GOVERNO DO ESTADO DA BAHIA
SECRETARIA DE TURISMO-SETUR

TERMO DE REFERÊNCIA

SERVIÇOS SEM DEDICAÇÃO EXCLUSIVA DE MÃO DE OBRA

(X) Contratação Direta – Dispensa de Licitação Eletrônica com disputa (ComprasNet)

(Processo Administrativo nº 032.2305.2026.0001175-60)

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1 Objeto:

(X) Serviço: O objeto da presente contratação direta é a contratação de solução de tecnologia da informação, compreendendo o fornecimento e renovação de 100 licenças de uso do antivírus corporativo WithSecure Elements EPP+EDR, incluindo upgrade das licenças, serviços de suporte técnico especializado, gerenciamento da solução e demais atividades correlatas, conforme especificações técnicas, quantitativos e condições estabelecidas neste Termo de Referência.

1.1.1 As especificações do objeto obedecerão às condições e exigências estabelecidas neste Termo de Referência , observado o disposto na tabela abaixo.

Participação [ampla/exclusiva]	Lote/ Item	Código SIMPAS	Descrição	Unidade de Fornecimento (UF)	Quantitativo	Cronograma/Prazo
Ampla	02.81.32.00000562-2	100	LICENCA DE USO antivírus, WithSecure Elements EPP + EDR Premium para Desktops e Servidores. Com atualização, suporte e manutencao de 24 meses, Governo	Unidade	100	24 meses

1.1.2. As especificações do objeto constam:

1.1.2.1. A solução de antivírus deve estar devidamente licenciada e atender a todos os requisitos descritos abaixo, garantindo uma proteção abrangente e eficiente contra ameaças cibernéticas, As especificações técnicas listadas descrevem **capacidades mínimas e funcionais**, podendo ser atendidas por produtos equivalentes que comprovem desempenho igual ou superior;

1.1.2.2. Deverá possuir a capacidade de varrer, detectar, analisar e remover malwares, riskwares, spywares e demais formas de ameaças e códigos maliciosos conhecidos, que estão associadas a tipos específicos de malware para detectar e prevenir ataques semelhantes.

1.1.2.3. Deverá possuir a capacidade de proteção uma combinação de inteligência artificial, detecção comportamental, algoritmos de aprendizado de máquina e mitigação de exploração, que utiliza de consulta em nuvem do fabricante para antecipar e prevenir ameaças conhecidas e desconhecidas (zero-day), usando uma abordagem não dependente de assinatura para fornecer uma segurança de endpoint complementar e mais eficaz;

1.1.2.4. Além dos mecanismos de proteção contra malware, tanto via assinatura quanto com base em consulta em nuvem, o produto deverá possuir capacidade de quarentena de arquivos centralizada, bem como Firewall, IDS/IPS/HIPS, controle de aplicativos, controle de conexões, atualizador de softwares, proteção para a navegação, reversão de arquivos comprometidos, controle de conteúdo web por categorias, criptografia de disco, controle de dispositivos e quarentena de rede. Estas devem ser totalmente

integradas, instaladas através de um único agente sem a necessidade de instalação de módulos adicionais ou agente de comunicação prévio;

1.1.2.5. O conjunto de softwares que compõe a solução de antivírus deverão ser totalmente gerenciáveis através de uma única console de gerenciamento centralizado, em nuvem (Cloud) e de forma que todos os produtos sejam monitorados através desta.

1.1.2.6. Ter a funcionalidade de repositório remoto centralizado e integrado de atualizações do produto, bem como a lista de vacinas de vírus (assinatura de malwares), do mecanismo da solução (engines) e principalmente do cache/repositório de atualizações de software da Microsoft e de terceiros (atualizador de softwares), podendo o administrador instalar sem ônus, com suporte para as plataformas Windows e Linux, podendo o administrador escolher a plataforma desejada de acordo com seu ambiente;

1.1.2.7. Ter a função de prevenção de epidemia ou isolamento do host na rede, de forma manual ou automática;

1.1.2.8. O fabricante deve possuir site próprio para envio de amostras de arquivos e URL, infectados, suspeitos ou falso positivos, e que registre por e-mail através de um código identificado (por exemplo, número do chamado, protocolo ou solicitação).

1.1.2.9. Possuir suporte à integração com soluções no padrão Syslog/SIEM (Security Information and Event Management);

1.1.2.10. O fabricante deverá ser membro do programa "Microsoft Active Protection Program" para obtenção de acesso antecipado a informações de vulnerabilidade para que eles possam fornecer proteções atualizadas aos clientes mais rapidamente;

1.1.2.11. O fabricante deve seguir e respeitar o Framework de Cibersegurança do NIST (National Institute of Standards and Technology) e a NBR ISO/IEC 27001 com suas soluções de segurança;

1.1.2.12. A solução deve ser certificada pela organização independente e reconhecida, AV-TEST;

1.1.2.13. A solução deve usar o MITRE ATT&CK para fornecer informações correlacionadas;

1.1.2.14. Suportar o gerenciamento de todos os endpoints a partir da nuvem do próprio fabricante, sendo vedada a possibilidade de hospedar em terceiros;

1.1.2.15. A console de administração deve centralizar a administração dos sistemas operacionais Windows, macOS, Linux e dispositivos móveis;

1.1.2.16. Permitir a criação de tipo de usuários para acesso à console de gerenciamento, com no mínimo as opções de usuário administrador e usuário para leitura (read only);

1.1.2.17. Não possuir restrições para múltiplos logins simultâneos de usuários ao sistema de gerenciamento da solução;

1.1.2.18. Deve ser possível implementar MFA (Multi-Fator de Autenticação) para todos os usuários da console de Administração;

1.1.2.19. Manter um registro de ações realizadas pelos administradores no sistema de gerenciamento da solução de segurança;

1.1.2.20. Atualização de listas, vacinas, mecanismos de varredura e desinfecção através da Internet via protocolo HTTP/80 ou HTTPS/443 (visando evitar conflitos com protocolos e portas ou não permitidos em nossa rede/datacenter/DMZ/VPN) e disponibilizando estas atualizações para todas as demais ferramentas que compõem a solução de antimalware automaticamente sem a intervenção do administrador;

1.1.2.21. Comunicação segura entre a console de gerenciamento e clientes gerenciados utilizando protocolo seguro HTTPS através da porta TCP/443, visando ter mais segurança da comunicação e proteção das configurações de políticas do produto, além de evitar conflitos com protocolos e portas não permitidos em nossa rede/datacenter/DMZ/VPN.

1.1.2.22. Ser capaz de atrelar uma política de configuração automaticamente para novas máquinas ingressadas no domínio;

1.1.2.23. Ser capaz de atrelar uma política de configuração do produto à uma Unidade Organizacional do MS Active Directory, ou seja, ser possível atrelar uma política de configuração Financeiro às máquinas da OU de nome Financeiro no MS AD;

1.1.2.24. A console de gerenciamento dos endpoints em Nuvem deve ser capaz de propor recomendações de segurança baseado nas detecções do ambiente;

1.1.2.25. A solução deve conter um único agente de instalação para gerenciar todas as funções nas estações de trabalho e fazer comunicação direta com a plataforma de gerenciamento, sem a necessidade de interfaces ou equipamentos intermediários;

1.1.2.26. A solução deve ter um único agente conectado a console de administração para todos os recursos descritos nesse documento;

1.1.2.27. Deverá ser possível e estar licenciado para coletar as seguintes informações dos dispositivos gerenciados:

1.1.2.27.1. Versão do agente instalado;

1.1.2.27.2. Nome e versão do sistema operacional;

1.1.2.27.3. Quantidade de memória RAM;

1.1.2.27.4. Tamanho total e espaço livre do Disco;

1.1.2.27.5. Fabricante e modelo da CPU;

1.1.2.27.6. Versão da BIOS;

1.1.2.27.7. Endereços IP atribuídos;

1.1.2.27.8. Endereço IP externo da origem da conexão;

1.1.2.27.9. Chave de recuperação de sistemas operacionais criptografados;

1.1.2.27.10. Endereço físico (MAC);

1.1.2.27.11. Nome do Host;

1.1.2.27.12. Nome do usuário conectado no dispositivo;

1.1.2.28. Permitir a alteração das configurações do produto/agentes endpoint nos clientes de maneira remota;

1.1.2.29. Deve ser capaz de bloquear as configurações nos endpoints, evitando que os usuários ou administradores locais alterem as configurações do produto;

1.1.2.30. Deve ser capaz de bloquear o encerramento dos processos do produto e a sua desinstalação nos endpoints, mesmo os usuários com privilégios de administradores locais ou do domínio;

1.1.2.31. Deve ser capaz de configurar uma senha através da console de gerenciamento, que será solicitada ao usuário, caso seja executado uma das seguintes ações no endpoint: desinstalar o produto, desativar todos os recursos de segurança ou desativar temporariamente os recursos de segurança;

1.1.2.32. A solução deve permitir fácil acesso às estações de trabalho através de conexão RDP (Remote Desktop Protocol), proporcionando meios como atalhos (rdp://hostname) ou botões de acesso direto;

1.1.2.33. Geração de relatórios que contenham informações sobre as infecções e atualizações da solução;

1.1.2.34. Deve ter a capacidade de exportar relatórios gerados pela solução;

1.1.2.35. Enviar alertas em caso de epidemias através de e-mail;

1.1.2.36. Permitir a visualização de relatórios contendo as seguintes informações:

1.1.2.36.1. Visão geral do status de proteção;

1.1.2.36.2. Relatório de uso de assinatura;

1.1.2.36.3. Relatório de eventos de segurança;

1.1.2.36.4. Relatório de registro de auditoria;

1.1.2.37. Possuir no dashboard informações do estado geral da solução de segurança e hosts gerenciados;

1.1.2.38. Possuir no dashboard status geral de atualizações de software do ambiente;

1.1.2.39. Os logs de eventos gerados e armazenados na plataforma devem possuir no mínimo as seguintes informações:

1.1.2.39.1. Data e hora do evento;

1.1.2.39.2. Gravidade;

1.1.2.39.3. Módulo de proteção que gerou o evento;

1.1.2.39.4. Máquina em que ocorreu o evento de segurança;

1.1.2.39.5. Descrição do evento;

1.1.2.39.6. Nome do usuário;

1.1.2.39.7. Identificar eventos similares;

1.1.2.40. Deve ser possível exportar os logs de eventos;

1.1.2.41. Deve ser possível facilitar e customizar a identificação do dispositivo na console, através de: grupos de máquinas, TAGs e/ou grupos;

1.1.2.42. Deve ser possível através da console de gerenciamento, realizar manualmente as seguintes tarefas nos dispositivos, de forma individual ou agrupado:

1.1.2.42.1. Aplicar atualizações de Software;

1.1.2.42.2. Verificar atualizações pendentes;

1.1.2.42.3. Realizar a verificação de existência de malware (Scan);

1.1.2.42.4. Remover e/ou desinstalar o dispositivo da console de gerenciamento;

1.1.2.42.5. Entrar ou sair do modo de isolamento de rede;

1.1.2.42.6. Reiniciar o sistema operacional;

1.1.2.42.7. Reiniciar o serviço do agente de Endpoint Protection;

1.1.2.42.8. Enviar mensagens customizadas para o dispositivo;

1.1.2.42.9. Desativar e/ou reativar recursos individuais de segurança;

1.1.2.43. A solução deverá possuir suporte, no mínimo, aos seguintes sistemas operacionais:

1.1.2.43.1. Microsoft Windows 11 (todas as edições 64-bits, incluindo ARM64);

1.1.2.43.2. Microsoft Windows 10 (edições 32-bit e 64-bits);

1.1.2.43.3. macOS 12 "Monterey", 13 "Ventura" e 14 "Sonoma";

1.1.2.43.4. AlmaLinux 8, 9;

1.1.2.43.5. Amazon Linux 2;

1.1.2.43.6. CentOS 7 e 8;

1.1.2.43.7. Debian 10, 11, 12;

1.1.2.43.8. Oracle Linux 7, 8, 9;

1.1.2.43.9. RHEL 7, 8, 9;

1.1.2.43.10. Ubuntu 18.04, 20.04, 22.04, 24.04;

1.1.2.44. A interface dos clientes de proteção do endpoint deve ter a opção de ser instalada em português do Brasil;A solução de proteção do endpoint deve permitir ser instalada, no mínimo, através das seguintes opções:
1.1.2.45. Via pacote MSI compatível com MS GPO;
1.1.2.46. Através de scripts de instalação;
1.1.2.47. Instalação manual com envio de informações automáticas por e-mail;
1.1.2.48. Ter a possibilidade de configuração de políticas diferenciadas para cada estação ou grupo de estações;
1.1.2.49. Deve ser possível ocultar a interface do agente de segurança do endpoint da barra de tarefas do sistema para evitar a intrusão do usuário e higienização da barra de tarefas dos aplicativos;
1.1.2.50. A solução deve incluir um mecanismo de atualização automática dos agntes de endpoints instalados, eliminando a necessidade de intervenção manual por parte do administrador, garantindo que todos os endpoints permaneçam atualizados com as últimas definições de segurança do agente;
1.1.2.51. Os endpoints devem ter a capacidade de consultar um proxy HTTP, definido através da console de gerenciamento, para realizar as atualizações automáticas;
1.1.2.52. Deve ser possível definir pastas, arquivos e hashes de arquivo do tipo SHA-1, possibilitando estes serem excluídos de todas as verificações e medidas de segurança;
1.1.2.53. Deve ser possível exibir ou ocultar as notificações relacionadas à expiração da licença;
1.1.2.54. Deve ser possível definir a quantidade de dias anteriores à expiração da licença para começar a mostrar notificações;
1.1.2.55. Deve ser possível definir uma mensagem que será exibida para os usuários antes que a licença expire;
1.1.2.56. **Proteção em tempo real**
1.1.2.57. Deve possuir verificação em tempo real de todos os objetos / artefatos que os usuários finais acessam ou executam;
1.1.2.58. Possuir gerenciamento e configuração remota para a funcionalidade de antivírus, anti-spyware, anti-malwares, detecção de rootkit e proteção de browser;
1.1.2.59. Possuir gerenciamento e configuração remota para a funcionalidade de Zero Hour e/ou Zero Day, análise comportamental de ameaças, deverá também ter ação contra arquivos raros ou suspeitos;
1.1.2.60. Deve possuir integração da Interface de Verificação de Antimalware (AMSI), que permite que os sistemas operacionais usem mecanismos fabricante de Antimalware para fornecer segurança adicional. Por exemplo, o Windows usa o AMSI para verificar scripts do PowerShell e macros do Office VBA com as soluções antimalware instaladas;
1.1.2.61. Deve ser possível verificar automaticamente todos os arquivos que serão executados;
1.1.2.62. Deve ser possível definir extensões de arquivos que serão excluídos da varredura em tempo real;
1.1.2.63. Deve ser possível definir processos que serão excluídos da varredura em tempo real;
1.1.2.64. Deve ser possível decidir a ação automaticamente em caso de detectção de uma infecção. As ações no objeto infectado devem ser pelo menos:
    1.1.2.64.1. Renomear;
    1.1.2.64.2. Excluir;
    1.1.2.64.3. Desinfetar;
    1.1.2.64.4. Quarentenar;
1.1.2.65. deve ser possível atribuir ações diferentes para Riskware e Spywares detectados;
1.1.2.66. Deve possibilitar proteger o arquivo "Hosts". Com esse recurso ativado todas as alterações serão revertidas para um arquivo limpo;
1.1.2.67. Deve possibilitar verificar arquivos armazenados em unidades de rede;
1.1.2.68. A solução deve integrar-se com um sistema de análise de ameaças cibernéticas baseado em nuvem, que utilize inteligência artificial e aprendizado de máquina para analisar e refinar dados de ameaças. Este sistema deve fornecer uma rede de proteção em tempo real, aproveitando dados de milhões de dispositivos conectados, garantindo detecção rápida e precisa de novas ameaças;
1.1.2.69. **Verificação Manual e Agendada**
1.1.2.70. Deve permitir que o escaneamento seja configurado pelo administrador, com frequência diária, em horário definido, para todas as estações, para um grupo ou estações específicas;
1.1.2.71. Possuir capacidade de diminuir a prioridade do processo evitando a sobrecarga do processamento da estação de trabalho, e dessa forma causando menos impacto para o usuário final;
1.1.2.72. Deve ser possível controlar o que acontece quando um dispositivo de armazenamento USB é conectado ao computador, possuindo pelo menos as seguintes ações:
    1.1.2.72.1. Não fazer nada;
    1.1.2.72.2. Pedir para o usuário para verificar o USB;
    1.1.2.72.3. Verificar o USB silenciosamente;
    1.1.2.72.4. Fazer a verificação do USB e mostrar o resultado para o usuário;

1.1.2.73. Deve ser possível definir uma frequência de escaneamento de malware, possibilitando escolher pelo escaneamento diário, semanal ou mensal;

1.1.2.74. Deve ser possível especificar os dias da semana e o horário do escaneamento de procura por malwares no disco;

1.1.2.75. Deve ser possível especificar por extensões (por exemplo: COM EXE SYS BIN SCR DLL SHS HTM HTML HTT VBS JS), os arquivos que serão escaneados pelo produto;

1.1.2.76. Deve ser possível habilitar ou desabilitar a verificação de arquivos dentro de arquivos compactados (por exemplo, arquivos ZIP);

1.1.2.77. Deve ser possível habilitar ou desabilitar a verificação de arquivos que estão dentro dos arquivos da caixa de correio (por exemplo, arquivos pst);

1.1.2.78. Deve ser possível definir uma das seguintes ações, após detecção de um arquivo malicioso encontrado:

1.1.2.78.1. Limpar;

1.1.2.78.2. Excluir;

1.1.2.78.3. Renomear;

1.1.2.78.4. Quarentenar;

1.1.2.78.5. Perguntar ao usuário;

1.1.2.79. Deve ser possível definir a quantidade de recursos do sistema que a verificação pode usar, podendo definir um modo de menor consumo de recursos no host analisado;

1.1.2.80. Deve ser possível a definição de arquivos ou pastas que serão excluídos da verificação;

1.1.2.81. Controle de conteúdo web

1.1.2.82. Deve possuir gerenciamento e configuração remota para a funcionalidade de controle do Conteúdo da Web por categorização do conteúdo, independente do firewall da rede, pois, em caso dos equipamentos estiverem fora do parque computacional (por exemplo home office ou em trânsito) as políticas da corporação podem continuar sendo adotadas, além de controle específico para proteger equipamentos que necessitam de conexões bancárias;

1.1.2.83. Possuir controle de conteúdo da navegação web, com no mínimo 15 categorias, que sejam atualizadas e fornecidas pelo fabricante, sem necessidade de criar/acrescentar ou customizar novas categoria manualmente), as categorias desejadas são:

1.1.2.83.1. Serviços de Pagamento;

1.1.2.83.2. Bancos/Transações Bancárias;

1.1.2.83.3. Hacking/Invasão;

1.1.2.83.4. Navegação anonima/proxy/vpn;

1.1.2.83.5. Chat/Bate Papo/Namoro;

1.1.2.83.6. Golpe/Phishing/Spam;

1.1.2.83.7. Downloads considerados Ilegais;

1.1.2.83.8. Downloads de Softwares (em geral);

1.1.2.83.9. Streaming;

1.1.2.83.10. Entretenimento;

1.1.2.83.11. Jogos;

1.1.2.83.12. Redes Sociais;

1.1.2.83.13. Compras Online;

1.1.2.83.14. Webmails;

1.1.2.83.15. Conteúdo Adulto;

1.1.2.84. O controle de conteúdo por categorização deve permitir a configuração por grupos, podendo o administrador determinar, por grupo, quais categorias serão permitidas ou não e se o controle estará ativado para aquele grupo ou não;

1.1.2.85. Deve possibilitar adicionar manualmente através da console de gerenciamento, websites que serão permitidos ou bloqueados nos grupos de estações de trabalho;

1.1.2.86. Deve possibilitar através de uma opção de configuração, o bloqueio imediato de acesso a todos os sites e deve ser possível especificar uma lista de websites de exceção que serão permitidos caso esta opção seja configurada;

1.1.2.87. Deve possibilitar que os usuários com direitos administrativos na estação de trabalho prossigam ou não para as páginas bloqueadas;

1.1.2.88. A solução de proteção de navegação deve usar mecanismos para identificar a reputação de websites, classificando-os como:

1.1.2.88.1. Perigosos;

1.1.2.88.2. Suspeitos;

1.1.2.88.3. Proibidos;

1.1.2.89. Deve ser possível mostrar a reputação dos websites nos resultados de pesquisa da Web (Google e Bing);

1.1.2.90. Deve possibilitar a imposição de busca segura (conceito SafeSearch) nos endpoints, que faz com que os mecanismos de pesquisa usem o nível estrito para ocultar conteúdo adulto;

1.1.2.91. Deve possibilitar o controle de execução no navegador de tipos de conteúdo/mídias da Web, tais como: pdf, msword, x-excel, silverlight, flash e java;

1.1.2.92. Deve possibilitar adicionar regras customizadas para o controle de execução de tipos de conteúdo/mídias da Web;

1.1.2.93. Deve possibilitar armazenar na console de gerenciamento em Cloud todos os eventos de URL do website bloqueado;

1.1.2.94. **Controle de Conexões Bancárias**

1.1.2.95. Deve possuir a funcionalidade de bloqueio automático de novas conexões quando for detectado que foi aberta uma conexão bancária e/ou conexão que utilize protocolo seguro;

1.1.2.96. Além da detecção automática, deve ser possível também adicionar um conjunto de websites que processam informações confidenciais para serem protegidas pelo controle conexão;

1.1.2.97. Quando conectado a um portal de pagamento, a solução deverá restringir acesso remoto ao equipamento para evitar a exposição de dados sensíveis através de conexões remotas (Remote Desktop, Logmein, VNC, Anydesk, Teamviewer e etc);

1.1.2.98. A área de transferência do Windows deverá ser limpa após o encerramento das conexões bancárias, visando evitar equívocos dos usuários e a maior proteção dos dados que possam estar presentes na área de transferência durante o trabalho realizado em uma conexão com o banco (senhas, dados sensíveis, informações pessoais, etc.);

1.1.2.99. Quando conectado a um portal de pagamento, deverá ser possível bloquear automaticamente as conexões de rede de ferramentas de linha de comando e scripts;

1.1.2.100. **Gerenciamento Firewall**

1.1.2.101. Deve possibilitar o gerenciamento e configuração remota para a funcionalidade de firewall através da console de gerenciamento em Cloud;

1.1.2.102. Deve ser possível a criação de pelo menos 03 (três) perfis diferentes de firewall;

1.1.2.103. Deve permitir controlar as conexões de entrada e saída dos endpoints;

1.1.2.104. Deve possibilitar a definição de regras de entrada e saída baseadas em controle de portas TCP e UDP;

1.1.2.105. Deve ser integrado ao Firewall do Windows, possibilitando escolher pela definição de novas regras de entrada e saída, bem como a definição apenas de regras adicionais as já existentes no Firewall do Windows;

1.1.2.106. Deve ser possível habilitar a notificação para o usuário final quando um novo evento de bloqueio de conexão for realizado pelo Firewall;

1.1.2.107. Deve possibilitar o isolamento da estação de trabalho, restringindo a comunicação da máquina com outros hosts da rede e da internet;

1.1.2.108. Deve possibilitar definir um conjunto de domínios ou FQDN, ao qual a estação de trabalho poderá se comunicar durante o tempo que estiver em modo de isolamento;

1.1.2.109. Deve possibilitar a retirada da máquina do isolamento através da console de gerenciamento em nuvem;

1.1.2.110. Deve ser possível definir uma mensagem personalizada, que será exibida para o usuário quando a estação de trabalho entrar em modo de isolamento;

1.1.2.111. **Atualizador de softwares**

1.1.2.112. Possuir gerenciamento e configuração remota para a funcionalidade de atualização de softwares de terceiros;

1.1.2.113. Se baixar todas as atualizações diretamente da internet, os dispositivos de uma rede consomem uma enorme quantidade de tráfego externo. Para reduzir isso, deve ser possível usar um servidor local de cache, que baixará os arquivos solicitados apenas uma vez e, em seguida, os distribuirá para os dispositivos dentro da rede;

1.1.2.114. O repositório de atualizações local deverá possibilitar ser instalado em Sistemas Operacionais Windows e Linux;

1.1.2.115. A solução de atualização de softwares de terceiros deve ter a capacidade e estar licenciado devidamente para implementar um repositório de atualizações local, que funcione como um armazenador de atualizações de software e vacinas para toda a rede corporativa;

1.1.2.116. O repositório centralizado e local das atualizações de software, deve haver compatibilidade com Microsoft e softwares de terceiros, tais como softwares da Google (Chrome), Oracle (Java), Mozilla (Thunderbird), dentre outros;

1.1.2.117. Deve ter a capacidade de verificar a disponibilidade de atualizações, gerenciar, obter os pacotes de instalação de forma centralizada, armazenar (cache local) e aplicar/instalar automaticamente as atualizações de softwares, melhorias e patches de correções disponibilizados pela Microsoft, para seus sistemas operacionais, aplicativos de escritório da família Microsoft Office e demais aplicativos como o .NET, Internet Explorer e Edge, entre outros softwares deste mesmo fabricante, através de configurações na console de gerenciamento central da solução de proteção para endpoints;

1.1.2.118. Capacidade de verificar a disponibilidade de atualizações, gerenciar, obter os pacotes de instalação de forma centralizada, armazenar (cache local) e aplicar/instalar automaticamente as atualizações de softwares, melhorias e patches de correções para softwares de terceiros (Adobe, Oracle Java, Google Chrome, Zoom, 7-Zip, aplicativos Open Source como a família Open Office, Notepad++, Mozilla Firefox e Thunderbird, etc), através de configurações na console de gerenciamento central da solução de proteção para endpoints;

1.1.2.119. Deve ter a capacidade de aplicar as atualizações e correções de produtos Microsoft e de terceiros:

1.1.2.119.1. Em horário agendado;

1.1.2.119.2. Sem a necessidade de intervenção ou ação do usuário final;

1.1.2.119.3. Mesmo quando o usuário logado não possui privilégios administrativo;

1.1.2.119.4. Mesmo quando o computador estiver bloqueado ou quando não houver usuário conectado;

1.1.2.119.5. Quando necessário reiniciar o equipamento após um update, ser capaz de adiar o reboot para evitar atrapalhar o usuário em horário de trabalho;

1.1.2.119.6. Ter a capacidade de excluir atualizações especificas da varredura ou da instalação automatizada, seja ela pelo seu ID ou simplesmente pelo nome do produto, por exemplo "java";

1.1.2.119.7. Deve ser capaz de gerar alertas sobre atualizações críticas de segurança pendentes de instalação;

1.1.2.119.8. Deve ser capaz de apontar através da console de gerenciamentos os CVEs (Common Vulnerabilities and Exposures) de cada atualização pendente no ambiente;

1.1.2.119.9. Possibilidade de criar lista de programas para exclusão da verificação da necessidade de atualização de software;

1.1.2.120. **Controle de Dispositivos**

1.1.2.121. Deve possuir gerenciamento e configuração remota para liberação ou restrição de funcionalidade de controle de dispositivos (Ex.: pen drives, hd externo, impressoras, wifi, bluetooth). Deverá possuir a capacidade de alertar caso um equipamento seja conectado, restringir acesso e a gravação em dispositivos de armazenamento removíveis (pen drive e hd externo, por exemplo);

1.1.2.122. Deve permitir bloquear dispositivos no mínimo pelo Hardware ID, ID do dispositivo, ID compatível e Classe GUID;

1.1.2.123. Deve ter a capacidade de bloquear a escrita em dispositivos de armazenamento em massa, permitindo somente a leitura;

1.1.2.124. Deve ter a capacidade de bloquear a execução de binários (executáveis) a partir de dispositivos de armazenamento em massa;

1.1.2.125. O bloqueio de dispositivos deve permitir bloquear um único dispositivo e liberar todos os demais, bem como liberar um único dispositivo e bloquear os demais. Ex.: Bloquear qualquer Pendrive exceto um em um único computador;

1.1.2.126. Deve emitir alertas de tentativa de uso do dispositivo bloqueado por ordem do administrador do sistema, contendo no alerta o ID do dispositivo bloqueado e a identificação da máquina que tentou utilizá-lo;

1.1.2.127. **Tarefas Automatizadas**

1.1.2.128. Deve possuir a capacidade que criar backups do sistema operacional ou pontos de restauração do sistema de forma agendada e centralizada através da console de gerenciamento;

1.1.2.129. Deverá ter a capacidade de buscar e upgrade do "instalador do agente de segurança" (tecnologia do cliente do endpoint, não referente a update de vacinas ou mecanismos internos do produto) e implementá-la automaticamente se disponível, para que ele possa estar sempre na versão mais moderna, com novas funcionalidade e atualizada, consequentemente deixando o ambiente mais protegido;

1.1.2.130. Deverá ter a capacidade de automaticamente ou de forma agendada, bloquear, hibernar, reiniciar ou desligar o sistema operacional do endpoint;

1.1.2.131. **Reversão de comprometimento**

1.1.2.132. Deverá possuir a capacidade de efetuar backup em tempo real e reverter/restaurar arquivos ao estado original e o registro do sistema Windows em caso de uma infecção/ataque bem-sucedida por ransomware, tanto na estação de trabalho, quanto nos servidores;

1.1.2.133. Deve possibilitar apenas o monitoramento do sistema operacional e apenas relatar alterações não autorizadas;

1.1.2.134. Deverá ser possível especificar um caminho nos hosts protegidos que serão armazenados os arquivos de backup;

1.1.2.135. Deve possibilitar especificar o tamanho máximo para os arquivos de backup. Desta forma se o tamanho de um arquivo exceder o valor fornecido, não será realizado o backup do arquivo, possibilitando assim evitar cópias de arquivos muito grandes;

1.1.2.136. **Configuração locais de rede**

1.1.2.137. A solução de proteção de endpoint deve oferecer a funcionalidade de configuração de diferentes locais de rede. Essa funcionalidade deve permitir que os administradores controlem e ajustem as configurações de segurança com base no local onde o dispositivo está conectado, proporcionando uma proteção adaptativa e específica para cada ambiente de rede;

1.1.2.138. Um administrador pode configurar um perfil de rede "Em casa" onde o firewall e o Atualizador de Software estão ativados para garantir proteção máxima em uma rede possivelmente menos segura. Simultaneamente, o administrador pode configurar um perfil de rede "No escritório" onde o firewall pode ser desativado (supondo que a rede do escritório já esteja protegida por um firewall centralizado) e o Atualizador de Software pode ser desativado para evitar interferências durante o horário de trabalho. A solução deve automaticamente aplicar as regras correspondentes assim que o dispositivo muda de uma rede para outra, garantindo uma segurança adaptada e eficaz em todos os cenários de uso;

1.1.2.139. A solução deve permitir a criação e gerenciamento de múltiplos perfis de rede, cada um representando um ambiente de rede específico, tais como "Em casa", "No escritório" e "Rede pública";

1.1.2.140. Cada perfil de rede deve incluir um conjunto de regras e políticas de segurança que se aplicam automaticamente quando um dispositivo é detectado em um determinado local de rede;

1.1.2.141. A solução deve ser capaz de identificar o local de rede com base em pelo menos:

1.1.2.141.1. Máscara de rede;

1.1.2.141.2. Endereço IP do servidor DHCP;

1.1.2.141.3. Endereço IP do gateway padrão;

1.1.2.142. Deve ser possível configurar múltiplos gatilhos para um mesmo local, assegurando uma identificação precisa;

1.1.2.143. A solução deve permitir a criação de regras específicas para cada perfil de rede configurado. Essas regras podem incluir, mas não se limitam a:

1.1.2.143.1. Ativação ou desativação do firewall;

1.1.2.143.2. Ativação ou desativação do Atualizador de Software;

1.1.2.143.3. Regras específicas de acesso à internet e restrições de aplicativos;

1.1.2.144. As regras devem ser aplicadas automaticamente quando o dispositivo é detectado no local de rede correspondente;

1.1.2.145. A solução deve fornecer uma interface de gestão centralizada que permita aos administradores configurar, visualizar e gerenciar os perfis de rede, locais e regras de segurança;

1.1.2.146. A interface deve oferecer facilidade de uso, com opções intuitivas para adicionar, modificar e remover locais e regras, bem como monitorar o status e a eficácia das políticas aplicadas;

1.1.2.147. **Coleta de chaves da Criptografia de disco**

1.1.2.148. A solução deve incluir ferramentas para o gerenciamento eficaz da criptografia nos dispositivos, permitindo sua ativação, configuração e monitoramento centralizado.

1.1.2.149. A solução de proteção de endpoint deve oferecer funcionalidades de criptografia de disco, garantindo a confidencialidade dos dados armazenados nos dispositivos. A criptografia deve ser gerenciável a partir de uma visão geral do estado da criptografia em todos os dispositivos protegidos;

1.1.2.150. A solução deve permitir a visualização do status da criptografia de disco ao selecionar um endpoint na console de administração, também deve ser possível observar através de relatórios de dispositivo, proporcionando uma gestão completa e centralizada;

1.1.2.151. A solução deve incluir ferramentas para a coleta e gerenciamento de chaves de recuperação. A funcionalidade deve garantir que as chaves de recuperação estejam acessíveis e visíveis em um portal centralizado;

1.1.2.152. A solução deve suportar a criptografia de discos utilizando o Bitlocker com o "protetor de senha de recuperação". Deve ser possível configurar e verificar a coleta bem-sucedida das chaves de recuperação em um portal de segurança centralizado, garantindo a disponibilidade dessas chaves para procedimentos de recuperação de dados;

1.1.2.153. **Proteção contra Ransomware**

1.1.2.154. A solução deve monitorar pastas em busca de alterações potencialmente prejudiciais feitas por ransomware ou outro software prejudicial semelhante;

1.1.2.155. A solução deve possibilitar que aplicativos confiáveis possam ter acesso a pasta;

1.1.2.156. A solução deve possibilitar que aplicativos desconhecidos pelo fabricante possam ser adicionados a lista de aplicativos confiáveis;

1.1.2.157. A solução deve ser capaz de identificar pastas que contém documentos, imagens ou outro conteúdo de usuário final e fazer o monitoramento da mesma;

1.1.2.158. A solução deve possibilitar adicionar pastas para serem excluídas do monitoramento, ou seja, não serão verificadas;

1.1.2.159. **Controle de aplicativos**

1.1.2.160. A solução de deve ser capaz de realizar no mínimo as seguintes ações quando executado uma aplicação:

1.1.2.161. Permitir;

1.1.2.162. Bloquear;

1.1.2.163. Permitir e monitorar;

1.1.2.164. A solução dever ser capaz de identificar o evento executado pela aplicação, possibilitando assim a capacidade de criar regras de bloqueio ou de acesso, correspondendo com no mínimo os eventos abaixo:

1.1.2.165. Execução do aplicativo;

1.1.2.166. Carga de modulo;

1.1.2.167. Início do instalador;

1.1.2.168. Inicialização do aplicativo e carregamento do modulo;

1.1.2.169. Acesso a arquivo;

1.1.2.170. A solução dever possuir no mínimo os tipos de condições(gatilhos) abaixo para possibilitar a criação de regras de bloqueio ou de acesso:

1.1.2.171. Caminho do arquivo;

1.1.2.172. SHA1 de identificação;

1.1.2.173. SHA256 de identificação;

1.1.2.174. Reputação do software;

1.1.2.175. Versão do software;

1.1.2.176. Nome do software;

1.1.2.177. Empresa que fabricou o software;

1.1.2.178. A solução dever possuir no mínimo os tipos de condicional abaixo para possibilitar a criação de regras de bloqueio ou de acesso:

1.1.2.179. Contém;

1.1.2.180. Começa com;

1.1.2.181. Termina com;

1.1.2.182. É igual a;

1.1.2.183. Não é igual a;

1.1.2.184. É menor que;

1.1.2.185. É maior que;

1.1.2.186. É menor que ou igual a;

1.1.2.187. É maior ou igual a;

1.1.2.188. Detecção de eventos do sistema

1.1.2.189. A solução deve ser capaz de centralizar os logs de eventos dos sistemas Windows na console de gerenciamento. É essencial que permita uma análise detalhada dos eventos relacionados a possíveis ataques em máquinas Windows, incluindo, por exemplo: contas bloqueadas, tentativas de alteração de senha, falhas de logon, registros de auditoria apagados, tentativas de instalação de serviço, erros fatais do Windows (BSoD), entre outros eventos relevantes.

1.1.2.190. Características gerais do Endpoint Detection e Response (EDR)

1.1.2.191. A solução deve prover funcionalidades de Endpoint Detection and Response (EDR) baseadas em sensores leves instalados em estações de trabalho e servidores, coletando eventos comportamentais como criação de processos, conexões de rede, acesso a arquivos e alterações de sistema para análise centralizada em nuvem.

1.1.2.192. A solução deve utilizar o mesmo agente de Endpoint protection (EPP) para a função também de EDR, possibilitando a operação do EDR sem a necessidade de instalar agentes específicos.

1.1.2.193. A solução deve utilizar análise comportamental em tempo real, reputação e big data com apoio de machine learning para diferenciar atividades legítimas de comportamentos suspeitos ou maliciosos, reduzindo falsos positivos e destacando apenas detecções relevantes.

1.1.2.194. A solução deve apresentar as detecções em uma linha do tempo (timeline) que consolide todos os eventos e hosts impactados, permitindo entender o encadeamento do ataque, a origem provável e o alcance do incidente em múltiplos dispositivos.

1.1.2.195. A solução deve suportar estações de trabalho e servidores com sistemas operacionais Windows, macOS e distribuições Linux contempladas pelo fabricante do sistema operacional, utilizando sensores desenhados para resistir a tentativas de sabotagem por atacantes.

1.1.2.196. A solução deve disponibilizar console de gerenciamento baseado em navegador, acessível por HTTPS, sem necessidade de infraestrutura local dedicada, permitindo a administração centralizada de todos os dispositivos protegidos.

1.1.2.197. A solução deve disponibilizar funcionalidades que orientem o analista na análise passo a passo, sugerindo verificações adicionais e ações recomendadas conforme o tipo de ameaça identificado.

1.1.2.198. A solução deve permitir exploração avançada de eventos (Event Search), com filtros sofisticados sobre os dados brutos coletados dos endpoints, possibilitando threat hunting proativo pelo time de segurança.

1.1.2.199. A solução deve permitir implantação manual utilizando um arquivo executável (.EXE), adequado para ambientes menores, onde os usuários podem visualizar e utilizar a chave de assinatura.

1.1.2.200. A solução deve permitir implantação manual utilizando um arquivo MSI, possibilitando instalação off-line em estações de trabalho e servidores sem necessidade de conexão direta com o portal.

1.1.2.201. A solução deve oferecer a opção de convidar usuários por e-mail, permitindo que eles realizem a instalação em seus dispositivos de forma autônoma, sem acesso direto à chave de assinatura

1.1.2.202. A solução deve suportar métodos automatizados de implantação, garantindo distribuição eficiente e padronizada para organizações que utilizam ferramentas de gerenciamento de TI.

1.1.2.203. A solução deve permitir implantação centralizada via GPO do Active Directory, possibilitando a distribuição automatizada para múltiplos dispositivos dentro do domínio.

1.1.2.204. A solução deve fornecer templates ou scripts MSI configuráveis para integração com GPO.

1.1.2.205. A solução deve permitir distribuição automatizada pelo Microsoft Intune, garantindo instalação remota e centralizada em dispositivos Windows.

1.1.2.206. A solução deve suportar instalação como um aplicativo Win32 no Microsoft Intune, garantindo compatibilidade com diferentes políticas de gerenciamento de endpoints corporativos.

1.1.2.207. **Detecção de contexto**

1.1.2.208. A solução deve correlacionar diversos eventos aparentemente independentes em um mesmo contexto de ataque, formando incidentes de "contexto amplo" que incluam usuários, dispositivos, processos e comunicações associados à ameaça.

1.1.2.209. A solução deve atribuir níveis de risco, confiança e criticidade às detecções, permitindo priorizar o tratamento dos incidentes com maior impacto potencial ao ambiente monitorado.

1.1.2.210. A solução deve utilizar o histórico de decisões (incidentes confirmados e falsos positivos) para treinar continuamente o mecanismo de detecção, aprimorando a capacidade de identificar ataques reais e reduzir ruídos ao longo do tempo.

1.1.2.211. A solução deve oferecer recursos de investigação que permitam detalhar cada incidente, com visualização de processos envolvidos, conexões de rede, arquivos acessados, comandos executados e demais evidências coletadas pelos sensores.

1.1.2.212. A plataforma deve estar licenciada para armazenar e disponibilizar Logs de eventos e incidentes do EDR pelo período de 12 meses.

1.1.2.213. A solução deve disponibilizar assistente de investigação ou funcionalidades equivalentes que orientem o analista na análise passo a passo, sugerindo verificações adicionais e ações recomendadas conforme o tipo de ameaça identificado.

1.1.2.214. A solução deve permitir a exportação ou coleta de pacotes de evidências para análise forense detalhada, incluindo arquivos, artefatos de sistema e informações de rede relevantes ao incidente.

1.1.2.215. **Resposta a incidentes (manual e automatizada)**

1.1.2.216. A solução deve oferecer um conjunto de ações de resposta remota diretamente a partir do console, como encerramento de processos maliciosos, bloqueio de executáveis suspeitos, coleta de evidências adicionais e restauração de arquivos, conforme suportado pelo sistema operacional.

1.1.2.217. A solução deve permitir configurar respostas avançadas que, uma vez habilitadas em perfis de política, ampliem o conjunto de ações disponíveis para resposta remota e automação de contramedidas.

1.1.2.218. A solução deve permitir a criação de regras de ações automatizadas para incidentes, de forma que determinadas categorias de detecção disparem automaticamente respostas predefinidas, como isolamento do dispositivo ou elevação do caso para atendimento especializado.

1.1.2.219. A solução deve possibilitar o isolamento de um ou mais dispositivos da rede, manualmente ou de forma automatizada, permitindo apenas o tráfego mínimo necessário para administração enquanto todo o restante do tráfego é bloqueado, de forma a conter movimentação lateral do atacante.

1.1.2.220. A solução deve registrar e exibir claramente no console todas as ações de resposta executadas (manuais ou automáticas), incluindo data, hora, usuário responsável e dispositivos afetados, para fins de auditoria e rastreabilidade.

1.1.2.221. A solução deve permitir a criação de regras de resposta automatizada por organização, com condições baseadas em tipo de incidente, nível de risco e outros critérios, permitindo ajustar o comportamento da automação ao apetite de risco do contratante.

1.1.2.222. A solução deve disponibilizar recomendações de melhores práticas para uso do EDR (frequência de revisão de incidentes, verificação do estado geral do parque, acompanhamento de aplicações em uso, etc.), acessíveis pelo próprio console de gerenciamento.

1.1.2.223. **Gestão de acesso, SSO federado e identidades**

1.1.2.224. A solução deve permitir autenticação de administradores por meio de single sign-on (SSO) federado, possibilitando integração com provedores de identidade corporativos compatíveis (por exemplo, serviços compatíveis com Microsoft Entra ID e protocolos amplamente adotados no mercado).

1.1.2.225. A solução deve suportar a federação de domínios de e-mail da organização, de forma que os usuários possam autenticar-se utilizando suas credenciais corporativas, sem necessidade de senhas específicas adicionais para o portal de segurança.

1.1.2.226. A solução deve suportar o uso de autenticação multifator (MFA) conforme as políticas definidas no provedor de identidade federado, reforçando o controle de acesso ao console de gerenciamento de segurança.

1.1.2.227. A solução deve disponibilizar painel de controle que consolide o estado dos incidentes, dispositivos monitorados e tendências de segurança, permitindo que o contratante ou seu parceiro de serviços gerenciados acompanhem rapidamente a postura de segurança dos endpoints.

1.1.2.228. **Operação**

1.1.2.229. A solução deve permitir a criação de relatórios de e-mail personalizados sobre eventos de segurança, possibilitando ao administrador:

1.1.2.229.1. selecionar o conjunto de eventos de segurança a ser incluído por meio de filtros,

1.1.2.229.1.1.1. definir o layout/modelo do relatório, configurar o agendamento e os destinatários dos e-mails, de forma que os relatórios sejam enviados automaticamente com a periodicidade definida.

1.1.2.230. A solução deve permitir elevar o incidente para a equipe especializada do fabricante, a partir de opção específica dentro do próprio incidente, possibilitando que casos complexos sejam analisados por especialistas em ameaças avançadas, com fornecimento de orientação detalhada de resposta.

1.1.2.231. A solução deve prever que o serviço de elevação de casos ao fabricante (serviço de análise especializada de incidentes) seja contratado por meio de créditos, de forma que o contratante possa adquirir futuramente créditos de uso para acionar a equipe especializada apenas quando necessário.

1.1.2.232. A solução deve permitir a visualização detalhada da Árvore de Processos, exibindo os processos envolvidos na detecção e seus impactos, incluindo:

1.1.2.232.1. Origem do processo

1.1.2.232.2. Usuário associado à execução

1.1.2.232.3. Linha de comando utilizada

1.1.2.232.4. Localização do arquivo executável

1.1.2.232.5. Soma de verificação (SHA1) para análise de integridade

1.1.2.232.6. Atividades executadas pelo processo e relações com outros eventos

1.1.2.233. Classificação mínima de incidentes

1.1.2.234. Os proponentes deverão comprovar, por meio de documentação técnica oficial do fabricante, que a solução proposta implementa detecção e classificação de todos os tipos de incidentes listados neste item.

1.1.2.235. A solução deve possuir mecanismo de detecção e classificação automática de incidentes capaz de identificar, no mínimo, os seguintes tipos de incidentes e atividades suspeitas, com correlação e geração de alertas no console:

1.1.2.235.1. Acessos anormais a arquivos – acesso incomum a arquivos, incluindo múltiplos tipos de documentos ou arquivos de sistema sem privilégio adequado.

1.1.2.235.2. Modificação de arquivo anormal – alteração de arquivos ou binários de sistema, conversão de arquivos em executáveis, exclusão de logs, cópias de sombra ou executáveis após a execução.

1.1.2.235.3. Biblioteca ou módulo anormal – uso de bibliotecas/módulos incomuns ou com má reputação em serviços de reputação.

1.1.2.235.4. Localização anormal – arquivos presentes em locais não convencionais.

1.1.2.235.5. Conexão de rede anormal – conexões de rede atípicas, como portas incomuns, conexões a serviços externos não usuais (por exemplo, redes sociais), downloads anômalos ou outras atividades de rede fora do padrão.

1.1.2.235.6. Parâmetros anormais – uso de parâmetros de processo que divergem das normas de operação, sugerindo risco de segurança ou má configuração.

1.1.2.235.7. Privilégios anormais – discrepância entre os privilégios atribuídos a um processo e o esperado para sua função, incluindo elevação ou redução anormal de privilégios.

1.1.2.235.8. Processo anormal – ocorrência de processos considerados incomuns para o ambiente.

1.1.2.235.9. Relação de processos anormais – cadeia de processos incomum, por exemplo, cliente de e-mail executando cmd.exe ou powershell.exe.

1.1.2.235.10. Execução de processo anormal – processos ou scripts executados com parâmetros suspeitos ou a partir de locais de arquivo atípicos.

1.1.2.235.11. Atividade anormal do usuário – atividades suspeitas de usuários, como alteração de grupos de permissão.

1.1.2.235.12. Anomalia – eventos estatisticamente incomuns no comportamento normal dos ativos monitorados.

1.1.2.235.13. Arquivo de backdoor – execução de arquivo que concede acesso não autorizado ou controle remoto do sistema.

1.1.2.235.14. Conexão de rede de comando e controle (C2/CC) – conexões a servidores de comando e controle conhecidos ou suspeitos.

1.1.2.235.15. Alteração de visibilidade de arquivos – ocultação ou criação de arquivos e diretórios ocultos.

1.1.2.235.16. Alterando configurações de segurança – alterações em configurações de segurança, como regras de firewall, usuários administrativos ou acesso a modo desenvolvedor.

1.1.2.235.17. Alterando informações de usuário – criação, remoção ou modificação de contas e atributos de usuários.

1.1.2.235.18. Incidentes em ambientes de nuvem – anomalias relacionadas principalmente a identidades e uso indevido de credenciais em serviços de nuvem.

1.1.2.235.19. Processo limpo comprometido – processos legítimos executando atividades não previstas em seu código original, indicando possível injeção ou comprometimento.

1.1.2.235.20. Criação de ferramentas de ataque – geração ou implantação de ferramentas maliciosas ou de uso dual no host.

1.1.2.235.21. Roubo de credencial – uso de métodos ou ferramentas conhecidos para exfiltrar credenciais.

1.1.2.235.22. Ataque dirigido – atividades indicativas de ataque planejado e direcionado a alvos específicos.

1.1.2.235.23. Injeção de código – execução de código customizado dentro de outro processo.

1.1.2.235.24. Destino de injeção – processos ou componentes sendo alvo de injeção de código malicioso.

1.1.2.235.25. Movimento lateral – tentativas de obter mais acesso movendo-se entre hosts na rede.

1.1.2.235.26. Iniciador de movimento lateral – processos responsáveis por iniciar ações de movimento lateral.

1.1.2.235.27. Destino de movimento lateral – processos ou hosts alvo de ações de movimento lateral.

1.1.2.235.28. Anomalias de registro (logs) – entradas de log incomuns ou suspeitas.

1.1.2.235.29. Parâmetros maliciosos – parâmetros de execução com alta probabilidade de intenção maliciosa.

1.1.2.235.30. Processo malicioso – processos identificados como maliciosos por inteligência de ameaças.

1.1.2.235.31. Malware – software projetado para causar dano a sistemas, redes ou dados.

1.1.2.235.32. Persistência – tentativas de manter presença contínua no host (por exemplo, criação de tarefas agendadas, serviços, autoruns).

1.1.2.235.33. Phishing – atividades relacionadas a tentativas de induzir usuários a revelar informações pessoais ou confidenciais, inclusive via e-mail enganoso.

1.1.2.235.34. Escalação de privilégio – tentativas de obter privilégios mais elevados, como tentativas repetidas de logon administrativo.

1.1.2.235.35. PUP (Programas Potencialmente Indesejados) – detecção de programas que, embora não estritamente maliciosos, são indesejados (adware, barras de ferramentas, pop-ups, etc.).

1.1.2.235.36. Atividades de reconhecimento – varreduras de rede e outras ações para identificação de vulnerabilidades e mapeamento do ambiente.

1.1.2.235.37. Abuso de script – uso indevido de componentes programáveis (Bash, Python, PowerShell, cscript e similares).

1.1.2.235.38. Modificação de arquivo confidencial – alterações em arquivos sensíveis que possam afetar autenticação ou controle de acesso.

1.1.2.235.39. Alteração de sensor – tentativas de modificar, desativar ou burlar o sensor/agent de segurança.

1.1.2.235.40. Falsificação de arquivos – coleta ou inspeção de documentos, histórico de navegação e outras informações a partir de arquivos locais.

1.1.2.235.41. Falsificação de entradas (input) – captura de dados de entrada, como pressionamentos de tecla e capturas de tela.

1.1.2.235.42. Falsificação de memória – criação de despejos de memória ou acesso indevido a conteúdo de memória.

1.1.2.235.43. Falsificação de rede – atividades como varredura de portas, sondagem de endereços IP, sniffing de DNS ou outras formas de coleta de informações de rede.

1.1.2.235.44. Falsificação de configurações de segurança – leitura ou inspeção das configurações de segurança (regras de firewall, políticas, etc.).

1.1.2.235.45. Falsificação de informações de usuário – tentativas de acessar arquivos de credenciais, hashes de senha ou informações relacionadas a autenticação.

1.1.2.235.46. Falsificação de vulnerabilidades – tentativas de localizar e explorar vulnerabilidades conhecidas.

1.1.2.235.47. Uso inadequado do sistema ou da ferramenta – uso malicioso de componentes ou ferramentas do sistema que não foram projetados para programação, mas que são abusados em ataques.

1.1.2.236. O objeto desta contratação não se enquadra como bem de luxo, nos termos do art. 20 da Lei Federal nº 14.133/2021 e sua regulamentação.

1.1.2.237. Na contratação de que trata este TR/Habilitação não será exigida da contratada a realização de transição contratual com transferência de conhecimento, tecnologia e técnicas empregadas.

1.2 O prazo de vigência do Contrato é de 24 meses, a **contar da data subscrição da Autorização de Prestação de Serviços – APS**, observado o artigo 105 da Lei Federal n° 14.133/2021.

1.3 O Contrato apresenta maior detalhamento das regras que serão aplicadas ao prazo de vigência.

2. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

2.1 A fundamentação da contratação, da caracterização do objeto e de seus quantitativos está especificada:
(X) em tópico próprio do Estudo Técnico Preliminar

3. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO, CONSIDERADO O CICLO DE VIDA DO OBJETO

3.1 A descrição da solução como um todo está especificada:
(X) em tópico próprio do Estudo Técnico Preliminar (ETP) 00132394531

4. REQUISITOS DA CONTRATAÇÃO

4.1 Sustentabilidade:

4.1.1 Não serão definidos critérios e práticas de sustentabilidade na contratação, conforme justificativa apresentada pelo gestor competente no processo administrativo de que trata este TR, **doc. Estudo Técnico Preliminar (ETP) 00132394531**

4.2 Indicação de marcas ou modelos

4.2.1 Na contratação serão exigidas a(s) seguinte(s) marca(s), característica(s) ou modelo(s), de acordo com as justificativas contidas no:

(X) Estudo Técnico Preliminar

1. Marca e similaridade - excepcionalmente será permitida a indicação de uma ou mais marcas ou modelos, desde que justificada tecnicamente no processo, nas hipóteses descritas no art. 41, inc. I, da Lei Federal nº 14.133/2021.

2. O disposto neste item se aplica à contratação de serviços, desde que justificadamente.

4.3 Exame de adequação do objeto (amostras, exame de conformidade, prova de conceito, ou outros testes destinados à aferição da aceitabilidade da proposta)

4.3.1 Não será exigido(a) exame de adequação do objeto.

4.3.2 Durante o prazo de vigência do contrato ou da ata de registro de preços, a Administração poderá, justificadamente, exigir amostra ou prova de conceito do bem (art. 41, inc. II, da Lei Federal nº 14.133/2021).

4.4 Vistoria

4.4.1 Não será exigida a realização de vistoria prévia.

4.5 Subcontratação

4.5.1 Não será admitida a subcontratação do objeto contratual.

4.6 Garantia

4.6.1 Garantia de proposta

4.6.1.1 Não haverá exigência da garantia de proposta de que trata o art. 58 da Lei Federal n° 14.133/2021.

4.6.2 Garantia da contratação

4.6.2.1 Não haverá exigência da garantia da contratação, pelas razões constantes no processo administrativo de que trata este TR , previsto no **art. 96 da Lei Federal nº 14.133/2021** e na **Lei Estadual nº 14.634/2023**, considerando que o objeto da contratação consiste no fornecimento de licenças de software com serviços acessórios, classificado como de baixo risco e sem complexidade operacional que justifique a exigência da garantia.

4.7 Participação de pessoas jurídicas reunidas em consórcio

(X) Não se aplica — procedimento de Dispensa Eletrônica não admite consórcios.

5. MODELO DE EXECUÇÃO DO OBJETO

5.1 Regime de execução

5.1.1 Condições de execução

5.1.1.1 A execução do objeto se dará da seguinte forma:

5.1.1.1.1 O prazo de execução do objeto será de 24 meses a contar da data

(X) da subscrição da Autorização de Prestação de Serviços – APS.

5.1.1.1.2 Cronograma de realização do objeto: até 20 dias após a assinatura da APS

5.2 Local da execução

5.2.1 As especificações do endereço para execução do objeto constam:

A prestação dos serviços deverá ser feita no Município de Salvador, Estado da Bahia, no seguinte endereço: SUFOTUR, 3ª Avenida, Nº 390, 2º andar Plataforma 4 - Ala Norte Centro Administrativo da Bahia - CAB. CEP: 41.745-005

5.3 Materiais a serem disponibilizados

5.3.1 Para a perfeita execução do objeto, a contratada deverá disponibilizar os materiais, equipamentos, ferramentas e utensílios necessários, nas quantidades suficientes e adequadas.

5.4 Garantia, manutenção e assistência técnica

5.4.1 O período de licenciamento do software será de 24 (Vinte quatro) meses, com suporte técnico de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, na cidade de Salvador (BA). Durante o período de licenciamento o fabricante vai garantir o funcionamento do software, com suporte técnico prestado em caso de falha. Deverá ser garantida neste prazo a atualização de versões, releases, componentes (bibliotecas, filtros etc.) e módulos dos produtos. Todos os produtos deverão ter o mesmo período de licenciamento., contado da entrega efetiva do produto ou do término da execução dos serviços (art. 26, incs. I e II, e §1º, do CDC).

5.5 Informações relevantes para o dimensionamento da proposta

5.5.1 As informações relevantes para o dimensionamento da proposta constam deste TR/Habilitação.

5.5.2 O prazo de validade da proposta será de, no mínimo, 60 (sessenta) dias, a contar da data de abertura da etapa competitiva no sistema ComprasNet .

5.5.2.1 Será considerada não escrita a fixação de prazo de validade inferior ao mínimo, ficando facultado aos proponentes ampliá-lo.

5.5.3 O proponente deverá apresentar a sua proposta e declaração de elaboração independente de proposta, conforme modelo integrante deste TR/Habilitação.

5.5.4 Além das informações que já constam neste TR/Habilitação, constituem, ainda, informações relevantes para o dimensionamento da proposta as que constam do **anexo** integrante deste TR/Habilitação.

5.6 ACORDO DE NÍVEL DE SERVIÇO

5.6.1 A CONTRATADA será responsável pelo cumprimento e medição dos índices estabelecidos neste item que serão auditados pela CONTRATANTE durante todo o prazo de vigência do contrato, e que poderão ser revistos, a qualquer tempo, com vistas à melhoria ou ajustes na qualidade dos serviços prestados, mediante acordo entre as partes;

5.6.2 Níveis de Serviço e Tempo esperados:

5.6.2.1 Plantão Telefônico por número 0800 como serviço de uso ilimitado, ou ao custo de uma ligação local, no período de (8x5) oito horas por dia, de segunda-feira a sexta-feira;

5.6.2.2 No Local (on site) – Serviço prestado em caso de emergência, ou outra necessidade maior e compreendendo os níveis de severidade 1 e 2;

Para efeito dos atendimentos técnicos, a Contratada deverá observar os níveis de severidade e respectivos prazos máximos fixados abaixo:

Níveis de Severidade dos Chamados	
Nível	**Descrição**
1	Serviços totalmente indisponíveis
2	Serviços parcialmente indisponíveis ou com degradação de tempo de resposta no acesso aos aplicativos.
3	Serviços disponíveis com ocorrência de alarmes de avisos, consultas sobre problemas, dúvidas gerais sobre o equipamento fornecido.

Tabela de Prazos de Atendimento ao Software		
Modalidade	Prazos	Níveis de Severidade

		1	2	3
On Site	Início atendimento	4 horas	6 horas	-
	Término atendimento	-	48 horas	-
Telefone, e-mail e web	Início atendimento	4 horas	8 horas	24 horas
	Término atendimento	-	48 horas	72 horas

5.6.2.3 Para cada incidente em que a solução definitiva demande ações do fabricante e/ou de terceiros, os acordos de níveis de serviço serão renegociados mediante acordo entre as partes.

5.6.2.4 Após a conclusão do serviço é obrigação da CONTRATADA verificar o restabelecimento das condições operacionais normais;

5.6.2.5 Todo o chamado somente será caracterizado como "encerrado" mediante concordância da CONTRATANTE;

5.6.2.6 Para as situações em que a solução definitiva de problemas no ambiente demande reimplantação, reestruturação ou reinstalação do produto, este deverá ser programado e planejado, com a antecedência necessária, de modo a não prejudicar a operação dos demais sistemas da CONTRATANTE;

6. MODELO DE GESTÃO DO CONTRATO

6.1 O Contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei Federal nº 14.133/2021, e da Lei Estadual n° 14.634/2023, respondendo cada parte pelas consequências de sua inexecução total ou parcial (art. 115, *caput*, da Lei Federal n° 14.133/2021).

6.2 Em caso de impedimento, ordem de paralisação ou suspensão do Contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila (art. 115, §5°, da Lei Federal n° 14.133/2021).

6.2.1 O impedimento a que se refere o subitem anterior, total ou parcial, da execução do Contrato por fato ou ato de terceiro, deve ser reconhecido pela Administração em documento contemporâneo à sua ocorrência.

6.3 As comunicações entre o órgão ou entidade e a contratada devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se, para esse fim, o uso de mensagem eletrônica por meio do Sistema Eletrônico de Informações – SEI.

6.4 O órgão ou entidade poderá convocar representante da contratada para adoção de providências que devam ser cumpridas de imediato.

6.5 O acompanhamento da execução do Contrato compreenderá as atividades de gestão e fiscalização na forma dos arts. 15 a 23 do Decreto nº 22.885/2024, observando-se, ainda, o disposto nos arts. 7º e 17 do Decreto nº 23.059/2024.

6.5.1 Constatando-se a situação de irregularidade da contratada, será providenciada sua intimação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua justificativa.

6.5.2 O prazo de que trata o subitem 6.5.1 poderá ser prorrogado uma vez, por igual período, a critério do Contratante.

6.5.3 Não havendo regularização ou não sendo aceita a justificativa apresentada, a Administração deverá adotar as medidas necessárias à apuração dos fatos nos autos do processo administrativo correspondente, assegurada à contratada a ampla defesa.

6.6 Após a assinatura do Contrato ou instrumento equivalente, o órgão ou entidade poderá convocar o representante da empresa contratada para reunião inicial para alinhamento da execução do Contrato e demais procedimentos de gestão do ajuste.

7. CRITÉRIOS DE RECEBIMENTO DO OBJETO, LIQUIDAÇÃO E PAGAMENTO

7.1 RECEBIMENTO DO OBJETO

7.1.1 Recebimento provisório

7.1.1.1 O objeto do Contrato será recebido provisoriamente, no prazo de **5 (cinco) dias** úteis, pelo(s) fiscal(is) do Contrato, mediante termo(s) detalhado(s), quando verificado o cumprimento das exigências de caráter técnico e administrativo (art. 140, inc. I, "a", da Lei Federal n° 14.133/2021).

7.1.1.1.1 O prazo de que trata este subitem anterior será contado do recebimento de comunicação escrita da contratada

com a comprovação da execução do objeto a que se refere a parcela a ser paga.

7.1.1.2 A contratada fica obrigada a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados (art. 119 da Lei Federal n° 14.133/2021).

7.1.1.3 O objeto poderá ser rejeitado, no todo ou em parte, inclusive antes do recebimento provisório, quando em desacordo com as especificações constantes neste TR/Habilitação e na proposta, devendo ser substituído ou corrigido no prazo de **5 (cinco) dias úteis**, a contar da intimação da contratada, às suas custas, sem prejuízo da aplicação das penalidades (art. 140, §1º da Lei Federal nº 14.133/2021).

7.1.1.4 Para efeito de recebimento provisório, ao final de cada período de faturamento, o(s) fiscal(is) do Contrato deverá(ão) emitir relatório sobre o efetivo cumprimento das obrigações da contratada e, se for o caso, analisar o desempenho na execução do Contrato nos termos do art. 144 da Lei Federal nº 14.133/2021, em consonância com os indicadores que deverão integrar este TR/Habilitação como anexo, encaminhando-o ao gestor do Contrato.

7.1.1.4.1 A análise do desempenho na execução do Contrato de que trata o art. 144 da Lei Federal nº 14.133/2021 poderá resultar no redimensionamento de valores a serem pagos à contratada, circunstância que deverá ser registrada pelo(s) fiscal(is) em relatório(s) a ser encaminhado ao gestor do Contrato.

7.1.1.5 A fiscalização não efetuará o ateste da última e/ou única medição do objeto até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas durante o recebimento provisório.

7.1.1.6 O recebimento provisório estará sujeito, quando cabível, à conclusão de todos os testes de campo e à entrega dos Manuais e Instruções exigíveis.

7.1.1.7 Quando a fiscalização for exercida por um único servidor, o termo detalhado de recebimento provisório deverá conter o registro, a análise e a conclusão sobre todas as ocorrências na execução do Contrato, acompanhado dos demais documentos que julgar necessários, encaminhando-o ao servidor ou comissão designada pela autoridade competente para recebimento definitivo.

7.1.2 Recebimento definitivo

7.1.2.1 O recebimento definitivo ocorrerá no **prazo de 20 (vinte) dias úteis**, contados do recebimento provisório, por servidor ou comissão designada pela autoridade competente, mediante termo detalhado que comprove o atendimento das exigências contratuais, observados os seguintes procedimentos (art. 140, inc. I, "b" da Lei Federal n° 14.133/2021):

a) emissão de documento comprobatório da avaliação realizada pelo(s) fiscal(is) sobre o cumprimento de obrigações assumidas pela contratada, com menção ao seu desempenho na execução contratual, baseado em indicadores objetivamente definidos e aferidos nos termos do Decreto nº 23.059/2024, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações;

b) análise dos relatórios e de toda a documentação apresentada pela fiscalização e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicação das cláusulas contratuais correspondentes, solicitando à contratada por escrito, as respectivas correções;

c) emissão de termo detalhado para efeito de recebimento definitivo dos serviços, com base nos relatórios elaborados e documentações apresentadas;

d) comunicação à contratada para emissão de nota(s) fiscal(is) ou instrumento(s) de cobrança equivalente(s), com o valor exato dimensionado pela fiscalização;

e) envio da documentação correspondente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão;

f) exigência de apresentação pela contratada do Relatório "*AS BUILT*", no caso de obras e serviços de engenharia.

7.1.2.1.1 O prazo para recebimento definitivo poderá ser excepcionalmente prorrogado, de forma justificada, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais.

7.1.2.1.2 O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança da obra ou serviço nem a responsabilidade ético-profissional pela perfeita execução do Contrato (art. 140, §§2° e 6º da Lei Federal n° 14.133/2021).

7.1.2.2 No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, a parcela incontroversa, conforme art. 143 da Lei Federal nº 14.133/2021, deverá ser liberada no prazo previsto para pagamento.

7.1.2.2.1 Para fins do subitem anterior, o valor da parcela incontroversa deverá ser comunicado à contratada para emissão de nota(s) fiscal(is) ou instrumento(s) de cobrança equivalente(s).

7.1.2.3 Nenhum prazo de recebimento ocorrerá enquanto pendente a solução, pela contratada, de inconsistências verificadas na execução do objeto ou nota(s) fiscal(is) ou instrumento(s) de cobrança equivalente(s).

7.2 LIQUIDAÇÃO

7.2.1 Recebida(s) nota(s) fiscal(is) ou instrumento(s) de cobrança equivalente(s), a Administração, no **prazo de 5 (cinco) dias úteis**, prorrogáveis por até **5 (dias) dias úteis**, adotará, na forma deste subitem, as providências para fins de liquidação da despesa.

7.2.2 Para fins de liquidação, o setor competente deverá verificar se a(s) nota(s) fiscal(is) ou instrumento(s) de cobrança equivalente(s) apresentado(s) pela contratada possui(em) os elementos necessários e essenciais do documento, tais como: a) o prazo de validade; b) a data da emissão; c) os dados do Contrato e do Contratante; d) o período respectivo de execução do Contrato; e) o valor a pagar; e f) eventual destaque do valor de retenções tributárias cabíveis.

7.3.3 Havendo erro na apresentação da(s) nota(s) fiscal(is) ou instrumento(s) de cobrança equivalente(s), ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que a contratada providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus para o Contratante;

7.4.4 A(s) nota(s) fiscal(is) ou instrumento(s) de cobrança equivalente(s) deverá(ão) ser obrigatoriamente acompanhado (s) da comprovação da regularidade fiscal da contratada mediante consulta aos sítios eletrônicos oficiais ou à documentação de habilitação fiscal, social e trabalhista, na forma exigida neste TR/Habilitação.

7.3 PAGAMENTO

7.3.1 Prazo para pagamento

7.3.1.1 O pagamento será efetuado no **prazo de 30 (trinta) dias úteis**, contados da finalização da liquidação da despesa, conforme subitem anterior.

Nota: a Administração, na definição do prazo de pagamento, deverá observar as disposições do art. 137, §2°, inc. IV da Lei Federal n° 14.133/2021.

7.3.1.2 No caso de atraso pelo Contratante, os valores devidos à contratada serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, de acordo com a variação do IPCA-E (Índice Nacional de Preços ao Consumidor Amplo Especial), *pro rata tempore*.

7.3.2 Forma de pagamento

7.3.2.1 O pagamento será realizado por meio de ordem bancária ou crédito em conta da contratada aberta em instituição financeira contratada pelo Estado da Bahia.

7.3.2.1.1 Optando a contratada por receber os créditos em instituição financeira diversa da indicada neste subitem, deverá arcar com os custos de transferências bancárias, os quais serão deduzidos dos pagamentos devidos.

7.3.2.2 A(s) nota(s) fiscal(is) ou instrumento(s) de cobrança equivalente(s) deverá(ão) atender as exigências legais pertinentes aos tributos e encargos relacionados com a obrigação, inclusive os destaques necessários às retenções tributárias previstas em lei, e, as situações específicas, à adoção da forma eletrônica.

7.3.2.3 Independentemente do percentual de tributo inserido na proposta de preço, serão retidos na fonte, por ocasião da realização do pagamento, os percentuais estabelecidos na legislação vigente, quando houver incidência tributária.

7.3.2.4 A contratada regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123/2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime, estando o pagamento condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

8. FORMA E CRITÉRIOS DE SELEÇÃO DA PROPOSTA E EXIGÊNCIAS DE HABILITAÇÃO

8.1 Forma de seleção e critério de julgamento da proposta

8.1.1 A seleção da proposta será feita em procedimento de:

(X) A seleção da proposta será realizada por meio de Dispensa de Licitação Eletrônica com disputa, conforme art. 75 da Lei nº 14.133/2021 e Decreto Estadual nº 22.886/2024, adotando-se o critério de menor preço entre as propostas enviadas no sistema ComprasNet.

(X) menor preço

8.2 Exigências de habilitação

8.2.1 Para fins de habilitação, deverá o proponente comprovar os seguintes requisitos:

8.2.1.1 Habilitação jurídica

8.2.1.1.1 Para **Pessoas Jurídicas**:

a) empresário individual: inscrição no registro público de empresas mercantis;

b) microempreendedor individual – MEI: certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio https://www.gov.br/empresas-e-negocios/pt-br/empreendedor;

c) sociedade empresária, sociedade limitada unipessoal: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, com suas eventuais alterações supervenientes em vigor, devidamente registrados, acompanhados, quando for o caso, dos documentos societários comprobatórios de eleição ou designação e investidura dos atuais administradores.

d) sociedades simples: inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, com suas eventuais alterações supervenientes em vigor, devidamente registrados, acompanhados dos atos comprobatórios de eleição e investidura dos atuais administradores.

e) empresa ou sociedade estrangeira: portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, observando-se a Instrução Normativa DREI/ME nº 77, de 18 de março de 2020, quando a atividade assim o exigir.

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

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

8.2.1.2 Habilitação fiscal, social e trabalhista

a) prova de inscrição no Cadastro Nacional de Pessoas Jurídicas;

b) prova de inscrição no cadastro de contribuintes ( ) Estadual/Distrital (x) Municipal/Distrital relativo ao domicílio ou sede do proponente pertinente ao seu ramo de atividade e compatível com o objeto contratual;

c) prova de regularidade com a Fazenda (X) Estadual/Distrital ( ) Municipal/Distrital do domicílio ou sede do proponente, ou outro equivalente, na forma da lei;

c.1) Caso o proponente seja considerado isento dos tributos relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.

d) prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social.

e) prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

f) prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;

g) em se tratando de contratação direta, prova de regularidade com a Fazenda do Estado da Bahia, ou o compromisso de sua regularização e sua efetiva realização, como condição para celebração do Contrato, nos termos do art. 65 da Lei estadual n° 14.634/2023.

8.2.1.2.1 As microempresas e empresas de pequeno porte, beneficiárias do tratamento diferenciado e favorecido previsto na Lei Complementar n° 123/2006, deverão apresentar toda a documentação exigida para efeito de comprovação de regularidade fiscal, mesmo que esta apresente alguma restrição.

8.2.1.3 Habilitação Econômico-Financeira

(X) **dispensável parcialmente** (IN SAEB Nº 10/2024), consistindo em:

Nota: assinalar a hipótese pertinente

(x) contratação para entrega imediata: aquisição remunerada para fornecimento de uma só vez, com prazo de entrega de até 30 (trinta) dias da expedição da ordem de fornecimento; (item 3, inc. I, da IN SAEB Nº 10/2024)

8.2.1.3.1 Na hipótese de dispensa parcial, será exigida, para efeito de habilitação econômico-financeira:

a) certidão negativa de falência expedida pelo distribuidor da sede do proponente, com data de expedição ou revalidação dos últimos 90 (noventa) dias anteriores à data da realização da dispensa eletrônica ou da contratação direta, caso o documento não consigne prazo de validade;

8.2.1.4 Qualificação Técnica

Apresentação de comprovação de que a empresa possui, em seu quadro funcional ou que mantenha vínculo com a empresa, no mínimo, 02 (dois) profissionais certificados, distribuídos da seguinte forma:

a) Pelo menos 1 (um) profissional certificado equivalente ao nível Especialista na solução de Endpoint;
b) Este profissional detém habilidades avançadas para projetar e implementar soluções de segurança baseadas em proteção de Endpoint. Sua presença assegura que a arquitetura e configuração sejam feitas de maneira especializada, alinhadas com as melhores práticas de mercado e requisitos específicos da nossa instituição.
c) A empresa deve apresentar comprovação de que possui, em seu quadro funcional ou através de contrato vigente, pelo menos 1 (um) profissional certificado como CEH (Certified Ethical Hacker) ou CompTIA Security+ ou certificação similar reconhecida. A comprovação deve ser realizada mediante apresentação de certificações válidas emitidas pelo fabricante. A presença de um profissional com essa certificação complementa a equipe de suporte técnico,

8.3 Disposições gerais

8.3.1 As empresas criadas no exercício financeiro da dispensa eletrônica ou da contratação direta deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura (art. 65, §1º, da Lei Federal nº 14.133/2021).

8.3.2 Regras acerca da participação de matriz e filial:

a) se o proponente for a matriz, todos os documentos devem estar em nome da matriz;

b) se o proponente for filial, todos os documentos devem estar em nome da filial, exceto aqueles que a legislação permita ou exija a emissão apenas em nome da matriz;

c) a comprovação de capacidade operacional para o desempenho de atividade pertinente e compatível em características, quantidades e prazos com o objeto da dispensa eletrônica ou da contratação direta poderá ser feita em nome da matriz ou da filial;

d) se o proponente participar do certame apresentando os documentos de habilitação e qualificação da matriz e desejar executar o Contrato pela filial, ou vice-versa, deverá fazer prova, por ocasião da assinatura do Contrato, da regularidade do estabelecimento que executará o objeto licitado, a qual deverá ser mantida durante todo o curso da avença.

8.3.3 O Certificado de Registro Cadastral-CRC ou Certificado de Registro Simplificado-CRS poderá substituir os documentos de habilitação, na forma indicada neste TR.

8.3.3.1 Caso conste do registro algum documento vencido, o proponente deverá apresentar a versão atualizada do referido documento junto aos demais documentos de habilitação.

8.3.3.2 A substituição dos documentos está condicionada à verificação da regularidade destes, mediante a emissão do extrato do fornecedor pela Administração.

8.3.3.3 O Certificado de Registro Cadastral-CRC ou Certificado de Registro Simplificado–CRS, estando no prazo de validade, poderá substituir os documentos relativos à habilitação constantes do sistema, exceto os concernentes à Qualificação Técnica.

8.3.4 Na hipótese de participação de pessoas jurídicas em consórcio, a habilitação técnica, quando exigida, será feita por meio do somatório dos quantitativos de cada consorciado e, para efeito de habilitação econômico-financeira, quando exigida, será observado o somatório dos valores de cada consorciado (art. 15, inc. III, da Lei Federal nº 14.133/2021).

9. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

9.1 O valor estimado total da contratação é de R$ 62.638,00 (Sessenta e dois mim seiscentos e trinta e oito reais), conforme planilha de quantitativos e preços unitários e global ( ) abaixo ( ) em anexo, os quais correspondem ao critério máximo de aceitabilidade dos preços unitários e global.

LOTE/ ITEM	Código SIMPAS	Descrição	Unidade de Fornecimento (UF)	Quantitativo	PREÇO UNITÁRIO	PREÇO GLOBAL
1	02.81.32.00000562-2	LICENCA DE USO antivírus, WithSecure Elements EPP + EDR Premium para Desktops. Com atualização, suporte e manutencao de 24 meses, Governo	Unidade	100	R$ 626,38	R$ 62.638,00
				VALOR ESTIMADO TOTAL		

10. ADEQUAÇÃO ORÇAMENTÁRIA

10.1 As despesas para o pagamento da presente contratação correrão à conta de recursos da Dotação Orçamentária a seguir especificada:

Unidade Orçamentária: 32.802 – Superintendência de Fomento ao Turismo do Estado da Bahia - SUFOTUR
Unidade Gestora: 0001 - Superintendência de Fomento ao Turismo do Estado da Bahia - SUFOTUR - Executora
Ação (Projeto/Atividade): 23.126.502.2002 – Manutenção de Serviços de Tecnologia da Informação e Comunicação
Elemento de Despesa: 3.3.90.40 – Serviços de Tecnologia da Informação e Comunicação - Pessoa Jurídica
Fontes de Recurso:1.500.0.100.000000.00.00.00 – Recursos Ordinários Não Vinculados do Tesouro

Nota: conforme o art. 106, inc. II, da Lei Federal nº 14.133/2021, nas hipóteses de serviços contínuos, " ***a Administração deverá atestar, no início da contratação e de cada exercício, a existência de créditos orçamentários vinculados à contratação e a vantagem em sua manutenção*****".**

10.1.1 A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

11. PRAZO PARA ASSINATURA DO CONTRATO

11.1 O prazo para assinatura do termo de contrato ou, nas hipóteses previstas no art. 95 da Lei Federal nº 14.133/2021, do instrumento hábil que lhe substitua: Autorização de Fornecimento de Material - AFM ou Autorização de Prestação de Serviços – APS, será de **10 (dez) dias úteis.**

11.1.1 O prazo de convocação poderá ser prorrogado uma vez, por igual período, mediante solicitação do adjudicatário durante seu transcurso, devidamente justificada, e desde que o motivo apresentado seja aceito pela Administração.

11.2 A assinatura do termo de contrato ou do instrumento hábil, conforme o disposto no art. 90 da Lei Federal n° 14.133/2021, observará a disciplina constante do componente Rito Procedimental do edital.

12. ANEXOS INTEGRANTES DO TR/HABILITAÇÃO

12.1 Vinculam-se a este TR/Habilitação, independentemente de transcrição (art. 92, inc. II, da Lei Federal n° 14.133/2021):
(X) Modelo para descrição auxiliar do objeto (no caso de listagem extensa)
(X) Modelo de descrição de proposta de preço e de declaração de elaboração independente de proposta;
( ) Modelos de prova de qualificação técnica:
( ) Capacidade técnico-operacional;

( ) Declaração de indicação do pessoal técnico, instalações e aparelhamento
(x) Declaração de pleno conhecimento, sem exigência de vistoria
( ) Declaração de pleno conhecimento, com exigência de vistoria
(X) Estudo Técnico Preliminar, quando cabível.

Salvador , 30 de Janeiro de 2026

_____

Fabio Luciano de Castro Oliveira

Coordenador de TIC
Matricula 02584758

Documento assinado eletronicamente por **Fábio Luciano de Castro Oliveira**, **Coordenador II**, em 31/01/2026, às 16:23, conforme horário oficial de Brasília, com fundamento no art. 13º, Incisos I e II, do Decreto nº 15.805, de 30 de dezembro de 2014 .

A autenticidade deste documento pode ser conferida no site https://seibahia.ba.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **00132394528** e o código CRC **C6FD2FDA**.

Referência: Processo nº 032.2305.2026.0001175-60 SEI nº 00132394528