

TERMO DE REFERÊNCIA

ANEXO I - MATRIZ DE RISCO

ANEXO II - MODELO DE PROPOSTA

ANEXO III - TERMO DE COMPROMISSO

Processo Nº 0060407931.000050/2025-38

1. DO OBJETO

1.1. Aquisição de **subscrição de licenças de solução de Segurança Integrada de Proteção Avançada de Endpoints** (estações de trabalho e servidores de rede) e **Deteção e Resposta de Endpoint (Endpoint Detection and Response - EDR)** por 12 meses, incluindo capacitação e serviço especializado de implantação, para os dispositivos de TI do Laboratório Farmacêutico do Estado de Pernambuco Governador Miguel Arraes, bem como suporte técnico durante o período de validade das licenças.

2. DESCRIÇÕES DO OBJETO

ITEM	OBJETO	OBJETO	QUANTIDADE	PERÍODO
1	SOLUÇÃO DE PROTEÇÃO E RESPOSTA DE AMEAÇAS A ENDPOINTS, COM GERENCIAMENTO CENTRALIZADO E SUPORTE TÉCNICO POR 12 MESES	LICENÇA	500	12 MESES
2	IMPLANTAÇÃO DA SOLUÇÃO E TREINAMENTO ESPECIALIZADO PARA A OPERAÇÃO	SERVIÇO	1	N/A

2.1. ESPECIFICAÇÕES DO OBJETO

2.1. A solução a ser adquirida deverá estar alinhada com os princípios estabelecidos nas normas e frameworks internacionais de segurança da informação, especialmente a **ISO/IEC 27001** e o **NIST Cybersecurity Framework (CSF)**. A ISO/IEC 27001 estabelece os requisitos para a implementação de um Sistema de Gestão de Segurança da Informação (SGSI), com foco na proteção da confidencialidade, integridade e disponibilidade das informações institucionais. A solução deve contribuir diretamente para os controles de segurança previstos na norma, como o tratamento de vulnerabilidades, proteção contra softwares maliciosos, gestão de acessos e monitoramento contínuo.

2.2. Adicionalmente, a solução deverá apoiar as cinco funções básicas do **NIST CSF**:

- Identificar** ativos e riscos;
- Proteger** os sistemas contra ameaças conhecidas e desconhecidas;
- Detectar** atividades suspeitas ou incidentes em tempo real;
- Responder** de forma automatizada ou manual a eventos de segurança;
- Recuperar** os ativos afetados, com capacidade de análise pós-incidente.

- 2.3. As licenças devem ser disponibilizadas por meio de subscrição e devem estar plenamente ativas em até 02 dias corridos após disponibilização da Ordem de Fornecimento autorizada pelo LAFEPE;
- 2.4. Capacidade de remover remotamente, de forma nativa ou com uso de scripts, qualquer solução de segurança (própria ou de terceiros) que estiver presente nas estações e servidores;
- 2.5. Capacidade de instalar remotamente a solução de segurança nas estações e servidores Windows, através de compartilhamento administrativo, *login script* e/ou *GPO* de *Active Directory*;
- 2.6. Deve registrar em arquivo de *log* todas as atividades efetuadas pela solução e deve enviar também essas informações para a console de gerência centralizada da solução;
- 2.7. Capacidade de gerar pacotes customizados (autoexecutáveis) contendo a licença e configurações do produto;
- 2.8. A comunicação de rede entre o cliente e o servidor de administração deve ser criptografada;
- 2.9. Integração com serviços de diretórios da solução *Microsoft Active Directory* ou *OpenLDAP*;
- 2.10. Todas as funcionalidades dos módulos especificados devem ser, conforme requisitos de implantação da solução, ser plenamente compatíveis com as seguintes versões de sistemas operacionais:
- a) Endpoints Windows 10 ou superior;
 - b) Servidores Windows Server 2019 ou superior;
- 2.11. O licitante vencedor deverá fornecer todos os softwares auxiliares necessários para o funcionamento da solução e sem custo adicional;
- 2.12. Não será permitido o envio de arquivos, links, endereços e quaisquer outras informações proprietárias do LAFEPE para a nuvem. Será permitido apenas o tráfego de dados e metadados imprescindíveis para o funcionamento da solução;
- 2.13. A solução deve ser capaz de gerenciar o agendamento de atualizações e instalações de políticas e agentes;
- 2.14. Qualquer adaptação ou configuração das funcionalidades dos módulos especificados da solução que precisem, por ventura, se integrar com soluções externas deve ser realizada de forma nativa;
- 2.15. Todas as funcionalidades dos módulos especificados devem ser otimizadas, adaptativa ou manualmente, para endpoints e servidores com poucos recursos computacionais (CPU, RAM e disco) de modo a não comprometer a utilização do ativo protegido;
- 2.16. Todos os módulos auxiliares imprescindíveis ao funcionamento da console de gerenciamento devem ser implementados em alta disponibilidade.
- 2.17. O fabricante da Solução deve ter figurado no Quadrante Mágico *Gartner*, na categoria de *Endpoint Protection Platforms*, em suas 02 publicações mais recentes.
- 2.18. **SOLUÇÃO DE PROTEÇÃO DE COMPUTADORES**
- 2.18.1. A solução de gerência centralizada deve:
- 2.18.2. permitir a geração de relatórios, visualizar eventos, gerenciar políticas e, se possível, a criação de painéis de controle customizados;
- 2.18.3. permitir, de forma nativa ou por meio da utilização de scripts, a visualização da situação, dos recursos instalados (CPU, memória, discos, conexões de rede, dentre outros), softwares instalados, em tempo real, de todos os ativos administrados pela console de gerenciamento centralizada;
- 2.18.4. gerenciar estações de trabalho, servidores de rede e servidores de arquivos

protegidos pela solução de segurança;

2.18.5. ser capaz de importar a estrutura da solução Microsoft Active Directory para descoberta de máquinas;

2.18.6. permitir, por meio da console de gerenciamento, a criação de políticas para a retenção em servidor de rede de arquivos que violam as políticas de segurança definidas para os ativos abrangidos pela solução;

2.18.7. monitorar diferentes sub-redes a fim de encontrar máquinas novas para serem adicionadas à proteção, para soluções em nuvem será aceito o uso do *Microsoft Active Directory, scripts* ou outras ferramentas para executar tal função;

2.18.8. 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;

2.18.9. ser capaz de, assim que detectar máquinas novas, nativamente ou através de Script nos diretórios da solução *Microsoft Active Directory*, sub-redes ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possua, deve instalar o antivírus automaticamente;

2.18.10. 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;

2.18.11. fornecer, de forma nativa ou por meio da exportação de relatório, as seguintes informações dos ativos protegidos:

- a) Quais módulos de segurança estão instalados;
- b) Quais módulos de segurança estão com o serviço iniciado;
- c) Quais módulos de segurança estão atualizados;
- d) Minutos/horas desde a última conexão do ativo com o servidor administrativo;
- e) Minutos/horas desde a última atualização;
- f) Data e horário da última varredura executada no ativo;
- g) Versão dos módulos de segurança instalados no ativo;
- h) Quantidade de ameaças identificadas no ativo;
- i) Nome do ativo;
- j) Domínio ou grupo de trabalho do ativo;
- k) Sistema operacional;
- l) Endereço IP;
- m) Eventos de segurança relacionados aos aplicativos instalados no ativo;
- n) Informações sobre incidentes no painel central.

2.18.12. exportar relatórios, de forma nativa ou por meio de API, para os tipos de arquivos PDF e HTML e, opcionalmente, para os tipos de arquivos XML, CSV e JSON.

2.18.13. enviar e-mails para contas específicas em caso de algum evento específico.

2.18.14. realizar atualização incremental da base de assinatura de *malware*.

2.18.15. realizar a atualização incremental das bases de reputação.

2.18.16. reportar vulnerabilidades de softwares presentes nos ativos ou possuir mecanismos de proteção contra exploração de vulnerabilidades.

2.18.17. disponibilizar a criação de perfis e papéis de acesso. Exemplo: Administradores, operadores, monitores.

2.18.18. ser capaz de se integrar com a solução *Microsoft Active Directory* ou serviço de diretório *OpenLDAP* para a autenticação no painel central de gerência.

- 2.18.19. ser capaz de gerar relatório forense detalhando o modus operandi de cada *malware* identificado e informar qual foi o vetor de contaminação/entrada em cada ocorrência.
- 2.18.20. possuir console única de visibilidade e de consolidação de gerenciamento integrado do ambiente monitorado por múltiplos ativos (*endpoints*, servidores e dispositivos).
- 2.18.21. possuir integração com soluções SIEM ou SOAR.
- 2.18.22. ser capaz de desativar temporariamente funcionalidades da solução, quando necessário para efeitos de suporte, localmente, mas protegida com senha.
- 2.18.23. ser capaz de gerenciar o envio de alertas e notificações.
- 2.18.24. centralizar a gerência de todos os recursos e funcionalidades especificadas.
- 2.18.25. permitir o agendamento e envio de relatórios por email.
- 2.18.26. permitir a criação de relatórios customizados.
- 2.18.27. possuir modelos predefinidos de relatórios de forma a facilitar a geração de relatórios
- 2.18.28. ser capaz de criptografar toda comunicação entre o painel de gerenciamento e a solução.
- 2.18.29. ser gerenciada totalmente por console web.
- 2.18.30. A solução de Proteção de Computadores:
- 2.18.31. deve possuir as seguintes características e funcionalidades:
- 2.18.31.1. ser capaz de atualizar os pacotes de instalação com as últimas vacinas;
- 2.18.31.2. ser capaz de identificar e bloquear, no mínimo, os seguintes tipos de malwares: ameaças de dia zero (*zero-day*), direcionado, *ransomware*, *spyware*, *worm*, *adware*, *bot(nets)*, *rootkits*, *trojan*, *fileless virus*, *vírus*.
- 2.18.32. ser capaz de, no mínimo, identificar artefatos maliciosos por meio das seguintes técnicas: análise baseada em assinaturas, análise baseada em reputação (hashes de Indicadores de Comprometimento) machine learning com pré-execução, análise comportamental, análise heurística, mecanismo de emulação, mecanismo de inteligência artificial, análise de comunicações de rede.
- 2.18.33. possuir os seguintes módulos de segurança:
- a) firewall;
 - b) IPS;
 - c) proteção de navegadores *web*;
 - d) controle de aplicação;
 - e) filtro de reputação *web*;
 - f) controle de dispositivos;
 - g) detecção e resposta para computadores (*endpoint detection and response - EDR*);
 - h) proteção de memória;
 - i) proteção *anti-malware* para computadores com GNU/Linux;
 - j) aplicação de políticas e mecanismos de segurança que alertem e protejam contra ameaças a vulnerabilidades em sistemas operacionais e nas aplicações instaladas;
- 2.18.34. ser dotada de um módulo de controle de aplicação com as seguintes características:
- 2.18.35. possibilitar a criação de política de bloqueio de execução de aplicações por: nome de arquivo ou diretório ou *hash*;
- 2.18.36. possibilitar a liberação e bloqueio de aplicações por meio de *white list* e *black list*

de aplicações;

2.18.37. aplicar o controle de aplicação em tempo de execução;

2.18.38. monitorar alterações em arquivos e chaves de registro em tempo real e possuir mecanismos de proteção;

2.18.39. possuir proteção contra adulteração de programas (executáveis, binários, DLLs, scripts, etc);

2.18.40. possibilitar a criação de políticas para computadores específicos, onde somente será permitido executar programas autorizados (*white list*) ou serão bloqueados os programas não autorizados (*black list*); na lista de bloqueio via política de controle de aplicação;

2.18.41. ser capaz de permitir e bloquear a instalação e a execução de programas específicos, categorias de programas (no caso de *endpoints*), de acordo com política definida pelo LAFEPE;

2.18.42. analisar as ações de cada aplicação em execução no *endpoint* ou servidor, gravando tais ações executadas e comparando-as com sequências características de atividades suspeitas ou perigosas;

2.18.43. analisar qualquer tentativa de edição, exclusão ou gravação do registro do Windows ou de arquivos de configuração em distribuições GNU/Linux antes de sugerir ações e bloquear comportamentos suspeitos e perigosos;

2.18.44. **ser dotada de um módulo de controle de dispositivos com as seguintes características:**

2.18.44.1. capaz de controlar a utilização de dispositivos removíveis permitindo a identificação e o controle de leitura, escrita e execução;

2.18.44.2. ser capaz de identificar, permitir e bloquear a utilização de dispositivos acoplados nos ativos protegidos pela solução;

2.18.44.3. ser capaz de identificar e impedir movimentos laterais suspeitos e maliciosos por meio do isolamento do equipamento gerenciado;

2.18.44.4. verificar a confiabilidade dos executáveis e caso não seja confiável, deverá possuir capacidade para impedir sua execução.

2.18.44.5. ser capaz de bloquear a execução de executáveis em geral em dispositivos removíveis.

2.18.44.6. ser capaz de verificar a integridade de arquivos do sistema operacional e de programas instalados.

2.18.44.7. ser capaz de registrar na base de reputação os novos *malwares* identificados.

2.18.44.8. ser dotada de um módulo de proteção de memória capaz de identificar e bloquear ações maliciosas realizadas por softwares permitidos. Exemplo: execução de shellcodes, comandos, ações com privilégios elevados, etc.

2.18.44.9. capaz de remover arquivos maliciosos automaticamente.

2.18.44.10. ser capaz, caso possua funcionalidade de quarentena local, de mover arquivos suspeitos para área protegida no computador ou tomar alguma ação de mitigação de tais arquivos, de acordo com a definição em política.

2.18.44.11. ser capaz de mover, caso possua funcionalidade de quarentena local, arquivos maliciosos para servidor de rede de acordo com a definição em política ou permitir a recuperação do arquivo no computador por meio da console de gerenciamento centralizada.

2.18.44.12. ser capaz de tratar exceções, evitando o bloqueio e até mesmo a verificação de processos, diretórios e executáveis especificados em políticas.

2.18.45. ser capaz de se integrar com sistemas SIEM ou SOAR externos.

2.18.46. ser capaz de detectar a presença de soluções de proteção de computadores de outro fabricante que possa causar incompatibilidade.

2.18.47. ser dotada de um módulo de proteção de navegação web capaz de verificar

tráfego nos browsers mais utilizados no mercado executando bloqueio por reputação ou categorização do URL.

2.18.48. ser dotada de um módulo de filtro de conteúdo web capaz de adicionar sites da web em uma lista de exclusão (*black list*) e em uma lista de permissão (*white list*).

2.18.49. ser dotada de proteção contra desinstalação por meio de senha.

2.18.50. ser dotada de um módulo de firewall para endpoints e servidores gerenciado a partir da console de gerência centralizada, com filtragem de pacotes e de aplicativos;

2.18.51. utilizar um agente único nos endpoints e servidores, de modo a atender todas as funcionalidades, não sendo permitido o uso de agentes simultâneos no mesmo ativo.

2.18.52. ser dotada de um módulo de proteção contra ransomware capaz de desfazer quaisquer alterações criptográficas nos arquivos dos *endpoints* e servidores.

2.19. **SOLUÇÃO DE DETECÇÃO E RESPOSTA DE AMEAÇAS CONTRA COMPUTADORES**

2.19.1. O módulo de *Endpoint Detection and Response* (EDR) deve possuir as seguintes características:

2.19.1.1. possibilitar a investigação nos *endpoints Windows* e servidores GNU/Linux via console de gerenciamento, por meio de consultas customizadas que serão realizadas em todos os computadores com o módulo ativado;

2.19.1.2. possibilitar a detecção e identificação de atividades suspeitas em todos os computadores com o módulo ativado;

2.19.2. gerar trilha de auditoria dos eventos nos computadores com o módulo ativo. As informações de auditoria devem conter, no mínimo:

a) informações sobre processos: criados, finalizados, hash SHA-1, ID, Time, *User*, comando que iniciou o processo, *RAM* utilizada pelo processo e *Threads* criados pelo processo, registros e bibliotecas alteradas,

b) informações sobre conexões de rede: endereço IP de origem e destino, portas de origem e destino;

c) informações sobre arquivos: nome do arquivo, data de criação, data de modificação e data de exclusão;

d) informações sobre registros de sistema: nomes de chaves e valores correspondentes. Os valores deverão constar nos registros;

e) informações sobre Sistema Operacional: versão, grupo de usuários locais, membros de grupos de usuários locais e usuários locais.

2.19.3. consultas à trilha de auditoria via console de gerenciamento centralizada;

2.19.4. permitir a execução de scripts (*PowerShell*, *VisualBasic*, *BAT* ou *Python* em computadores *Windows* e *ShellScript* ou *Python* em servidores GNU/Linux) ou de ações pré-definidas e customizáveis (no mínimo: isolar o *host*, verificar *IoC's* e isolar ou prevenir a execução de arquivos);

2.19.5. possuir políticas pré-configuradas;

2.19.6. permitir a criação de coletores de informações e a execução de scripts sob demanda em computadores;

2.19.7. armazenar os eventos nos computadores e disponibilizar consulta a eles via console de gerenciamento;

2.19.8. 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;

2.19.9. ser capaz de, assim que detectar máquinas novas, nativamente ou através de Script nos diretórios da solução *Microsoft Active Directory*, sub-redes ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possua, deve instalar o antivírus

automaticamente;

2.19.10. 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;

2.19.11. fornecer, de forma nativa ou por meio da exportação de relatório, as seguintes informações dos ativos protegidos:

- a) Quais módulos de segurança estão instalados;
- b) Quais módulos de segurança estão com o serviço iniciado;
- c) Quais módulos de segurança estão atualizados;
- d) Minutos/horas desde a última conexão do ativo com o servidor administrativo;
- e) Minutos/horas desde a última atualização;
- f) Data e horário da última varredura executada no ativo;
- g) Versão dos módulos de segurança instalados no ativo;
- h) Quantidade de ameaças identificadas no ativo;
- i) Nome do ativo;
- j) Domínio ou grupo de trabalho do ativo;
- k) Sistema operacional;
- l) Endereço IP;
- m) Eventos de segurança relacionados aos aplicativos instalados no ativo;
- n) Informações sobre incidentes no painel central.

2.19.12. exportar relatórios, de forma nativa ou por meio de API, para os tipos de arquivos PDF e HTML e, opcionalmente, para os tipos de arquivos XML, CSV e JSON.

2.19.13. enviar e-mails para contas específicas em caso de algum evento específico.

2.19.14. realizar atualização incremental da base de assinatura de malware.

2.19.15. realizar a atualização incremental das bases de reputação.

2.19.16. reportar vulnerabilidades de softwares presentes nos ativos ou possuir mecanismos de proteção contra exploração de vulnerabilidades.

2.19.17. disponibilizar a criação de perfis e papéis de acesso. Exemplo: Administradores, operadores, monitores.

2.19.18. ser capaz de se integrar com a solução Microsoft Active Directory ou serviço de diretório OpenLDAP para a autenticação no painel central de gerência.

2.19.19. ser capaz de gerar relatório forense detalhando o modus operandi de cada malware identificado e informar qual foi o vetor de contaminação/entrada em cada ocorrência.

2.19.20. possuir console única de visibilidade e de consolidação de gerenciamento integrado do ambiente monitorado por múltiplos ativos (endpoints, servidores e dispositivos).

2.19.21. possuir integração com soluções SIEM ou SOAR.

2.19.22. ser capaz de desativar temporariamente funcionalidades da solução, quando necessário para efeitos de suporte, localmente, mas protegida com senha.

2.19.23. ser capaz de gerenciar o envio de alertas e notificações.

2.19.24. centralizar a gerência de todos os recursos e funcionalidades especificadas.

2.19.25. permitir o agendamento e envio de relatórios por email.

2.19.26. permitir a criação de relatórios customizados.

2.19.27. possuir modelos predefinidos de relatórios de forma a facilitar a geração de relatórios

- 2.19.28. ser capaz de criptografar toda comunicação entre o painel de gerenciamento e a solução.
- 2.19.29. ser gerenciada totalmente por console web.
- 2.19.30. A solução de Proteção de Computadores:
- 2.19.31. deve possuir as seguintes características e funcionalidades:
- 2.19.31.1. ser capaz de atualizar os pacotes de instalação com as últimas vacinas;
- 2.19.31.2. ser capaz de identificar e bloquear, no mínimo, os seguintes tipos de *malwares*: ameaças de dia zero (*zero-day*), direcionado, *ransomware*, *spyware*, *worm*, *adware*, *bot(nets)*, *rootkits*, *trojan*, *fileless virus*, *vírus*.
- 2.19.32. ser capaz de, no mínimo, identificar artefatos maliciosos por meio das seguintes técnicas: análise baseada em assinaturas, análise baseada em reputação (hashes de Indicadores de Comprometimento) *machine learning* com pré-execução, análise comportamental, análise heurística, mecanismo de emulação, mecanismo de inteligência artificial, análise de comunicações de rede.
- 2.19.33. possuir os seguintes módulos de segurança:
- a) firewall;
 - b) IPS;
 - c) proteção de navegadores web;
 - d) controle de aplicação;
 - e) filtro de reputação web;
 - f) controle de dispositivos;
 - g) detecção e resposta para computadores (endpoint detection and response - EDR);
 - h) proteção de memória;
 - i) proteção anti-malware para computadores com GNU/Linux;
 - j) aplicação de políticas e mecanismos de segurança que alertem e protejam contra ameaças a vulnerabilidades em sistemas operacionais e nas aplicações instaladas;
- 2.19.34. ser dotada de um módulo de controle de aplicação com as seguintes características:
- 2.19.35. possibilitar a criação de política de bloqueio de execução de aplicações por: nome de arquivo ou diretório ou hash;
- 2.19.36. possibilitar a liberação e bloqueio de aplicações por meio de white list e black list de aplicações;
- 2.19.37. aplicar o controle de aplicação em tempo de execução;
- 2.19.38. monitorar alterações em arquivos e chaves de registro em tempo real e possuir mecanismos de proteção;
- 2.19.39. possuir proteção contra adulteração de programas (executáveis, binários, DLLs, scripts, etc);
- 2.19.40. possibilitar a criação de políticas para computadores específicos, onde somente será permitido executar programas autorizados (white list) ou serão bloqueados os programas não autorizados (black list); na lista de bloqueio via política de controle de aplicação;
- 2.19.41. ser capaz de permitir e bloquear a instalação e a execução de programas específicos, categorias de programas (no caso de endpoints), de acordo com política definida pelo LAFEPE;
- 2.19.42. analisar as ações de cada aplicação em execução no endpoint ou servidor, gravando tais ações executadas e comparando-as com sequências características de

atividades suspeitas ou perigosas;

2.19.43. analisar qualquer tentativa de edição, exclusão ou gravação do registro do Windows ou de arquivos de configuração em distribuições GNU/Linux antes de sugerir ações e bloquear comportamentos suspeitos e perigosos;

2.19.44. **ser dotada de um módulo de controle de dispositivos com as seguintes características:**

2.19.44.1. capaz de controlar a utilização de dispositivos removíveis permitindo a identificação e o controle de leitura, escrita e execução;

2.19.44.2. ser capaz de identificar, permitir e bloquear a utilização de dispositivos acoplados nos ativos protegidos pela solução;

2.19.44.3. ser capaz de identificar e impedir movimentos laterais suspeitos e maliciosos por meio do isolamento do equipamento gerenciado;

2.19.44.4. verificar a confiabilidade dos executáveis e caso não seja confiável, deverá possuir capacidade para impedir sua execução.

2.19.44.5. ser capaz de bloquear a execução de executáveis em geral em dispositivos removíveis.

2.19.44.6. ser capaz de verificar a integridade de arquivos do sistema operacional e de programas instalados.

2.19.44.7. ser capaz de registrar na base de reputação os novos malwares identificados.

2.19.44.8. ser dotada de um módulo de proteção de memória capaz de identificar e bloquear ações maliciosas realizadas por softwares permitidos. Exemplo: execução de shellcodes, comandos, ações com privilégios elevados, etc.

2.19.44.9. capaz de remover arquivos maliciosos automaticamente.

2.19.44.10. ser capaz, caso possua funcionalidade de quarentena local, de mover arquivos suspeitos para área protegida no computador ou tomar alguma ação de mitigação de tais arquivos, de acordo com a definição em política.

2.19.44.11. ser capaz de mover, caso possua funcionalidade de quarentena local, arquivos maliciosos para servidor de rede de acordo com a definição em política ou permitir a recuperação do arquivo no computador por meio da console de gerenciamento centralizada.

2.19.44.12. ser capaz de tratar exceções, evitando o bloqueio e até mesmo a verificação de processos, diretórios e executáveis especificados em políticas.

2.19.45. ser capaz de se integrar com sistemas SIEM ou SOAR externos.

2.19.46. ser capaz de detectar a presença de soluções de proteção de computadores de outro fabricante que possa causar incompatibilidade.

2.19.47. ser dotada de um módulo de proteção de navegação web capaz de verificar tráfego nos browsers mais utilizados no mercado executando bloqueio por reputação ou categorização do URL.

2.19.48. ser dotada de um módulo de filtro de conteúdo web capaz de adicionar sites da web em uma lista de exclusão (black list) e em uma lista de permissão (white list).

2.19.49. ser dotada de proteção contra desinstalação por meio de senha.

2.19.50. ser dotada de um módulo de firewall para endpoints e servidores gerenciado a partir da console de gerência centralizada, com filtragem de pacotes e de aplicativos;

2.19.51. utilizar um agente único nos endpoints e servidores, de modo a atender todas as funcionalidades, não sendo permitido o uso de agentes simultâneos no mesmo ativo.

2.19.52. ser dotada de um módulo de proteção contra ransomware capaz de desfazer quaisquer alterações criptográficas nos arquivos dos endpoints e servidores.

2.20. **SOLUÇÃO DE DETECÇÃO E RESPOSTA DE AMEAÇAS CONTRA COMPUTADORES**

2.20.1. O módulo de Endpoint Detection and Response (EDR) deve possuir as seguintes

características:

2.20.1.1. possibilitar a investigação nos endpoints Windows e servidores GNU/Linux via console de gerenciamento, por meio de consultas customizadas que serão realizadas em todos os computadores com o módulo ativado;

2.20.1.2. possibilitar a detecção e identificação de atividades suspeitas em todos os computadores com o módulo ativado;

2.20.2. gerar trilha de auditoria dos eventos nos computadores com o módulo ativo. As informações de auditoria devem conter, no mínimo:

a) informações sobre processos: criados, finalizados, hash SHA-1, ID, Time, User, comando que iniciou o processo, RAM utilizada pelo processo e Threads criados pelo processo, registros e bibliotecas alteradas,

b) informações sobre conexões de rede: endereço IP de origem e destino, portas de origem e destino;

c) informações sobre arquivos: nome do arquivo, data de criação, data de modificação e data de exclusão;

d) informações sobre registros de sistema: nomes de chaves e valores correspondentes. Os valores deverão constar nos registros;

e) informações sobre Sistema Operacional: versão, grupo de usuários locais, membros de grupos de usuários locais e usuários locais.

2.20.3. consultas à trilha de auditoria via console de gerenciamento centralizada;

2.20.4. permitir a execução de scripts (PowerShell, VisualBasic, BAT ou Python em computadores Windows e ShellScript ou Python em servidores GNU/Linux) ou de ações pré-definidas e customizáveis (no mínimo: isolar o host, verificar loC's e isolar ou prevenir a execução de arquivos);

2.20.5. possuir políticas pré-configuradas;

2.20.6. permitir a criação de coletores de informações e a execução de scripts sob demanda em computadores;

2.20.7. armazenar os eventos nos computadores e disponibilizar consulta a eles via console de gerenciamento

2.21. **GARANTIA E SUPORTE TÉCNICO:**

2.21.1. Devem ser fornecidos serviços de garantia e manutenção técnica, a ser prestado pelo Fabricante da solução ou por empresa credenciada por este, de forma remota, pelo período de 12 meses, a contar da data de entrega dos produtos.

2.21.2. Atendimento presencial que venha a se tornar necessário para evento crítico pode ser autorizado mediante proposta comercial enviada pelo CONTRATADO e aprovada pelo CONTRATANTE.

2.21.3. Deve ser fornecido por todo o período de garantia, serviço de suporte e garantia oficial do Fabricante e/ou CONTRATADA para todos os elementos do subsistema pelo período de 12 meses, incluindo:

a) Suporte técnico 24x7 pelo fabricante ou autorizado com acionamento através de 0800, sistema próprio de chamados, email ou chat;

b) Atualização de firmware e softwares.

2.21.4. A Contratada/Fabricante deverá disponibilizar especialista com conhecimento técnico e com expertise nas configurações dos softwares ou equipamentos disponibilizados a prestar os serviços de Suporte Operacional e configurações, atender a todas as normas técnicas e boas práticas de segurança e garantindo o funcionamento e Manutenção Preventiva e Corretiva, com fornecimento de peça e serviços, pelo período de 12 (doze) meses;

2.21.5. Os serviços de assistência técnica deverão ser prestados diretamente pelo fabricante e/ou através de sua rede de assistência técnica autorizada, podendo ser a

CONTRATADA, desde que devidamente comprovado por declaração e/ou cópia do contrato;

3. **DA JUSTIFICATIVA DA CONTRATAÇÃO**

3.1. A crescente complexidade e sofisticação das ameaças cibernéticas exige a adoção de soluções de segurança que vão além da proteção tradicional baseada em assinaturas. O cenário atual apresenta riscos constantes como **malwares avançados, ransomwares, ataques zero-day, phishing direcionado e ameaças persistentes avançadas (APTs)**, que demandam tecnologias modernas de detecção e resposta. É indispensável prover segurança avançada para endpoints, a saber: computadores, desktops, notebooks, servidores de arquivo e rede físicos e virtuais, tornando o ambiente tecnológico fortalecido.

Neste contexto, é imprescindível a aquisição de uma **solução de proteção de endpoints com capacidade de EDR (Endpoint Detection and Response)**, que permita:

- Detecção comportamental de ameaças;
- Resposta automatizada e em tempo real a incidentes;
- Isolamento de máquinas infectadas;
- Análise forense e auditoria centralizada de eventos de segurança.

3.2. A gestão descentralizada dos ativos de TI e o aumento do trabalho remoto reforçam a necessidade de uma solução com **console de gerenciamento centralizado** — acessível em nuvem — que possibilite **a aplicação de políticas de segurança unificadas**, o controle de atualizações, relatórios detalhados e integração com diretórios como o Active Directory.

3.3. Adicionalmente, a solução buscada deve estar **em conformidade com os princípios da LGPD** e aderente a frameworks de segurança reconhecidos, como **ISO/IEC 27001** e **NIST CSF**, a fim de garantir **proteção dos dados pessoais e institucionais, rastreabilidade de incidentes e governança de segurança da informação**.

3.4. Por fim, justifica-se a contratação também pelos seguintes fatores técnicos:

- Proximidade do fim de cobertura da solução atual;
- Necessidade de atendimento aos requisitos de conformidade e auditoria exigidos por órgãos de controle;
- Adoção de uma arquitetura de segurança baseada em camadas e foco em **resposta proativa a incidentes**.
- Necessidade de contínua evolução frente a ameaças cibernéticas, especialmente grupos voltados a atingir instituições públicas.

3.5. Portanto, a presente contratação visa garantir a **continuidade operacional, a integridade dos ativos de informação, a mitigação de riscos cibernéticos e o suporte técnico qualificado**, necessários para uma infraestrutura moderna, segura e resiliente.

3.6. **DA JUSTIFICATIVA DO QUANTITATIVO ESTIMADO**

3.6.1. A estimativa de demanda foi realizada através de levantamento do parque computacional do LAFEPE - atual e prevista: desktops, servidores, hosts, servidores virtuais, máquinas analíticas e notebooks, levando-se em conta que a quantidade atualmente contratada tornou-se insuficiente para suprir a cobertura do total de dispositivos, e que há realidade de acréscimo no período proposto de validade das licenças.

3.7. **DA JUSTIFICATIVA ATRAVÉS DE DISPENSA DE LICITAÇÃO**

3.7.1. Devido ao valor estimado, a contratação por meio de dispensa de Licitação torna-se aplicável, ficando a disposição de todas as análises cabíveis e convenientes que o caso requer.

3.7.2. Após análise prévia de preços de mercado, tencionando a viabilidade da modalidade de contratação, foram observados que a utilização desta formalidade atende a necessidade e se revela vantajosa e econômica para este órgão.

3.7.3. A contratação se dará por meio de dispensa de licitação, conforme:

Art. 29. É dispensável a realização de licitação por empresas públicas e sociedades de economia mista:

II - para outros serviços e compras de valor até R\$ 50.000,00 (cinquenta mil reais) e para alienações, nos casos previstos nesta Lei, desde que não se refiram a parcelas de um mesmo serviço, compra ou alienação de maior vulto que possa ser realizado de uma só vez;

Considerando ainda o que estabelece o art. 29, §3º,

"Art. 29 (...)

§ 3o Os valores estabelecidos nos incisos I e II do caput podem ser alterados, para refletir a variação de custos, por deliberação do Conselho de Administração da empresa pública ou sociedade de economia mista, admitindo-se valores diferenciados para cada sociedade."

Nesse contexto, em aplicando o disposto pela Lei, o CONSAD - Conselho de Administração do LAFEPE, conforme registrado na Ata da Reunião do Conselho de Administração, realizada em 30 de abril de 2025, arquivada na JUCEPE em 21/07/2025, sob o protocolo nº 258861266, deliberou e aprovou a correção dos valores de dispensa de licitação utilizando-se o IPCA-IBGE de 2023 a 2024, corrigindo-se os valores dispostos pelos incisos I e II do art 29 da lei 13.303/2016, que passam a vigor com os seguintes limites:

(...)

II - para outros serviços e compras o valor de até R\$ 68.399,08 (sessenta e oito mil, trezentos e noventa e nove reais e oito centavos) fica corrigido para R\$ 72.105,18 (setenta e dois mil, cento e cinco reais e dezoito centavos).

3.8. **DO PREÇO A SER CONTRATADO**

3.8.1. Após realização de cotações pelo Setor de suprimentos (COSUP), observou-se que a **BIG COMPANY**, CNPJ/MF sob o nº 23.726.941/0001-02, apresentou menor preço dentre as empresas que atendem as especificações do objeto deste procedimento, vejamos:

BIG COMPANY	EVOLUTIA	TOTALWARE	AVANTIA	BRICON
R\$ 60.000,00	R\$ 68.478,50	R\$ 95.000,00	R\$ 562.480,93	R\$ 464.517,16

3.8.2. **EMPRESA VENCEDORA: BIG COMPANY**, CNPJ/MF sob o nº 23.726.941/0001-02 por ter apresentado o menor preço, resultando no valor a ser contratado de **R\$ 60.000,00** (Sessenta mil reais). Insta frisar que as cotações/proposta de preços foram conferidas e validados pela Coordenadoria de Informática - COINF, sendo atestada a sua vantajosidade e a sua compatibilidade com os preços do mercado.

4. **DA HABILITAÇÃO JURÍDICA**

4.1. A documentação relativa à regularidade Jurídica será em conformidade com o §5º, ART 7, do Regulamento Interno de Licitações e Contratos

4.1.1. A documentação relativa à **habilitação jurídica** consistirá em:

4.1.1.1. **No caso de empresário individual:** inscrição na Junta Comercial, Registro Público de Empresas Mercantis ou órgão equivalente, acompanhado de todas as alterações ou da consolidação respectiva;

4.1.2. **No caso de sociedades comerciais ou empresa individual de responsabilidade limitada:** ato constitutivo em vigor, devidamente registrado na Junta Comercial ou órgão equivalente, e, no caso de sociedades por ações, acompanhado de documentos de eleição de seus administradores, acompanhado de todas as alterações ou da consolidação respectiva;

4.1.3. **No caso de ser o participante sucursal, filial ou agência:** inscrição no Registro Público de Empresas Mercantis onde opera com averbação no Registro onde tem sede a matriz, acompanhado de todas as alterações ou da consolidação respectiva;

4.1.4. **No caso de sociedades simples:** inscrição do ato constitutivo no Registro Civil das Pessoas Jurídicas, acompanhada de prova de diretoria em exercício, acompanhado de todas as alterações ou da consolidação respectiva;

4.1.5. **No caso de sociedade empresária estrangeira em funcionamento no País:** decreto de autorização de funcionamento

5. **DA QUALIFICAÇÃO TÉCNICA**

5.1. Apresentar comprovação de aptidão para desempenho de atividade pertinente e compatível em características, quantidades e prazos com o objeto, mediante atestado (s) fornecido (s) por pessoa (s) de direito público ou privado, demonstrando a prestação de fornecimento do objeto executado pelo licitante.

5.1.1. O **LAFEPE** se reserva o direito de realizar diligências para comprova a veracidade dos atestados, podendo requisitar cópias dos respectivos contratos e aditivos e/ou outros documentos comprobatório do conteúdo declarado.

6. **DA CAPACIDADE ECONÔMICA E FINANCEIRA**

6.1. Certidão Negativa de Falência ou Recuperação Judicial, ou Liquidação Judicial, ou de Execução Patrimonial, conforme o caso, emitida pelo Cartório distribuidor da sede do licitante, ou de seu domicílio, dentro do prazo de validade previsto na própria certidão, ou, na omissão, expedida a menos de 180 (cento e oitenta) dias, contados da data de apresentação dos documentos de Habilitação e da Proposta Comercial, caso no documento não conste o prazo de validade.

6.2. Certidão Negativa de Falência, Recuperação Judicial ou Extrajudicial referente aos processos distribuídos pelo PJE (**Processos Judiciais Eletrônicos**) da sede da pessoa jurídica;

6.3. A certidão descrita no subitem "6.2." somente é exigível quando a Certidão Negativa de Falência ou Recuperação Judicial, ou Liquidação Judicial, ou de Execução Patrimonial Falência, Recuperação Judicial ou Extrajudicial do Estado da sede da licitante contiver a **ressalva expressa** de que não abrange os processos judiciais eletrônicos.

6.4. Empresas em recuperação judicial poderão participar da presente contrato, desde que, para tanto, comprovem mediante a apresentação de certidão judicial específica, o seu regular cumprimento do plano homologado e que certifique que a contratada está apta econômica e financeiramente a participar de procedimento licitatório e **desde que** atenda as condições para comprovação da capacidade econômica e financeira prevista neste Edital.

7. DA HABILITAÇÃO FISCAL E TRABALHISTA

- 7.1. A documentação relativa à **habilitação** consistirá em:
- 7.1.1. Prova de regularidade perante o **Instituto Nacional de Seguro Social - INSS**, através da Certidão Conjunta Negativa de Débitos Relativa aos Tributos Federais da Dívida Ativa da União.
- 7.1.2. Prova de Regularidade de débitos com o **Fundo de Garantia por Tempo de Serviço - FGTS, a través de Certificado de Regularidade do FGTS.**
- 7.1.3. Prova de inexistência de débitos com a **Fazenda Estadual do Estado do domicílio sede do contratado**, através de certidão expedida pelo órgão competente e que estejam dentro do prazo de validade.
- 7.1.4. Apresentar **Certidão Negativa de Débitos Trabalhistas - CNDT.**
- 7.1.5. Prova de inscrição no **CNPJ - Cadastro Nacional de Pessoa Jurídica.**

8. PRAZO, LOCAL E DEMAIS CONDIÇÕES DE EXECUÇÃO DO SERVIÇO

- 8.1. O fornecimento dos itens do objeto deste Termo de Referência se darão de forma **INTEGRAL em até 02 (dois) dias corridos, contados da emissão da Ordem de Fornecimento**, através de liberação de licenças para uso do software em nuvem e, se necessário, acesso remoto, para ajustes e configurações complementares, mantendo contato com a COINF – Coordenadoria de Informática, de segunda à sexta-feira, das 08h00min às 17h00min horas, de acordo com a necessidade do LAFEPE, obedecendo ao prazo contratual e às especificações descritas neste Termo de Referência; O Telefone para eventual agendamento será: (81) 3183- 1185, ou através do e-mail: diinf@lafepe.pe.gov.br.
- 8.2. Nos casos dos itens serem entregues em desconformidade com as condições, especificações e legislação respectiva, a Contratada será notificada para realizar as correções e entregar novamente o objeto licitado em até 15 (quinze) dias úteis, às suas expensas, renovando-se, dessa forma, o prazo para nova análise da Contratante.
- 8.3. Caso haja algum feriado local ou nacional, o fornecedor deverá realizar a entrega no primeiro dia útil subsequente.
- 8.4. Finalizada a implantação, deverá ser agendado junto à COINF o período de treinamento aos responsáveis pela operação da solução.
- 8.5. A aceitação do software e início das operações pelo LAFEPE não eximem a CONTRATADA das responsabilidades por ela garantidas;

9. DAS INFORMAÇÕES SOBRE OS RECURSOS

- 9.1. Os recursos financeiros para custear as despesas com o objeto desta contratação são provenientes de receita própria do LABORATÓRIO FARMACÊUTICO DO ESTADO DE PERNAMBUCO GOVERNADOR MIGUEL ARRAES S. A- LAFEPE.

10. DO PRAZO DE VIGÊNCIA DO CONTRATO

- 10.1. O prazo de vigência do Contrato decorrente desta dispensa de 12 (doze) meses contados da data de sua assinatura, podendo ser prorrogado de acordo com o art. 71 da Lei 13.303/2016.

11. DO PRAZO DE COMPARECIMENTO DO INTERESSADO PARA ASSINATURA DO CONTRATO

- 11.1. O contrato terá o prazo de 05 (cinco) dias para assinatura do contrato, contados a partir da convocação pela CONTRATANTE.

12. OBRIGAÇÕES DA CONTRATADA

- 12.1. Implantar a aquisição discriminada neste termo de referência;
- 12.2. Fornecer todo material e equipamento necessário à perfeita operação do software, devendo ser de primeira qualidade;
- 12.3. Será vedada a subcontratação total e parcial do objeto do presente contrato;
- 12.4. Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas neste processo;
- 12.5. A contratada é obrigada a obedecer a legislação trabalhista (Consolidação das Leis do Trabalho - CLT) - decreto-lei n.º 5.452, de 1º de Maio de 1943 e a Legislação Previdenciária - Lei nº 8.213, de 24 de julho de 1991, Lei nº 8.212, de 24 de julho de 1991 e Decreto nº 3.048, de 06 de Maio de 1999 e suas alterações posteriores;
- 12.6. A equipe técnica deverá ser qualificada para execução do trabalho;
- 12.7. O pagamento das despesas com alimentação e transporte da equipe durante o período de trabalho será de responsabilidade da contratada;
- 12.8. A contratada deverá obedecer às normas técnicas da associação brasileira de normas técnicas (ABNT) e também às normas internacionais;
- 12.9. Disponibilizar empregados em quantidades necessárias para a implantação do objeto adquirido.
- 12.10. Responsabilização pelo fiel pagamento dos salários, demais benefícios trabalhistas, encargos sociais e tributos, consoante a legislação vigente;
- 12.11. Arcar com a responsabilidade civil por todos e quaisquer danos materiais e morais causados pela ação ou omissão de seus empregados ou representantes, dolosa ou culposamente, à contratante ou a terceiros;
- 12.12. Instruir seus empregados a manterem sigilo a respeito das informações e quaisquer outros assuntos ligados a documentos e seus conteúdos, que porventura cheguem ao seu conhecimento por força da execução dos serviços;
- 12.13. Levar, imediatamente, ao conhecimento do fiscal do contrato do Laboratório Farmacêutico do Estado de Pernambuco Governador Miguel Arraes S/A - LAFEPE, qualquer fato extraordinário ou anormal que ocorrer na implantação do objeto contratado, para adoção das medidas cabíveis;
- 12.14. Todos os testes deverão ser efetuados conforme a especificação das normas adotadas pelo Laboratório Farmacêutico do Estado de Pernambuco Governador Miguel Arraes S/A - LAFEPE;
- 12.15. Os serviços ou materiais rejeitados pela fiscalização, devido ao uso de materiais que não sejam especificados e/ou materiais que não sejam qualificados como de primeira qualidade ou serviços mal executados, terão que ser refeitos pela contratada, sem nenhum ônus adicional para a contratante;
- 12.16. Responsabilizar-se pelas condições de serviço dando a devida assistência para que os mesmos sejam realizados de maneira adequada pela Contratante.
- 12.17. Orientações quanto ao procedimento de instalação e manutenção dos itens adquiridos.
- 12.18. Manter pessoa credenciada para supervisionar a execução da instalação dos equipamentos de monitoramento, e informar por escrito seu nome à Contratante, para receber orientações e comunicações e repassar às equipes que operarão o sistema.
- 12.19. Não efetuar despesas e/ou celebrar acordos em nome da Contratante;
- 12.20. Dirimir, sempre que solicitado pela Contratante, quaisquer dúvidas técnicas ou operacionais, fornecendo suporte via telefone, chat ou correio eletrônico;
- 12.21. O transporte dos materiais, inclusive para troca, quando houver a necessidade, será por conta e risco da proponente.

12.22. Caso a contratada não promova a reparação ou substituição previstas no item anterior acima, fica a contratada autorizada a contratar terceiro para fazê-lo, obrigando-se a contratada a ressarcir o LAFEPE em todos os custos, diretos e indiretos, incorridos por esta para a reparação ou substituição em questão, incluindo, porém não se limitando aos custos de aquisição de mercadorias para substituir a materiais defeituosos num prazo de 10 (dez) dias corridos a partir da data de notificação.

12.23. Empresa contratada deverá apresentar lista de produtos, com suas respectivas fichas técnicas e de segurança a contratante e informar através de documentação caso ocorra de alterações no fornecimento desses produtos.

12.24. Garantir que os produtos adquiridos atendam às normas de segurança, regulamentações técnicas aplicáveis e padrões de qualidade;

12.25. Elaborar cronograma de execução das atividades;

12.26. Garantia de suporte técnico com custos previstos na proposta da contratada;

13. OBRIGAÇÕES DO CONTRATANTE

o contratante obriga-se a:

13.1. Fiscalizar, como lhe prouver e no seu exclusivo interesse, o exato cumprimento das cláusulas e condições contratuais;

13.2. Acompanhar a implantação dos objetos adquiridos junto à contratada, e no caso de constatar quaisquer irregularidades, comunicá-las, por escrito, para que sejam tomadas as providências;

13.3. Quaisquer exigências da fiscalização, inerentes ao objeto do contrato, deverão ser prontamente atendidas pela contratada, sob pena de multa;

13.4. Designar funcionário para centralizar e fornecer informações pertinentes ao objeto do presente contrato à contratada;

13.5. A existência do gestor por parte da contratante de nenhum modo, diminui ou altera a responsabilidade da contratada na prestação dos serviços assumidos e a serem executados, inclusive perante terceiros, por qualquer irregularidade, não importando co-responsabilidade na eventual ocorrência;

13.6. Conferir e atestar Nota Fiscal/Fatura, através do gestor contratual, para pagamento, e ocorrendo irregularidades, solicitar à contratada a imediata correção;

13.7. Disponibilizar todas as informações e esclarecimentos que venham a ser solicitados pela CONTRATADA, em relação ao objeto;

13.8. Adotar as providências necessárias ao satisfatório cumprimento do contrato;

13.9. Fiscalizar o cumprimento das cláusulas e condições acordadas, registrando as deficiências, porventura existentes, devendo comunicá-la, por escrito, à CONTRATADA, para correção das irregularidades apontadas;

13.10. Efetuar a conferência entre a fatura apresentada, a solicitação do fornecimento e os demais documentos;

13.11. Efetuar o pagamento à CONTRATADA no prazo estipulado.

13.12. Aprovar objeto, desde que atendidas às necessidades acordadas;

13.13. Rejeitar, no todo ou em parte, o objeto em desacordo com as especificações contidas neste termo de referência;

14. DA FORMA, CONDIÇÕES E PRAZO DE PAGAMENTO

14.1. O pagamento será efetuado em moeda brasileira (Real) através de depósito bancário, em conta corrente da empresa Contratada, mediante atesto na nota fiscal/fatura pela área demandante, em até 30 (trinta) dias, mediante a atesto da nota fiscal pela fiscalização e gestão contratual;

14.2. O LAFEPE efetuará a CONTRATADA o pagamento do objeto deste Termo de Referência pelo valor global, dividido nas seguintes condições:

- a) 1ª parcela - 30 dias após emissão da Ordem de Fornecimento autorizada pelo LAFEPE - correspondente ao item 01 da descrição do objeto;
- b) 2ª parcela - 30 dias após conclusão dos serviços de implantação e treinamento aos responsáveis pela operação - correspondente ao item 02 da descrição do objeto;

14.3. Deverão estar inclusos nos preços apresentados todos os gastos do frete, inclusive quaisquer tributos, sejam eles sociais, trabalhistas, previdenciários, fiscais, comerciais ou de qualquer outra natureza resultantes da execução do contrato;

14.4. O LAFEPE reserva-se o direito de suspender o pagamento se o(s) produto(s) for(em) entregue(s) em desacordo com as condições e especificações constantes neste Termo de Referência, Edital e seus respectivos anexos;

14.5. Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido de alguma forma para tanto, o valor devido deverá ser acrescido de encargos moratórios proporcionais aos dias de atraso, apurados desde a data limite prevista para o pagamento até a data do efetivo pagamento, com base na variação do Índice de Preços ao Consumidor Ampliado - IPCA, do IBGE, aplicando-se a seguinte fórmula:

$$EM = I \times N \times VP$$

EM = Encargos Moratórios a serem acrescidos ao valor originariamente devido

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

VP = Valor da Parcela em atraso

I = Índice de atualização financeira, assim apurado: $I = (TX/100)/365$

TX = Percentual do IPCA anual TX = Percentual do IPCA anual

15. DO VALOR A SER CONTRATADO

15.1. Conforme Mapa de cotações elaborado pela COSUP, no valor de **R\$ 60.000,00** (Sessenta mil reais).

16. SANÇÕES

16.1. Além do que dispõe neste Termo de Referência e no contrato a CONTRATADA, em caso de inadimplemento de suas obrigações, garantindo o contraditório e a ampla defesa anteriormente a sua aplicação definida, ficará sujeita às sanções previstas no Capítulo X da RILC (Regulamento de Licitações e Contratos do LAFEPE) e a Seção III da Lei 13.303/2016.

17. DO ACOMPANHAMENTO E DA FISCALIZAÇÃO DO CONTRATO

17.1. A gestão do contrato será exercida pela COINF - Coordenadoria de Informática do LAFEPE.

17.2. O acompanhamento e a fiscalização do objeto do contrato serão exercidos por funcionário designado pelo coordenador de Informática, ao qual competirá acompanhar, fiscalizar, conferir e avaliar a execução, bem como dirimir e desembaraçar quaisquer dúvidas e pendências que surgirem, determinando o que for necessário à regularização das faltas, falhas, problemas ou defeitos observados, dando ciência de tudo à Contratada, conforme disposto nos artigos 169 e 170 do Regulamento LAFEPE.

17.3. O Contratante ao constatar qualquer irregularidade na execução do serviço por parte da Contratada expedirá notificação, para que a mesma regularize a situação, em até

72 horas, sob pena de, não o fazendo, ser aplicada a multa pertinente.

17.4. A existência do gestor por parte da contratante de nenhum modo, diminui ou altera a responsabilidade da contratada na prestação dos serviços assumidos e a serem executados, inclusive perante terceiros, por qualquer irregularidade, não importando corresponsabilidade na eventual ocorrência;

18. DOS CRITÉRIOS DE ACEITAÇÃO

18.1. O objeto deste contrato será recebido da seguinte forma:

a) PROVISORIAMENTE - pelo responsável na fiscalização, mediante visto no relatório dos serviços realizados, e posterior atesto na Nota fiscal;

b) DEFINITIVAMENTE - pelo gestor do contrato, mediante conferência dos serviços, quantitativos e valores contratados, com o atesto final da nota Fiscal.

18.2. O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da contratada pelos prejuízos resultantes da incorreta execução do contrato

19. MODO DE FORNECIMENTO

19.1. Os serviços a serem contratados serão prestados por meio de aquisição com **FORNECIMENTO INTEGRAL**.

19.2. Critério de julgamento: menor preço.

20. DO REAJUSTE

20.1. O Preço contratado poderá vir ser reajustado após 12 (doze) meses contados a partir da data limite para apresentação da proposta ou do orçamento a que essa se referir, utilizando-se para tanto, até o limite máximo do IPCA, fornecido pelo IBGE, ou outro que venha a substituí-lo, nos termos da Lei nº 12.525/03.

20.2. Havendo interesse das partes contratantes em prorrogar a avença, a empresa contratante deverá pleitear o reajuste dos preços até a data anterior à efetivação da prorrogação contratual, sob pena de, não fazendo tempestivamente, ocorrer a preclusão do seu direito.

20.3. Será assegurado o restabelecimento do equilíbrio econômico-financeiro inicial, 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, de acordo com o art. 81, inciso VI, da Lei nº 13.303/2016.

21. DA PROPOSTA

21.1. A proposta deverá conter o detalhamento da aquisição de forma clara, incluindo todos os itens e descritivos necessários ao fiel cumprimento dos serviços;

21.2. As propostas serão julgadas por **MENOR PREÇO**.

21.3. As propostas deverão seguir o modelo descrito no ANEXO II deste termo.

22. DA PROPRIEDADE, SIGILO E RESTRIÇÕES

22.1. Entre as medidas de segurança a serem tomadas no tocante à execução contratual, ao sigilo de todas as informações e à segurança dos documentos que compõem este instrumento, deve a CONTRATADA seguir as seguintes recomendações:

22.1.1. Identificar qualquer equipamento da empresa que venha a ser instalado nas dependências do CONTRATANTE, utilizando placas de controle patrimonial, selos de segurança, etc;

22.1.2. Manter sigilo absoluto sobre informações, dados e documentos integrantes dos serviços a serem executados, inclusive com a assinatura, pelo representante legal da CONTRATADA, do Termo de Compromisso (modelo conforme Anexo III);

22.1.3. Não permitir que dados ou informações do CONTRATANTE aos quais tenha acesso a CONTRATADA e/ou seus colaboradores sejam retirados das dependências do CONTRATANTE, não importando o veículo em que estes se encontrem, notadamente discos rígidos, discos óticos, pentes de memórias, documentos, mensagens eletrônicas e outros meios;

22.1.4. Observar, rigorosamente, todas as normas e procedimentos de segurança implementados no ambiente de Tecnologia da Informação do CONTRATANTE.

22.2. Do Termo de Compromisso

22.2.1. A **contratada** é integralmente responsável pela manutenção de sigilo sobre quaisquer dados e informações contidos em quaisquer documentos e em quaisquer mídias de que venha a ter conhecimento ou acesso durante a execução dos trabalhos, não podendo, sob qualquer pretexto e forma divulgar, reproduzir ou utilizar se não para os objetivos do Termo de Referência e do Contrato.

22.2.2. A **contratada** deverá apresentar o Termo de Compromisso de Sigilo constante dos anexo III do Termo de Referência preenchido até a data da assinatura do contrato.

22.3. Da Conformidade com a Lei Geral de Proteção de Dados Pessoais

22.3.1. A **CONTRATADA** declara estar ciente de que pode vir a receber ou ter acesso a dados pessoais de fornecedores, prestadores de serviço, colaboradores etc. da **CONTRATANTE** (os “Dados Pessoais”), para a exclusiva finalidade de cumprimento do Contrato de acordo com o objeto delimitado neste Termo de Referência (a “Finalidade”).

22.3.2. A **CONTRATADA** declara, por si e quaisquer terceiros sob sua responsabilidade, incluindo, mas não se limitando a funcionários, prepostos, colaboradores, terceirizados, prestadores de serviços, subcontratados e quaisquer pessoas, diretas ou indiretamente ligadas a ela, que tenham acesso aos Dados Pessoais por seu intermédio ou responsabilidade (as “Pessoas Autorizadas”) que, no desenvolvimento das atividades previstas no presente Termo de Referência, cumprirá integralmente a legislação aplicável à privacidade e ao tratamento de dados pessoais, incluindo, mas não se limitando à Lei 12.965/2014 (“Marco Civil da Internet”) e à Lei nº 13.709/2018 (“Lei Geral de Proteção de Dados” ou “LGPD”), empenhando-se em proceder a todo o tratamento necessários à execução do Contrato no estrito e rigoroso cumprimento da Lei.

22.3.3. A **CONTRATADA** se compromete a utilizar os Dados Pessoais a que tiver acesso em razão do Contrato apenas para a Finalidade e a armazená-los apenas e unicamente durante o período necessário ao cumprimento do Contrato e de sua Finalidade. Encerrado o referido prazo ou na hipótese de rescisão antecipada do Contrato, a Contratada deverá cessar, inteira e imediatamente, quaisquer processamentos realizados envolvendo os Dados Pessoais, utilizando todas as medidas de segurança necessárias e exigidas pela LGPD para a exclusão desses Dados Pessoais, independentemente de qualquer solicitação da **CONTRATANTE** sobre o tema, devendo comprovar por todos os meios possíveis e permitidos pela LGPD a cessação do tratamento dos Dados Pessoais.

22.3.4. A **CONTRATADA** reconhece ainda que a **CONTRATANTE** poderá solicitar, a qualquer momento, a exclusão ou a portabilidade dos Dados Pessoais, parcial ou inteiramente, obrigando-se a **CONTRATADA**, por si e pelas eventuais Pessoas Autorizadas, a interromper o tratamento dos Dados Pessoais e excluí-los ou efetuar a sua portabilidade, permanentemente, de seus ambientes físicos e virtuais, no prazo de 5 (cinco) dias úteis, contados da data de solicitação, comprovando tal exclusão mediante relatório competente. Não obstante a exclusão dos Dados Pessoais, a **CONTRATADA** continuará responsável, por si e pelas Pessoas Autorizadas, pelas obrigações assumidas no Contrato em relação à privacidade dos Dados Pessoais referente ao período durante o qual obteve acesso aos mesmos.

22.3.5. Constituem, ainda, obrigações da **CONTRATADA**:

- a) notificar a **CONTRATANTE** em quaisquer casos de violações aos Dados Pessoais fornecidos, como, por exemplo, incidentes de segurança, uso desautorizado, dentre outros;
- b) prestar assistência à **CONTRATANTE** para que esta cumpra com o seu dever de respostas aos titulares de Dados Pessoais, assim como junto à Autoridade Nacional de Proteção de Dados (ANPD) e qualquer outro órgão fiscalizador, sempre que assim requisitado;
- c) cumprir o dever de excluir/descartar, devolver, retificar e/ou limitar o tratamento de um Dado Pessoal, inclusive de eventuais cópias existentes, incluindo backups automáticos;
- d) disponibilizar para a Contratante todas as informações necessárias para demonstrar o seu cumprimento à legislação de proteção de dados, sempre que assim solicitadas, além de facilitar e contribuir com auditorias e inspeções, incluindo processos de prestação de contas (*accountability*);
- e) prover a todos os seus colaboradores treinamentos de conscientização em privacidade e segurança da informação sempre que necessário, nos termos da LGPD; e
- f) adotar as medidas de segurança descritas artigo 46 da LGPD.

23. DAS DISPOSIÇÕES FINAIS

23.1. Em caso de manifestação de desistência, fica caracterizado o descumprimento total da obrigação assumida, consoante o estabelecido no Art. 183 do Regulamento LAFEPE, sujeitando-o às penalidades legalmente estabelecidas.

23.2. A eventual rescisão do ajuste se dará nas hipóteses previstas na Lei nº 13.303/2016 e no regulamento do LAFEPE, não cabendo, à Contratada, direito a qualquer indenização.

Sweet Gallegher Caetano Costa
DIINF - Divisão de Informática
LAFEPE

ANEXO I - MATRIZ DE RISCO

MATRIZ DE RISCO			
CATEGORIA DO RISCO	DESCRIÇÃO	CONSEQUÊNCIA	ALOCÇÃO DO RISCO

RISCO ATINENTE AO TEMPO DA EXECUÇÃO	Atraso na execução do objeto contratual por culpa do Contratado.	Paralisação temporária das atividades	Contratado
	Fatores retardadores ou impeditivos da execução do contrato próprios do risco ordinário da atividade empresarial ou da execução.	Paralisação temporária das atividades.	Contratado
	Fatos retardadores ou impeditivos da execução do contrato que não estejam na sua álea ordinária, tais como fatos do príncipe.	Paralisação temporária das atividades.	Contratante
RISCO DA ATIVIDADE EMPRESARIAL	Alteração de enquadramento tributário, em razão do resultado ou de mudança da atividade empresarial, bem como por erro do Contratado na avaliação da hipótese de incidência tributária	Aumento ou diminuição do lucro do Contratado	Contratado
	Variação da taxa de câmbio	Aumento ou diminuição do custo do produto e/ou do serviço.	Contratado
	Elevação dos custos operacionais para o desenvolvimento da atividade empresarial em geral e para a execução do objeto em particular, tais como aumento de preço de insumos, prestadores de serviço e mão de obra devidamente comprovados	Aumento do custo do produto e/ou do serviço.	Contratado
RISCO TRABALHISTA E PREVIDENCIÁRIO	Responsabilização do LAFEPE por verbas trabalhistas e previdenciárias dos profissionais do Contratado alocados na execução do objeto contratual	Geração de Custos trabalhistas e/ou previdenciário para o LAFEPE, além de eventuais honorários advocatícios, multas e verbas sucumbenciais	Contratado
RISCO TRIBUTÁRIO E FISCAL (NÃO TRIBUTÁRIO)	Responsabilização do LAFEPE por recolhimento indevido em valor menor ou maior que o necessário, ou ainda de ausência de recolhimento, quando devido, sem que haja culpa do LAFEPE	Débito ou crédito tributário ou fiscal (não tributário)	Contratado

ANEXO II - MODELO DE PROPOSTA
MODELO DE PROPOSTA

Recife, de de 2025.

Ao
Laboratório Farmacêutico do Estado de Pernambuco Governador Miguel Arraes S.A. – Lafepe
Largo de Dois Irmãos, 1117 – Dois Irmãos
Recife/PE

Prezado Senhor,

A (nome da empresa), apresenta a sua proposta para contratação de empresa especializada para a execução dos prestação de serviços de **subscrição de licenças de solução de Segurança Integrada de Proteção Avançada de Endpoints** (estações de trabalho e servidores de rede) e **Detecção e Resposta de Endpoint (Endpoint Detection and Response - EDR)**, incluindo capacitação, serviço especializado de implantação, bem como suporte técnico por 12 meses no Laboratório Farmacêutico do Estado de Pernambuco.

A aquisição será realizada de acordo com o preconizado no Termo de Referência objeto desta proposta, e conforme abaixo informado:

1 -PREÇOS:

Valor Total dessa proposta:

- R\$ xxxxxxxxx(-----)

Em conformidade com a planilha (preço unitário)

2 - CONDIÇÕES DE PAGAMENTO

- Faturamento em 30 dias contados a partir da emissão da Nota fiscal

3 -VALIDADE DA PROPOSTA

A presente proposta é válida por 90 (noventa) dias.

4 - DECLARAÇÕES

Declaramos que em nossos preços estão incluídas as despesas indiretas (custo de apoio do escritório central), as operacionais (equipamentos de informática básicos, EPI's , hospedagem e deslocamento ao local da obra) e ainda as tributárias, fiscais ou contribuições sociais (PIS, COFINS, IR, ISS, Contribuição Social e INSS).

Sendo o que se apresenta para o momento e no aguardo de um pronunciamento favorável por parte de V.Sas., subscrevemo-nos,

RESPONSÁVEL DA EMPRESA

Nome Legível e Assinatura

ANEXO III - TERMO DE COMPROMISSO

O LABORATÓRIO FARMACÊUTICO DO ESTADO DE PERNAMBUCO GOVERNADOR MIGUEL ARRAES - LAFEPE - sediado no Largo de Dois Irmãos, 1117, Dois Irmãos, CEP 52171-010, Recife-PE, CNPJ nº 10.877.926/0001-13, doravante denominado CONTRATANTE, e, de outro lado, a <NOME DA EMPRESA>, sediada em <ENDEREÇO>, CNPJ n.º <CNPJ>, doravante denominada CONTRATADA;

CONSIDERANDO que, em razão do CONTRATO N.º XX/20XX doravante denominado CONTRATO PRINCIPAL, a CONTRATADA poderá ter acesso a informações sigilosas do CONTRATANTE;

CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção;

CONSIDERANDO o disposto na Política de Segurança da Informação da CONTRATANTE;

Resolvem celebrar o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO, doravante TERMO, vinculado ao CONTRATO PRINCIPAL, mediante as seguintes cláusulas e condições:

Cláusula Primeira - DO OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sensíveis e sigilosas, disponibilizadas pela CONTRATANTE, por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes para informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado.

Cláusula Segunda - DOS CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

Informação: é o conjunto de dados organizados de acordo com procedimentos executados por meios eletrônicos ou não, que possibilitam a realização de atividades específicas e/ou tomada de decisão.

Informação Pública ou Ostensiva: são aquelas cujo acesso é irrestrito, obtida por divulgação pública ou por meio de canais autorizados pela CONTRATANTE.

Informações Sensíveis: são todos os conhecimentos estratégicos que, em função de seu potencial no aproveitamento de oportunidades ou desenvolvimento nos ramos econômico, político, científico, tecnológico, militar e social, possam beneficiar a Sociedade e o Estado brasileiros.

Informações Sigilosas: são aquelas cujo conhecimento irrestrito ou divulgação possam

acarretar qualquer risco à segurança da sociedade e do Estado, bem como aquelas necessárias ao resguardo da inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas.

Contrato Principal: contrato celebrado entre as partes, ao qual este TERMO se vincula.

Cláusula Terceira - DAS INFORMAÇÕES SIGILOSAS

Serão consideradas como informação sigilosa, toda e qualquer informação escrita ou oral, revelada a outra parte, contendo ou não a expressão confidencial e/ou reservada. O TERMO informação abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: know-how, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades da CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominados INFORMAÇÕES, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes.

Parágrafo Primeiro - Comprometem-se, as partes, a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do CONTRATO PRINCIPAL, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas informações, que se restringem estritamente ao cumprimento do CONTRATO PRINCIPAL.

Parágrafo Segundo - As partes deverão cuidar para que as informações sigilosas fiquem restritas ao conhecimento das pessoas que estejam diretamente envolvidas nas atividades relacionadas à execução do objeto do CONTRATO PRINCIPAL.

Parágrafo Terceiro - As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que:

I - Sejam comprovadamente de domínio público no momento da revelação;

II - Tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;

III - Sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

Cláusula Quarta - DOS DIREITOS E OBRIGAÇÕES

As partes se comprometem e se obrigam a utilizar a informação sigilosa revelada pela outra parte exclusivamente para os propósitos da execução do CONTRATO PRINCIPAL, em conformidade com o disposto neste TERMO.

Parágrafo Primeiro - A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento expresso e prévio da CONTRATANTE.

Parágrafo Segundo - A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO bem como da natureza sigilosa das informações. I - A CONTRATADA deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência à CONTRATANTE dos documentos comprobatórios.

Parágrafo Terceiro - A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa da CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pela CONTRATANTE.

Parágrafo Quarto - Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste TERMO.

I - Quando requeridas, as informações deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

Parágrafo Quinto - A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados, contratados e subcontratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do CONTRATO PRINCIPAL.

Parágrafo Sexto - A CONTRATADA, na forma disposta no parágrafo primeiro, acima, também se obriga a:

- I - Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das informações, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;
- II - Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmo judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das Informações Proprietárias por seus agentes, representantes ou por terceiros;
- III - Comunicar à CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das informações, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e
- IV - Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações sigilosas.

Cláusula Quinta - DA VIGÊNCIA

O presente TERMO tem natureza irrevogável e irretroatável, permanecendo em vigor desde a data de sua assinatura até expirar o prazo de classificação da informação a que a CONTRATADA teve acesso em razão do CONTRATO PRINCIPAL.

Cláusula Sexta - DAS PENALIDADES

A quebra do sigilo e/ou da confidencialidade das informações, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pela CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme Art. 87 da Lei nº. 8.666/93.

Cláusula Sétima - DISPOSIÇÕES GERAIS

Este TERMO de Confidencialidade é parte integrante e inseparável do CONTRATO PRINCIPAL.

Parágrafo Primeiro - Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa fé, da equidade, da razoabilidade, da economicidade e da moralidade.

Parágrafo Segundo - O disposto no presente TERMO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tal como aqui definidas.

Parágrafo Terceiro - Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:

- I - A CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;
- II - A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pela

CONTRATANTE, todas as informações requeridas pertinentes ao CONTRATO PRINCIPAL.

III - A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;

IV - Todas as condições, TERMOS e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;

V - O presente TERMO somente poderá ser alterado mediante TERMO aditivo firmado pelas partes;

VI - Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VII - O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações disponibilizadas para a CONTRATADA, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessário a formalização de TERMO aditivo a CONTRATO PRINCIPAL;

VIII - Este TERMO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar Informações Sigilosas para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

Cláusula Oitava - DO FORO

A CONTRATANTE elege o foro da cidade de Recife, onde está localizada a sede da CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO é assinado pelas partes em 2 vias de igual teor e um só efeito.

_____, _____ de _____ de 20____

De Acordo,

CONTRATANTE CONTRATADA

<Nome> <Nome>

<Matrícula> <Qualificação>



Documento assinado eletronicamente por **Sweet Gallegher Caetano Costa**, em 22/10/2025, às 14:09, conforme horário oficial de Recife, com fundamento no art. 10º, do [Decreto nº 45.157, de 23 de outubro de 2017](#).



Documento assinado eletronicamente por **Clovis Vieira de Aquino**, em 22/10/2025, às 14:14, conforme horário oficial de Recife, com fundamento no art. 10º, do [Decreto nº 45.157, de 23 de outubro de 2017](#).



A autenticidade deste documento pode ser conferida no site http://sei.pe.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **75571622** e o código CRC **DA5291D2**.

Referência: Processo nº 0060407938.000006/2025-68

SEI nº 68071826