TERMO DE DISPENSA DE LICITAÇÃO N.º 03/2023.

1. **Objeto**:

Constitui objeto deste Termo a aquisição de 100 (cem) licenças para Solução de Antivírus, conforme especificações técnico/operacionais e administrativas e de acordo com os demais dispositivos que constituem o presente Termo.

2. **Vigência do contrato:**

36 (trinta e seis) meses contínuos, a partir da ativação das licenças, quanto a garantia, atualizações e suporte.

3. **Motivação**:

A aquisição das licenças de antivírus tem o objetivo prevenir a contaminação por vírus, malwares e suas variantes bem como ameaças cibernéticas distintas nos Servidores da Administração Municipal de Pelotas, que podem colocar em risco o sigilo, a integridade e disponibilidade das informações.

Com o grande volume de utilização e com o crescimento da utilização de compartilhamento de arquivos, acesso a banco de dados, emails e acesso a páginas de internet a aquisição de um software de antivírus é necessária para fornecer um mínimo de segurança à infraestrutura de rede de computadores do município de Pelotas. As aquisições propõe uma maior proteção aos Servidores, resguardando problemas que podem prejudicar os serviços públicos prestados à população.

Assim, a aquisição das licenças de antivírus é considerada imprescindível para garantir a disponibilidade, integridade e confiabilidade dos dados e continuidade das atividades digitais exercidas nos Servidores da Administração Municipal de Pelotas.

4. **Fornecedor**:

KS Soluções Corporativas, CNPJ nº. 09.537.164/0001-27, à Avenida Mariland nº 1135/201, Bairro Mont'Serrat, CEP nº. 90.440-191, Porto Alegre/RS telefone (51) 3024.3131.

5. **Razão da Escolha do Fornecedor (futura Contratada)**:

Dentre 3 (três) cotações registradas neste parágrafo, a KS Soluções Corporativas forneceu o menor preço.

Empresas – cotações apresentadas	Valor R$
KS Soluções Corporativas	R$16.298,58 (dezesseis mil, duzentos e noventa e oito reais e cinquenta e oito centavos)
Prothree Technologies	R$28.530,00 (vinte e oito mil, quinhentos e trinta reais)
Maestech Inteligência em TI Ltda.	R$29.835,00 (vinte e nove mil, oitocentos e trinta e cinco reais)

6. **Características / Requisitos, Gestão e Forma de Execução da prestação dos serviços**:

6.1 Características técnicas para Solução de Antivírus:

6.1.1 Console de Gerenciamento

6.1.1.1. Compatibilidade de instalação com os seguintes sistemas operacionais:

6.1.1.1.1. Microsoft Windows 10 Enterprise 2015 LTSB 32-bit/64-bit
6.1.1.1.2. Microsoft Windows 10 Enterprise 2016 LTSB 32-bit/64-bit

6.1.1.1.3. Microsoft Windows 10 Pro RS5 32-bit/64-bit
6.1.1.1.4. Microsoft Windows 10 Pro for Workstations RS5 32-bit / 64-bit
6.1.1.1.5. Microsoft Windows 10 Enterprise RS5 32-bit/64-bit
6.1.1.1.6. Microsoft Windows 10 Education RS5 32-bit/64-bit
6.1.1.1.7. Microsoft Windows 8.1 Pro 32-bit/64-bit
6.1.1.1.8. Microsoft Windows 8.1 Enterprise 32-bit/64-bit
6.1.1.1.9. Microsoft Windows 8 Pro 32-bit/64-bit
6.1.1.1.10. Microsoft Windows 8 Enterprise 32-bit/64-bit
6.1.1.1.11. Microsoft Windows 7 Professional Service Pack 1 32-bit / 64-bit
6.1.1.1.12. Microsoft Windows 7 Enterprise / Ultimate Service Pack 1 32-bit / 64-bit
6.1.1.1.13. Microsoft Windows Small Business Server 2008 Standard / Premium 64-bit
6.1.1.1.14. Microsoft Windows Small Business Server 2011 Essentials 64-bit
6.1.1.1.15. Microsoft Windows Small Business Server 2011 Premium Add-on 64-bit
6.1.1.1.16. Microsoft Windows Small Business Server 2011 Standard 64-bit
6.1.1.1.17. Microsoft Windows Server 2008 Datacenter Service Pack 1 32-bit / 64-bit
6.1.1.1.18. Microsoft Windows Server 2008 Enterprise Service Pack 1 32-bit / 64-bit
6.1.1.1.19. Microsoft Windows Server 2008 Foundation Service Pack 2 32-bit / 64-bit
6.1.1.1.20. Microsoft Windows Server 2008 Service Pack 1 Server Core 32-bit / 64-bit
6.1.1.1.21. Microsoft Windows Server 2008 Standard Service Pack 1 32-bit / 64-bit
6.1.1.1.22. Microsoft Windows Server 2008 Standard / Enterprise / Datacenter 32-bit / 64-bit
6.1.1.1.23. Microsoft Windows Server 2008 R2 Server Core 64-bit
6.1.1.1.24. Microsoft Windows Server 2008 R2 Datacenter 64-bit
6.1.1.1.25. Microsoft Windows Server 2008 R2 Datacenter Service Pack 1 32-bit / 64-bit
6.1.1.1.26. Microsoft Windows Server 2008 R2 Enterprise 64-bit
6.1.1.1.27. Microsoft Windows Server 2008 R2 Enterprise Service Pack 1 64-bit
6.1.1.1.28. Microsoft Windows Server 2008 R2 Foundation 64-bit
6.1.1.1.29. Microsoft Windows Server 2008 R2 Foundation Service Pack 1 64-bit
6.1.1.1.30. Microsoft Windows Server 2008 R2 Core Mode Service Pack 64-bit
6.1.1.1.31. Microsoft Windows Server 2008 R2 Standard 64-bit
6.1.1.1.32. Microsoft Windows Server 2008 R2 Standard Service Pack 1 64-bit
6.1.1.1.33. Microsoft Windows Server 2012 Server Core 64-bit
6.1.1.1.34. Microsoft Windows Server 2012 Datacenter 64-bit
6.1.1.1.35. Microsoft Windows Server 2012 Essentials 64-bit
6.1.1.1.36. Microsoft Windows Server 2012 Foundation 64-bit
6.1.1.1.37. Microsoft Windows Server 2012 Standard 64-bit
6.1.1.1.38. Microsoft Windows Server 2012 R2 Server Core 64-bit
6.1.1.1.39. Microsoft Windows Server 2012 R2 Datacenter 64-bit
6.1.1.1.40. Microsoft Windows Server 2012 R2 Essentials 64-bit
6.1.1.1.41. Microsoft Windows Server 2012 R2 Foundation 64-bit
6.1.1.1.42. Microsoft Windows Server 2012 R2 Standard 64-bit
6.1.1.1.43. Microsoft Windows Server 2016 Datacenter (LTSB) 64-bit
6.1.1.1.44. Microsoft Windows Server 2016 Standard (LTSB) 64-bit
6.1.1.1.45. Microsoft Windows Server 2019 64-bit
6.1.1.1.46. Microsoft Windows Storage Server 2008 R2 64-bit
6.1.1.1.47. Microsoft Windows Storage Server 2016 64-bit
6.1.1.1.48. Microsoft Windows Storage Server 2012 64-bit
6.1.1.1.49. Microsoft Windows Storage Server 2012 R2 64-bit

6.1.1.2.Suportar as seguintes plataformas virtuais:

6.1.1.2.1. VMware vSphere 6

6.1.1.2.2. VMware vSphere 6.5
6.1.1.2.3. VMware Workstation 14 Pro
6.1.1.2.4. Microsoft Hyper-V Server 2008 64-bit
6.1.1.2.5. Microsoft Hyper-V Server 2008 R2 64-bit
6.1.1.2.6. Microsoft SQL Server 2008 R2 Service Pack 1 64-bit
6.1.1.2.7. Microsoft Hyper-V Server 2012 64-bit
6.1.1.2.8. Microsoft Hyper-V Server 2012 R2 64-bit
6.1.1.2.9. Microsoft Hyper-V Server 2016 64-bit
6.1.1.2.10. Citrix XenServer 7
6.1.1.2.11. Citrix XenServer 7.1 LTSR
6.1.1.2.12. Parallels Desktop 11
6.1.1.2.13. Oracle VM VirtualBox 5.x

6.1.1.3.Possuir compatibilidade com os seguintes bancos de dados:

6.1.1.3.1. Microsoft SQL Server 2008 Express 32-bit
6.1.1.3.2. Microsoft SQL Server 2008 R2 Express 64-bit
6.1.1.3.3. Microsoft SQL Server 2012 Express 64-bit
6.1.1.3.4. Microsoft SQL Server 2014 Express 64-bit
6.1.1.3.5. Microsoft SQL Server 2016 Express 64-bit
6.1.1.3.6. Microsoft SQL Server 2017 Express 64-bit
6.1.1.3.7. Microsoft SQL Server 2008 (todas as versões) 32-bit/64-bit
6.1.1.3.8. Microsoft SQL Server 2008 R2 (todas as versões) 64-bit
6.1.1.3.9. Microsoft SQL Server 2008 R2 Service Pack 2 (todas as versões) 64-bit
6.1.1.3.10. Microsoft SQL Server 2012 (todas as versões) 64-bit
6.1.1.3.11. Microsoft SQL Server 2014 (todas as versões) 64-bit
6.1.1.3.12. Microsoft SQL Server 2016 (todas as versões) 64-bit
6.1.1.3.13. Microsoft SQL Server 2017 on Windows 64-bit
6.1.1.3.14. MySQL Standard Edition 5.6 32-bit/64-bit
6.1.1.3.15. MySQL Enterprise Edition 5.6 32-bit/64-bit
6.1.1.3.16. MySQL Standard Edition 5.7 32-bit/64-bit
6.1.1.3.17. MySQL Enterprise Edition 5.7 32-bit/64-bit

6.1.1.4.Características da console de gerenciamento da solução:

6.1.1.4.1. A console deve ser acessada via WEB (HTTPS) ou MMC;
6.1.1.4.2. Estar presente no Programa de proteção ativa da Microsoft (MAPP);
6.1.1.4.3. Console deve ser baseada no modelo cliente/servidor;
6.1.1.4.4. Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade;
6.1.1.4.5. Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus;
6.1.1.4.6. Deve permitir incluir usuários do Active Direcoty para acessarem a console de administração;
6.1.1.4.7. Console deve ser totalmente integrada com suas funções e módulos caso haja a necessidade no futuro de adicionar novas tecnologias, tais como: Criptografia, Gerenciamento de Patches e Módulo de Gerenciamento Mobile;
6.1.1.4.8. As licenças deverão ser perpétuas, ou seja, expirado a validade da mesma o produto deverá permanecer funcional para a proteção contra códigos maliciosos utilizando as definições até o momento da expiração da licença;
6.1.1.4.9. Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores;
6.1.1.4.10. Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, login script e/ou GPO de Active Directory;

6.1.1.4.11. Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;
6.1.1.4.12. Deve armazenar histórico das alterações feitas em políticas;
6.1.1.4.13. Deve permitir voltar para uma configuração antiga da política de acordo com o histórico de alterações efetuadas pelo administrador apenas selecionando a data em que a política foi alterada;
6.1.1.4.14. Deve ter a capacidade de comparar a política atual com a anterior, informando quais configurações foram alteradas;
6.1.1.4.15. A solução de gerência deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas;
6.1.1.4.16. Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador;
6.1.1.4.17. Capacidade de instalar remotamente a solução de segurança em smartphones e tablets de sistema iOS e Android;
6.1.1.4.18. Capacidade de instalar remotamente aplicativos em smartphones e tablets de sistema Android;
6.1.1.4.19. A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle;
6.1.1.4.20. Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por subrede com os seguintes parâmetros: KB/s e horário;
6.1.1.4.21. Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução antivírus;
6.1.1.4.22. Capacidade de gerenciar smartphones e tablets (dos sistemas operacionais Android e iOS) protegidos pela solução de segurança;
6.1.1.4.23. Capacidade de instalar atualizações em computadores de testes antes de instalar nos demais computadores da rede;
6.1.1.4.24. Capacidade de gerar pacotes customizados (auto executáveis) contendo a licença e configurações do produto;
6.1.1.4.25. Capacidade de atualizar os pacotes de instalação com as últimas vacinas;
6.1.1.4.26. Capacidade de fazer distribuição remota de qualquer software, ou seja, deve ser capaz de remotamente enviar qualquer software pela estrutura de gerenciamento de antivírus para que seja instalado nas máquinas clientes;
6.1.1.4.27. A comunicação entre o cliente e o servidor de administração deve ser criptografada;
6.1.1.4.28. Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes;
6.1.1.4.29. Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado utilizando os seguintes parâmetros:
    6.1.1.4.29.1. Nome do computador;
    6.1.1.4.29.2. Nome do domínio;
    6.1.1.4.29.3. Domínio do DNS
    6.1.1.4.29.4. Range de IP;
    6.1.1.4.29.5. Unidade organizacional do Active Directory;
    6.1.1.4.29.6. Grupo de Active Directory;
    6.1.1.4.29.7. Sistema Operacional;
    6.1.1.4.29.8. Máquina virtual;
    6.1.1.4.29.9. Segmento de nuvem.
6.1.1.4.30. Capacidade de executar a regra de realocação das seguintes formas:
    6.1.1.4.30.1. Executar apenas uma vez para cada dispositivo;
    6.1.1.4.30.2. Executar apenas uma vez para cada dispositivo, a cada instalação do Agente de Rede da solução endpoint;
    6.1.1.4.30.3. Regra funcionar permanentemente;
6.1.1.4.31. Deve encontrar computadores na rede através de no mínimo três formas: Domínio, Active Directory e subredes;
6.1.1.4.32. Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas;

6.1.1.4.33. Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas à proteção;
6.1.1.4.34. Capacidade de monitorar grupos de trabalhos já existentes e quaisquer grupos de trabalho que forem criados na rede, a fim de encontrar máquinas novas para serem adicionadas a proteção;
6.1.1.4.35. Capacidade de, assim que detectar máquinas novas no Active Directory, subnets ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possuir, deve instalar o antivírus automaticamente;
6.1.1.4.36. Capacidade de agrupamento de máquina por características comuns entre as mesmas, por exemplo: agrupar todas as máquinas que não tenham o antivírus instalado, agrupar todas as máquinas que não receberam atualização nos últimos 2 dias;
6.1.1.4.37. Listar em um único local, todos os computadores não gerenciados na rede;
6.1.1.4.38. Capacidade de definir políticas de configurações diferentes por grupos de estações, permitindo que sejam criados subgrupos e com função de herança de políticas entre grupos e subgrupos;
6.1.1.4.39. Deve fornecer as seguintes informações dos computadores:
- 6.1.1.4.39.1. Se o antivírus está instalado;
- 6.1.1.4.39.2. Se o antivírus está iniciado;
- 6.1.1.4.39.3. Se o antivírus está atualizado;
- 6.1.1.4.39.4. Minutos/horas desde a última conexão da máquina com a console;
- 6.1.1.4.39.5. Minutos/horas desde a última atualização de vacinas;
- 6.1.1.4.39.6. Data e horário da última verificação executada na máquina;
- 6.1.1.4.39.7. Versão do antivírus instalado na máquina;
- 6.1.1.4.39.8. Se é necessário reiniciar o computador para aplicar mudanças;
- 6.1.1.4.39.9. Data e horário de quando a máquina foi ligada;
- 6.1.1.4.39.10. Quantidade de vírus encontrados (contador) na máquina;
- 6.1.1.4.39.11. Nome do computador;
- 6.1.1.4.39.12. Domínio ou grupo de trabalho do computador;
- 6.1.1.4.39.13. Data e horário da última atualização de vacinas;
- 6.1.1.4.39.14. Sistema operacional com Service Pack;
- 6.1.1.4.39.15. Quantidade de processadores;
- 6.1.1.4.39.16. Quantidade de memória RAM;
- 6.1.1.4.39.17. Usuário(s) logado(s) naquele momento;
- 6.1.1.4.39.18. Endereço IP;
- 6.1.1.4.39.19. Vulnerabilidades de aplicativos instalados na máquina;
- 6.1.1.4.39.20. Atualizações do Windows Updates instaladas;
- 6.1.1.4.39.21. Aplicativos instalados, inclusive aplicativos de terceiros, contendo:
  - 6.1.1.4.39.21.1. Histórico de instalação;
  - 6.1.1.4.39.21.2.Data e hora que o software foi instalado;
  - 6.1.1.4.39.21.3.Data e hora que o software foi removido;
- 6.11.4.39.22. Informação completa de hardware contendo:
  - 6.1.1.4.39.22.1.Processadores;
  - 6.1.1.4.39.22.2.Memória;
  - 6.1.1.4.39.22.3.Adaptadores de vídeo;
  - 6.1.1.4.39.22.4.Discos de armazenamento;
  - 6.1.1.4.39.22.5.Adaptadores de áudio;
  - 6.1.1.4.39.22.6.Adaptadores de rede;
  - 6.1.1.4.39.22.7.Monitores;
  - 6.1.1.4.39.22.8.Drives de CD/DVD;

6.1.1.4.40. Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:
- 6.1.1.4.40.1. Alteração de Gateway Padrão;
- 6.1.1.4.40.2. Alteração de Subrede;

6.1.1.4.40.3. Alteração de domínio;
6.1.1.4.40.4. Alteração de servidor DHCP;
6.1.1.4.40.5. Alteração de servidor DNS;
6.1.1.4.40.6. Alteração de servidor WINS;
6.1.1.4.40.7. Alteração de Subrede;
6.1.1.4.40.8. Resolução de Nome;
6.1.1.4.40.9. Disponibilidade de endereço de conexão SSL;
6.1.1.4.41. Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;
6.1.1.4.42. Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;
6.1.1.4.43. Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede;
6.1.1.4.44. Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo;
6.1.1.4.45. Capacidade de realizar atualização incremental de vacinas nos computadores clientes;
6.1.1.4.46. Capacidade de baixar novas versões do antivírus direto pela console de gerenciamento, sem a necessidade de importá-los manualmente;
6.1.1.4.47. Deve possuir compatibilidade com Microsoft NAP, quando instalado em um Windows 2008 Server;
6.1.1.4.48. Deve permitir a configuração de senha no endpoint e configurar quando que será necessário a utilizá-la, por exemplo: Solicitar senha quando alguma tarefa de escaneamento for criada localmente no endpoint;
6.1.1.4.49. Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;
6.1.1.4.50. Capacidade de reportar vulnerabilidades de softwares presentes nos computadores;
6.1.1.4.51. Capacidade de listar updates nas máquinas com o respectivo link para download;
6.1.1.4.52. Deve permitir, por meio da console de gerenciamento, extrair um artefato em quarentena de um cliente sem a necessidade de um servidor ou console de quarentena adicional;
6.1.1.4.53. Deve ter uma quarentena na própria console de gerenciamento, permitindo baixar um artefato ou enviar direto para análise do fabricante;
6.1.1.4.54. Deve armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo:
6.1.1.4.54.1. Nome do vírus;
6.1.1.4.54.2. Nome do arquivo infectado;
6.1.1.4.54.3. Data e hora da detecção;
6.1.1.4.54.4. Nome da máquina ou endereço IP;
6.1.1.4.54.5. Ação realizada.
6.1.1.4.55. Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;
6.1.1.4.56. Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;
6.1.1.4.57. Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);
6.1.1.4.58. Deve através de opções de optimizações fazer com que o computador gerenciado conceda recursos à outras aplicações, mantendo o antivírus ativo, porém sem comprometer o desempenho do computador
6.1.1.4.59. Permitir fazer uma verificação rápida ou detalhada de um dispositivo removível assim que conectado no computador, podendo configurar a capacidade máxima em GB da verificação;
6.1.1.4.60. Capacidade de ligar máquinas via Wake on Lan para realização de tarefas (varredura, atualização, instalação), inclusive de máquinas que estejam em subnets diferentes do servidor;
6.1.1.4.61. Deve criar um backup de todos arquivos deletados em computadores para que possa ser restaurado através de comando na Console de administração;

6.1.1.4.62. Capacidade de realizar inventário de hardware de todas as máquinas clientes;
6.1.1.4.63. Capacidade de realizar inventário de aplicativos de todas as máquinas clientes;
6.1.1.4.64. Capacidade de diferenciar máquinas virtuais de máquinas físicas;
6.1.1.4.65. Deve ser capaz de configurar quais eventos serão armazenados localmente, nos eventos do windows ou ainda se serão mostrados na tela para o colaborador, sejam estes eventos informativos, de alertas ou de erros;
6.1.1.4.66. Capacidade de enviar e-mails para contas específicas em caso de algum evento;
6.1.1.4.67. Capacidade de gerar traps SNMP para monitoramento de eventos;
6.1.1.4.68. Capacidade de exportar relatórios para pelo menos nos seguintes tipos de arquivos: PDF, HTML e XML;
6.1.1.4.69. Possuir, no mínimo, 30 (trinta) relatórios pré-configurados na console de gerenciamento da solução;
6.1.1.4.70. Capacidade de customizar relatórios de acordo com preferência do cliente nos seguintes campos:
- 6.1.1.4.70.1. Cabeçalho do relatório;
- 6.1.1.4.70.2. Logotipo do cliente;

6.1.1.4.71. Capacidade de gerar tarefa com agendamento de envio de relatório por E-mail;
6.1.1.4.72. Capacidade de gerar tarefa de agendamento de envio de relatório para Pasta Compartilhada na rede;
6.1.1.4.73. Possuir informações estatísticas na console de gerenciamento com, no mínimo, as seguintes informações:
- 6.1.1.4.73.1. Status da proteção;
- 6.1.1.4.73.2. Informações de implementação;
- 6.1.1.4.73.3. Atualizações;
- 6.1.1.4.73.4. Ameaças;
- 6.1.1.4.73.5. Informação Geral;
- 6.1.1.4.73.6. Atualizações das Aplicações;

6.1.1.4.74. Possibilitar customização de visualização das estatísticas diretamente na console;

6.1.2. Proteção para estações de trabalho Windows

6.1.2.1. Compatibilidade de instalação nos seguintes sistemas operacionais:

6.1.2.1.1. Microsoft Windows 10 Home / Pro / Education / Enterprise x86 / x64
6.1.2.1.2. Microsoft Windows 8.1 Pro / Enterprise x86 / x64
6.1.2.1.3. Microsoft Windows 8 Pro / Enterprise x86 / x64
6.1.2.1.4. Microsoft Windows 7 Home / Professional / Enterprise x86 / x64 SP1 e superior
6.1.2.1.5. Microsoft Windows Server 2019 Essentials / Standard / Datacenter
6.1.2.1.6. Microsoft Windows Server 2016 Essentials / Standard / Datacenter
6.1.2.1.7. Microsoft Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter
6.1.2.1.8. Microsoft Windows Server 2012 Foundation / Essentials / Standard / Datacenter
6.1.2.1.9. Microsoft Small Business Server 2011 Essentials / Standard x64
6.1.2.1.10. Microsoft Windows Server 2008 R2 Foundation / Standard / Enterprise SP1
6.1.2.1.11. Microsoft Windows Server 2008 Standard / Enterprise / Datacenter SP2
6.1.2.1.12. Microsoft Small Business Server 2008 Standard / Premium x64

6.1.2.2.Suportar as seguintes plataformas virtuais:

6.1.2.2.1. VMware Workstation 14;
6.1.2.2.2. VMware ESXi 6.5 U1;
6.1.2.2.3. Microsoft Hyper-V 2016 Server;
6.1.2.2.4. Microsoft Hyper-V 2019 Server;
6.1.2.2.5. Citrix XenServer 7.2;
6.1.2.2.6. Citrix XenDesktop 7.17;

6.1.2.2.7. Citrix XenApp 7.17;
6.1.2.2.8. Citrix Provisioning Services 7.17;

6.1.2.3.Características da solução de proteção para estação de trabalho Windows

6.1.2.3.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware) que verifique qualquer arquivo criado, acessado ou modificado;
6.1.2.3.2. Antivírus de Web (módulo para verificação de sites e downloads contra vírus);
6.1.2.3.3. Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos);
6.1.2.3.4. Proteção contra Ameaças de Rede (módulo de verificação de atividades suspeitas na rede);
6.1.2.3.5. Firewall com IDS (sistema de detecção de intrusos);
6.1.2.3.6. Proteção contra ameaças utilizando de exploração BadUSB;
6.1.2.3.7. Integração com o Antimalware Scan Interface da Microsoft (AMSI), para os seguintes sistemas operacionais:
- 6.1.2.3.7.1. Microsoft Windows 10 Pro x64/x86;
- 6.1.2.3.7.2. Microsoft Windows 10 Enterprise x64/x86;
- 6.1.2.3.7.3. Microsoft Windows Server 2016;

6.1.2.3.8. Possuir Controle de dispositivos externos;
6.1.2.3.9. Possuir Controle de acesso a sites por categoria;
6.1.2.3.10. Possuir, no mínimo, 15 (quinze) categorias de sites pré-configuradas
6.1.2.3.11. Capacidade de customização de acesso a sites com, no mínimo, as seguintes maneiras:
- 6.1.2.3.11.1. Controle de acesso a sites por horário;
- 6.1.2.3.11.2. Controle de acesso a sites por usuários;
- 6.1.2.3.11.3. Controle de acesso a websites por dados, como por exemplo: Bloquear websites com conteúdos de vídeo e áudio;

6.1.2.3.12. Possuir controle de execução de aplicativos;
6.1.2.3.13. Controle de vulnerabilidades do Windows e dos aplicativos instalados;
6.1.2.3.14. Possuir Autodefesa contra ataques aos serviços e processos do antivírus no endpoint;
6.1.2.3.15. Capacidade de escolher quais módulos serão instalados tanto na instalação local quanto na instalação remota;
6.1.2.3.16. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
6.1.2.3.17. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
6.1.2.3.18. O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza;
6.1.2.3.19. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluílos da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, por exemplo: “Win32.Trojan.banker”, para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
6.1.2.3.20. Capacidade de adicionar aplicativos a uma lista de “aplicativos confiáveis”, onde as atividades de rede, atividades de disco e acesso ao registro do Windows não serão monitoradas;
6.1.2.3.21. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
6.1.2.3.22. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
6.1.2.3.23. Capacidade de verificar somente arquivos novos e alterados;
6.1.2.3.24. Capacidade de verificar objetos usando heurística;
6.1.2.3.25. Capacidade de agendar uma pausa na verificação;
6.1.2.3.26. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;

6.1.2.3.27. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa);
6.1.2.3.28. Ter a capacidade de fazer detecções por comportamento, identificando ameaças avançadas sem a necessidade de assinaturas;
6.1.2.3.29. Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias;
6.1.2.3.30. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
- 6.1.2.3.30.1. Perguntar o que fazer;
- 6.1.2.3.30.2. Bloquear acesso ao objeto;
- 6.1.2.3.30.3. Deletar o objeto;
- 6.1.2.3.30.4. Realizar a limpeza do objeto;

6.1.2.3.31. Em caso positivo de limpeza deve restaurar o objeto para uso;
6.1.2.3.32. Em caso negativo de limpeza deve mover para quarentena ou apagar;
6.1.2.3.33. Anteriormente a qualquer tentativa de limpeza ou exclusão permanente, o antivírus deve realizar um backup do objeto;
6.1.2.3.34. Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, IMAP, NNTP e SMTP, assim como conexões criptografadas (SSL) para POP3 e IMAP (SSL);
6.1.2.3.35. Possuir extensão para Microsoft Outlook, com a possibilidade de escaneamento de 3 (três) maneiras distintas:
- 6.1.2.3.35.1. Realizar varredura ao receber a mensagem;
- 6.1.2.3.35.2. Realizar varredura quando lê a mensagem;
- 6.1.2.3.35.3. Realizar varredura quando envia a mensagem;

6.1.2.3.36. Capacidade de realizar filtro em anexos de e-mail;
6.1.2.3.37. Ter capacidade de renomear anexo de e-mail, de acordo com a extensão escolhida, por exemplo: .exe, .bat, .cmd, entre outras.
6.1.2.3.38. Ter capacidade de remover anexo de e-mail, de acordo com a extensão escolhida, por exemplo: .exe, .bat, .cmd, entre outras.
6.1.2.3.39. Capacidade de verificação de corpo e anexos de e-mails usando heurística
6.1.2.3.40. O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve:
- 6.1.2.3.40.1. Perguntar o que fazer;
- 6.1.2.3.40.2. Bloquear o e-mail;
- 6.1.2.3.40.3. Deletar o objeto;
- 6.1.2.3.40.4. Realizar a limpeza do objeto;
- 6.1.2.3.40.5. Em caso positivo de limpeza deve restaurar o e-mail para o usuário;
- 6.1.2.3.40.6. Em caso negativo de limpeza deve mover para quarentena ou apagar;

6.1.2.3.41. Capacidade de verificar links inseridos em e-mails contra phishings;
6.1.2.3.42. Capacidade de verificar tráfego nos browsers: Internet Explorer, Firefox, Google Chrome e Opera;
6.1.2.3.43. Caso o e-mail conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena;
6.1.2.3.44. Capacidade de verificação de tráfego HTTP e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc), usando heurística;
6.1.2.3.45. Na verificação de tráfego web, caso encontrado código malicioso o programa deve:
- 6.1.2.3.45.1. Perguntar o que fazer;
- 6.1.2.3.45.2. Bloquear o acesso e informar sobre a ação com uma mensagem;
- 6.1.2.3.45.3. Permitir o acesso ao objeto;

6.1.2.3.46. Capacidade de alterar as portas monitoradas pelos módulos de Web e E-mail
6.1.2.3.47. Deve ter suporte total ao protocolo IPV6;
6.1.2.3.48. O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:
- 6.1.2.3.48.1. Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em tempo real;
- 6.1.2.3.48.2. Verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação;

6.1.2.3.49. Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web;
6.1.2.3.50. Deve possuir módulo que analise as ações de cada aplicação em execução no computador, gravando as ações executadas e comparando-as com sequências características de atividades perigosas. Tais registros de sequências devem ser atualizados juntamente com as vacinas;
6.1.2.3.51. Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa;
6.1.2.3.52. Deve possuir módulo que analise qualquer tentativa de edição, exclusão ou gravação do registro, de forma que seja possível escolher chaves específicas para serem monitoradas e/ou bloqueadas;
6.1.2.3.53. Deve possuir módulo de bloqueio de Phishing, com atualizações incluídas nas vacinas, obtidas pelo Anti-Phishing Working Group (http://www.antiphishing.org/)
6.1.2.3.54. Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica;
6.1.2.3.55. Deve possuir módulo IDS (Intrusion Detection System) para proteção contra port scans e exploração de vulnerabilidades de softwares. A base de dados de análise deve ser atualizada juntamente com as vacinas;
6.1.2.3.56. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
6.1.2.3.56.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
6.1.2.3.56.2. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados;
6.1.2.3.57. Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:
6.1.2.3.57.1. Discos de armazenamento locais;
6.1.2.3.57.2. Armazenamento removível;
6.1.2.3.57.3. Impressoras;
6.1.2.3.57.4. CD/DVD;
6.1.2.3.57.5. Drives de disquete;
6.1.2.3.57.6. Modems;
6.1.2.3.57.7. Dispositivos de fita;
6.1.2.3.57.8. Dispositivos multifuncionais;
6.1.2.3.57.9. Leitores de smart card;
6.1.2.3.57.10. Dispositivos de sincronização via ActiveSync
6.1.2.3.57.11. Wi-Fi;
6.1.2.3.57.12. Adaptadores de rede externos;
6.1.2.3.57.13. Dispositivos portáteis (MTP);
6.1.2.3.57.14. Dispositivos Bluetooth;
6.1.2.3.57.15. Câmeras e Scanners;
6.1.2.3.58. Deve possuir módulo que habilite ou não o funcionamento das seguintes conexões, no mínimo:
6.1.2.3.58.1. Infravermelho;
6.1.2.3.58.2. Porta Serial;
6.1.2.3.58.3. Porta Paralela;
6.1.2.3.58.4. USB;
6.1.2.3.58.5. FireWire;
6.1.2.3.58.6. PCMCIA;
6.1.2.3.59. Capacidade de liberar acesso a um dispositivo e usuários por um período de tempo específico, sem a necessidade de desabilitar a proteção e o gerenciamento central ou de intervenção local do administrador na máquina do usuário;
6.1.2.3.60. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário, este podendo ser vinculado há um usuário do Active Directory;

6.1.2.3.61. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento;
6.1.2.3.62. Capacidade de habilitar "logging" em dispositivos removíveis tais como Pendrive, Discos externos, entre outros;
6.1.2.3.63. Capacidade de configurar novos dispositivos por Class ID/Hardware ID;
6.1.2.3.64. Capacidade de limitar a execução de aplicativos por hash MD5, nome do arquivo, versão do arquivo, nome do aplicativo, versão do aplicativo, fabricante/desenvolvedor, categoria, por exemplo: navegadores, gerenciador de download, jogos, aplicação de acesso remoto;
6.1.2.3.65. Capacidade de bloquear execução de aplicativo que está em armazenamento externo;
6.1.2.3.66. Capacidade de limitar o acesso dos aplicativos a recursos do sistema, como chaves do registro e pastas/arquivos do sistema, por categoria, fabricante ou nível de confiança do aplicativo;
6.1.2.3.67. Capacidade de, em caso de epidemia, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web;
6.1.2.3.68. Capacidade de, caso o computador cliente saia da rede corporativa, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web;

6.1.3. Proteção para estações de trabalho Mac 3.1.Compatibilidade de instalação nos seguintes sistemas operacionais:

6.1.3.1.1. macOS Mojave 10.14
6.1.3.1.2. macOS High Sierra 10.13
6.1.3.1.3. macOS Sierra 10.12

6.1.3.2.Características da solução de proteção para estação de trabalho Mac

6.1.3.2.1. Deve prover proteção residente para arquivos (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado
6.1.3.2.2. Possuir módulo de Antivírus Web para proteger contra ameaças durante navegação na internet com possibilidade de analisar endereços HTTPS;
6.1.3.2.3. Possuir módulo de bloqueio á ataques na rede;
6.1.3.2.4. Possibilidade de bloquear a comunicação entre a máquina atacante e os demais computadores por tempo definido pelo administrador;

6.1.3.2.5. Capacidade de criar exclusões para computadores que não devem ser monitorados pelo módulo de bloqueio à ataques na rede;
6.1.3.2.6. Possibilidade de importar uma chave no pacote de instalação;
6.1.3.2.7. Deve possuir suportes a notificações utilizando o Growl;
6.1.3.2.8. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
6.1.3.2.9. A instalação e primeira execução do produto deve ser feita sem necessidade de reinicialização do computador, de modo que o produto funcione com toda sua capacidade;
6.1.3.2.10. Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas;
6.1.3.2.11. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluílos da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, por exemplo: "Win32.Trojan.banker", para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
6.1.3.2.12. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
6.1.3.2.13. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;

6.1.3.2.14. Capacidade de verificar somente arquivos novos e alterados;
6.1.3.2.15. Capacidade de verificar objetos usando heurística;
6.1.3.2.16. Capacidade de agendar uma pausa na verificação;
6.1.3.2.17. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
- 6.1.3.2.17.1. Perguntar o que fazer;
- 6.1.3.2.17.2. Bloquear o objeto;
- 6.1.3.2.17.3. Deletar o objeto;
- 6.1.3.2.17.4. Realizar a limpeza do objeto;
- 6.1.3.2.17.5. Em caso positivo de limpeza deve restaurar o objeto;
- 6.1.3.2.17.6. Em caso negativo de limpeza deve mover para quarentena ou apagar;

6.1.3.2.18. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
6.1.3.2.19. Capacidade de verificar arquivos de formato de e-mail;
6.1.3.2.20. Possibilidade de trabalhar com o produto pela linha de comando, com no mínimo opções para atualizar as vacinas, iniciar uma varredura, para o antivírus e iniciar o antivírus pela linha de comando;
6.1.3.2.21. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa);
6.1.3.2.22. Capacidade de voltar para a base de dados de vacina anterior;
6.1.3.2.23. Capacidade de ser instalado, removido e administrado pela mesma console de gerenciamento da solução de proteção para Windows; 4. Proteção para estações de trabalho Linux 4.1.Compatibilidade de instalação nos seguintes sistemas operacionais 32-bits:

6.1.4.1.1. Ubuntu 16.04 LTS e superior;
6.1.4.1.2. Red Hat® Enterprise Linux® 6.7 e superior;
6.1.4.1.3. CentOS-6.7 e superior;
6.1.4.1.4. Debian GNU / Linux 8.6 e superior;
6.1.4.1.5. Debian GNU / Linux 9.4 e superior;
6.1.4.1.6. Linux Mint 18.2 e superior;
6..1.4.1.7. Linux Mint 19 e superior;
6.1.4.1.8. Alt Linux SPT 8.0.0 Work Station;
6.1.4.1.9. Alt Linux SPT 8.0.0 Server;
6.1.4.1.10. Alt Linux 8.2 Work Station;
6.1.4.1.11. Alt Linux 8.2 Work Station;
6.1.4.1.12. Alt Linux 8.2 Server;
6.1.4.1.13. Alt Linux 8.2 Education;
6.1.4.1.14. GosLinux 6.6;
6.1.4.1.15. Lotos;
6.1.4.1.16. Mageia 4;

6.1.4.2.Compatibilidade de instalação nos seguintes sistemas operacionais 64-bits:

6.1.4.2.1. Ubuntu 16.04 LTS e superior
6.1.4.2.2. Ubuntu 18.04 LTS
6.1.4.2.3. Red Hat Enterprise Linux 6.7 e superior
6.1.4.2.4. Red Hat Enterprise Linux 7.2 e superior
6.1.4.2.5. CentOS-6.7 e superior
6.1.4.2.6. CentOS-7.2 e superior
6.1.4.2.7. Debian GNU / Linux 8.6 e superior
6.1.4.2.8. Debian GNU / Linux 9.4 e superior
6.1.4.2.9. OracleLinux 7.3 e superior
6.1.4.2.10. SUSE® Linux Enterprise Server 15

6.1.4.2.11. openSUSE® 15
6.1.4.2.12. Alt Linux SPT 8.0.0 Work Station
6.1.4.2.13. Alt Linux SPT 8.0.0 Server
6.1.4.2.14. Alt Linux 8.2 Work Station
6.1.4.2.15. Alt Linux 8.2 Work Station K
6.1.4.2.16. Alt Linux 8.2 Server
6.1.4.2.17. Alt Linux 8.2 Education
6.1.4.2.18. Amazon Linux AMI
6.1.4.2.19. Linux Mint 18.2 e superior
6.1.4.2.20. Linux Mint 19 e superior
6.1.4.2.21. Micro Focus Open Enterprise Server 2018
6.1.4.2.22. Astra Linux Special Edition 1.5
6.1.4.2.23. Astra Linux Special Edition 1.6
6.1.4.2.24. Astra Linux Common Edition Orel 2.12
6.1.4.2.25. GosLinux 6.6
6.1.4.2.26. Lotos
6.1.4.2.27. RED OS 7.1
6.1.4.2.28. RED OS 7.2 4.3.Características da solução de proteção para estação de trabalho Linux

6.1.4.3.1. Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware) que verifique qualquer arquivo criado, acessado ou modificado;
6.1.4.3.2. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
6.1.4.3.3. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
6.1.4.3.3.1. Capacidade de criar exclusões por local, máscara e nome da ameaça;
6.1.4.3.3.2. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
6.1.4.3.3.3. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;
6.1.4.3.4. Dectectar aplicações que possam ser utilizadas como vetor de ataque por hackers;
6.1.4.3.5. Fazer detecções através de heurística utilizando no mínimo as seguintes opções de nível:
6.1.4.3.5.1. Alta;
6.1.4.3.5.2. Média;
6.1.4.3.5.3. Baixa;
6.1.4.3.5.4. Recomendado;
6.1.4.3.6. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;
6.1.4.3.7. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados;
6.1.4.3.8. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;
6.1.4.3.9. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
6.1.4.3.10. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
6.1.4.3.11. Capacidade de verificar objetos usando heurística;
6.1.4.3.12. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
6.1.4.3.13. Deve possuir módulo escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados

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

6.1.5. Proteção para servidores Windows

6.1.5.1.Compatibilidade de instalação nos seguintes sistemas operacionais 32-bits:
6.1.5.1.1. Windows Server 2003 Standard / Enterprise / Datacenter SP2 e superior;
6.1.5.1.2. Windows Server 2003 R2 Standard / Enterprise / Datacenter SP2 e superior;
6.1.5.1.3. Windows Server 2008 Standard / Enterprise / Datacenter SP1 e superior;
6.1.5.1.4. Windows Server 2008 Core Standard / Enterprise / Datacenter SP1 e superior;

6.1.5.2.Compatibilidade de instalação nos seguintes sistemas operacionais 64-bits:
6.1.5.2.1. Windows Server 2003 Standard / Enterprise / Datacenter SP2 e superior
6.1.5.2.2. Windows Server 2003 R2 Standard / Enterprise / Datacenter SP2 e superior
6.1.5.2.3. Windows Server 2008 Standard / Enterprise / Datacenter SP1 e superior
6.1.5.2.4. Windows Server 2008 Core Standard / Enterprise / Datacenter SP1 e superior
6.1.5.2.5. Microsoft Small Business Server 2008 Standard / Premium
6.1.5.2.6. Windows Server 2008 R2 Foundation / Standard / Enterprise SP1 e superior
6.1.5.2.7. Windows Server 2008 R2 Core Standard / Enterprise / Datacenter SP1 e superior
6.1.5.2.8. Windows Hyper-V Server 2008 R2 SP1 e superior
6.1.5.2.9. Microsoft Small Business Server 2011 Essentials / Standard
6.1.5.2.10. Microsoft Windows MultiPoint Server 2011
6.1.5.2.11. Windows Server 2012 Foundation / Essentials / Standard / Datacenter
6.1.5.2.12. Windows Server 2012 Core Standard / Datacenter
6.1.5.2.13. Windows Storage Server 2012
6.1.5.2.14. Windows Hyper-V Server 2012
6.1.5.2.15. Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter
6.1.5.2.16. Windows Server 2012 R2 Core Standard / Datacenter
6.1.5.2.17. Windows Storage Server 2012 R2
6.1.5.2.18. Windows Hyper-V Server 2012 R2
6.1.5.2.19. Windows Server 2016 Essentials / Standard / Datacenter
6.1.5.2.20. Windows Server 2016 Core Standard / Datacenter
6.1.5.2.21. Windows Storage Server 2016
6.1.5.2.22. Windows Hyper-V Server 2016
6.1.5.2.23. Windows Server 2019 all editions (including Core / Terminal / Hyper-V)

6.1.5.3.Compatibilidade de instalação nos seguintes sistemas de servidores terminais:

6.1.5.3.1. Windows 2008 Server Microsoft Remote Desktop Services;
6.1.5.3.2. Windows 2008 Server R2 Microsoft Remote Desktop Services;
6.1.5.3.3. Windows 2012 Server Microsoft Remote Desktop Services;
6.1.5.3.4. Windows 2012 Server R2 Microsoft Remote Desktop Services;
6.1.5.3.5. Windows 2016 Server Microsoft Remote Desktop Services;
6.1.5.3.6. Windows 2019 Server Microsoft Remote Desktop Services;
61.5.3.7. Citrix XenApp 6.0, 6.5, 7.0, 7.5 - 7.9, 7.15;
6.1.5.3.8. Citrix XenDesktop 7.0, 7.1, 7.5 - 7.9, 7.15;

6.1.5.4.Características da solução de proteção para servidores Windows
6.1.5.4.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware) que verifique qualquer arquivo criado, acessado ou modificado;
6.1.5.4.2. Possuir Auto defesa contra-ataques aos serviços e processos do antivírus no endpoint;

6.1.5.4.3. Firewall com IDS;
6.1.5.4.4. Controle de vulnerabilidades do Windows e dos aplicativos instalados;
6.1.5.4.5. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
6.1.5.4.6. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
6.1.5.4.7. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
6.1.5.4.7.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
6.1.5.4.7.2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação);
6.1.5.4.7.3. Leitura de configurações;
6.1.5.4.7.4. Modificação de configurações;
6.1.5.4.7.5. Gerenciamento de Backup e Quarentena;
6.1.5.4.7.6. Visualização de relatórios;
6.1.5.4.7.7. Gerenciamento de relatórios;
6.1.5.4.7.8. Gerenciamento de chaves de licença;
6.1.5.4.7.9. Gerenciamento de permissões (adicionar/excluir permissões acima);
6.1.5.4.8. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
6.1.5.4.8.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
6.1.5.4.8.2. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados;
6.1.5.4.8.3. Possibilidade de criar horários em que o firewall entrará em funcionamento.
6.1.5.4.9. Módulo de proteção de ransomware, especifico para a linha de servidores.
6.1.5.4.10. Capacidade de separadamente selecionar o número de processos que irão executar funções de varredura em tempo real, o número de processos que executarão a varredura sob demanda e o número máximo de processos que podem ser executados no total;
6.1.5.4.11. Bloquear malwares tais como Cryptlockers mesmo quando o ataque vier de um computador sem antivírus na rede;
6.1.5.4.12. Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros);
6.1.5.4.13. Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja em rodando com fonte ininterrupta de energia (uninterruptible Power supply – UPS);
6.1.5.4.14. Em caso de erros, deve ter capacidade de criar logs e traces automaticamente, sem necessidade de outros softwares;
6.1.5.4.15. Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor;
6.1.5.4.16. Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor;
6.1.5.4.17. Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas;
6.1.5.4.18. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
6.1.5.4.19. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluílos da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, por exemplo: “Win32.Trojan.banker”, para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
6.1.5.4.20. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
6.1.5.4.21. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
6.1.5.4.22. Capacidade de verificar somente arquivos novos e alterados;

6.1.5.4.23. Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários);
6.1.5.4.24. Capacidade de verificar objetos usando heurística;
6.1.5.4.25. Capacidade de configurar diferentes ações para diferentes tipos de ameaças;
6.1.5.4.26. Capacidade de agendar uma pausa na verificação;
6.1.5.4.27. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;
6.1.5.4.28. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
- 6.1.5.4.28.1. Perguntar o que fazer;
- 6.1.5.4.28.2. Bloquear o objeto;
- 6.1.5.4.28.3. Deletar o objeto;
- 6.1.5.4.28.4. Realizar a limpeza do objeto;
- 6.1.5.4.28.5. Em caso positivo de limpeza deve restaurar o objeto;
- 6.1.5.4.28.6. Em caso negativo de limpeza deve mover para quarentena ou apagar;

6.1.5.4.29. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
6.1.5.4.30. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
6.1.5.4.31. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
6.1.5.4.32. Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa;

6.1.6. Proteção para servidores Linux

6.1.6.1.Compatibilidade de instalação nos seguintes sistemas operacionais 32-bits:

6.1.6.1.1. Ubuntu 16.04 LTS e superior;
6.1.6.1.2. Red Hat® Enterprise Linux® 6.7 e superior;
6.1.6.1.3. CentOS-6.7 e superior;
6.1.6.1.4. Debian GNU / Linux 8.6 e superior;
6.1.6.1.5. Debian GNU / Linux 9.4 e superior;
6.1.6.1.6. Linux Mint 18.2 e superior;
6.1.6.1.7. Linux Mint 19 e superior;
6.1.6.1.8. Alt Linux SPT 8.0.0 Work Station;
6.1.6.1.9. Alt Linux SPT 8.0.0 Server;
6.1.6.1.10. Alt Linux 8.2 Work Station;
6.1.6.1.11. Alt Linux 8.2 Work Station;
6.1.6.1.12. Alt Linux 8.2 Server;
6.1.6.1.13. Alt Linux 8.2 Education;
6.1.6.1.14. GosLinux 6.6;
6.1.6.1.15. Lotos
6.1.6.1.16. Mageia 4;

6.1.6.2.Compatibilidade de instalação nos seguintes sistemas operacionais 64-bits:
6.1.6.2.1. Ubuntu 16.04 LTS e superior
6.1.6.2.2. Ubuntu 18.04 LTS
6.1.6.2.3. Red Hat Enterprise Linux 6.7 e superior
6.1.6.2.4. Red Hat Enterprise Linux 7.2 e superior
6.1.6.2.5. CentOS-6.7 e superior
6.1.6.2.6. CentOS-7.2 e superior
6.1.6.2.7. Debian GNU / Linux 8.6 e superior
6.1.6.2.8. Debian GNU / Linux 9.4 e superior
6.1.6.2.9. OracleLinux 7.3 e superior
6.1.6.2.10. SUSE® Linux Enterprise Server 15

6.1.6.2.11. openSUSE® 15
6.1.6.2.12. Alt Linux SPT 8.0.0 Work Station
6.1.6.2.13. Alt Linux SPT 8.0.0 Server Alt Linux 8.2 Work Station
6.1.6.2.14. Alt Linux 8.2 Work Station K
6.1.6.2.15. Alt Linux 8.2 Server
6.1.6.2.16. Alt Linux 8.2 Education
6.1.6.2.17. Amazon Linux AMI
6.1.6.2.18. Linux Mint 18.2 e superior
6.1.6.2.19. Linux Mint 19 e superior
6.1.6.2.20. Micro Focus Open Enterprise Server 2018
6.1.6.2.21. Astra Linux Special Edition 1.5
6.1.6.2.22. Astra Linux Special Edition 1.6
6.1.6.2.23. Astra Linux Common Edition Orel 2.12
6.1.6.2.24. GosLinux 6.6
6.1.6.2.25. Lotos
6.1.6.2.26. RED OS 7.1
6.1.6.2.27. RED OS 7.2

6.1.6.3.Características da solução de proteção para servidores Linux

6.1.6.3.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware) que verifique qualquer arquivo criado, acessado ou modificado;
6.1.6.3.2. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
6.1.6.3.3. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
6.1.6.3.3.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
6.1.6.3.3.2. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;
6.1.6.3.3.3. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;
6.1.6.3.4. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados;
6.1.6.3.5. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;
6.1.6.3.6. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
6.1.6.3.7. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
6.1.6.3.8. Capacidade de verificar objetos usando heurística;
6.1.6.3.9. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
6.1.6.3.10. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
6.1.6.3.11. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux);

6.1.7. Proteção para Smartphones e Tablets

6.1.7.1.Compatibilidade de instalação nos seguintes sistemas operacionais;
6.1.7.1.1. Android 4.2–4.4.4;
6.1.7.1.2. Android 5.0–5.1.1;

6.1.7.1.3. Android 6.0–6.0.1;
6.1.7.1.4. Android 7.0–7.1.2;
6.1.7.1.5. Android 8.0–8.1;
6.1.7.1.6. Android 9.0;
6.1.7.1.7. iOS 9.0–9.3.5;
6.1.7.1.8. iOS 10.0–10.3.3;
6.1.7.1.9. iOS 11.0-11.4.1;

6.1.7.2.Características da solução de proteção para smartphones e tablets

6.1.7.2.1. Proteção em tempo real do sistema de arquivos do dispositivo;
6.1.7.2.2. Proteção contra adware e autodialers;
6.1.7.2.3. Todos os objetos transmitidos usando conexões wireless (porta de infravermelho, Bluetooth) e mensagens EMS, durante sincronismo com PC e ao realizar download usando o browser;
6.1.7.2.4. Arquivos abertos no smartphone;
6.1.7.2.5. Programas instalados usando a interface do smartphone;
6.1.7.2.6. Verificação dos objetos na memória interna do smartphone e nos cartões de expansão sob demanda do usuário e de acordo com um agendamento;
6.1.7.2.7. Deverá isolar em área de quarentena os arquivos infectados;
6.1.7.2.8. Deverá atualizar as bases de vacinas de modo agendado;
6.1.7.2.9. Deverá bloquear spams de SMS através de Black lists;
6.1.7.2.10. Deverá ter função de bloqueio do aparelho caso o SIM CARD for trocado para outro não autorizado com mensagem de aviso ao utilizador do dispositivo;
6.1.7.2.11. Capacidade de desativar por política:
    6.1.7.2.11.1. Wi-FI;
    6.1.7.2.11.2. Câmera;
    6.1.7.2.11.3. Bluetooth;
6.1.7.2.12. Deverá ter função de limpeza de dados pessoais a distância, em caso de roubo, por exemplo;
6.1.7.2.13. Capacidade de requerer uma senha para desbloquear o dispositivo e personalizar a quantidade de caracteres para esta senha;
6.1.7.2.14. Deverá ter firewall pessoal (Android);
6.1.7.2.15. Capacidade de tirar fotos quando a senha for inserida incorretamente;
6.1.7.2.16. Possibilidade de instalação remota utilizando o Microsoft System Center Mobile Device Manager 2008 SP1;
6.1.7.2.17. Capacidade de enviar comandos remotamente de:
    6.1.7.2.17.1. Localizar;
    6.1.7.2.17.2. Bloquear;
    6.1.7.2.17.3. Limpeza Remota;
6.1.7.2.18. Capacidade de detectar Jailbreak em dispositivos iOS;
6.1.7.2.19. Capacidade de bloquear o acesso a site por categoria em dispositivos;
6.1.7.2.20. Capacidade de bloquear o acesso a sites phishing ou malicioso;
6.1.7.2.21. Capacidade de criar containers de aplicativos, separando dados corporativos de dados pessoais;
6.1.7.2.22. Capacidade de bloquear o dispositivo quando o cartão “SIM” for substituído;
6.1.7.2.23. Capacidade de configurar White e blacklist de aplicativos;
6.1.7.2.24. Capacidade de localizar o dispositivo quando necessário;
6.1.7.2.25. Permitir atualização das definições quando estiver em “roaming”;
6.1.7.2.26. Capacidade de selecionar endereço do servidor para buscar a definição de vírus;
6.1.7.2.27. Deve permitir verificar somente arquivos executáveis;
6.1.7.2.28. Deve ter a capacidade de desinfectar o arquivo se possível;
6.1.7.2.29. Capacidade de agendar uma verificação;
6.1.7.2.30. Capacidade de enviar URL de instalação por e-mail;

6.1.7.2.31. Capacidade de fazer a instalação através de um link QRCode;
6.1.7.2.32. Capacidade de executar as seguintes ações caso a desinfecção falhe:
- 6.1.7.2.32.1. Deletar;
- 6.1.7.2.32.2. Ignorar;
- 6.1.7.2.32.3. Quarentenar;
- 6.1.7.2.32.4. Perguntar ao usuário;

6.1.7.2.33. Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange
6.1.7.2.34. Capacidade de ajustar as configurações de:
- 6.1.7.2.34.1. Sincronização de e-mail;
- 6.1.7.2.34.2. Uso de aplicativos;
- 6.1.7.2.34.3. Senha do usuário
- 6.1.7.2.34.4. Criptografia de dados;
- 6.1.7.2.34.5. Conexão de mídia removível;

6.1.7.2.35. Capacidade de instalar certificados digitais em dispositivos móveis;
6.1.7.2.36. Capacidade de, remotamente, resetar a senha de dispositivos iOS;
6.1.7.2.37. Capacidade de, remotamente, apagar todos os dados de dispositivos iOS;
6.1.7.2.38. Capacidade de, remotamente, bloquear um dispositivo iOS;
6.1.7.2.39. Deve permitir configurar horário para sincronização do dispositivo com a console de gerenciamento;
6.1.7.2.40. Possibilidade de exigir senha para abrir aplicações instaladas em container;
6.1.7.2.41. Deve permitir que o usuário utilize autenticação do Active Directory para abrir aplicações em container;
6.1.7.2.42. Deve permitir que uma senha seja digitada a cada x(minutos) para continuar utilizando uma aplicação em container;
6.1.7.2.43. Deve permitir a criptografia de dados salvos pelas aplicações em container;
6.1.7.2.44. Permitir sincronização com perfil do “Touch Down”;
6.1.7.2.45. Capacidade de desinstalar remotamente o antivírus do dispositivo;
6.1.7.2.46. Deve permitir fazer o upgrade do antivírus de forma remota sem a necessidade de desinstalar a versão atual;
6.1.7.2.47. Capacidade de sincronizar com Samsung Knox;
6.1.7.2.48. Deve permitir criar perfis de políticas para out-of-office no caso de BYOD.

6.1.8. Criptografia

6.1.8.1.Compatibilidade de instalação nos seguintes sistemas operacionais:
6.1.8.1.1. Microsoft Windows 7 Ultimate SP1 ou superior x86/x64;
6.1.8.1.2. Microsoft Windows 7 Enterprise SP1 ou superior x86/x64;
6.1.8.1.3. Microsoft Windows 7 Professional SP1 ou superior x86/x64;
6.1.8.1.4. Microsoft Windows 8 Enterprise x86/x64;
6.1.8.1.5. Microsoft Windows 8 Pro x86/x64;
6.1.8.1.6. Microsoft Windows 8.1 Pro x86/x64;
6.1.8.1.7. Microsoft Windows 8.1 Enterprise x86/x64;
6.1.8.1.8. Microsoft Windows 10 Enterprise x86/x64;
6.1.8.1.9. Microsoft Windows 10 Pro x86/x64;
6.1.8.2. O acesso ao recurso criptografado (arquivo, pasta ou disco) deve ser garantido mesmo em caso o usuário tenha esquecido a senha, através de procedimentos de recuperação;
6.1.8.3. Utilizar, no mínimo, algoritmo AES com chave de 256 bits;
6.1.8.4.Capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de pré-boot para autenticação do usuário;
6.1.8.5.Capacidade de utilizar Single Sign-On para a autenticação de pré-boot;
6.1.8.6.Permitir criar vários usuários de autenticação pré-boot;

6.1.8.7.Capacidade de criar um usuário de autenticação pré-boot comum com uma senha igual para todas as máquinas a partir da console de gerenciamento;
6.1.8.8.Capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções:
6.1.8.9.Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes;
6.1.8.10. Criptografar todos os arquivos individualmente;
6.1.8.11. Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas;
6.1.8.12. Criptografar o dispositivo em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha;
6.1.8.13. Capacidade de selecionar pastas e arquivos (por tipo, ou extensão) para serem criptografados automaticamente. Nesta modalidade, os arquivos devem estar acessíveis para todas as máquinas gerenciadas pela mesma console de maneira transparente para os usuários;
6.1.8.14. Capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados;
6.1.8.15. Capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados;
6.1.8.16. Verifica compatibilidade de hardware antes de aplicar a criptografia;
6.1.8.17. Possibilita estabelecer parâmetros para a senha de criptografia;
6.1.8.18. Bloqueia o reuso de senhas;
6.1.8.19. Bloqueia a senha após um número de tentativas pré-estabelecidas;
6.1.8.20. Capacidade de permitir o usuário solicitar permissão a determinado arquivo criptografado para o administrador mediante templates customizados;
6.1.8.21. Permite criar exclusões para não criptografar determinados “discos rígidos” através de uma busca por nome do computador ou nome do dispositivo
6.1.8.22. Permite criptografar as seguintes pastas pré-definidas: “meus documentos”, “Favoritos”, “Desktop”, “Arquivos temporários” e “Arquivos do outlook”;
6.1.8.23. Permite utilizar variáveis de ambiente para criptografar pastas customizadas;
6.1.8.24. Capacidade de criptografar arquivos por grupos de extensão, tais como: Documentos do office, Document, arquivos de audio, etc;
6.1.8.25. Permite criar um grupo de extensões de arquivos a serem criptografados;
6.1.8.26. Capacidade de criar regra de criptografia para arquivos gerados por aplicações;
6.1.8.27. Permite criptografia de dispositivos móveis mesmo quando o endpoint não possuir comunicação com a console de gerenciamento.
6.1.8.28. Capacidade de deletar arquivos de forma segura após a criptografia;
6.1.8.29. Capacidade de criptografar somente o espaço em disco utilizado;
6.1.8.30. Deve ter a opção de criptografar arquivos criados a partir de aplicações selecionadas pelo administrador;
6.1.8.31. Capacidade de bloquear aplicações selecionadas pelo administrador de acessarem arquivos criptografados;
6.1.8.32. Deve permitir criptografar somente o espaço utilizado em dispositivos removíveis tais como pendrives, HD externo, etc;
6.1.8.33. Capacidade de criptografar discos utilizando a criptografia BitLocker da Microsoft;
6.1.8.34. Deve ter a opção de utilização de TPM para criptografia através do BitLocker;
6.1.8.35. Capacidade de fazer “Hardware encryption”;

6.1.9. Gerenciamento de Sistemas

6.1.9.1.Capacidade de criar imagens de sistema operacional remotamente e distribuir essas imagens para computadores gerenciados pela solução e para computadores bare-metal;
6.1.9.2.Deve possibilitar a utilização de servidores PXE na rede para deploy de imagens;

6.1.9.3. Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares vulneráveis
6.1.9.4.Capacidade de corrigir as vulnerabilidades de softwares, fazendo o download centralizado da correção ou atualização e aplicando essa correção ou atualização nas máquinas gerenciadas de maneira transparente para os usuários;
6.1.9.5.Capacidade de gerenciar licenças de softwares de terceiros;
6.1.9.6.Capacidade de registrar mudanças de hardware nas máquinas gerenciadas;
6.1.9.7.Capacidade de gerenciar um inventário de hardware, com a possibilidade de cadastro de dispositivos (ex: router, switch, projetor, acessório, etc), informando data de compra, local onde se encontra, service tag, número de identificação e outros;
6.1.9.8.Possibilita fazer distribuição de software de forma manual e agendada;
6.1.9.9.Suporta modo de instalação silenciosa;
6.1.9.10. Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis;
6.1.9.11. Possibilita fazer a distribuição através de agentes de atualização;
6.1.9.12. Utiliza tecnologia multicast para evitar tráfego na rede;
6.1.9.13. Possibilita criar um inventário centralizado de imagens;
6.1.9.14. Capacidade de atualizar o sistema operacional direto da imagem mantendo os dados do usuário;
6.1.9.15. Suporte a WakeOnLan para deploy de imagens;
6.1.9.16. Capacidade de atuar como servidor de atualização do Windows podendo fazer deploy de patches;
6.1.9.17. Suporta modo de teste, podendo atribuir alguns computadores para receberem as atualizações de forma automática para avaliação de alterações no comportamento;
6.1.9.18. Capacidade de gerar relatórios de vulnerabilidades e patches;
6.1.9.19. Possibilita criar exclusões para aplicação de patch por tipo de sistema operacional, Estação de trabalho e Servidor ou por grupo de administração;
6.1.9.20. Permite iniciar instalação de patch e correções de vulnerabilidades ao reiniciar ou desligar o computador;
6.1.9.21. Permite baixar atualizações para o computador sem efetuar a instalação;
6.1.9.22. Permite o administrador instalar somente atualizações aprovadas, instalar todas as atualizações (exceto as bloqueadas) ou instalar todas as atualizações incluindo as bloqueadas;
6.1.9.23. Capacidade de instalar correções de vulnerabilidades de acordo com a severidade;
6.1.9.24. Permite selecionar produtos a serem atualizados pela console de gerenciamento;
6.1.9.25. Permite selecionar categorias de atualizações para serem baixadas e instaladas, tais como: atualizações de segurança, ferramentas, drivers, etc;
6.1.9.26. Capacidade de adicionar caminhos específicos para procura de vulnerabilidades e updates em arquivos;
6.1.9.27. Capacidade de instalar atualizações ou correções somente em computadores definidos, em grupos definidos ou em uma porcentagem de computadores conforme selecionado pelo administrador;
6.1.9.28. Capacidade de configurar o reinício do computador após a aplicação das atualizações e correções de vulnerabilidades;
6.1.9.29. Deve permitir selecionar o idioma das aplicações que serão atualizadas;
6.1.9.30. Permitir agendar o sincronismo entre a console de gerenciamento e os sites da Microsoft para baixar atualizações recentes;

6.2**.** Requisitos dos Futuros Serviços Contratados

Para prestar os serviços a futura Contratada deverá possuir infraestrutura tecnológica e de serviços comprovada.

6.2.1. Requisitos da Futura Contratada:

Para prestar os serviços a futura Contratada deverá:

I - Ser empresa com especialização em soluções de antivírus para ambientes corporativos de tecnologia da informação;

II - Trabalhar em conformidade com as leis de licenciamento de softwares;

III - Possuir acervo técnico de soluções que envolvam a Solução de Antivírus seu gerenciamento;

IV - Disponibilizar equipe técnica com as qualificações exigidas para o objeto deste Termo de Dispensa e prestação de serviços decorrente deste;

V - Possuir Central de Serviços para atendimento ao Cliente, por e-mail e telefone DDG 0800.

6.3.2. Requisitos da Equipe Técnica:

I - Os serviços descritos neste Termo de Dispensa, bem como qualquer outro não descrito, mas que sua utilização seja necessária para a aquisição aqui descrita, serão de responsabilidade da futura Contratada e serão executados por técnicos contratados para este fim, não havendo nenhuma relação empregatícia desses profissionais com a futura Contratante;

II - A futura Contratada deverá conciliar os serviços com os prazos definidos no presente Termo. Deverá também dimensionar sua equipe para manter o nível de serviço contratado e alocar mais profissionais quando necessário;

III - As equipes constituídas para a prestação de serviços à futura Contratante deverão ter amplo conhecimento e experiência profissional em suas respectivas áreas.

6.4 Gestão da Prestação dos Serviços

I - A futura Contratante e a futura Contratada farão reuniões ordinárias, se necessário, para acompanhar a evolução dos serviços, avaliar os resultados específicos e verificar a conformidade destes resultados com os requisitos definidos;

II - As reuniões deverão ser realizadas de forma virtual, em sala de conferencia disponibilizada pela futura Contratante, em data e horário a ser combinado, ter a participação dos 'Representantes Técnicos Operacionais' da futura Contratante e da futura Contratada e, quando necessário, de técnicos convocados de ambos os lados;

III - A futura Contratada deverá notificar a futura Contratante qualquer incidente, bem como acionar todos os mecanismos para solucionar o problema;

IV - A futura Contratante informará a futura Contratada quais empregados ou fornecedores deverão ser acionados para escalonamento de problemas, dependendo da área de atuação;

V - O Representante Técnico Operacional da futura Contratada deverá notificar os incidentes detectados, mesmo que já solucionados, para efeito de registro, acompanhamento, estatística e contabilização;

VI - A futura Contratante poderá realizar auditorias para: prevenir, fiscalizar, identificar possíveis causas de resultados insatisfatórios e sugerir soluções que possam aumentar a efetividade e a eficiência dos serviços contratados.

6.5 Forma de Execução e Entrega de Serviços

I - O prazo de ativação das licenças deve ser de, no máximo 07 (sete) dias úteis contados a partir da assinatura do Contrato.

§ 1º - A operacionalização do objeto da presente dispensa de licitação será recebida em caráter provisório através de um Termo de Recebimento Provisório, emitido pela futura Contratante. A partir da emissão do termo haverá um prazo de até 10 (dez) dias úteis para aprovação da operacionalização, que se ocorrer será formalizada através de um 'Termo de Recebimento Definitivo'.

§ 2º - Não sendo total ou parcialmente aprovada a operacionalização, a futura Contratada terá um prazo de até 5 (cinco) dias úteis da ciência da não aprovação, para sanar as irregularidades constadas, sendo novamente considerados os prazos dispostos no parágrafos imediatamente anteriores do presente inciso.

II - A utilização das licenças adquiridas será de forma continuada, nos 7 (sete) dias da semana, 24 (vinte e quatro) horas por dia, conforme necessidade da futura Contratante.

III - Os serviços de suporte serão prestados de forma continuada, no período de vigência contratual, de segunda a sexta-feita (12x5), das 08h às 20h, por telefone, chat e/ou e-mail.

IV - No caso de erro crítico do sistema, a futura Contratada terá o prazo de 01 (um) dia útil para sua solução;

V - A futura Contratada disponibilizará uma Biblioteca on-line para a futura Contratante realizar pesquisas e auto-atendimento.

7. **Valor Contratual final:** (inclusos custos relativos a assistência técnica, impostos, taxas, fretes, etc.)

O valor contratual será de R$16.298,58 (dezesseis mil, duzentos e noventa e oito reais e cinquenta e oito centavos) no período de vigência contratual.

8. **Pagamento**:

Em moeda corrente do Brasil, em 01 (uma) parcela, com vencimento 01 (um) dia após a emissão do Termo de Recebimento Definitivo (item 6.5), contra nota fiscal-fatura emitida pela Contratada.

II - A COINPEL subordina-se a aplicação do Decreto Municipal 6.648 de 27/09/2022, portanto, caso a futura contratada se enquadre na norma citada, será realizada a retenção do IR conforme o Decreto e a IN Municipal 22/2022.

9. **Base legal**:

Art. 29, inciso II, da Lei Federal nº. 13.303/16 e alterações.

10. **Do Contrato e dos documentos de Habilitação**:

Com base no presente Termo, estando devidamente assegurada a verba orçamentária, que se providencie a elaboração do Contrato e sua assinatura, com base na Lei Federal 13.303/16 e alterações, e na proposta da futura contratada, mediante o fornecimento prévio, por esta, de via original, ou cópia autenticada, ou extraídas de sites oficiais, dos seguintes documentos, conforme o caso:

I - habilitação jurídica; apresentação de documentos que comprovem a aptidão para a aquisição de direitos e da assunção de obrigações por parte do licitante, conforme o caso, consistindo em:

a) cédula de identidade, no caso de pessoa física;
b) prova de inscrição no CNPJ ou CPF, conforme o caso;
c) no caso de empresário individual, registro da empresa acompanhado de cédula de identidade;
d) no caso de empresário individual de responsabilidade limitada, ato constitutivo com indicação do administrador;

e) no caso de sociedade simples, inclusive cooperativas, ato constitutivo, devidamente registrado no órgão competente, acompanhado de ata de eleição de seus administradores, quando for o caso;
f) no caso de sociedades empresárias, ato constitutivo, acompanhado de eleição de seus administradores, quando for o caso;
g) inscrição do ato constitutivo, no caso de sociedades civis, acompanhada de ato formal de designação de diretoria em exercício;
h) decreto de autorização ou equivalente, em se tratando de empresa ou sociedade estrangeira em funcionamento no País, acompanhado do ato de registro ou autorização para funcionamento expedido pelo órgão competente, quando a atividade assim o exigir;
i) termo de compromisso de constituição de consórcio, público ou particular, quando a contratação permitir a participação de empresas em consórcio nos termo da Lei Federal 13.303/16

II - regularidade fiscal consistindo em:

a) prova de regularidade com o INSS, mediante apresentação de Certidão Negativa de Débitos relativos aos Tributos Federais e Dívida Ativa da União;
b) prova de regularidade relativa ao Fundo de Garantia por Tempo de Serviço (FGTS), mediante a apresentação do Certificado de Regularidade do FGTS – CRF.

§ 1º –Os documentos necessários à habilitação poderão ser apresentados em original, mediante cópia autenticada por cartório competente ou por empregado da COINPEL, membro da comissão de licitação ou pregoeiro, por publicação em órgão da imprensa oficial, enviados para o e-mail sandra.nunes@pelotas.rs.gov.br desde que produzidos por cartório com a utilização de processo de certificação disponibilizada pela ICP-Brasil ou por site com verificação de autenticidade, ou obtidos pela internet em sítios oficiais do órgão emissor.

§ 2º – Os documentos de habilitação poderão ser substituídos, total ou parcialmente, pelo SICAF, desde que atualizado.

§ 3º – As certidões expedidas pelos órgãos da administração fiscal e tributária, desde que assim instituídas pelo órgão emissor, poderão ser emitidas pela internet, sendo válidas independentemente de assinatura ou chancela de servidos dos órgãos emissores.

§ 4º – Se, por força de lei, a futura contratada estiver dispensada da posse de alguns dos documentos elencados no presente item, conforme o caso, deverá apresentar declaração por escrito, neste sentido, informando no corpo da mesma, qual a base legal de tal dispensa.

§ 5º – Documentos oficiais que contenham prazo de validade em seu corpo, devem ser válidos, pelo menos, até a data de 'conhecimento' deste Termo, pela futura contratada.

§ 6º – Os documentos de habilitação devem vincular-se especificamente a futura contratada.

Pelotas,RS, 30 de junho de 2023.
Leandro Felix

LEANDRO DA SILVA FÉLIX
Diretor-Presidente

Ciente
Sandra Nunes

SANDRA REGINA NUNES DA SILVA
Coord. Adm. e Financeira.

SOLUÇÕES CORPORATIVAS
SUPPORT, PRODUCTS AND SOLUTIONS

kaspersky

Proposta Comercial

COINPEL
Companhia de Informática de Pelotas.

De fornecimento de Solução Antivírus kaspersky

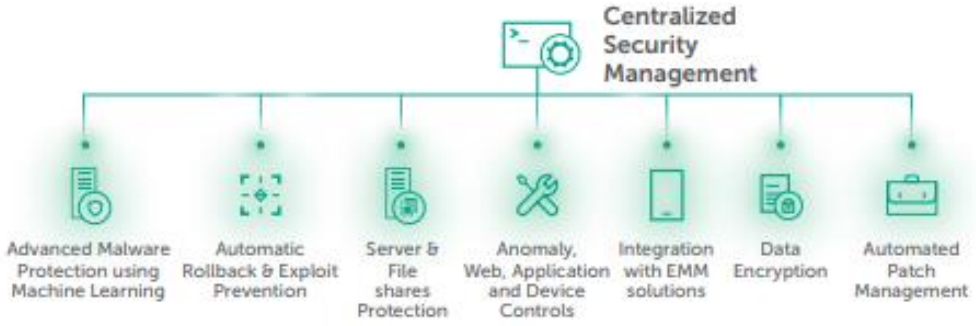
threatpost
End: Av. Mariland, 1135/201 - Telefone: 0XX(51)3024-3131 - e-mail: comercial@kscorp.com.br
Bairro: Mont`Serrat - CEP: 90440-191 – Porto Alegre / RS.

Porto Alegre, 20 de junho de 2023.

À
COINPEL - Companhia de Informática de Pelotas.
A/C Sr. Nataniel Vieira

Prezados senhores, encaminhamos para as vossas considerações nossa **proposta para renovação do licenciamento do Antivírus Kaspersky Endpoint Security For Business - Versão Advanced.** Com essa ação estamos adequando o nosso produto a nova realidade de TI da vossa empresa. Nosso compromisso é estar contribuindo para que o resultado da tecnologia apresentada beneficie o vosso trabalho.

Kaspersky Endpoint Security for Business – ADVANCED



Como sua empresa tem dados confidenciais que devem ser mantidos em segurança, vamos além da proteção de todos os endpoints. O Gerenciamento de Correções ajuda a eliminar vulnerabilidades de segurança, enquanto a criptografia evita que criminosos virtuais acessem seus dados.

- **Oferece proteção adaptativa contra ameaças conhecidas e desconhecidas.**
- **Reduz sua exposição aos ataques, fortalecendo os endpoints.**
- **Ajuda a impedir a perda ou o roubo de dados comerciais confidenciais.**
- **Protege de vulnerabilidades para reduzir os pontos de entrada dos ataques.**
- **Economiza tempo automatizando o sistema operacional e as tarefas de implementação de software.**
- **Simplifica o gerenciamento da segurança com um console da Web unificado.**

O Kaspersky Endpoint Security for Business Advanced inclui todos os recursos oferecidos pelo Kaspersky Endpoint Security for Business Select, além de tecnologias adicionais que fazem ainda mais para proteger a sua empresa

End: Av. Mariland, 1135/201 - Telefone: 0XX(51)3024-3131 - e-mail: comercial@kscorp.com.br
Bairro: Mont`Serrat - CEP: 90440-191 – Porto Alegre / RS.

Segurança adaptativa para todos

Reduzindo sua exposição a ataques baseados em aplicativos, o Adaptive Anomaly Control eleva automaticamente a segurança ao nível mais alto, apropriado para todos na organização. Além disso, ele é complementado pelo Controle de Aplicativos de nível corporativo e por um console de gerenciamento flexível.

Prevenção avançada de ameaças

Bloqueia ataques em tempo real, usando o Sistema de Prevenção de Invasões Baseado em Host. Identifica vulnerabilidades e aplica as correções mais recentes para fechar os pontos de entrada de ataques. Também permite controlar quais aplicativos podem ser executados em seus servidores.

Prevenção avançada de ameaças

As funções de criptografia com certificação FIPS 140.2 e Common Criteria, além do gerenciamento da criptografia incorporada no sistema operacional, protegem os dados corporativos e as informações confidenciais de clientes para ajudar a cumprir as principais metas de conformidade, incluindo o GDPR.

Gerenciamento simplificado de sistemas

Automatiza a criação, o armazenamento e a clonagem de imagens do sistema para que você economize tempo sempre que sua empresa precisar distribuir novos sistemas ou atualizar o software nos sistemas existentes.

Abertura que nenhum outro fornecedor oferece

Somos pioneiros no fornecimento dos mais altos níveis de transparência e soberania de dados, além de neutralidade. Processamos os dados centrais na Suíça, um país geopoliticamente neutro, onde nossos parceiros podem analisar nosso código fonte**.**

A ESCOLHA INTELIGENTE DE SEGURANÇA

Obtenha uma segurança de endpoints que se adapta a novas ameaças

Somos reconhecidos pela inovação e identificamos mais ameaças avançadas do que qualquer outro fornecedor. Independentemente de seu departamento de TI ser local ou terceirizado, nossa segurança se adapta para proteger você contra novas ameaças.

Controle rigorosamente seus custos

Como incluímos várias tecnologias de segurança — inclusive da próxima geração — em um só produto, nossos preços são diretos. Você precisa adquirir apenas um produto, com uma licença.

Combine desempenho e proteção de várias camadas

A segurança não pode torná-lo mais lento. Por isso, nossa segurança adaptativa tem impacto mínimo sobre o desempenho do sistema. Quando você é atacado, a reversão automática desfaz a maioria das ações mal-intencionadas para que os usuários possam continuar trabalhando.

Testes e análises nos ajudam a oferecer mais segurança

A segurança não pode torná-lo mais lento. Por isso, nossa segurança adaptativa tem impacto mínimo sobre o desempenho do sistema. Quando você é atacado, a reversão automática desfaz a maioria das ações mal-intencionadas para que os usuários possam continuar trabalhando.

End: Av. Mariland, 1135/201 - Telefone: 0XX(51)3024-3131 - e-mail: comercial@kscorp.com.br
Bairro: Mont`Serrat - CEP: 90440-191 – Porto Alegre / RS.

Segurança sob medida para qualquer organização

Nosso modelo com base em funções ajuda a dividir as responsabilidades entre suas equipes. O console de gerenciamento na Web pode ser configurado para garantir que cada administrador tenha acesso somente às ferramentas e aos dados de que precisa.

Economize tempo com administração e aumente a proteção

Usando inteligência em tempo real sobre explorações, nosso Vulnerability Assessment & Patch Management pode aplicar as correções mais recentes de segurança em uma grande variedade de aplicativos bastante usados.

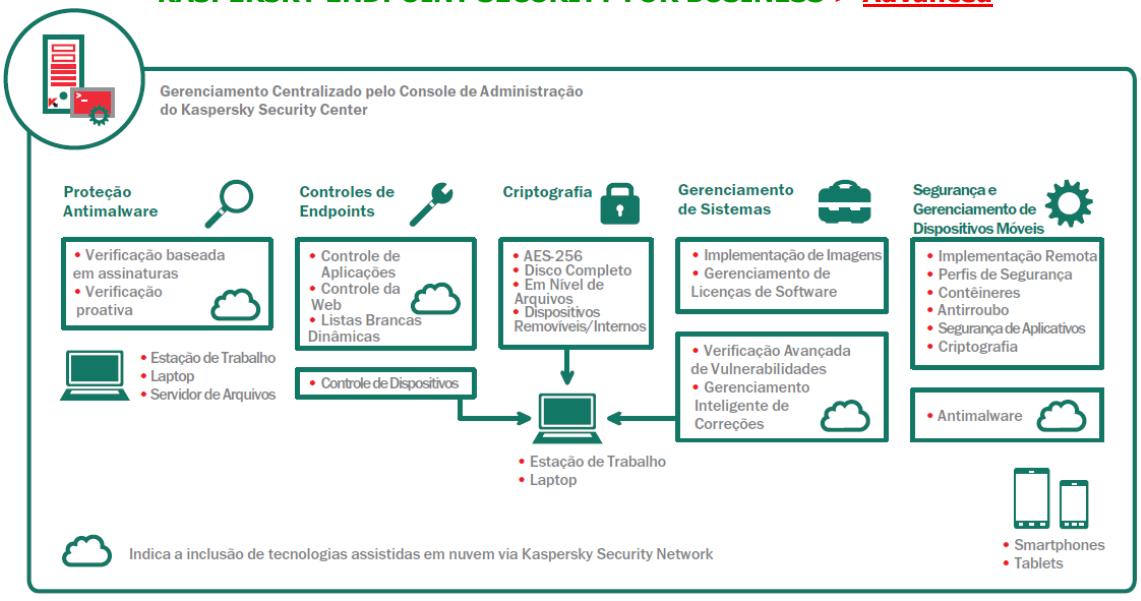
- **Conheça mais sobre o produto:**
  https://media.kaspersky.com/br/business-security/endpoint-security-advanced-datasheet.pdf

End: Av. Mariland, 1135/201 - Telefone: 0XX(51)3024-3131 - e-mail: comercial@kscorp.com.br
Bairro: Mont`Serrat - CEP: 90440-191 – Porto Alegre / RS.

SOLUÇÕES CORPORATIVAS
SUPPORT, PRODUCTS AND SOLUTIONS

kaspersky

KASPERSKY ENDPOINT SECURITY FOR BUSINESS > Advanced



VALORES PARA RENOVAÇÃO EM 2023 DA VERSÃO ADVANCED

OPÇÃO 1.

VALORES PARA 100 LICENÇAS	
LICENÇAS PERÍODO =	1 ANO
Valor Unitário : R$	108,66
Valor Total : R$	10.865,72
LICENÇAS PERÍODO =	2 ANOS
Valor Unitário : R$	162,99
Valor Total : R$	16.298,58
LICENÇAS PERÍODO =	3 ANOS
Valor Unitário : R$	217,31
Valor Total : R$	21.731,44

OPÇÃO 2.

VALORES PARA 300 LICENÇAS	
LICENÇAS PERÍODO =	1 ANO
Valor Unitário : R$	85,14
Valor Total : R$	25.541,46
LICENÇAS PERÍODO =	2 ANOS
Valor Unitário : R$	128,28
Valor Total : R$	38.484,45
LICENÇAS PERÍODO =	3 ANOS
Valor Unitário : R$	170,85
Valor Total : R$	51.255,18

A KASPERSKY ESTÁ CONCEDENDO EXCLUSIVAMENTE PARA A SUA RENOVAÇÃO A CONDIÇÃO DO PAGUE 2 ANOS E RECEBA 3 ANOS DE LICENCIAMENTO.
1 ANO GRATUITO DE PROTEÇÃO. - CONDIÇÃO EXCLUSIVA PARA A SUA EMPRESA

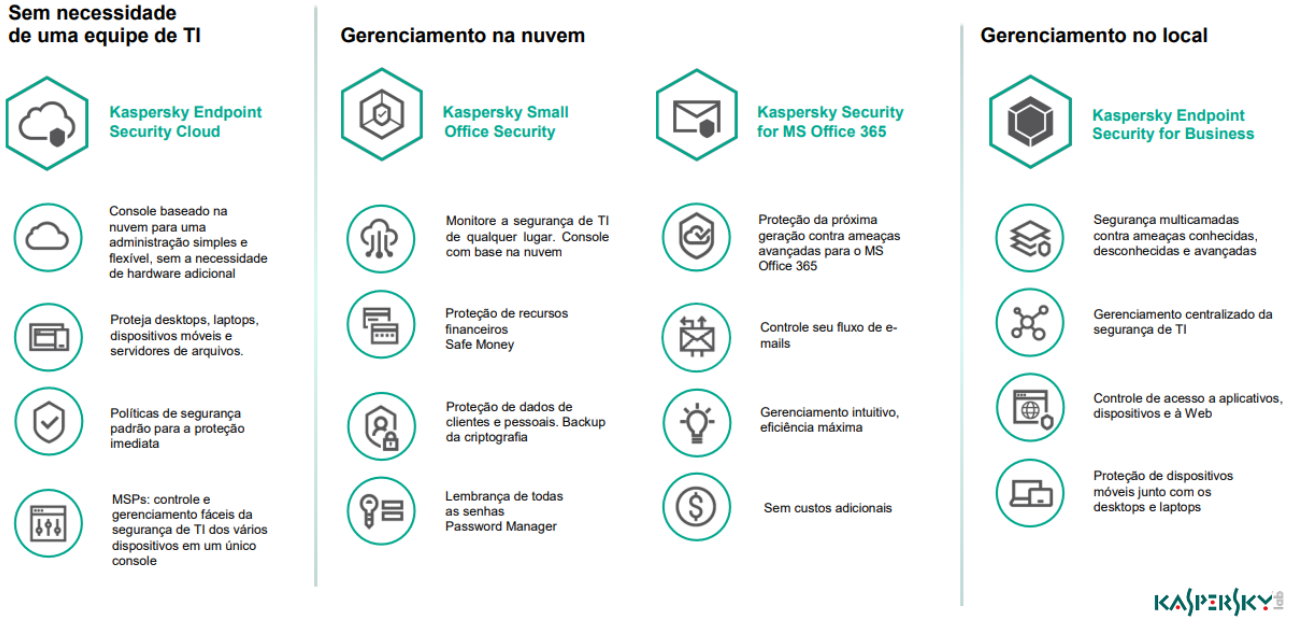
CAMPANHA VÁLIDA SOMENTE ATÉ O DIA 30/06/2023 – IMPRETERIVELMENTE

threatpost
End: Av. Mariland, 1135/201 - Telefone: 0XX(51)3024-3131 - e-mail: comercial@kscorp.com.br
Bairro: Mont`Serrat - CEP: 90440-191 – Porto Alegre / RS.

SOLUÇÕES CORPORATIVAS
SUPPORT, PRODUCTS AND SOLUTIONS

kaspersky

SOLUÇÕES KASPERSKY LAB. PARA PEQUENAS E MÉDIAS EMPRESAS



Condições de Pagamento: A) 100% contra empenho

Suporte: Lembramos aos senhores que concedemos todo o suporte remoto e treinamentos on-line sem custos para a vossa Instituição. – Acesse a nossa página na web e solicite a sua senha de acesso para a nossa área do cliente – https://companyaccount.kaspersky.com

Valores em Reais

Prazo de Entrega: 07 dias úteis.

Garantia: 1, 2 ou 3 anos, de acordo com o período contratado.

Validade da Proposta: Sujeito a alterações sem aviso prévio.

Sem outro assunto a tratar, agradecemos a sua atenção e colocamo-nos à sua disposição para maiores esclarecimentos sobre o assunto.

Atenciosamente;

Newton Souza

threatpost
End: Av. Mariland, 1135/201 - Telefone: 0XX(51)3024-3131 - e-mail: comercial@kscorp.com.br
Bairro: Mont`Serrat - CEP: 90440-191 – Porto Alegre / RS.

Caxias do Sul, 29 de Junho de 2023.

À
Companhia de Informática de Pelotas – COINPEL
A/C Sr. Nataniel da Silva Vieira

Prezados Senhores,

Atendendo a vossa solicitação, vimos apresentar nossa proposta para a renovação do licenciamento do antivírus Kaspersky Endpoint Security for Business Advanced, para 100 (cem) licenças, sendo que a referida versão atende Endpoints, Servidores de Arquivos e Dispositivos Móveis.

Produto: (100 Licenças) Kaspersky Endpoint Security for Business Advanced.

Período	Valor Unit (R$)	Valor Total (R$)
1 ano:	R$ 142,60	R$ 14.260,00
2 anos:	R$ 203,40	R$ 20.340,00
3 anos:	R$ 285,30	R$ 28.530,00

Prazo de entrega: 10 dias úteis
Prazo de garantia: conforme o período de contratação.
Validade desta proposta: 30 dias

Caso haja qualquer dúvida, não hesite em nos contatar.

Cordialmente,

Arielson Pimmel
Diretor Comercial

Caxias do Sul, 28 de Junho de 2023.

Á

Coinpel – Pelotas / RS

Prezados Senhores,

Atendendo a vossa solicitação, geramos uma Proposta Comercial de Fornecimento de Solução para o Antivírus Kaspersky – versão Advanced. A partir de nossas negociações, a Maestech apresenta esta proposta para a vossa apreciação.

Caso haja qualquer dúvida, não hesite em nos contatar.

Cordialmente,

Paulo Lazzarotto
Departamento Comercial

DESCRIÇÃO DA SOLUÇÃO:

Kaspersky
Endpoint Security for Business
ADVANCED

Segurança adaptativa como nenhuma outra

Sua empresa detém dados sigilosos que devem ser mantidos em segurança, e é por isso que fazemos mais do que apenas proteger todos os endpoints. O EDR automatizado detecta ameaças avançadas, enquanto o fortalecimento do servidor aprimora a proteção de alto desempenho com controles adicionais de aplicativos, da Web e de dispositivos, para evitar o roubo de informações corporativas e financeiras.

- Detecta e corrige vulnerabilidades para reduzir os pontos de entrada dos ataques
- Economiza tempo automatizando as tarefas de implementação de software e do sistema operacional
- Simplifica o gerenciamento da segurança centralizado com um console na Web ou na nuvem
- Criptografa dados para evitar danos causados por vazamento de dados em um dispositivo Perdido

Essa camada inclui todas as funcionalidades disponíveis no Kaspersky Endpoint Security for Business Select, além de tecnologias avançadas adicionais que fazem ainda mais para proteger a sua empresa.

INFORMAÇÕES COMERCIAIS

Produto: **Kaspersky Endpoint Security For Business – Advanced**
Operação: **Renovação do licenciamento Kaspersky**
Nº de Licenças solicitadas**: 100 licenças**

Período de Contratação:	**1 Ano.**	**2 anos.**	**3 anos.**
Valor Unitário por licença:	**R$ 138,90**	**R$ 207,40**	**R$ 298,35**
Valor Total da Solução:	**R$ 13.890,00**	**R$ 20.740,00**	**R$ 29.835,00**

CONDIÇÕES COMERCIAIS DE FORNECIMENTO:

1. Valores expressos em Reais.
2. Impostos Inclusos.
3. Forma de Pagamento: 100 % em 10 dias do pedido.
4. Prazo de Entrega: até 7 dias para emissão das licenças.
5. Validade da Proposta: 3 (Três) dias.

Qualquer dúvida, estarei à disposição.

Att.

Paulo Lazzarotto
Departamento Comercial

Datas e horários baseados em Brasília, Brasil
Sincronizado com o NTP.br e Observatório Nacional (ON) em 30/06/2023 às 11:33:43

Dispensa 03/2023 KS Soluções

Data e Hora de Criação: 30/06/2023 às 09:32:07

Documentos que originaram esse envelope:

- Termo_de_dispensa_032023_Antivirus.pdf (Arquivo PDF) - 24 página(s)
- proposta KS.pdf (Arquivo PDF) - 8 página(s)
- orçamento Phrothee.pdf (Arquivo PDF) - 1 página(s)
- proposta Maestech.pdf (Arquivo PDF) - 3 página(s)

Hashs únicas referente à esse envelope de documentos

[SHA256]: 67321d8c6ae76dfa59c838af3b6e9ca9da6433da868b655366ab5c52c54d33fd
[SHA512]: 6b418b93a68b33a77227d494fee566645c8813a0c5df2caff18edce409b5b1962770d0982bd9988485ff12dd4f9809bc682084b7168167a51fb489a17b05b5bd

Lista de assinaturas solicitadas e associadas à esse envelope

ASSINADO - Leandro Da Silva Félix (leandro.felix@pelotas.rs.gov.br)
Data/Hora: 30/06/2023 - 10:01:17, IP: 187.86.132.227, Geolocalização: [-31.76625, -52.342867]
[SHA256]: c207be1fc720579fe993c3af6c88e92f7aae1de42875b3ced1d4001a89644bbe

Leandro Félix

ASSINADO - Sandra Regina Nunes Da Silva (sandra.nunes@pelotas.rs.gov.br)
Data/Hora: 30/06/2023 - 11:33:43, IP: 187.86.132.227, Geolocalização: [-31.769014, -52.342868]
[SHA256]: 21a82b4a5f9c8c3028f20be8a7c0139ce3a7c9e0c28b8dd9f4f0e9b36804bd0e

Sandra Nunes

Histórico de eventos registrados neste envelope

30/06/2023 11:34:25 - Envelope finalizado por sandra.nunes@pelotas.rs.gov.br, IP 187.86.132.227
30/06/2023 11:33:43 - Assinatura realizada por sandra.nunes@pelotas.rs.gov.br, IP 187.86.132.227
30/06/2023 11:33:28 - Envelope visualizado por sandra.nunes@pelotas.rs.gov.br, IP 187.86.132.227
30/06/2023 10:01:17 - Assinatura realizada por leandro.felix@pelotas.rs.gov.br, IP 187.86.132.227
30/06/2023 10:00:05 - Envelope visualizado por leandro.felix@pelotas.rs.gov.br, IP 187.86.132.227
30/06/2023 09:47:12 - Envelope registrado na Blockchain por cristina.farinha@pelotas.rs.gov.br, IP 177.194.204.231
30/06/2023 09:46:58 - Envelope encaminhado para assinaturas por cristina.farinha@pelotas.rs.gov.br, IP 177.194.204.231
30/06/2023 09:32:19 - Envelope criado por cristina.farinha@pelotas.rs.gov.br, IP 177.194.204.231