e nove mil, setecentos e trinta e seis reais), conforme tabela a seguir:

ITEM	OBJETO	QTD	PREÇO UNT.	PREÇO TOTAL
1	Licença de direito de uso do Software Kaspersky Endpoint Security Advanced, com garantia para 36 meses	252	R$ 118,00	R$ 29.736,00

CLÁUSULA OITAVA - DA DOTAÇÃO ORÇAMENTÁRIA

A despesa orçamentária para a execução do presente contrato correrá por conta da Natureza de Despesas 449040, PI B1DIINVSTIC, FONTE 0100000000, descentralizada por meio da Nota de Crédito n° 2023NC000505, de 28 de abril de 2023.

CLÁUSULA NONA - DO PRAZO PARA EXECUÇÃO DO CONTRATO E DA PUBLICAÇÃO

9.1. O prazo execução do contrato se houver, será de 36 (trinta e seis) meses contados a partir do dia da sua assinatura.

9.2. A **IMBEL** providenciar a publicação resumida do contrato se houver, até o quinto dia útil do mês seguinte ao da sua assinatura de acordo com o § único do Art. 169 do Regulamento de Licitações e Contratos da **IMBEL**.

CLÁUSULA DÉCIMA - DO PREÇO

10.1. Nos preços cotados deverão estar inclusos todos os valores que os compõem, tais como impostos, taxas, frete e outros que incidam direta ou indiretamente no preço final.

10.2. Os preços a serem praticados neste contrato, são os constantes da tabela abaixo:

ITEM	ESPECIFICAÇÃO	UND	QTD	VALOR UNIT.	VALOR TOTAL
01	Licença de direitos de uso do Software Kaspersky Endpoint Security – Advanced, com garantia e suporte para 36 (trinta e seis) meses	Und.	252	R$ 118,00	R$ 29.736,00

10.3. Desde já fica empenhado o valor de R$ 29.736,00 (vinte e nove mil, setecentos e trinta e seis reais), referente à Nota de Empenho n° 2023NE000225, de 02 de maio de 2023.

CLÁUSULA DÉCIMA PRIMEIRA DAS OBRIGAÇÕES E DIREITOS DA CONTRATADA

11.1. Executar os serviços de acordo com as especificações exigidas e da proposta apresentada, bem como de cumprir todos os requisitos de acordo com as condições gerais e prazos para a execução do objeto assentados no Termo de Referência.

11.2. Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, no prazo fixado, os serviços efetuados e os materiais em que se verificarem vícios, defeitos ou incorreções resultantes da execução dos serviços ou dos materiais entregues.

11.3. Responsabilizar-se pelos vícios e danos decorrentes da execução dos serviços contratados e entrega do material, de acordo com os artigos 14 e 17 a 27 do Código de Defesa do Consumidor (Lei nº 8.078/90), ficando a **CONTRATANTE** autorizada a descontar do pagamento devido à **CONTRATADA** o valor correspondente aos danos por ela sofridos.

11.4. Utilizar, somente, de empregados habilitados e com conhecimentos básicos acerca dos serviços a serem executados, em conformidade com as normas e determinações vigentes.

11.5. Assumir e responsabilizar-se por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e todas as demais previstas na legislação vigente, cuja inadimplência não transfere responsabilidade à **CONTRATANTE**, como também por quaisquer danos que eventualmente venham a ser causados por seus empregados no que se refere aos serviços e o material entregue executados para consecução do objeto licitado.

11.6. Relatar à **CONTRATANTE** toda e qualquer ocorrência de irregularidade verificada no decorrer da prestação dos serviços para fins de correção.

11.7. Manter durante a execução deste contrato em compatibilidade com as obrigações assumidas, todas as condições de habilitação e de qualificações previstas neste Edital.

11.7.1. O descuprimento do item anterior poderá ensejar a rescisão do contrato e a instauração de processo administrativo.

11.8. Guardar sigilo sobre os dados cadastrais e todas as informações obtidas, sendo vedado, sob qualquer argumento, utilizá-las em benefício próprio, revelar, reproduzir ou delas dar conhecimento a terceiros, responsabilizando-se em caso de descumprimento, por eventuais perdas e danos, sujeitando-se às cominações legalmente estabelecidas.

11.9. Prestar todo e qualquer esclarecimento solicitado pela **IMBEL**, no que diz respeito ao objeto contratado.

11.10. Comunicar imediatamente à **CONTRATANTE**, por escrito, as dificuldades de qualquer ordem ou natureza que eventualmente surjam durante a execução do objeto.

11.11. Os serviços devem ser executados inobstante de contratempos internos enfrentados pela **CONTRATADA**.

11.12. Respeitar os preços máximos estabelecidos nas normas de regência de contratações públicas federais, a exemplo do Decreto nº 7983, de 8 de abril de 2013.

11.13. Cumprir das regras supramencionadas pela Administração por parte dos contratos pode ensejar a fiscalização do Tribunal de Contas da União e, após o devido processo legal, gerar as seguintes consequências:

11.13.1. Assinatura de prazo para a adoção das medidas necessárias ao exato cumprimento da Lei, nos termos do Art. 71, Inciso IX da Constituição; ou

11.13.2. Condenação dos agentes públicos responsáveis e da empresa contratada ao pagamento dos prejuízos ao erário, caso verificada a ocorrência de superfaturamento por sobrepreço na execução do contrato.

11.14. Solicitar atestado de capacidade técnica pelos serviços prestados e materiais entregues.

11.15. Receber o pagamento pelos materiais entregues e os serviços prestados.

CLÁUSULA DÉCIMA SEGUNDA DAS OBRIGAÇÕES E DIREITOS DO CONTRATANTE

12.1. Exigir o cumprimento de todas as obrigações assumidas pela **CONTRATADA**, de acordo com as cláusulas previstas neste instrumento e nos termos de sua proposta.

12.2. Notificar a **CONTRATADA**, por escrito, da ocorrência de eventuais imperfeições na execução do serviço ora contratados, fixando prazo para a sua correção.

12.3. Prestar as informações e os esclarecimentos que venham a ser solicitados pela **CONTRATADA** com relação ao objeto aqui tratado.

12.4. Proporcionar todas as condições para a execução do objeto, estabelecidas neste instrumento, permitindo, inclusive, o acesso aos técnicos, prepostos e/ou representantes da **CONTRATADA** às dependências da **CONTRATANTE**.

12.5. Rejeitar os serviços em desacordo com as condições estabelecidas em até 5 (cinco) dias úteis, contados a partir da entrega pela **CONTRATADA**, mediante Termo Circunstanciado celebrado entre os gestores dos entes signatários.

12.6. A **CONTRATANTE** somente deve considerar aceitos definitivamente os serviços entregues após o saneamento das irregularidades mencionadas no item anterior, o que deverá ser

atestado, mediante atesto em termo circunstanciado celebrado entre os gestores dos entes signatários.

12.7. Fornecer Termos de Capacidade Técnica sempre que requeridos, desde que cumpridas as obrigações previstas.

12.8. Pagar à **CONTRATADA** o valor resultante da prestação dos serviços nos prazos e nas condições aqui pactuados.

12.9. Proceder as retenções tributárias sobre o valor na Nota Fiscal/Fatura emitida pela **CONTRATADA**, sempre que devido.

12.10. Cumprir as demais obrigações previstas neste instrumento.

CLÁUSULA DÉCIMA TERCEIRA - DAS SANÇÕES ADMINISTRATIVAS E PENALIDADES

13.1. Cometer condutas reprováveis e passíveis de sancionamento, nos termos da Lei nº 13.303/16 e dos artigos 188 a 193 do Regulamento de Licitações e Contratos da **IMBEL**, de 22 de maio de 2018, a **CONTRATADA** que:

13.1.1. não atender, sem a devida e tempestiva justificativa, à convocação da **IMBEL** para assinatura da ata de registro de preços;

13.1.2. apresentar documento falso em qualquer em qualquer procedimento licitatório ou processo administrativo instaurado pela **IMBEL**;

13.1.3. frustrar ou fraudar, mediante ajuste, combinação ou qualquer outro expediente o processo de contratação, caracterizando má-fé na relação contratual;

13.1.4. incorrer em inexecução da ata de registro de preços; e

13.1.5. comportar-se de modo inidôneo.

13.2. Pela inexecução total ou parcial do objeto, a **IMBEL** pode aplicar à **CONTRATADA** as seguintes sanções:

13.2.1. Advertência - quando do ato praticado não acarretar prejuízo à **IMBEL**, suas instalações, seus integrantes, imagem, meio ambiente ou a terceiros, devendo ocorrer o registro do ato no SICAF.

13.2.2. multa de 10% (dez por cento) sobre o valor total do contrato, no caso de recusa injustificada para assinatura do contrato, da Ata de Registro de Preços e do recebimento da Nota de Empenho.

13.2.3. multa de 10% (dez por cento) em caso de atraso ou recusa injustificada para a entrega do objeto;

13.2.4. multa de 0,3% (zero vírgula três por cento) em caso de situação irregular de habilitação, por dia de atraso até o limite de 30 dias, sobre o valor total da Nota de Empenho; e

13.2.5. A multa aplicada deverá ser recolhida ao Tesouro Nacional por meio de GRU (guia de recolhimento da união), no prazo máximo de 20 (vinte) dias úteis, a contar do dia útil imediato ao recebimento da notificação enviada pela **IMBEL** e o recibo entregue na Divisão de Finanças da **IMBEL**.

13.3. Suspensão do direito de licitar e impedimento de contratar com a **IMBEL**, por até 2 (dois) anos, registro no SICAF e no CEIS, de acordo com o preconizado no artigo 23 da Lei nº 12.846/13, em virtude do cometimento de fraude fiscal; pela prática de atos ilícitos no intento de prejudicar os objetivos almejados pela **IMBEL**, por intermédio da ARP; pela manifesta demonstração de inidoneidade para contratar com a **IMBEL** em virtude do cometimento de atos ilícitos; bem como por falhar ou fraudar na execução do objeto.

13.4. As penalidades de multas decorrentes de fatos diversos serão consideradas independentes entre si e poderão ser aplicadas à **CONTRATADA** juntamente com as sanções previstas nos subitens 13.2.1; 13.3.

13.5. A aplicação de qualquer das penalidades acima elencadas realizar-se-á por intermédio de procedimento administrativo que garantirá à **CONTRATADA** o pleno direito ao exercício pleno da ampla defesa e do contraditório no prazo de 5 (cinco) dias úteis, a contar da data em que for notificada pela **IMBEL**.

13.6. Após o processo administrativo pertinente, as importâncias decorrentes das multas aplicadas e não recolhidas nos prazos estipulados nas notificações correspondentes, devem ser descontadas dos pagamentos eventualmente devidos pela **IMBEL**, ou ainda, conforme cada caso, judicialmente cobradas.

13.7. A autoridade competente, quando da aplicação das sanções, deve considerar a natureza e a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano gerado à **IMBEL**, observados os princípios da razoabilidade e da proporcionalidade.

13.8. As penalidades devem, obrigatoriamente, ser registradas no SICAF, nas situações e momentos para as quais foram estabelecidas, podendo ser aplicadas isolada ou cumulativamente a critério da **IMBEL** após a análise das circunstâncias que ensejaram sua aplicação.

13.9. Aplicam-se à **CONTRATADA** as normas de direito penal preconizadas entre os artigos 89 e 99 da Lei nº 8.666/93, conforme o disposto no Art. 41 da Lei nº 13.303/16 e no Art. 2º do Regulamento de Licitações e Contratos da **IMBEL**.

13.10. Concluída a instrução processual, a **CONTRATADA** será intimada para, se assim desejar, apresentar, apresentar razões finais num prazo de até 5 (cinco) dias úteis.

CLÁUSULA DÉCIMA QUARTA - DO CONTROLE, DA FISCALIZAÇÃO E GERENCIAMENTO DO CONTRATO

14.1. O acompanhamento, a fiscalização e o gerenciamento da execução contratual, bem como quanto à qualidade do material e dos serviços relacionados no objeto, fica a cargo do Fiscal do Contrato a ser designado para essa finalidade e, na falta deste, por seu substituto, a quem caberá, também, dirimir as dúvidas que surgirem durante a execução dos serviços.

14.2. O Fiscal do Contrato deve ter a experiência necessária para acompanhamento e controle durante a execução dos serviços provenientes deste contrato.

14.3. A verificação da adequada prestação do serviço deve ser realizada conforme critérios preestabelecidos no Termo de Referência.

14.4. Não se admite que a própria **CONTRATADA** materialize a avaliação de desempenho e qualidade dos serviços por ela prestados.

14.5. O descumprimento total ou parcial das demais obrigações e responsabilidades assumidas pela **CONTRATADA** ensejará na aplicação das sanções administrativas previstas neste contrato, na legislação vigente e nos artigos 188 a 193 do Regulamento de Licitações e Contratos da **IMBEL**, em consonância com disposto entre os artigos 83 e 84 da Lei nº 13.303/16.

CLÁUSULA DÉCIMA QUINTA - DO RECEBIMENTO E DA ACEITAÇÃO DO OBJETO

15.1. O objeto será recebido pelo Fiscal do Contrato da **IMBEL** no ato da entrega da Nota Fiscal, por parte da **CONTRATADA**, após cumprido todas as exigências, para posterior verificação de sua conformidade com as especificações contidas no Termo de Referência.

15.2. O objeto poderá ser rejeitado, totalmente ou parcialmente, quando estiverem em desacordo com as especificações constantes do Termo de Referência ou deste contrato, devendo ser corrigidos, refeitos ou substituídos no prazo fixado pelo Fiscal do Contrato à custa da **CONTRATADA**, sem prejuízo da aplicação das demais penalidades provenientes do descumprimento contratual.

15.3. Após o prazo concedido pelo Fiscal do Contrato, os materiais e o serviço será novamente inspecionado para fins de aceitação e, caso ainda perdure alguma alteração será instaurado o devido processo administrativo contra a **CONTRATADA**, sem que isso a desobrigue de efetuar as correções ainda pendentes.

CLÁUSULA DÉCIMA SEXTA - DA INEXECUÇÃO E RESCISÃO

16.1. A inexecução total ou parcial do contrato poderá ensejar na sua rescisão, com a repercussão das consequências cabíveis.

16.2. Constituem razões para a rescisão contratual:

16.2.1. o descumprimento de obrigações contratuais.

16.2.2. a subcontratação total ou parcial do objeto, cessão ou transferência, total ou parcial, a quem não atenda aos pré-requisitos habilitatórios e sem prévia e expressa autorização da **IMBEL**.

16.2.3. a fusão, cisão, incorporação ou associação da **CONTRATADA** com outrem, quando não admitidas no Termo de Referência e se prévia e expressa autorização da **IMBEL**.

16.2.4. o desatendimento das determinações legais e regulares expedidas pelo Gestor ou Fiscal do Contrato.

16.2.5. o reiterado cometimento de faltas durante a execução contratual.

16.2.6. a dissolução da sociedade ou falecimento do **CONTRATADO**.

16.2.7. a decretação de falência ou insolvência civil do **CONTRATADO**.

16.2.8. a alteração social ou modificação da finalidade ou da estrutura da **CONTRATADA**, cuja repercussão possa prejudicar a consecução contratual.

16.2.9. razões de interesse da **IMBEL**, de alta relevância e amplo conhecimento, expressamente justificadas no processo administrativo.

16.2.10. o atraso nos pagamentos devidos pela **IMBEL**, provenientes de serviços ou fornecimentos, como também de parcelas destes, já recebidos ou executados, salvo nos casos de calamidade pública, grave perturbação da ordem interna ou guerra, restando assegurado à **CONTRATADA** o direito de optar pela suspensão do cumprimento de suas obrigações até que seja normalizada a situação.

16.2.11. a falta de liberação, por parte da **IMBEL**, de área, local ou dos objetos e condições necessárias para a execução dos serviços nos prazos contratualmente especificados, bem como das informações prescritas no Termo de Referência.

16.2.12. a ocorrência de caso fortuito, força maior ou fato do príncipe, regularmente comprovada, desde que esteja caracterizado o vínculo impeditivo da execução contratual.

16.2.13. a suspensão dos direitos da **CONTRATADA** de contratar e licitar com a **IMBEL**.

16.2.14. o descumprimento, por parte da **CONTRATADA**, da proibição de trabalho noturno, perigoso ou insalubre a menores de 18 (dezoito) anos e de qualquer trabalho de menores de 16 (dezesseis) anos, a não na condição de aprendiz a partir de 14 (quatorze) anos.

16.2.15. ter fraudado ou frustrado, mediante ajuste, combinação ou qualquer outro expediente, o caráter competitivo da Licitação.

16.2.16. ter impedido, perturbado ou fraudado a realização de qualquer ato de procedimento licitatório público.

16.2.17. ter afastado ou procurado afastar licitante, por intermédio de fraude ou oferecimento de vantagem de qualquer natureza.

16.2.18. ter fraudado licitação pública ou contrato dela decorrente.

16.2.19. ter criado, de modo fraudulento ou irregular, pessoa jurídica para participar de licitação pública ou celebrar contrato administrativo.

16.2.20. ter obtido vantagem ou benefício indevido, de modo fraudulento, de modificações ou prorrogação de contratos celebrados pela Administração Pública, sem autorização em lei no ato convocatório da licitação pública ou nos respectivos instrumentos contratuais.

16.2.21. ter manipulado ou fraudado o equilíbrio econômico-financeiro dos contratos celebrados com a Administração Pública, e

16.2.22. ter prejudicado atividade de investigação ou fiscalização de órgãos, entidades de controle ou agentes públicos, ou ter intervindo em sua atuação, inclusive no âmbito das agências reguladoras e de órgãos do sistema financeiro nacional.

16.2.23. as práticas passíveis de rescisão definidas entre os incisos 16.2.15 e 16.2.22, podem ser definidas, entre outras, como:

a) Corrupta - oferecer, dar, receber ou solicitar, direta ou indiretamente, qualquer vantagem com o objetivo de influenciar a ação do empregado da **IMBEL** no procedimento aquisitivo ou na execução contratual;

b) Fraudulenta - falsificar ou omitir fatos, com o objetivo de influenciar o procedimento licitatório ou a execução contratual;

c) Colusiva - esquematizar ou estabelecer um acordo entre dois ou mais licitantes, com ou sem conhecimento de representantes da **IMBEL**, visando o estabelecimento de preços em níveis artificiais e não competitivos;

d) Coercitiva - causar danos ou ameaçar, direta ou indiretamente, pessoas físicas ou jurídicas, visando influenciar sua participação em procedimento licitatório ou afetar a execução contratual; e

e) Obstrutiva - destruir, falsificar, alterar ou ocultar provas ou fazer declarações falsas, com o objetivo de impedir materialmente a apuração a apuração de práticas ilícitas.

16.2.24. As práticas retro mencionadas, além de acarretarem a responsabilização administrativa e judicial da pessoa jurídica, implicarão da responsabilização individual dos

dirigentes das empresas contratadas e dos administradores ou gestores, enquanto autores, nos termos da Lei nº 12.846/13.

16.3. A rescisão deste contrato pode ser:

16.3.1. amigável, em comum acordo entre as partes; ou

16.3.2. por determinação judicial.

16.4. A rescisão amigável não é cabível nos casos em que forem constados descumprimentos contratuais sem apuração de responsabilidade iniciada ou com procedimento apuratório ainda em curso.

16.5. Quando a rescisão ocorrer sem que haja culpa ou responsabilidade da parte **CONTRATANTE**, este será ressarcido dos prejuízos que eventualmente tiver sofrido, quando devida e regularmente comprovados, e no caso da **CONTRATADA** terá esta, ainda, o direito a:

16.5.1. pagamentos devidos pela execução contratual até a data da rescisão, e

16.5.2. pagamento referente ao custo de desmobilização.

16.6. Os casos de rescisão contratual devem ser formalmente motivados nos autos processuais, devendo ser assegurado o direito ao exercido prévio do contraditório e da ampla defesa.

16.7. A rescisão deverá ser formalizada por intermédio de Termo de Rescisão Contratual, devendo o respectivo extrato ser publicado no Diário Oficial da União – DOU.

CLÁUSULA DÉCIMA SÉTIMA - DA ALTERAÇÃO DO CONTRATO

17.1. O contrato poderá ser alterado por acordo entre as partes, nos seguintes casos:

17.1.1. quando houver modificação do projeto ou das especificações, para melhor adequação técnica aos seus objetivos;

17.1.2. quando necessária a modificação do valor contratual em decorrência de acréscimo ou diminuição quantitativa de seu objeto, nos limites permitidos na Lei nº 13.303/16;

17.1.3. quando conveniente a substituição da garantia de execução;

quando necessária a modificação do regime de execução do serviço, bem como do modo de fornecimento, em face de verificação técnica da inaplicabilidade dos termos contratuais originários;

17.1.4. quando necessária a modificação da forma de pagamento, por imposição de circunstâncias supervenientes, mantido o valor inicial atualizado, vedada a antecipação do pagamento, com relação ao cronograma financeiro fixado, sem a correspondente contraprestação de fornecimento de bens ou execução de obra ou serviço; e

17.1.5. para restabelecer a relação que as partes pactuaram inicialmente entre os encargos do contratado e a retribuição da administração para a justa remuneração do serviço, objetivando

a manutenção do equilíbrio econômico-financeiro inicial do contrato, na hipótese de sobrevirem fatos imprevisíveis, ou previsíveis porém de consequências incalculáveis, retardadores ou impeditivos da execução do ajustado, ou, ainda, em caso de força maior, caso fortuito ou fato do príncipe, configurando álea econômica extraordinária e extracontratual.

CLÁUSULA DÉCIMA OITAVA - DOS ACRÉSCIMOS E SUPRESSÕES

18.1. A **CONTRATADA** poderá aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem, até 25% (vinte e cinco por cento) do valor inicial do contrato

18.2. Nenhum acréscimo ou supressão poderá exceder os limites estabelecidos no subitem 18.1 acima, salvo as supressões resultantes de acordo celebrado entre as partes.

CLÁUSULA DÉCIMA NONA - DO REAJUSTAMENTO

19.1. A avença que poderá ser firmada, sofrerá reajuste de preços, obedecendo as seguintes regras:

19.1.1. O primeiro reajustamento poderá ocorrer após decorridos 12 (doze) meses, contados a partir da data efetiva da proposta de preços;

19.1.2. Os reajustes subsequentes ocorrerão decorridos 12 (doze) meses, a contar da data do primeiro reajustamento;

19.1.3. Será admitido pela **IMBEL** o reajustamento com base no Índice de Custos de Tecnologia da Informação (ICTI), de acordo com a Portaria nº 6.432/MPDG/STIC, de 11 de julho de 2018 sobre o valor praticado no contrato;

19.1.4. Caso ocorra a extinção do índice previsto no subitem anterior, o novo índice a ser aplicado será o Índice de Preços ao Consumidor Amplo – IPCA; e

19.1.5. O valor contratual poderá ser reajustado para mais ou para menos, de acordo com a variação do índice indicado no subitem 19.1.3. acima, com base na fórmula abaixo, vedada a periodicidade de reajuste inferior a um ano (12 meses), contados da data limite para apresentação da proposta (redação dada pelo Decreto nº 1.110, de 13/04/1994) - Decreto nº 1054, de 07/02/1994.

$R = V\left[\frac{I-Io}{Io}\right]$, onde,

R = valor do reajuste procurado.

V = valor contratual do fornecimento, obra ou 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 à data do reajuste.

CLÁUSULA VIGÉSIMA – DA SUBCONTRATAÇÃO

Não será admitida em nenhuma espécie a subcontração do objeto deste contrato.

CLÁUSULA VIGÉSIMA PRIMEIRA – DA ALTERAÇÃO SUBJETIVA

É admissível a fusão, cisão ou incorporação da **CONTRATADA** com/em outra pessoa jurídica, desde que sejam observados todos os requisitos de habilitação e qualificação ora exigidos, e sejam mantidas as condições deste contrato.

CLÁUSULA VIGÉSIMA SEGUNDA – DA VINCULAÇÃO

Consideram-se integrantes do presente instrumento contratual as condições prescritas no Termo de Referência, na Proposta de preços da **CONTRATADA**, de 24 de abril de 2023 e demais documentos pertinentes, independentes de sua transcrição.

CLÁUSULA VIGÉSIMA TERCEIRA- DA SUSTENTABILIDADE AMBIENTAL

23.1. A **CONTRATADA** deverá adotar as seguintes práticas de sustentabilidade ambiental, quando couber.

23.2. Usar produtos de limpeza e conservação de superfícies e objetos inanimados que obedeçam às classificações e especificações determinadas pela ANVISA.

23.3. Adotar medidas para evitar o desperdício de água tratada, conforme instituído no Decreto nº 48.138, de 8 de outubro de 2003.

23.4. Observar a Resolução CONAMA nº 20, de 7 de dezembro de 1994, quanto aos equipamentos de limpeza que gerem ruído no seu funcionamento.

23.5. Fornecer aos empregados os equipamentos de segurança que se fizerem necessários, para a execução de serviços.

23.6. Realizar um programa interno de treinamento de seus empregados, nos três primeiros meses de execução contratual, para redução de consumo de energia elétrica, de consumo de água e redução de produção de resíduos sólidos, observadas as normas ambientais vigentes.

23.7. Realizar a separação dos resíduos recicláveis descartados na fonte geradora, e a sua destinação às associações e cooperativas dos catadores de materiais recicláveis, que será procedida pela coleta seletiva do papel para reciclagem, quando couber, nos termos da IN/MARE nº 6, de 3 de novembro de 1995 e do Decreto nº 5.940, de 25 de outubro de 2006.

23.8. Respeitar as Normas Brasileiras – NBR publicadas pela Associação Brasileira de Normas Técnicas sobre resíduos sólidos; e

23.9. Prever, quando couber, a destinação ambiental adequada das pilhas e baterias usadas ou inservíveis, segundo disposto na Resolução CONAMA nº 257, de 30 de junho de 1999.

CLÁUSULA VIGÉSIMA QUARTA - DA GARANTIA CONTRATUAL

24.1. A **CONTRATADA** apresentará a garantia contratual de 5% (cinco por cento) do valor deste contrato, ou seja, R$ 1.486,80 (mil, quatrocentos e oitenta e seis reais e oitenta centavos) na modalidade de fiança bancária, com válida até 90 (noventa) dias após o encerramento deste contrato, para cobrir qualquer prejuízo verificado que a **CONTRATADA** tenha causado à **IMBEL** após o encerramento da avença, inclusive para cobrir o pagamento de multas aplicadas e não quitadas e deverá ser atualizada caso haja prorrogação da avença quando ultrapassar o interregno de 12 (doze) meses.

24.2. A garantia prestada pela **CONTRATADA** será liberada ou restituída após decorridos noventa dias do término deste contrato.

CLÁUSULA VIGÉSIMA QUINTA – DA LEGISLAÇÃO APLICÁVEL

Aplica-se à execução deste contrato, inclusive aos casos omissos, a Lei nº 13.303, de 2016, o Decreto nº 8.945 de 2016, a Lei Complementar nº 123, de 2006, a Lei nº 12.846, de 2013, o Regulamento de Licitações e Contratos da **IMBEL**, aprovado na 305ª Reunião do Conselho de Administração da **IMBEL**, ocorrida em 22/05/2018, conforme Resolução nº 06/2018-CA-**IMBEL**, de 22/05/2018, e as normas de direito civil acerca da matéria.

CLÁUSULA VIGÉSIMA SEXTA- DA MANUTENÇÃO DE QUALIFICAÇÃO E HABILITAÇÃO

A **CONTRATADA** se obriga a manter durante todo o período de execução do objeto deste contrato, relativamente às obrigações por intermédio deste assumidas, as condições de habilitação e qualificação exigidas.

CLÁUSULA VIGÉSIMA SÉTIMA - DOS RECURSOS

27.1. Do ato de rescisão deste contrato e da respectiva aplicação das penalidades de advertência, suspensão temporária e multa, cabe recurso no prazo de 5 (cinco) dias úteis a contar do recebimento da intimação do ato, que deve ser dirigido à autoridade superior àquela que praticou o ato recorrido.

27.2. A intimação do ato de suspensão temporária deve ser efetuada por intermédio de publicação no DOU, e as de advertência ou multa registradas no SICAF e, concomitantemente, comunicadas por escrito à **CONTRATADA**.

CLÁUSULA VIGÉSIMA OITAVA - DA CONFIDENCIALIDADE

A Empresa **CONTRATADA** deverá respeitar e assegurar o sigilo relativamente às informações obtidas durante a execução dos serviços, não as divulgando, sob nenhuma circunstância, sem autorização expressa da **IMBEL**, salvo quando houver obrigação legal de fazê-lo.

CLÁUSULA VIGÉSIMA NONA - DA MATRIZ DE RISCO

29.1. A seguir, é apresentado as tabelas, que definem a probabilidade e o impacto que serão aplicados aos possíveis riscos.

Probabilidade	
Situação	**Pontuação**
Improvável	0
Pouco provável	1
Possível	2
Muito possível	3

Impacto	
Situação	**Pontuação**
Sem impacto	0
Baixo impacto	1
Médio impacto	2
Alto impacto	3

29.2. Listagem de possíveis eventos supervenientes à assinatura desta avença que possam interferir no equilíbrio econômico-financeiro deste contrato.

EVENTO	**PROBABILIDADE**		**IMPACTO**	
	Situação	**Pontuação**	**Situação**	**Pontuação**
Fornecimento de licenças de antivírus em desconformidade com o previsto no Termo de Referência	Pouco provável	1	Médio impacto	2

29.3. Caso ocorra o previsto no item 29.2 acima, todas as despesas do aditamento ocorrerão por conta da **CONTRATADA**.

29.4. Apenas a execução do serviço previsto no objeto, haverá liberdade da **CONTRATADA** para inovação metodológica ou tecnológica, nas obrigações de resultado ou na melhoria no padrão das soluções previamente estabelecidas no Termo de Referência.

CLÁUSULA TRIGÉSIMA – DO FORO

30.1. As partes elegem o foro da Justiça Federal na cidade de Brasília-DF para conhecer e julgar disputas judiciais que possam resultar da execução do presente contrato.

30.2. E, por estarem justas, a **CONTRATANTE** e a **CONTRATADA** assinam o presente contrato, por intermédio de seus representantes legais, em 02 (duas) vias de igual forma e teor, para um só efeito que, depois de lido e achado conforme, produza seus efeitos jurídicos e legais.

Brasília-DF, 03 de maio de 2023.

Pela CONTRATANTE:

E. X. C.
Ordenador de Despesas
CPF ***.178.581-**
RG **568** SSP/DF

Pela CONTRATADA:

L. DA S. C.
Diretor de Tecnologia
CPF ***.892.271-**
RG *.377.*** SSP/DF

R. DE A. S.
Diretor Executivo
CPF ***.171.621-**
RG *.191.*** SSP/DF

Testemunhas:

Assinatura: C.I.S
CPF: ***.298.271-**

Assinatura: N.F.C.L.S
CPF: ***.470.071-**

APENDICE AO CONTRATO Nº 05/2023-UA IMBEL

TERMO DE MANUTENÇÃO DO SIGILO

A Empresa **E-SEC TECNOLOGIA EM SEGURANÇA DE DADOS LTDA**, pessoa jurídica de direito privado, inscrita no CNPJ sob o nº 03.242.841/0001-01, localizada no SHS, Quadra 06, Brasil 21, Bloco A, Sala 501, Asa Sul, Brasília-DF, CEP 90316-12, se compromete que manterá a manutenção do sigilo e respeito das normas de segurança vigentes na Indústria de Material Bélico do Brasil/Sede (UG 168003).

Brasília-DF, 03 de maio de 2023.

L. DA S. C.
Diretor de Tecnologia
CPF ***.892.271-**
RG *.377.*** SSP/DF

R. DE A. S.
Diretor Executivo
CPF ***.171.621-**
RG *.191.*** SSP/DF

(Nome, CPF e RG protegidos pela lei n° 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais – LGPD, Redação dada pela Lei n° 13.853, de 2019.)