Contrato Administrativo de Prestação de Serviços nº. 02/2023.

No 03 dia do mês de julho do ano de dois mil e vinte e três, de um lado a **COMPANHIA DE INFORMÁTICA DE PELOTAS - COINPEL**, Empresa Pública Municipal de Direito Privado, CNPJ n.º 91.560.573/0001-25, com sede à av. Domingos de Almeida 1785, salas 27, 28 e 29, CEP nº. 96.085-470, bairro Areal, Pelotas/RS, neste ato representada pelo seus diretores Presidente, e, Técnico, respectivamente Sr. **Leandro da Silva Félix** (brasileiro, RG nº. 1089460032, CPF nº. 016.013.640-75), e Sr. **William da Cruz Sinotti** (brasileiro, RG nº. 9102153922, CPF nº. 017.659.320-92) doravante denominada simplesmente **CONTRATANTE**, e de outro lado, a empresa **KSCORP Trade and Services Ltda.**, 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. representada neste ato pelo seu sócio Sr. **Newton Alves de Souza** (brasileiro, CPF/MF n.º 387.073.060-91, RG n.º 6021200958), e-mail newton@kscorp.com.br; doravante denominada simplesmente **CONTRATADA**, lavrou-se este mediante as cláusulas e condições a seguir:

CLÁUSULA PRIMEIRA: Do Objeto

O objeto do presente Contrato é o fornecimento (direito de uso / venda), por parte da CONTRATADA, de 100 (cem) licenças para Solução de Antivírus Kaspersky Advanced, com atualizações, garantia e suporte técnico pelo período de 36 (trinta e seis) meses, nos termos dispostos nas demais cláusulas do presente Contrato.

I - Este contrato não implica, em hipótese alguma, em vínculo empregatício entre as partes.

II - Durante a vigência deste Contrato, toda a correspondência trocada entre as partes será no formato de ofício, com retorno de cópia constando "nome, assinatura e data" do recebimento pelo destinatário ou aplicativo de assinador/validador virtual, salvo disposição diferente ja especificada no corpo do presente Contrato;

III - Quanto aos prazos especificados neste Contrato, se considera apenas os dias úteis de expediente da **Contratante;** onde não houver menção explícita em contrário, será excluído sempre o dia do ato ou da sua comunicação, e incluir-se-á sempre o dia de vencimento do mesmo.

CLÁUSULA SEGUNDA: Condições Gerais

2.1. **Direito Patrimonial:**

Toda a infraestrutura e know-how necessários para a presente aquisição e fornecimento de garantia será inteiramente de propriedade e responsabilidade da Contratada.

2.2. **Propriedade Intelectual:**

A metodologia empregada neste fornecimento de bens e de serviços de garantia é de propriedade e responsabilidade da Contratada.

2.3. **Confidencialidade:**

Todos os termos e as informações trocadas entre a Contratante e a Contratada, durante a execução dos serviços objeto do presente Contrato, serão utilizados somente para alcançar os fins previstos. Desta forma, as

partes tratarão estas informações com o devido sigilo e não as farão de conhecimento de terceiros sem o prévio consentimento da empresa a qual elas pertencem.

2.4. **Aderência aos Padrões:**

A infraestrutura e os serviços de garantia a serem fornecidos pela Contratada deverão ser projetados de acordo com os padrões da Indústria de Tecnologia da Informação, para atender plenamente e serem ajustáveis às necessidades da Contratante.

CLÁUSULA TERCEIRA: Requisitos dos Serviços Contratados

3.1 **Características técnicas para Solução de Antivírus:**

3.1.1 Console de Gerenciamento

3.1.1.1. Compatibilidade de instalação com os seguintes sistemas operacionais:

3.1.1.1.1. Microsoft Windows 10 Enterprise 2015 LTSB 32-bit/64-bit
3.1.1.1.2. Microsoft Windows 10 Enterprise 2016 LTSB 32-bit/64-bit
3.1.1.1.3. Microsoft Windows 10 Pro RS5 32-bit/64-bit
3.1.1.1.4. Microsoft Windows 10 Pro for Workstations RS5 32-bit / 64-bit
3.1.1.1.5. Microsoft Windows 10 Enterprise RS5 32-bit/64-bit
3.1.1.1.6. Microsoft Windows 10 Education RS5 32-bit/64-bit
3.1.1.1.7. Microsoft Windows 8.1 Pro 32-bit/64-bit
3.1.1.1.8. Microsoft Windows 8.1 Enterprise 32-bit/64-bit
3.1.1.1.9. Microsoft Windows 8 Pro 32-bit/64-bit
3.1.1.1.10. Microsoft Windows 8 Enterprise 32-bit/64-bit
3.1.1.1.11. Microsoft Windows 7 Professional Service Pack 1 32-bit / 64-bit
3.1.1.1.12. Microsoft Windows 7 Enterprise / Ultimate Service Pack 1 32-bit / 64-bit
3.1.1.1.13. Microsoft Windows Small Business Server 2008 Standard / Premium 64-bit
3.1.1.1.14. Microsoft Windows Small Business Server 2011 Essentials 64-bit
3.1.1.1.15. Microsoft Windows Small Business Server 2011 Premium Add-on 64-bit
3.1.1.1.16. Microsoft Windows Small Business Server 2011 Standard 64-bit
3.1.1.1.17. Microsoft Windows Server 2008 Datacenter Service Pack 1 32-bit / 64-bit
3.1.1.1.18. Microsoft Windows Server 2008 Enterprise Service Pack 1 32-bit / 64-bit
3.1.1.1.19. Microsoft Windows Server 2008 Foundation Service Pack 2 32-bit / 64-bit
3.1.1.1.20. Microsoft Windows Server 2008 Service Pack 1 Server Core 32-bit / 64-bit
3.1.1.1.21. Microsoft Windows Server 2008 Standard Service Pack 1 32-bit / 64-bit
3.1.1.1.22. Microsoft Windows Server 2008 Standard / Enterprise / Datacenter 32-bit / 64-bit
3.1.1.1.23. Microsoft Windows Server 2008 R2 Server Core 64-bit
3.1.1.1.24. Microsoft Windows Server 2008 R2 Datacenter 64-bit
3.1.1.1.25. Microsoft Windows Server 2008 R2 Datacenter Service Pack 1 32-bit / 64-bit
3.1.1.1.26. Microsoft Windows Server 2008 R2 Enterprise 64-bit
3.1.1.1.27. Microsoft Windows Server 2008 R2 Enterprise Service Pack 1 64-bit
3.1.1.1.28. Microsoft Windows Server 2008 R2 Foundation 64-bit
3.1.1.1.29. Microsoft Windows Server 2008 R2 Foundation Service Pack 1 64-bit
3.1.1.1.30. Microsoft Windows Server 2008 R2 Core Mode Service Pack 64-bit
3.1.1.1.31. Microsoft Windows Server 2008 R2 Standard 64-bit

3.1.1.1.32. Microsoft Windows Server 2008 R2 Standard Service Pack 1 64-bit
3.1.1.1.33. Microsoft Windows Server 2012 Server Core 64-bit
3.1.1.1.34. Microsoft Windows Server 2012 Datacenter 64-bit
3.1.1.1.35. Microsoft Windows Server 2012 Essentials 64-bit
3.1.1.1.36. Microsoft Windows Server 2012 Foundation 64-bit
3.1.1.1.37. Microsoft Windows Server 2012 Standard 64-bit
3.1.1.1.38. Microsoft Windows Server 2012 R2 Server Core 64-bit
3.1.1.1.39. Microsoft Windows Server 2012 R2 Datacenter 64-bit
3.1.1.1.40. Microsoft Windows Server 2012 R2 Essentials 64-bit
3.1.1.1.41. Microsoft Windows Server 2012 R2 Foundation 64-bit
3.1.1.1.42. Microsoft Windows Server 2012 R2 Standard 64-bit
3.1.1.1.43. Microsoft Windows Server 2016 Datacenter (LTSB) 64-bit
3.1.1.1.44. Microsoft Windows Server 2016 Standard (LTSB) 64-bit
3.1.1.1.45. Microsoft Windows Server 2019 64-bit
3.1.1.1.46. Microsoft Windows Storage Server 2008 R2 64-bit
3.1.1.1.47. Microsoft Windows Storage Server 2016 64-bit
3.1.1.1.48. Microsoft Windows Storage Server 2012 64-bit
3.1.1.1.49. Microsoft Windows Storage Server 2012 R2 64-bit

3.1.1.2.Suportar as seguintes plataformas virtuais:

3.1.1.2.1. VMware vSphere 6
3.1.1.2.2. VMware vSphere 6.5
3.1.1.2.3. VMware Workstation 14 Pro
3.1.1.2.4. Microsoft Hyper-V Server 2008 64-bit
3.1.1.2.5. Microsoft Hyper-V Server 2008 R2 64-bit
3.1.1.2.6. Microsoft SQL Server 2008 R2 Service Pack 1 64-bit
3.1.1.2.7. Microsoft Hyper-V Server 2012 64-bit
3.1.1.2.8. Microsoft Hyper-V Server 2012 R2 64-bit
3.1.1.2.9. Microsoft Hyper-V Server 2016 64-bit
3.1.1.2.10. Citrix XenServer 7
3.1.1.2.11. Citrix XenServer 7.1 LTSR
3.1.1.2.12. Parallels Desktop 11
3.1.1.2.13. Oracle VM VirtualBox 5.x

3.1.1.3.Possuir compatibilidade com os seguintes bancos de dados:

3.1.1.3.1. Microsoft SQL Server 2008 Express 32-bit
3.1.1.3.2. Microsoft SQL Server 2008 R2 Express 64-bit
3.1.1.3.3. Microsoft SQL Server 2012 Express 64-bit
3.1.1.3.4. Microsoft SQL Server 2014 Express 64-bit
3.1.1.3.5. Microsoft SQL Server 2016 Express 64-bit
3.1.1.3.6. Microsoft SQL Server 2017 Express 64-bit
3.1.1.3.7. Microsoft SQL Server 2008 (todas as versões) 32-bit/64-bit
3.1.1.3.8. Microsoft SQL Server 2008 R2 (todas as versões) 64-bit
3.1.1.3.9. Microsoft SQL Server 2008 R2 Service Pack 2 (todas as versões) 64-bit
3.1.1.3.10. Microsoft SQL Server 2012 (todas as versões) 64-bit
3.1.1.3.11. Microsoft SQL Server 2014 (todas as versões) 64-bit
3.1.1.3.12. Microsoft SQL Server 2016 (todas as versões) 64-bit

3.1.1.3.13. Microsoft SQL Server 2017 on Windows 64-bit
3.1.1.3.14. MySQL Standard Edition 5.6 32-bit/64-bit
3.1.1.3.15. MySQL Enterprise Edition 5.6 32-bit/64-bit
3.1.1.3.16. MySQL Standard Edition 5.7 32-bit/64-bit
3.1.1.3.17. MySQL Enterprise Edition 5.7 32-bit/64-bit

3.1.1.4.Características da console de gerenciamento da solução:

3.1.1.4.1. A console deve ser acessada via WEB (HTTPS) ou MMC;
3.1.1.4.2. Estar presente no Programa de proteção ativa da Microsoft (MAPP);
3.1.1.4.3. Console deve ser baseada no modelo cliente/servidor;
3.1.1.4.4. Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade;
3.1.1.4.5. Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus;
3.1.1.4.6. Deve permitir incluir usuários do Active Direcoty para acessarem a console de administração;
3.1.1.4.7. 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;
3.1.1.4.8. 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;
3.1.1.4.9. Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores;
3.1.1.4.10. 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;
3.1.1.4.11. Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;
3.1.1.4.12. Deve armazenar histórico das alterações feitas em políticas;
3.1.1.4.13. 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;
3.1.1.4.14. Deve ter a capacidade de comparar a política atual com a anterior, informando quais configurações foram alteradas;
3.1.1.4.15. A solução de gerência deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas;
3.1.1.4.16. Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador;
3.1.1.4.17. Capacidade de instalar remotamente a solução de segurança em smartphones e tablets de sistema iOS e Android;
3.1.1.4.18. Capacidade de instalar remotamente aplicativos em smartphones e tablets de sistema Android;
3.1.1.4.19. A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle;
3.1.1.4.20. 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;
3.1.1.4.21. Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução antivírus;
3.1.1.4.22. Capacidade de gerenciar smartphones e tablets (dos sistemas operacionais Android e iOS) protegidos pela solução de segurança;
3.1.1.4.23. Capacidade de instalar atualizações em computadores de testes antes de instalar nos demais computadores da rede;

3.1.1.4.24. Capacidade de gerar pacotes customizados (auto executáveis) contendo a licença e configurações do produto;
3.1.1.4.25. Capacidade de atualizar os pacotes de instalação com as últimas vacinas;
3.1.1.4.26. 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;
3.1.1.4.27. A comunicação entre o cliente e o servidor de administração deve ser criptografada;
3.1.1.4.28. Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes;
3.1.1.4.29. Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado utilizando os seguintes parâmetros:
3.1.1.4.29.1. Nome do computador;
3.1.1.4.29.2. Nome do domínio;
3.1.1.4.29.3. Domínio do DNS
3.1.1.4.29.4. Range de IP;
3.1.1.4.29.5. Unidade organizacional do Active Directory;
3.1.1.4.29.6. Grupo de Active Directory;
3.1.1.4.29.7. Sistema Operacional;
3.1.1.4.29.8. Máquina virtual;
3.1.1.4.29.9. Segmento de nuvem.
3.1.1.4.30. Capacidade de executar a regra de realocação das seguintes formas:
3.1.1.4.30.1. Executar apenas uma vez para cada dispositivo;
3.1.1.4.30.2. Executar apenas uma vez para cada dispositivo, a cada instalação do Agente de Rede da solução endpoint;
3.1.1.4.30.3. Regra funcionar permanentemente;
3.1.1.4.31. Deve encontrar computadores na rede através de no mínimo três formas: Domínio, Active Directory e subredes;
3.1.1.4.32. Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas;
3.1.1.4.33. Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas à proteção;
3.1.1.4.34. 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;
3.1.1.4.35. 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;
3.1.1.4.36. 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;
3.1.1.4.37. Listar em um único local, todos os computadores não gerenciados na rede;
3.1.1.4.38. 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;
3.1.1.4.39. Deve fornecer as seguintes informações dos computadores:
3.1.1.4.39.1. Se o antivírus está instalado;
3.1.1.4.39.2. Se o antivírus está iniciado;
3.1.1.4.39.3. Se o antivírus está atualizado;
3.1.1.4.39.4. Minutos/horas desde a última conexão da máquina com a console;
3.1.1.4.39.5. Minutos/horas desde a última atualização de vacinas;
3.1.1.4.39.6. Data e horário da última verificação executada na máquina;
3.1.1.4.39.7. Versão do antivírus instalado na máquina;

3.1.1.4.39.8. Se é necessário reiniciar o computador para aplicar mudanças;
3.1.1.4.39.9. Data e horário de quando a máquina foi ligada;
3.1.1.4.39.10. Quantidade de vírus encontrados (contador) na máquina;
3.1.1.4.39.11. Nome do computador;
3.1.1.4.39.12. Domínio ou grupo de trabalho do computador;
3.1.1.4.39.13. Data e horário da última atualização de vacinas;
3.1.1.4.39.14. Sistema operacional com Service Pack;
3.1.1.4.39.15. Quantidade de processadores;
3.1.1.4.39.16. Quantidade de memória RAM;
3.1.1.4.39.17. Usuário(s) logado(s) naquele momento;
3.1.1.4.39.18. Endereço IP;
3.1.1.4.39.19. Vulnerabilidades de aplicativos instalados na máquina;
3.1.1.4.39.20. Atualizações do Windows Updates instaladas;
3.1.1.4.39.21. Aplicativos instalados, inclusive aplicativos de terceiros, contendo:
3.1.1.4.39.21.1. Histórico de instalação;
3.1.1.4.39.21.2.Data e hora que o software foi instalado;
3.1.1.4.39.21.3.Data e hora que o software foi removido;
3.11.4.39.22. Informação completa de hardware contendo:
3.1.1.4.39.22.1.Processadores;
3.1.1.4.39.22.2.Memória;
3.1.1.4.39.22.3.Adaptadores de vídeo;
3.1.1.4.39.22.4.Discos de armazenamento;
3.1.1.4.39.22.5.Adaptadores de áudio;
3.1.1.4.39.22.6.Adaptadores de rede;
3.1.1.4.39.22.7.Monitores;
3.1.1.4.39.22.8.Drives de CD/DVD;
3.1.1.4.40. Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:
3.1.1.4.40.1. Alteração de Gateway Padrão;
3.1.1.4.40.2. Alteração de Subrede;
3.1.1.4.40.3. Alteração de domínio;
3.1.1.4.40.4. Alteração de servidor DHCP;
3.1.1.4.40.5. Alteração de servidor DNS;
3.1.1.4.40.6. Alteração de servidor WINS;
3.1.1.4.40.7. Alteração de Subrede;
3.1.1.4.40.8. Resolução de Nome;
3.1.1.4.40.9. Disponibilidade de endereço de conexão SSL;
3.1.1.4.41. Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;
3.1.1.4.42. Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;
3.1.1.4.43. 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;
3.1.1.4.44. 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;
3.1.1.4.45. Capacidade de realizar atualização incremental de vacinas nos computadores clientes;

3.1.1.4.46. Capacidade de baixar novas versões do antivírus direto pela console de gerenciamento, sem a necessidade de importá-los manualmente;
3.1.1.4.47. Deve possuir compatibilidade com Microsoft NAP, quando instalado em um Windows 2008 Server;
3.1.1.4.48. 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;
3.1.1.4.49. Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;
3.1.1.4.50. Capacidade de reportar vulnerabilidades de softwares presentes nos computadores;
3.1.1.4.51. Capacidade de listar updates nas máquinas com o respectivo link para download;
3.1.1.4.52. 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;
3.1.1.4.53. Deve ter uma quarentena na própria console de gerenciamento, permitindo baixar um artefato ou enviar direto para análise do fabricante;
3.1.1.4.54. Deve armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo:
3.1.1.4.54.1. Nome do vírus;
3.1.1.4.54.2. Nome do arquivo infectado;
3.1.1.4.54.3. Data e hora da detecção;
3.1.1.4.54.4. Nome da máquina ou endereço IP;
3.1.1.4.54.5. Ação realizada.
3.1.1.4.55. Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;
3.1.1.4.56. Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;
3.1.1.4.57. Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);
3.1.1.4.58. 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
3.1.1.4.59. 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;
3.1.1.4.60. 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;
3.1.1.4.61. Deve criar um backup de todos arquivos deletados em computadores para que possa ser restaurado através de comando na Console de administração;
3.1.1.4.62. Capacidade de realizar inventário de hardware de todas as máquinas clientes;
3.1.1.4.63. Capacidade de realizar inventário de aplicativos de todas as máquinas clientes;
3.1.1.4.64. Capacidade de diferenciar máquinas virtuais de máquinas físicas;
3.1.1.4.65. 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;
3.1.1.4.66. Capacidade de enviar e-mails para contas específicas em caso de algum evento;
3.1.1.4.67. Capacidade de gerar traps SNMP para monitoramento de eventos;
3.1.1.4.68. Capacidade de exportar relatórios para pelo menos nos seguintes tipos de arquivos: PDF, HTML e XML;
3.1.1.4.69. Possuir, no mínimo, 30 (trinta) relatórios pré-configurados na console de gerenciamento da solução;
3.1.1.4.70. Capacidade de customizar relatórios de acordo com preferência do cliente nos seguintes campos:
3.1.1.4.70.1. Cabeçalho do relatório;
3.1.1.4.70.2. Logotipo do cliente;
3.1.1.4.71. Capacidade de gerar tarefa com agendamento de envio de relatório por E-mail;

3.1.1.4.72. Capacidade de gerar tarefa de agendamento de envio de relatório para Pasta Compartilhada na rede;
3.1.1.4.73. Possuir informações estatísticas na console de gerenciamento com, no mínimo, as seguintes informações:
3.1.1.4.73.1. Status da proteção;
3.1.1.4.73.2. Informações de implementação;
3.1.1.4.73.3. Atualizações;
3.1.1.4.73.4. Ameaças;
3.1.1.4.73.5. Informação Geral;
3.1.1.4.73.6. Atualizações das Aplicações;
3.1.1.4.74. Possibilitar customização de visualização das estatísticas diretamente na console;

3.1.2. Proteção para estações de trabalho Windows

3.1.2.1. Compatibilidade de instalação nos seguintes sistemas operacionais:

3.1.2.1.1. Microsoft Windows 10 Home / Pro / Education / Enterprise x86 / x64
3.1.2.1.2. Microsoft Windows 8.1 Pro / Enterprise x86 / x64
3.1.2.1.3. Microsoft Windows 8 Pro / Enterprise x86 / x64
3.1.2.1.4. Microsoft Windows 7 Home / Professional / Enterprise x86 / x64 SP1 e superior
3.1.2.1.5. Microsoft Windows Server 2019 Essentials / Standard / Datacenter
3.1.2.1.6. Microsoft Windows Server 2016 Essentials / Standard / Datacenter
3.1.2.1.7. Microsoft Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter
3.1.2.1.8. Microsoft Windows Server 2012 Foundation / Essentials / Standard / Datacenter
3.1.2.1.9. Microsoft Small Business Server 2011 Essentials / Standard x64
3.1.2.1.10. Microsoft Windows Server 2008 R2 Foundation / Standard / Enterprise SP1
3.1.2.1.11. Microsoft Windows Server 2008 Standard / Enterprise / Datacenter SP2
3.1.2.1.12. Microsoft Small Business Server 2008 Standard / Premium x64

3.1.2.2.Suportar as seguintes plataformas virtuais:

3.1.2.2.1. VMware Workstation 14;
3.1.2.2.2. VMware ESXi 6.5 U1;
3.1.2.2.3. Microsoft Hyper-V 2016 Server;
3.1.2.2.4. Microsoft Hyper-V 2019 Server;
3.1.2.2.5. Citrix XenServer 7.2;
3.1.2.2.6. Citrix XenDesktop 7.17;
3.1.2.2.7. Citrix XenApp 7.17;
3.1.2.2.8. Citrix Provisioning Services 7.17;

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

3.1.2.3.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware) que verifique qualquer arquivo criado, acessado ou modificado;
3.1.2.3.2. Antivírus de Web (módulo para verificação de sites e downloads contra vírus);
3.1.2.3.3. Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos);
3.1.2.3.4. Proteção contra Ameaças de Rede (módulo de verificação de atividades suspeitas na rede);
3.1.2.3.5. Firewall com IDS (sistema de detecção de intrusos);
3.1.2.3.6. Proteção contra ameaças utilizando de exploração BadUSB;
3.1.2.3.7. Integração com o Antimalware Scan Interface da Microsoft (AMSI), para os seguintes sistemas

operacionais:
3.1.2.3.7.1. Microsoft Windows 10 Pro x64/x86;
3.1.2.3.7.2. Microsoft Windows 10 Enterprise x64/x86;
3.1.2.3.7.3. Microsoft Windows Server 2016;
3.1.2.3.8. Possuir Controle de dispositivos externos;
3.1.2.3.9. Possuir Controle de acesso a sites por categoria;
3.1.2.3.10. Possuir, no mínimo, 15 (quinze) categorias de sites pré-configuradas
3.1.2.3.11. Capacidade de customização de acesso a sites com, no mínimo, as seguintes maneiras:
3.1.2.3.11.1. Controle de acesso a sites por horário;
3.1.2.3.11.2. Controle de acesso a sites por usuários;
3.1.2.3.11.3. Controle de acesso a websites por dados, como por exemplo: Bloquear websites com conteúdos de vídeo e áudio;
3.1.2.3.12. Possuir controle de execução de aplicativos;
3.1.2.3.13. Controle de vulnerabilidades do Windows e dos aplicativos instalados;
3.1.2.3.14. Possuir Autodefesa contra ataques aos serviços e processos do antivírus no endpoint;
3.1.2.3.15. Capacidade de escolher quais módulos serão instalados tanto na instalação local quanto na instalação remota;
3.1.2.3.16. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
3.1.2.3.17. 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;
3.1.2.3.18. O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza;
3.1.2.3.19. 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;
3.1.2.3.20. 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;
3.1.2.3.21. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
3.1.2.3.22. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
3.1.2.3.23. Capacidade de verificar somente arquivos novos e alterados;
3.1.2.3.24. Capacidade de verificar objetos usando heurística;
3.1.2.3.25. Capacidade de agendar uma pausa na verificação;
3.1.2.3.26. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;
3.1.2.3.27. 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);
3.1.2.3.28. Ter a capacidade de fazer detecções por comportamento, identificando ameaças avançadas sem a necessidade de assinaturas;
3.1.2.3.29. Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias;
3.1.2.3.30. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
3.1.2.3.30.1. Perguntar o que fazer;
3.1.2.3.30.2. Bloquear acesso ao objeto;
3.1.2.3.30.3. Deletar o objeto;

3.1.2.3.30.4. Realizar a limpeza do objeto;
3.1.2.3.31. Em caso positivo de limpeza deve restaurar o objeto para uso;
3.1.2.3.32. Em caso negativo de limpeza deve mover para quarentena ou apagar;
3.1.2.3.33. Anteriormente a qualquer tentativa de limpeza ou exclusão permanente, o antivírus deve realizar um backup do objeto;
3.1.2.3.34. 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);
3.1.2.3.35. Possuir extensão para Microsoft Outlook, com a possibilidade de escaneamento de 3 (três) maneiras distintas:
3.1.2.3.35.1. Realizar varredura ao receber a mensagem;
3.1.2.3.35.2. Realizar varredura quando lê a mensagem;
3.1.2.3.35.3. Realizar varredura quando envia a mensagem;
3.1.2.3.36. Capacidade de realizar filtro em anexos de e-mail;
3.1.2.3.37. Ter capacidade de renomear anexo de e-mail, de acordo com a extensão escolhida, por exemplo: .exe, .bat, .cmd, entre outras.
3.1.2.3.38. Ter capacidade de remover anexo de e-mail, de acordo com a extensão escolhida, por exemplo: .exe, .bat, .cmd, entre outras.
3.1.2.3.39. Capacidade de verificação de corpo e anexos de e-mails usando heurística
3.1.2.3.40. O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve:
3.1.2.3.40.1. Perguntar o que fazer;
3.1.2.3.40.2. Bloquear o e-mail;
3.1.2.3.40.3. Deletar o objeto;
3.1.2.3.40.4. Realizar a limpeza do objeto;
3.1.2.3.40.5. Em caso positivo de limpeza deve restaurar o e-mail para o usuário;
3.1.2.3.40.6. Em caso negativo de limpeza deve mover para quarentena ou apagar;
3.1.2.3.41. Capacidade de verificar links inseridos em e-mails contra phishings;
3.1.2.3.42. Capacidade de verificar tráfego nos browsers: Internet Explorer, Firefox, Google Chrome e Opera;
3.1.2.3.43. Caso o e-mail conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena;
3.1.2.3.44. Capacidade de verificação de tráfego HTTP e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc), usando heurística;
3.1.2.3.45. Na verificação de tráfego web, caso encontrado código malicioso o programa deve:
3.1.2.3.45.1. Perguntar o que fazer;
3.1.2.3.45.2. Bloquear o acesso e informar sobre a ação com uma mensagem;
3.1.2.3.45.3. Permitir o acesso ao objeto;
3.1.2.3.46. Capacidade de alterar as portas monitoradas pelos módulos de Web e E-mail
3.1.2.3.47. Deve ter suporte total ao protocolo IPV6;
3.1.2.3.48. O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:
3.1.2.3.48.1. Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em tempo real;
3.1.2.3.48.2. Verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação;
3.1.2.3.49. Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web;
3.1.2.3.50. 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;
3.1.2.3.51. Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa;

3.1.2.3.52. 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;
3.1.2.3.53. Deve possuir módulo de bloqueio de Phishing, com atualizações incluídas nas vacinas, obtidas pelo Anti-Phishing Working Group (http://www.antiphishing.org/)
3.1.2.3.54. Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica;
3.1.2.3.55. 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;
3.1.2.3.56. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
3.1.2.3.56.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
3.1.2.3.56.2. 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;
3.1.2.3.57. Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:
3.1.2.3.57.1. Discos de armazenamento locais;
3.1.2.3.57.2. Armazenamento removível;
3.1.2.3.57.3. Impressoras;
3.1.2.3.57.4. CD/DVD;
3.1.2.3.57.5. Drives de disquete;
3.1.2.3.57.6. Modems;
3.1.2.3.57.7. Dispositivos de fita;
3.1.2.3.57.8. Dispositivos multifuncionais;
3.1.2.3.57.9. Leitores de smart card;
3.1.2.3.57.10. Dispositivos de sincronização via ActiveSync
3.1.2.3.57.11. Wi-Fi;
3.1.2.3.57.12. Adaptadores de rede externos;
3.1.2.3.57.13. Dispositivos portáteis (MTP);
3.1.2.3.57.14. Dispositivos Bluetooth;
3.1.2.3.57.15. Câmeras e Scanners;
3.1.2.3.58. Deve possuir módulo que habilite ou não o funcionamento das seguintes conexões, no mínimo:
3.1.2.3.58.1. Infravermelho;
3.1.2.3.58.2. Porta Serial;
3.1.2.3.58.3. Porta Paralela;
3.1.2.3.58.4. USB;
3.1.2.3.58.5. FireWire;
3.1.2.3.58.6. PCMCIA;
3.1.2.3.59. 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;
3.1.2.3.60. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário, este podendo ser vinculado há um usuário do Active Directory;
3.1.2.3.61. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento;
3.1.2.3.62. Capacidade de habilitar “logging” em dispositivos removíveis tais como Pendrive, Discos externos, entre outros;
3.1.2.3.63. Capacidade de configurar novos dispositivos por Class ID/Hardware ID;

3.1.2.3.64. 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;
3.1.2.3.65. Capacidade de bloquear execução de aplicativo que está em armazenamento externo;
3.1.2.3.66. 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;
3.1.2.3.67. 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;
3.1.2.3.68. 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;

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

3.1.3.1.1. macOS Mojave 10.14
3.1.3.1.2. macOS High Sierra 10.13
3.1.3.1.3. macOS Sierra 10.12

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

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

3.1.3.2.5. Capacidade de criar exclusões para computadores que não devem ser monitorados pelo módulo de bloqueio à ataques na rede;
3.1.3.2.6. Possibilidade de importar uma chave no pacote de instalação;
3.1.3.2.7. Deve possuir suportes a notificações utilizando o Growl;
3.1.3.2.8. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
3.1.3.2.9. 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;
3.1.3.2.10. Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas;
3.1.3.2.11. 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;
3.1.3.2.12. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
3.1.3.2.13. 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;
3.1.3.2.14. Capacidade de verificar somente arquivos novos e alterados;
3.1.3.2.15. Capacidade de verificar objetos usando heurística;

3.1.3.2.16. Capacidade de agendar uma pausa na verificação;
3.1.3.2.17. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
3.1.3.2.17.1. Perguntar o que fazer;
3.1.3.2.17.2. Bloquear o objeto;
3.1.3.2.17.3. Deletar o objeto;
3.1.3.2.17.4. Realizar a limpeza do objeto;
3.1.3.2.17.5. Em caso positivo de limpeza deve restaurar o objeto;
3.1.3.2.17.6. Em caso negativo de limpeza deve mover para quarentena ou apagar;
3.1.3.2.18. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
3.1.3.2.19. Capacidade de verificar arquivos de formato de e-mail;
3.1.3.2.20. 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;
3.1.3.2.21. 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);
3.1.3.2.22. Capacidade de voltar para a base de dados de vacina anterior;
3.1.3.2.23. 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:

3.1.4.1.1. Ubuntu 16.04 LTS e superior;
3.1.4.1.2. Red Hat® Enterprise Linux® 6.7 e superior;
3.1.4.1.3. CentOS-6.7 e superior;
3.1.4.1.4. Debian GNU / Linux 8.6 e superior;
3.1.4.1.5. Debian GNU / Linux 9.4 e superior;
3.1.4.1.6. Linux Mint 18.2 e superior;
3.1.4.1.7. Linux Mint 19 e superior;
3.1.4.1.8. Alt Linux SPT 8.0.0 Work Station;
3.1.4.1.9. Alt Linux SPT 8.0.0 Server;
3.1.4.1.10. Alt Linux 8.2 Work Station;
3.1.4.1.11. Alt Linux 8.2 Work Station;
3.1.4.1.12. Alt Linux 8.2 Server;
3.1.4.1.13. Alt Linux 8.2 Education;
3.1.4.1.14. GosLinux 6.6;
3.1.4.1.15. Lotos;
3.1.4.1.16. Mageia 4;

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

3.1.4.2.1. Ubuntu 16.04 LTS e superior
3.1.4.2.2. Ubuntu 18.04 LTS
3.1.4.2.3. Red Hat Enterprise Linux 6.7 e superior
3.1.4.2.4. Red Hat Enterprise Linux 7.2 e superior
3.1.4.2.5. CentOS-6.7 e superior
3.1.4.2.6. CentOS-7.2 e superior
3.1.4.2.7. Debian GNU / Linux 8.6 e superior
3.1.4.2.8. Debian GNU / Linux 9.4 e superior
3.1.4.2.9. OracleLinux 7.3 e superior
3.1.4.2.10. SUSE® Linux Enterprise Server 15

3.1.4.2.11. openSUSE® 15
3.1.4.2.12. Alt Linux SPT 8.0.0 Work Station
3.1.4.2.13. Alt Linux SPT 8.0.0 Server
3.1.4.2.14. Alt Linux 8.2 Work Station
3.1.4.2.15. Alt Linux 8.2 Work Station K
3.1.4.2.16. Alt Linux 8.2 Server
3.1.4.2.17. Alt Linux 8.2 Education
3.1.4.2.18. Amazon Linux AMI
3.1.4.2.19. Linux Mint 18.2 e superior
3.1.4.2.20. Linux Mint 19 e superior
3.1.4.2.21. Micro Focus Open Enterprise Server 2018
3.1.4.2.22. Astra Linux Special Edition 1.5
3.1.4.2.23. Astra Linux Special Edition 1.6
3.1.4.2.24. Astra Linux Common Edition Orel 2.12
3.1.4.2.25. GosLinux 6.6
3.1.4.2.26. Lotos
3.1.4.2.27. RED OS 7.1
3.1.4.2.28. RED OS 7.2 4.3.Características da solução de proteção para estação de trabalho Linux

3.1.4.3.1. Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware) que verifique qualquer arquivo criado, acessado ou modificado;
3.1.4.3.2. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
3.1.4.3.3. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
3.1.4.3.3.1. Capacidade de criar exclusões por local, máscara e nome da ameaça;
3.1.4.3.3.2. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
3.1.4.3.3.3. 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;
3.1.4.3.4. Dectectar aplicações que possam ser utilizadas como vetor de ataque por hackers;
3.1.4.3.5. Fazer detecções através de heurística utilizando no mínimo as seguintes opções de nível:
3.1.4.3.5.1. Alta;
3.1.4.3.5.2. Média;
3.1.4.3.5.3. Baixa;
3.1.4.3.5.4. Recomendado;
3.1.4.3.6. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;
3.1.4.3.7. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados;
3.1.4.3.8. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;
3.1.4.3.9. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
3.1.4.3.10. 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;
3.1.4.3.11. Capacidade de verificar objetos usando heurística;
3.1.4.3.12. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;

3.1.4.3.13. Deve possuir módulo escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados
3.1.4.3.14. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux);

3.1.5. Proteção para servidores Windows

3.1.5.1.Compatibilidade de instalação nos seguintes sistemas operacionais 32-bits:
3.1.5.1.1. Windows Server 2003 Standard / Enterprise / Datacenter SP2 e superior;
3.1.5.1.2. Windows Server 2003 R2 Standard / Enterprise / Datacenter SP2 e superior;
3.1.5.1.3. Windows Server 2008 Standard / Enterprise / Datacenter SP1 e superior;
3.1.5.1.4. Windows Server 2008 Core Standard / Enterprise / Datacenter SP1 e superior;

3.1.5.2.Compatibilidade de instalação nos seguintes sistemas operacionais 64-bits:
3.1.5.2.1. Windows Server 2003 Standard / Enterprise / Datacenter SP2 e superior
3.1.5.2.2. Windows Server 2003 R2 Standard / Enterprise / Datacenter SP2 e superior
3.1.5.2.3. Windows Server 2008 Standard / Enterprise / Datacenter SP1 e superior
3.1.5.2.4. Windows Server 2008 Core Standard / Enterprise / Datacenter SP1 e superior
3.1.5.2.5. Microsoft Small Business Server 2008 Standard / Premium
3.1.5.2.6. Windows Server 2008 R2 Foundation / Standard / Enterprise SP1 e superior
3.1.5.2.7. Windows Server 2008 R2 Core Standard / Enterprise / Datacenter SP1 e superior
3.1.5.2.8. Windows Hyper-V Server 2008 R2 SP1 e superior
3.1.5.2.9. Microsoft Small Business Server 2011 Essentials / Standard
3.1.5.2.10. Microsoft Windows MultiPoint Server 2011
3.1.5.2.11. Windows Server 2012 Foundation / Essentials / Standard / Datacenter
3.1.5.2.12. Windows Server 2012 Core Standard / Datacenter
3.1.5.2.13. Windows Storage Server 2012
3.1.5.2.14. Windows Hyper-V Server 2012
3.1.5.2.15. Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter
3.1.5.2.16. Windows Server 2012 R2 Core Standard / Datacenter
3.1.5.2.17. Windows Storage Server 2012 R2
3.1.5.2.18. Windows Hyper-V Server 2012 R2
3.1.5.2.19. Windows Server 2016 Essentials / Standard / Datacenter
3.1.5.2.20. Windows Server 2016 Core Standard / Datacenter
3.1.5.2.21. Windows Storage Server 2016
3.1.5.2.22. Windows Hyper-V Server 2016
3.1.5.2.23. Windows Server 2019 all editions (including Core / Terminal / Hyper-V)

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

3.1.5.3.1. Windows 2008 Server Microsoft Remote Desktop Services;
3.1.5.3.2. Windows 2008 Server R2 Microsoft Remote Desktop Services;
3.1.5.3.3. Windows 2012 Server Microsoft Remote Desktop Services;
3.1.5.3.4. Windows 2012 Server R2 Microsoft Remote Desktop Services;
3.1.5.3.5. Windows 2016 Server Microsoft Remote Desktop Services;
3.1.5.3.6. Windows 2019 Server Microsoft Remote Desktop Services;
3.1.5.3.7. Citrix XenApp 6.0, 6.5, 7.0, 7.5 - 7.9, 7.15;
3.1.5.3.8. Citrix XenDesktop 7.0, 7.1, 7.5 - 7.9, 7.15;

3.1.5.4.Características da solução de proteção para servidores Windows
3.1.5.4.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware) que verifique qualquer arquivo criado, acessado ou modificado;
3.1.5.4.2. Possuir Auto defesa contra-ataques aos serviços e processos do antivírus no endpoint;
3.1.5.4.3. Firewall com IDS;
3.1.5.4.4. Controle de vulnerabilidades do Windows e dos aplicativos instalados;
3.1.5.4.5. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
3.1.5.4.6. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
3.1.5.4.7. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
3.1.5.4.7.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
3.1.5.4.7.2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação);
3.1.5.4.7.3. Leitura de configurações;
3.1.5.4.7.4. Modificação de configurações;
3.1.5.4.7.5. Gerenciamento de Backup e Quarentena;
3.1.5.4.7.6. Visualização de relatórios;
3.1.5.4.7.7. Gerenciamento de relatórios;
3.1.5.4.7.8. Gerenciamento de chaves de licença;
3.1.5.4.7.9. Gerenciamento de permissões (adicionar/excluir permissões acima);
3.1.5.4.8. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
3.1.5.4.8.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
3.1.5.4.8.2. 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;
3.1.5.4.8.3. Possibilidade de criar horários em que o firewall entrará em funcionamento.
3.1.5.4.9. Módulo de proteção de ransomware, especifico para a linha de servidores.
3.1.5.4.10. 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;
3.1.5.4.11. Bloquear malwares tais como Cryptlockers mesmo quando o ataque vier de um computador sem antivírus na rede;
3.1.5.4.12. Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros);
3.1.5.4.13. Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja em rodando com fonte ininterrupta de energia (uninterruptible Power supply – UPS);
3.1.5.4.14. Em caso de erros, deve ter capacidade de criar logs e traces automaticamente, sem necessidade de outros softwares;
3.1.5.4.15. Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor;
3.1.5.4.16. Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor;
3.1.5.4.17. Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas;
3.1.5.4.18. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
3.1.5.4.19. 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;
3.1.5.4.20. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
3.1.5.4.21. 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;
3.1.5.4.22. Capacidade de verificar somente arquivos novos e alterados;
3.1.5.4.23. Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários);
3.1.5.4.24. Capacidade de verificar objetos usando heurística;
3.1.5.4.25. Capacidade de configurar diferentes ações para diferentes tipos de ameaças;
3.1.5.4.26. Capacidade de agendar uma pausa na verificação;
3.1.5.4.27. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;
3.1.5.4.28. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
3.1.5.4.28.1. Perguntar o que fazer;
3.1.5.4.28.2. Bloquear o objeto;
3.1.5.4.28.3. Deletar o objeto;
3.1.5.4.28.4. Realizar a limpeza do objeto;
3.1.5.4.28.5. Em caso positivo de limpeza deve restaurar o objeto;
3.1.5.4.28.6. Em caso negativo de limpeza deve mover para quarentena ou apagar;
3.1.5.4.29. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
3.1.5.4.30. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
3.1.5.4.31. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
3.1.5.4.32. Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa;

3.1.6. Proteção para servidores Linux

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

3.1.6.1.1. Ubuntu 16.04 LTS e superior;
3.1.6.1.2. Red Hat® Enterprise Linux® 6.7 e superior;
3.1.6.1.3. CentOS-6.7 e superior;
3.1.6.1.4. Debian GNU / Linux 8.6 e superior;
3.1.6.1.5. Debian GNU / Linux 9.4 e superior;
3.1.6.1.6. Linux Mint 18.2 e superior;
3.1.6.1.7. Linux Mint 19 e superior;
3.1.6.1.8. Alt Linux SPT 8.0.0 Work Station;
3.1.6.1.9. Alt Linux SPT 8.0.0 Server;
3.1.6.1.10. Alt Linux 8.2 Work Station;
3.1.6.1.11. Alt Linux 8.2 Work Station;
3.1.6.1.12. Alt Linux 8.2 Server;
3.1.6.1.13. Alt Linux 8.2 Education;
3.1.6.1.14. GosLinux 6.6;
3.1.6.1.15. Lotos
3.1.6.1.16. Mageia 4;

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

3.1.6.2.1. Ubuntu 16.04 LTS e superior
3.1.6.2.2. Ubuntu 18.04 LTS
3.1.6.2.3. Red Hat Enterprise Linux 6.7 e superior
3.1.6.2.4. Red Hat Enterprise Linux 7.2 e superior
3.1.6.2.5. CentOS-6.7 e superior
3.1.6.2.6. CentOS-7.2 e superior
3.1.6.2.7. Debian GNU / Linux 8.6 e superior
3.1.6.2.8. Debian GNU / Linux 9.4 e superior
3.1.6.2.9. OracleLinux 7.3 e superior
3.1.6.2.10. SUSE® Linux Enterprise Server 15
3.1.6.2.11. openSUSE® 15
3.1.6.2.12. Alt Linux SPT 8.0.0 Work Station
3.1.6.2.13. Alt Linux SPT 8.0.0 Server Alt Linux 8.2 Work Station
3.1.6.2.14. Alt Linux 8.2 Work Station K
3.1.6.2.15. Alt Linux 8.2 Server
3.1.6.2.16. Alt Linux 8.2 Education
3.1.6.2.17. Amazon Linux AMI
3.1.6.2.18. Linux Mint 18.2 e superior
3.1.6.2.19. Linux Mint 19 e superior
3.1.6.2.20. Micro Focus Open Enterprise Server 2018
3.1.6.2.21. Astra Linux Special Edition 1.5
3.1.6.2.22. Astra Linux Special Edition 1.6
3.1.6.2.23. Astra Linux Common Edition Orel 2.12
3.1.6.2.24. GosLinux 6.6
3.1.6.2.25. Lotos
3.1.6.2.26. RED OS 7.1
3.1.6.2.27. RED OS 7.2

3.1.6.3.Características da solução de proteção para servidores Linux

3.1.6.3.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware) que verifique qualquer arquivo criado, acessado ou modificado;
3.1.6.3.2. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
3.1.6.3.3. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
3.1.6.3.3.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
3.1.6.3.3.2. 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;
3.1.6.3.3.3. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;
3.1.6.3.4. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados;
3.1.6.3.5. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;
3.1.6.3.6. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
3.1.6.3.7. 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;
3.1.6.3.8. Capacidade de verificar objetos usando heurística;
3.1.3.3.9. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
3.1.3.3.10. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
3.1.6.3.11. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux);

3.1.7. Proteção para Smartphones e Tablets

3.1.7.1.Compatibilidade de instalação nos seguintes sistemas operacionais;
3.1.7.1.1. Android 4.2–4.4.4;
3.1.7.1.2. Android 5.0–5.1.1;
3.1.7.1.3. Android 6.0–6.0.1;
3.1.7.1.4. Android 7.0–7.1.2;
3.1.7.1.5. Android 8.0–8.1;
3.1.7.1.6. Android 9.0;
3.1.7.1.7. iOS 9.0–9.3.5;
3.1.7.1.8. iOS 10.0–10.3.3;
3.1.7.1.9. iOS 11.0-11.4.1;

3.1.7.2.Características da solução de proteção para smartphones e tablets

3.1.7.2.1. Proteção em tempo real do sistema de arquivos do dispositivo;
3.1.7.2.2. Proteção contra adware e autodialers;
3.1.7.2.3. 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;
3.1.7.2.4. Arquivos abertos no smartphone;
3.1.7.2.5. Programas instalados usando a interface do smartphone;
3.1.7.2.6. Verificação dos objetos na memória interna do smartphone e nos cartões de expansão sob demanda do usuário e de acordo com um agendamento;
3.1.7.2.7. Deverá isolar em área de quarentena os arquivos infectados;
3.1.7.2.8. Deverá atualizar as bases de vacinas de modo agendado;
3.1.7.2.9. Deverá bloquear spams de SMS através de Black lists;
3.1.7.2.10. 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;
3.1.7.2.11. Capacidade de desativar por política:
3.1.7.2.11.1. Wi-FI;
3.1.7.2.11.2. Câmera;
3.1.7.2.11.3. Bluetooth;
3.1.7.2.12. Deverá ter função de limpeza de dados pessoais a distância, em caso de roubo, por exemplo;
3.1.7.2.13. Capacidade de requerer uma senha para desbloquear o dispositivo e personalizar a quantidade de caracteres para esta senha;
3.1.7.2.14. Deverá ter firewall pessoal (Android);
3.1.7.2.15. Capacidade de tirar fotos quando a senha for inserida incorretamente;
3.1.7.2.16. Possibilidade de instalação remota utilizando o Microsoft System Center Mobile Device Manager 2008 SP1;
3.1.7.2.17. Capacidade de enviar comandos remotamente de:
3.1.7.2.17.1. Localizar;

3.1.7.2.17.2. Bloquear;
3.1.7.2.17.3. Limpeza Remota;
3.1.7.2.18. Capacidade de detectar Jailbreak em dispositivos iOS;
3.1.7.2.19. Capacidade de bloquear o acesso a site por categoria em dispositivos;
3.1.7.2.20. Capacidade de bloquear o acesso a sites phishing ou malicioso;
3.1.7.2.21. Capacidade de criar containers de aplicativos, separando dados corporativos de dados pessoais;
3.1.7.2.22. Capacidade de bloquear o dispositivo quando o cartão “SIM” for substituído;
3.1.7.2.23. Capacidade de configurar White e blacklist de aplicativos;
3.1.7.2.24. Capacidade de localizar o dispositivo quando necessário;
3.1.7.2.25. Permitir atualização das definições quando estiver em “roaming”;
3.1.7.2.26. Capacidade de selecionar endereço do servidor para buscar a definição de vírus;
3.1.7.2.27. Deve permitir verificar somente arquivos executáveis;
3.1.7.2.28. Deve ter a capacidade de desinfectar o arquivo se possível;
3.1.7.2.29. Capacidade de agendar uma verificação;
3.1.7.2.30. Capacidade de enviar URL de instalação por e-mail;
3.1.7.2.31. Capacidade de fazer a instalação através de um link QRCode;
3.1.7.2.32. Capacidade de executar as seguintes ações caso a desinfecção falhe:
3.1.7.2.32.1. Deletar;
3.1.7.2.32.2. Ignorar;
3.1.7.2.32.3. Quarentenar;
3.1.7.2.32.4. Perguntar ao usuário;
3.1.7.2.33. Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange
3.1.7.2.34. Capacidade de ajustar as configurações de:
3.1.7.2.34.1. Sincronização de e-mail;
3.1.7.2.34.2. Uso de aplicativos;
3.1.7.2.34.3. Senha do usuário
3.1.7.2.34.4. Criptografia de dados;
3.1.7.2.34.5. Conexão de mídia removível;
3.1.7.2.35. Capacidade de instalar certificados digitais em dispositivos móveis;
3.1.7.2.36. Capacidade de, remotamente, resetar a senha de dispositivos iOS;
3.1.7.2.37. Capacidade de, remotamente, apagar todos os dados de dispositivos iOS;
3.1.7.2.38. Capacidade de, remotamente, bloquear um dispositivo iOS;
3.1.7.2.39. Deve permitir configurar horário para sincronização do dispositivo com a console de gerenciamento;
3.1.7.2.40. Possibilidade de exigir senha para abrir aplicações instaladas em container;
3.1.7.2.41. Deve permitir que o usuário utilize autenticação do Active Directory para abrir aplicações em container;
3.1.7.2.42. Deve permitir que uma senha seja digitada a cada x(minutos) para continuar utilizando uma aplicação em container;
3.1.7.2.43. Deve permitir a criptografia de dados salvos pelas aplicações em container;
3.1.7.2.44. Permitir sincronização com perfil do “Touch Down”;
3.1.7.2.45. Capacidade de desinstalar remotamente o antivírus do dispositivo;
3.1.7.2.46. Deve permitir fazer o upgrade do antivírus de forma remota sem a necessidade de desinstalar a versão atual;
3.1.7.2.47. Capacidade de sincronizar com Samsung Knox;
3.1.7.2.48. Deve permitir criar perfis de políticas para out-of-office no caso de BYOD.

3.1.8. Criptografia

3.1.8.1.Compatibilidade de instalação nos seguintes sistemas operacionais:
3.1.8.1.1. Microsoft Windows 7 Ultimate SP1 ou superior x86/x64;
3.1.8.1.2. Microsoft Windows 7 Enterprise SP1 ou superior x86/x64;
3.1.8.1.3. Microsoft Windows 7 Professional SP1 ou superior x86/x64;
3.1.8.1.4. Microsoft Windows 8 Enterprise x86/x64;
3.1.8.1.5. Microsoft Windows 8 Pro x86/x64;
3.1.8.1.6. Microsoft Windows 8.1 Pro x86/x64;
3.1.8.1.7. Microsoft Windows 8.1 Enterprise x86/x64;
3.1.8.1.8. Microsoft Windows 10 Enterprise x86/x64;
3.1.8.1.9. Microsoft Windows 10 Pro x86/x64;
3.1.8.2. 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;
3.1.8.3. Utilizar, no mínimo, algoritmo AES com chave de 256 bits;
3.1.8.4.Capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de pré-boot para autenticação do usuário;
3.1.8.5.Capacidade de utilizar Single Sign-On para a autenticação de pré-boot;
3.1.8.6.Permitir criar vários usuários de autenticação pré-boot;
3.1.8.7.Capacidade de criar um usuário de autenticação pré-boot comum com uma senha igual para todas as máquinas a partir da console de gerenciamento;
3.1.8.8.Capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções:
3.1.8.9.Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes;
3.1.8.10. Criptografar todos os arquivos individualmente;
3.1.8.11. Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas;
3.1.8.12. Criptografar o dispositivo em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha;
3.1.8.13. 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;
3.1.8.14. Capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados;
3.1.8.15. Capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados;
3.1.8.16. Verifica compatibilidade de hardware antes de aplicar a criptografia;
3.1.8.17. Possibilita estabelecer parâmetros para a senha de criptografia;
3.1.8.18. Bloqueia o reuso de senhas;
3.1.8.19. Bloqueia a senha após um número de tentativas pré-estabelecidas;
3.1.8.20. Capacidade de permitir o usuário solicitar permissão a determinado arquivo criptografado para o administrador mediante templates customizados;
3.1.8.21. Permite criar exclusões para não criptografar determinados “discos rígidos” através de uma busca por nome do computador ou nome do dispositivo
3.1.8.22. Permite criptografar as seguintes pastas pré-definidas: “meus documentos”, “Favoritos”, “Desktop”, “Arquivos temporários” e “Arquivos do outlook”;
3.1.8.23. Permite utilizar variáveis de ambiente para criptografar pastas customizadas;
3.1.8.24. Capacidade de criptografar arquivos por grupos de extensão, tais como: Documentos do office, Document, arquivos de audio, etc;
3.1.8.25. Permite criar um grupo de extensões de arquivos a serem criptografados;

3.1.8.26. Capacidade de criar regra de criptografia para arquivos gerados por aplicações;
3.1.8.27. Permite criptografia de dispositivos móveis mesmo quando o endpoint não possuir comunicação com a console de gerenciamento.
3.1.8.28. Capacidade de deletar arquivos de forma segura após a criptografia;
3.1.8.29. Capacidade de criptografar somente o espaço em disco utilizado;
3.1.8.30. Deve ter a opção de criptografar arquivos criados a partir de aplicações selecionadas pelo administrador;
3.1.8.31. Capacidade de bloquear aplicações selecionadas pelo administrador de acessarem arquivos criptografados;
3.1.8.32. Deve permitir criptografar somente o espaço utilizado em dispositivos removíveis tais como pendrives, HD externo, etc;
3.1.8.33. Capacidade de criptografar discos utilizando a criptografia BitLocker da Microsoft;
3.1.8.34. Deve ter a opção de utilização de TPM para criptografia através do BitLocker;
3.1.8.35. Capacidade de fazer “Hardware encryption”;

3.1.9. Gerenciamento de Sistemas

3.1.9.1.Capacidade de criar imagens de sistema operacional remotamente e distribuir essas imagens para computadores gerenciados pela solução e para computadores bare-metal;
3.1.9.2.Deve possibilitar a utilização de servidores PXE na rede para deploy de imagens;
3.1.9.3. Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares vulneráveis
3.1.9.4.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;
3.1.9.5.Capacidade de gerenciar licenças de softwares de terceiros;
3.1.9.6.Capacidade de registrar mudanças de hardware nas máquinas gerenciadas;
3.1.9.7.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;
3.1.9.8.Possibilita fazer distribuição de software de forma manual e agendada;
3.1.9.9.Suporta modo de instalação silenciosa;
3.1.9.10. Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis;
3.1.9.11. Possibilita fazer a distribuição através de agentes de atualização;
3.1.9.12. Utiliza tecnologia multicast para evitar tráfego na rede;
3.1.9.13. Possibilita criar um inventário centralizado de imagens;
3.1.9.14. Capacidade de atualizar o sistema operacional direto da imagem mantendo os dados do usuário;
3.1.9.15. Suporte a WakeOnLan para deploy de imagens;
3.1.9.16. Capacidade de atuar como servidor de atualização do Windows podendo fazer deploy de patches;
3.1.9.17. Suporta modo de teste, podendo atribuir alguns computadores para receberem as atualizações de forma automática para avaliação de alterações no comportamento;
3.1.9.18. Capacidade de gerar relatórios de vulnerabilidades e patches;
3.1.9.19. Possibilita criar exclusões para aplicação de patch por tipo de sistema operacional, Estação de trabalho e Servidor ou por grupo de administração;
3.1.9.20. Permite iniciar instalação de patch e correções de vulnerabilidades ao reiniciar ou desligar o computador;
3.1.9.21. Permite baixar atualizações para o computador sem efetuar a instalação;
3.1.9.22. Permite o administrador instalar somente atualizações aprovadas, instalar todas as atualizações

(exceto as bloqueadas) ou instalar todas as atualizações incluindo as bloqueadas;
3.1.9.23. Capacidade de instalar correções de vulnerabilidades de acordo com a severidade;
3.1.9.24. Permite selecionar produtos a serem atualizados pela console de gerenciamento;
3.1.9.25. Permite selecionar categorias de atualizações para serem baixadas e instaladas, tais como: atualizações de segurança, ferramentas, drivers, etc;
3.1.9.26. Capacidade de adicionar caminhos específicos para procura de vulnerabilidades e updates em arquivos;
3.1.9.27. Capacidade de instalar atualizações ou correções somente em computadores definidos, em grupos definidos ou em uma porcentagem de computadores conforme selecionado pelo administrador;
3.1.9.28. Capacidade de configurar o reinício do computador após a aplicação das atualizações e correções de vulnerabilidades;
3.1.9.29. Deve permitir selecionar o idioma das aplicações que serão atualizadas;
3.1.9.30. Permitir agendar o sincronismo entre a console de gerenciamento e os sites da Microsoft para baixar atualizações recentes.

3.2 **Para fornecer o objeto a 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 Contrato e prestação de serviços decorrente deste;

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

3.3 **Requisitos da Equipe Técnica:**

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

II - A Contratada deverá conciliar os serviços com os prazos definidos no presente Contrato. 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 Contratante deverão ter amplo conhecimento e experiência profissional em suas respectivas áreas..

3.4 **Gestão da Prestação dos Serviços:**

I - A Contratante e a 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 Contratante, em data e horário a ser combinado, ter a participação dos 'Representantes Técnicos Operacionais' da Contratante e da Contratada e, quando necessário, de técnicos convocados de ambos os lados;

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

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

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

VI - A 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.

CLÁUSULA QUARTA: Da 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 contratação será recebida em caráter provisório através de um Termo de Recebimento Provisório, emitido pela 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 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 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 Contratada terá o prazo de 01 (um) dia útil para sua solução;

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

CLÁUSULA QUINTA: Do Valor Contratual

I - 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.

II - Está incluso no preço final proposto, todo e qualquer custo, dentre outros, por exemplo, com: fornecimento de equipamentos necessários à boa e correta execução dos serviços; serviços de configuração; suporte; assistência técnica; deslocamento de pessoal; diária/estadia; frete; comodato; tributo, imposto, taxa, seguro,

emolumento, contribuição fiscal e "para fiscal"; encargo social e/ou trabalhista e/ou previdenciário; despesa acessória e/ou necessária não especificada neste Contrato, não se admitindo qualquer tipo de valor (custo) não previsto no mesmo.

CLÁUSULA SEXTA: Do pagamento

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

§ 1º. Caso o vencimento recaia em dia não útil (domingos, feriados e pontos facultativos), será prorrogado automaticamente para o primeiro dia útil posterior.
§ 2º. A COINPEL subordina-se a aplicação do Decreto Municipal 6.648 de 27/09/2022, portanto, caso a Contratada se enquadre na norma citada, no pagamento será realizada a retenção do IR conforme o Decreto e a IN Municipal 22/2022.

II - No caso de eventual atraso no pagamento de nota fiscal, provocado exclusivamente pela Contratante, o valor devido será acrescido de atualização financeira e sua apuração se fará desde a data de seu vencimento até a data do efetivo pagamento, proporcionalmente, em que os juros de mora serão calculados à taxa de 0,5% (meio por cento) ao mês, ou 6% (seis por cento) ao ano, mediante a fórmula em destaque no parágrafo único deste inciso, observado o prazo limite para pagamento acima previsto.

Parágrafo único - a atualização financeira será mediante a aplicação da seguinte fórmula:

I = (TX/100) / 365, e, ***EM = I x N x VA***, onde:

I = índice de atualização financeira;
TX = percentual da taxa de juros de mora anual;
EM = encargos moratórios;
N = nº. de dias entre a data prevista para o pagamento e a do efetivo pagamento;
VA = valor em atraso.

III - A nota fiscal deverá, entre outros dados fazer referência:

a) A quantidade e descrição integral do seu objeto, registrando o número de série ou chave (conforme o caso);
b) Referência expressa ao Contrato Administrativo;
c) Ao Banco, agência e número da conta-corrente, boleto bancário ou PIX em anexo para o pagamento resultantes da aquisição objeto deste Contrato.

IV - Nenhum pagamento será efetuado à Contratada enquanto estiver pendente:

a) Entrega do objeto;
b) Liquidação de qualquer obrigação financeira que lhe tiver sido imposta em decorrência de penalidade ou inadimplemento contratual;
c) Fornecimento de qualquer documento ou esclarecimento solicitado pela Contratante.

§ 1º. Uma vez regularizadas as pendências mencionadas neste inciso, o pagamento será efetivado.

§ 2º. o não pagamento motivado pelas pendências mencionadas neste inciso não caracterizará atraso, não sendo aplicado o disposto no inciso II, da presente Cláusula.

V - A critério da Contratante, do valor contratualmente devido poderão ser deduzidos valores para cobrir dívidas de responsabilidade da Contratada para com aquela, relativas a multas que tenham sido aplicadas em decorrência de irregular execução contratual, desde que tenha sido garantido o direito a defesa prévia.

CLÁUSULA SÉTIMA: Das Responsabilidades e dos Fiscais

7.1. **Da Contratante**:

I - Na pessoa do seu 'Fiscal do Contrato', o Srª. Bárbara Rodrigues, telefone (53) 3284-3600, e-mail: barbara.rodrigues@pelotas.rs.gov.br, propiciar todos os meios, informações e orientações disponíveis e necessárias à eficiente prestação dos serviços contratados, cumprindo e fiscalizando a execução do Contrato;

Parágrafo único - A fiscalização pelo representante da Contratante, será feita no interesse desta, e não exclui nem reduz a responsabilidade da Contratada, inclusive perante terceiros, por quaisquer irregularidades, e, na sua ocorrência, não implica co-responsabilidade do 'Poder Público' ou de seus agentes e prepostos.

II - Informar à Contratada, através da Central de Atendimento desta, os casos de necessidade de acionamento da Garantia diretamente relacionados ao objeto deste Contrato;

7.2. **Da Contratada**:

I - Através do seu 'Fiscal do Contrato', Sr. Newton Alves de Souza, e-mail newton@kscorp.com.br, envidar todos os esforços à execução do objeto deste Contrato, nos termos nele insertos e de acordo com os instrumentos legais aos quais este se vincula e subordina;

II - Atender todas as orientações formuladas pelo 'Fiscal doo Contrato' da Contratante, a ele atinentes, quanto a aquisição objeto deste Contrato de acordo com as especificações nele contidas e de acordo com os instrumentos legais aos quais este se subordina, instruindo os profissionais responsáveis à execução contratual quanto a ética nos seus procedimentos;

Parágrafo único - Exemplo de procedimento ético é a manutenção do sigilo profissional, sob pena de responsabilidade civil, penal e administrativa, relativo a todo e qualquer assunto ou dado (informação) de interesse da Contratante, dos usuários desta, ou de terceiros envolvidos no processo, obtidas em razão do instrumento contratual.

III - Sujeitar-se a mais ampla e irrestrita fiscalização por parte da Contratante, inclusive quanto a obrigação da manutenção da sua condição de habilitação e qualificação, ao longo do Contrato, nos termos do inciso IX do art. 68 da Lei Federal 13.303/16, prestando todos os esclarecimentos solicitados, referentes a sua execução, e atendendo às solicitações e/ou observações formuladas;

IV - Garantido o direito a prévia defesa, responder por quaisquer prejuízos financeiros à Contratante, danos morais a integridade social desta ou de terceiros, ação ou omissão (dolosa ou culposa), imperícia,

negligência ou infração às normas trabalhistas, comerciais, de publicidade e de segurança, quando da execução do contrato, adotando medidas corretivas ou de ressarcimento num prazo máximo de 10 (dez) dias úteis contínuos da comunicação do fato;

V - Assumir todos os encargos de possível demanda trabalhista, civil ou penal, relacionada à execução do objeto deste Contrato, originariamente ou vinculada por prevenção, conexão ou contingência;

VI - Ao longo da vigência contratual, dar ciência à Contratante, expressa e formalmente, de eventual mudança na designação do seu 'Fiscal do Contrato', informando novos dados para contato: nome completo; e-mail; telefones;

VII - Informar à Contratante se, ao longo da vigência contratual, encontrar-se sob uma ou mais das situações elencadas no Art. 38 da Lei Federal 13.303/16.

VIII - Não usar o nome da Contratante para fins de publicidade, sendo vedada a vinculação em quaisquer meios de comunicação, portfólios, bem como a divulgação ou fornecimento a terceiros, de dados e/ou informações relativas ao presente contrato, salvo com autorização expressa.

IX - Entregar e manter a garantia dos objetos adquiridos, obedecendo o presente Contrato;

X - Arcar com despesas de impostos, seguros, taxas, tributos, de qualquer natureza ou espécie, trabalhistas, previdenciários, salários, encargos sociais e quaisquer outros encargos necessários a execução contratual.

CLÁUSULA OITAVA: Da Dotação Orçamentária

Os recursos orçamentários para a cobertura das obrigações financeiras decorrentes deste Contrato são provenientes de receita própria da Contratante.

CLÁUSULA NONA Do Reajuste

I - Ao longo do período de vigência o valor contratual não será corrigido.

II - Não se admitirá, em hipótese alguma, ao longo da vigência contratual, qualquer tipo de valor (custo) não previsto neste Contrato.

CLÁUSULA DEZ: Das Sanções

I - Pela inexecução total ou parcial do presente Contrato, poderá a Contratante aplicar a Contratada, garantida a prévia defesa conforme inciso III deste item, as seguintes sanções:

a) advertência por escrito, a cada ocorrência, com prazo para saneamento da infração nunca inferior a 10 (dez) dias úteis;
b) Não sanada a infração dentro do prazo especificado na advertência, e caso esta se referira ao atraso na execução do objeto contratual, ou seja, na entrega (fornecimento) inicial dos objetos adquiridos ou após a entrega, do serviço de garantia, multa de 2% (dois por cento) ao dia, até o limite de 20% (vinte por cento) sobre o valor contratual, multa esta descontada da nota fiscal ou cobrada por via administrativa ou judicial;

c) suspensão temporária de participação em licitação e impedimento de contratar com a Contratante, por um prazo de 2 (dois) anos.

II - A aplicação das sanções previstas neste item não exime a Contratada da reparação dos eventuais danos, perdas ou prejuízos que sua conduta venha a causar à Contratante, conforme já dispõe o presente Contrato e a Lei Federal 13.303/16;

III - A aplicação das sanções será precedida de prazo para defesa (especificado no corpo da "advertência"), nunca inferior a 10 (dez) dias uteis, por parte da Contratada, nos termos do § 2º, Art. 83, da Lei Federal 13.303/16 e alterações;

§ 1º. O documento da defesa, além desta, deverá mencionar expressamente: o destinatário (Contratante); a identificação do Contrato e da Advertência; dados de identificação do recorrente; devendo ser redigido na Língua Portuguesa (Brasil), em papel timbrado e com carimbo ou indicação do número do CNPJ, e sem rasuras ou entrelinhas.

§ 2º. a entrega da defesa (se houver) deve ser feita pessoalmente pelo Fiscal do Contrato da Contratada (mediante protocolo), ou outro representante detentor de procuração da Contratada, à Coordenadora Administrativa e Financeira da Contratante (porém direcionada ao Diretor-Presidente), no endereço à Avenida Domingos de Almeida nº. 1785, salas 27, 28 e 29, bairro Areal, Pelotas/RS, no horário das 08h00 às 14h00, em dias úteis de expediente desta, ou enviada anexada para o e-mail: sandra.nunes@pelotas.rs.gov.br (**desde que escaneada da original**), em dias úteis de expediente da Contratante, das 08h00 às 17h00, sendo que, no caso do uso do correio eletrônico (e-mail):

a) A Contratada deverá registrar no campo 'assunto', obrigatoriamente, a expressão 'DEFESA REF SANÇÃO – CTR 02/2023', sob pena de não ter sua mensagem considerada;
b) A Contratada deverá, imediatamente após seu envio (em até 00h30min deste, considerado o horário especificado no caput deste parágrafo), entrar em contato com a Coordenadora Administrativa e Financeira da Contratante, Sra. Sandra Regina Nunes da Silva, pelo telefone (53) 3284-3600, comunicando o envio da defesa e solicitando confirmação do seu recebimento;
c) A data de envio da defesa, via e-mail, deverá respeitar a forma e o prazo para defesa estabelecido no documento veículo da sanção, emitido pela Contratante.

CLÁUSULA ONZE: Das Possibilidades de Rescisão e Alteração Contratual

I - Sem prejuízo do disposto na Cláusula Dez, o presente contrato poderá ser rescindido por infrações aos seus dispositivos e demais instrumentos legais aos quais vincula-se / subordina-se.

II - O presente Contrato somente poderá ser alterado por acordo entre as partes, vedado o ajuste que resulte em violação da obrigação de licitar.

CLÁUSULA DOZE: Da Vigência e da Possibilidade de Prorrogação

Uma vez assinado vigerá por 36 (trinta e seis) meses, a partir da ativação das licenças, quanto a garantia, atualizações e suporte das licenças de uso, mesmo após a quitação do valor contratual.

CLÁUSULA TREZE: Da Vinculação e Subordinação

O presente Contrato se vincula a Dispensa de Licitação nº. 03/2023 (e seus anexos) e a proposta da Contratada, subordinando-se a Lei Federal 13.303/16 e alterações, e a Lei Federal Complementar nº. 123/2006 (no que couber).

CLÁUSULA QUATORZE: Do não Exercício de Direitos, e dos Casos Omissos

I - O não exercício, pelas partes, de quaisquer de seus direitos ou faculdades estabelecidos neste Contrato, não configurará desistência, transigência ou novação, podendo ser exercido na sua plenitude, a qualquer tempo.

II - As divergências de interpretação, incorreções e casos omissos, se ocorrerem, serão dirimidos por consulta aos instrumentos legais aos quais vincula-se/subordina-se o presente Contrato.

CLÁUSULA QUINZE: Da Compatibilização

Obriga-se a Contratada a manter, durante toda a vigência do contrato, em compatibilidade com as obrigações por ela assumidas, todas as condições de habilitação e qualificação exigidas na dispensa que deu origem ao presente Contrato.

CLÁUSULA DEZESSEIS: Do Foro

É o FORO da Administração Municipal, o competente para dirimir quaisquer dúvidas decorrentes deste Contrato, em detrimento de qualquer outro por mais privilegiado que seja.

E, por estarem acordes, assinam o presente Contrato, dando-o por bom, firme e valioso.

Pelotas, RS, 03 de julho de 2023.

Contratante

Leandro Félix

LEANDRO DA SILVA FÉLIX
Diretor-Presidente

Contratada

Newton A. Souza

NEWTON ALVES DE SOUZA
Sócio

William da Cruz Sinotti

WILLIAM DA CRUZ SINOTTI
Diretor Técnico

Ministério da Economia
Secretaria de Governo Digital
Departamento Nacional de Registro Empresarial e Integração
Secretaria de Desenvolvimento Econômico e Turismo

Nº DO PROTOCOLO (Uso da Junta Comercial)

NIRE (da sede ou filial, quando a sede for em outra UF)	Código da Natureza Jurídica	Nº de Matrícula do Agente Auxiliar do Comércio
43206128679	2062	

1 - REQUERIMENTO

ILMO(A). SR.(A) PRESIDENTE DA Junta Comercial, Industrial e Serviços do Rio Grande do Sul

Nome: KSCORP TRADE AND SERVICES LTDA

(da Empresa ou do Agente Auxiliar do Comércio)

Nº FCN/REMP

RSP2200380820

requer a V.Sª o deferimento do seguinte ato:

Nº DE VIAS	CÓDIGO DO ATO	CÓDIGO DO EVENTO	QTDE	DESCRIÇÃO DO ATO / EVENTO
1	002			ALTERACAO
		051	1	CONSOLIDACAO DE CONTRATO/ESTATUTO
		020	1	ALTERACAO DE NOME EMPRESARIAL
		2244	1	ALTERACAO DE ATIVIDADES ECONOMICAS (PRINCIPAL E SECUNDARIAS)
		2015	1	ALTERACAO DE OBJETO SOCIAL

PORTO ALEGRE
Local

11 Abril 2022
Data

Representante Legal da Empresa / Agente Auxiliar do Comércio:
Nome: _____
Assinatura: _____
Telefone de Contato: _____

2 - USO DA JUNTA COMERCIAL

☐ DECISÃO SINGULAR ☐ DECISÃO COLEGIADA

Nome(s) Empresarial(ais) igual(ais) ou semelhante(s):

☐ SIM ☐ SIM

_____ _____
_____ _____
_____ _____
_____ _____
_____ _____

☐ NÃO ___/___/_____ _____ ☐ NÃO ___/___/_____ _____
Data Responsável Data Responsável

Processo em Ordem
À decisão

___/___/_____
Data

_____
Responsável

DECISÃO SINGULAR

	2ª Exigência	3ª Exigência	4ª Exigência	5ª Exigência
☐ Processo em exigência. (Vide despacho em folha anexa)	☐	☐	☐	☐
☐ Processo deferido. Publique-se e arquive-se.				
☐ Processo indeferido. Publique-se.				

___/___/_____ _____
Data Responsável

DECISÃO COLEGIADA

	2ª Exigência	3ª Exigência	4ª Exigência	5ª Exigência
☐ Processo em exigência. (Vide despacho em folha anexa)	☐	☐	☐	☐
☐ Processo deferido. Publique-se e arquive-se.				
☐ Processo indeferido. Publique-se.				

___/___/_____ _____ _____ _____
Data Vogal Vogal Vogal

Presidente da _____ Turma

OBSERVAÇÕES

JUNTA COMERCIAL, INDUSTRIAL E SERVIÇOS DO RIO GRANDE DO SUL

Registro Digital

Capa de Processo

Identificação do Processo		
Número do Protocolo	Número do Processo Módulo Integrador	Data
22/120.628-1	RSP2200380820	11/04/2022

Identificação do(s) Assinante(s)		
CPF	Nome	Data Assinatura
551.865.990-34	MARTA KARPOUZAS	20/04/2022
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br ITI Selo Prata - Biometria Facial		
387.073.060-91	NEWTON ALVES DE SOUZA	18/04/2022
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br ITI Selo Ouro - Certificado Digital		

4ª ALTERAÇÃO E CONSOLIDAÇÃO DO CONTRATO SOCIAL

KARPOUZAS & SOUZA COMÉRCIO E SERVIÇOS LTDA.

CNPJ 09.537.164/0001-27
NIRE 43206128679

NEWTON ALVES DE SOUZA, brasileiro, solteiro, nascido em 12/08/1963, empresário, portador do RG nº 6021200958, CNH/RS e CPF nº 387.073.060-91, residente e domiciliado na Avenida Mariland, nº 1135, apto 201, Bairro São João, CEP 90440-191, em Porto Alegre/RS; e

MARTA KARPOUZAS, brasileira, solteira, nascida em 28/03/1967, empresária, portadora do RG nº 5031856271, SSP/RS e CPF nº 551.865.990-34, residente e domiciliada na Avenida Panamericana, nº 400, apto 301, Bairro Lindoia, CEP 91050-000, em Porto Alegre/RS.

Únicas sócias da empresa **KARPOUZAS & SOUZA COMÉRCIO E SERVIÇOS LTDA.**, inscrita no CNPJ sob nº **09.537.164/0001-27**, com sede na Avenida Mariland, nº 1135, apto 201, Bairro São João, CEP 90440-191, em Porto Alegre/RS, com registro arquivado na Junta Comercial do Estado do Rio Grande do Sul sob nº **43206128679**, resolvem, de comum acordo, alterar seu contrato social, conforme cláusulas e condições seguintes:

I – DA ALTERAÇÃO DE RAZÃO SOCIAL

A razão social da empresa passa a ser **KSCORP TRADE AND SERVICES LTDA.**

II – DA ALTERAÇÃO DO OBJETO SOCIAL

O objeto social da empresa passa a ser:

- Desenvolvimento de programas de computador sob encomenda (6201-5/01);

- Representantes comerciais e agentes do comercio de maquinas e equipamentos de informática (4614-1/00);

- Desenvolvimento e licenciamento de programas de computador customizáveis (6202-3/00);

- Desenvolvimento e licenciamento de programas de computador não-customizáveis (6203-1/00);

- Consultoria em tecnologia da informação (6204-0/00);

- Reparação e manutenção de computadores e de equipamentos periféricos (9511-8/00);

- Suporte técnico, manutenção e outros serviços em tecnologia da informação (6209-1/00).

III - DA CONSOLIDAÇÃO DO CONTRATO SOCIAL

KSCORP TRADE AND SERVICES LTDA.

CNPJ 09.537.164/0001-27

NIRE 43206128679

CLAÚSULA PRIMEIRA

A sociedade gira sob o nome empresarial **KSCORP TRADE AND SERVICES LTDA.,** e tem sede e domicílio na Avenida Mariland, nº 1135, apto 201, Bairro São João, CEP 90440-191, em Porto Alegre/RS.

CLAÚSULA SEGUNDA

O objeto da sociedade é:

- Desenvolvimento de programas de computador sob encomenda (6201-5/01);

- Representantes comerciais e agentes do comercio de maquinas e equipamentos de informática (4614-1/00);

- Desenvolvimento e licenciamento de programas de computador customizáveis (6202-3/00);

- Desenvolvimento e licenciamento de programas de computador não-customizáveis (6203-1/00);

- Consultoria em tecnologia da informação (6204-0/00);

- Reparação e manutenção de computadores e de equipamentos periféricos (9511-8/00);

- Suporte técnico, manutenção e outros serviços em tecnologia da informação (6209-1/00).

CLAÚSULA TERCEIRA

O capital social é de R$ 10.000,00 (dez mil reais), divididos em 10.000 (dez mil) quotas no valor nominal de R$ 1,00 cada, totalmente integralizadas em moeda corrente nacional, distribuindo–se entre as sócias da seguinte forma:

SÓCIO	%	VALOR (R$)
NEWTON ALVES DE SOUZA	98%	R$ 9.800,00
MARTA KARPOUZAS	2%	R$ 200,00
Total	**100%**	**R$ 10.000,00**

Parágrafo Único. A responsabilidade de cada sócio é restrita ao valor de suas quotas, mas todos respondem solidariamente pela integralização do capital social, conforme art. 1.052 CC/2002.

CLAÚSULA QUARTA

A sociedade terá prazo indeterminado de duração.

CLÁUSULA QUINTA

A administração da sociedade é exercida pelo sócio **NEWTON ALVES DE SOUZA**, assinando isoladamente, ficando-lhe conferido amplos poderes para a prática de todos e quaisquer atos relativos aos fins sociais, inclusive delegar poderes a terceiros mediante procuração firmada em cartório, mens aqueles que tragam à sociedade qualquer ônus, sendo-lhes vedado alienação ou venda de quaisquer bens imóveis da empresa. Para esta prática será necessário a concordância de ambos sócios.

CLÁUSULA SEXTA

O sócio administrador terá direito a uma retirada mensal a título de pró-labores, cujo valor será decidido por ambos os sócios.

CLAÚSULA SÉTIMA

O exercício social terminará em 31 de dezembro de cada ano, quando serão levantados o balanço patrimonial e as demais demonstrações financeiras e

será efetuada a apuração dos resultados com observância das disposições legais aplicáveis.

Parágrafo Único. Os lucros ou prejuízos serão distribuídos ou suportados na proporção da participação de cada sócio no capital social.

CLAÚSULA OITAVA

As quotas de capital da sociedade poderão ser cedidas ou alienadas a terceiros estranhos ao quadro social, após ofertadas previamente aos sócios remanescentes, ao qual fica assegurado a preferencia na aquisição, em igualdade de condições, devendo o sócio retirante oferecer suas quotas ao seu socio, sempre por escrito, em correspondência dirigida ao socio da qual constem as condições da alienação para que este se manifeste sobre o exercício da preferencia no prazo de 30 (trinta) dias.

CLAÚSULA NONA

Em caso de morte de um dos sócios, a sociedade não será dissolvida e continuará sendo gerida pelo sócio remanescente ou pelos herdeiros. Não sendo possível ou inexistindo interesse destes ou da sócia remanescente, os valores de seus haveres serão apurados e liquidados com base na situação patrimonial da empresa. O mesmo procedimento será adotado em qualquer dos casos em que a sociedade se resolva em relação a uma das sócias.

CLAÚSULA DÉCIMA

O administrador declara, sob as penas da lei, que não está incurso em qualquer crime previsto em lei ou restrições legais, que possam impedi-lo de exercer atividade empresarial conforme artigo 1.011, 1º do CC/2002.

CLAÚSULA DÉCIMA SEGUNDA

As partes elegem o foro de Porto Alegre para dirimir quaisquer dúvidas decorrentes do presente instrumento contratual, bem como para o exercício e cumprimento dos direitos e obrigações resultantes deste contrato, sendo que os administradores renunciam a qualquer outro, por mais privilegiado que possa ser.

E, por estarem justas e contratadas, assinam digitalmente o presente instrumento, para que surta seus jurídicos e legais efeitos.

Porto Alegre, 08 de abril de 2022.

NEWTON ALVES DE SOUZA
Sócio Administrador

MARTA KARPOUZAS
Sócia

JUNTA COMERCIAL, INDUSTRIAL E SERVIÇOS DO RIO GRANDE DO SUL

Registro Digital

Documento Principal

Identificação do Processo		
Número do Protocolo	Número do Processo Módulo Integrador	Data
22/120.628-1	RSP2200380820	11/04/2022

Identificação do(s) Assinante(s)		
CPF	Nome	Data Assinatura
551.865.990-34	MARTA KARPOUZAS	20/04/2022
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br ITI Selo Prata - Biometria Facial		
387.073.060-91	NEWTON ALVES DE SOUZA	18/04/2022
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br ITI Selo Ouro - Certificado Digital		

TERMO DE AUTENTICAÇÃO - REGISTRO DIGITAL

Certifico que o ato, assinado digitalmente, da empresa KSCORP TRADE AND SERVICES LTDA, de CNPJ 09.537.164/0001-27 e protocolado sob o número 22/120.628-1 em 20/04/2022, encontra-se registrado na Junta Comercial sob o número 8257575, em 27/04/2022. O ato foi deferido eletronicamente pelo examinador Veridiana da Silva Lopes Falcao.

Certifica o registro, o Secretário-Geral, Carlos Vicente Bernardoni Gonçalves. Para sua validação, deverá ser acessado o sitio eletrônico do Portal de Serviços / Validar Documentos (https://portalservicos.jucisrs.rs.gov.br/Portal/pages/imagemProcesso/viaUnica.jsf) e informar o número de protocolo e chave de segurança.

Capa de Processo

Assinante(s)		
CPF	Nome	Data Assinatura
387.073.060-91	NEWTON ALVES DE SOUZA	18/04/2022
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br ITI Selo Ouro - Certificado Digital		
551.865.990-34	MARTA KARPOUZAS	20/04/2022
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br ITI Selo Prata - Biometria Facial		

Documento Principal

Assinante(s)		
CPF	Nome	Data Assinatura
551.865.990-34	MARTA KARPOUZAS	20/04/2022
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br ITI Selo Prata - Biometria Facial		
387.073.060-91	NEWTON ALVES DE SOUZA	18/04/2022
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br ITI Selo Ouro - Certificado Digital		

Data de início dos efeitos do registro (art. 36, Lei 8.934/1994): 08/04/2022

SRM

Documento assinado eletronicamente por Veridiana da Silva Lopes Falcao, Servidor(a) Público(a), em 27/04/2022, às 13:20.

A autencidade desse documento pode ser conferida no portal de serviços da jucisrs informando o número do protocolo 22/120.628-1.

CARLOS GONÇALVES
SECRETÁRIO-GERAL

JUNTA COMERCIAL, INDUSTRIAL E SERVIÇOS DO RIO GRANDE DO SUL

Registro Digital

O ato foi assinado digitalmente por :

Identificação do(s) Assinante(s)	
CPF	Nome
193.107.810-68	CARLOS VICENTE BERNARDONI GONCALVES

Porto Alegre. quarta-feira, 27 de abril de 2022

REPÚBLICA FEDERATIVA DO BRASIL

CADASTRO NACIONAL DA PESSOA JURÍDICA

NÚMERO DE INSCRIÇÃO	COMPROVANTE DE INSCRIÇÃO E DE SITUAÇÃO CADASTRAL	DATA DE ABERTURA
09.537.164/0001-27 **MATRIZ**		**08/05/2008**

NOME EMPRESARIAL
KSCORP TRADE AND SERVICES LTDA

TÍTULO DO ESTABELECIMENTO (NOME DE FANTASIA)	PORTE
KS SOLUCOES CORPORATIVAS	**ME**

CÓDIGO E DESCRIÇÃO DA ATIVIDADE ECONÔMICA PRINCIPAL
62.01-5-01 - Desenvolvimento de programas de computador sob encomenda

CÓDIGO E DESCRIÇÃO DAS ATIVIDADES ECONÔMICAS SECUNDÁRIAS
46.14-1-00 - Representantes comerciais e agentes do comércio de máquinas, equipamentos, embarcações e aeronaves
62.02-3-00 - Desenvolvimento e licenciamento de programas de computador customizáveis
62.03-1-00 - Desenvolvimento e licenciamento de programas de computador não-customizáveis
62.04-0-00 - Consultoria em tecnologia da informação
62.09-1-00 - Suporte técnico, manutenção e outros serviços em tecnologia da informação
95.11-8-00 - Reparação e manutenção de computadores e de equipamentos periféricos

CÓDIGO E DESCRIÇÃO DA NATUREZA JURÍDICA
206-2 - Sociedade Empresária Limitada

LOGRADOURO	NÚMERO	COMPLEMENTO
AV MARILAND	**1135**	**APT 201**

CEP	BAIRRO/DISTRITO	MUNICÍPIO	UF
90.440-191	**SAO JOAO**	**PORTO ALEGRE**	**RS**

ENDEREÇO ELETRÔNICO	TELEFONE
	(51) 3028-3361

ENTE FEDERATIVO RESPONSÁVEL (EFR)
*****

SITUAÇÃO CADASTRAL	DATA DA SITUAÇÃO CADASTRAL
ATIVA	**08/05/2008**

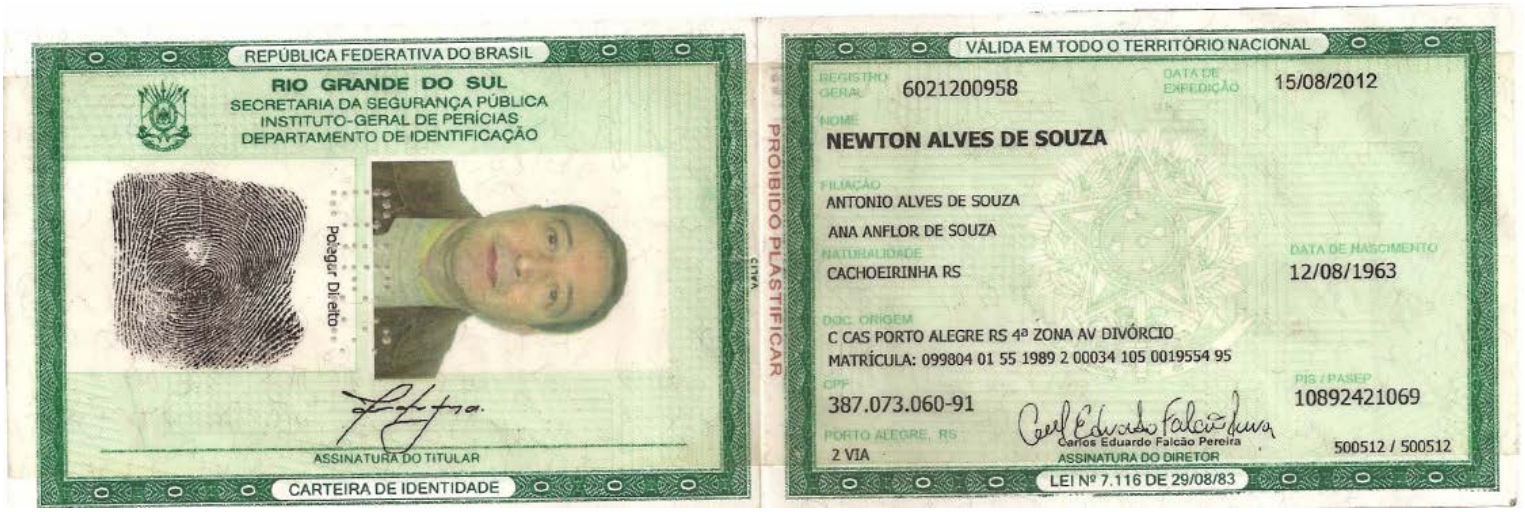
MOTIVO DE SITUAÇÃO CADASTRAL

SITUAÇÃO ESPECIAL	DATA DA SITUAÇÃO ESPECIAL
********	********

Aprovado pela Instrução Normativa RFB nº 1.863, de 27 de dezembro de 2018.

Emitido no dia **30/06/2023** às **11:53:04** (data e hora de Brasília). Página: **1/1**

Documento assinado eletronicamente nos moldes do art. 10 da MP 2200/01 e Lei 14063/20
[Hash SHA256] 482d438e7546c4d415ac60b07fad4b0d47d55cfe53998d2c7fe2e9a2a15efc5f



MINISTÉRIO DA FAZENDA
Secretaria da Receita Federal do Brasil
Procuradoria-Geral da Fazenda Nacional

CERTIDÃO NEGATIVA DE DÉBITOS RELATIVOS AOS TRIBUTOS FEDERAIS E À DÍVIDA ATIVA DA UNIÃO

Nome: KSCORP TRADE AND SERVICES LTDA
CNPJ: 09.537.164/0001-27

Ressalvado o direito de a Fazenda Nacional cobrar e inscrever quaisquer dívidas de responsabilidade do sujeito passivo acima identificado que vierem a ser apuradas, é certificado que não constam pendências em seu nome, relativas a créditos tributários administrados pela Secretaria da Receita Federal do Brasil (RFB) e a inscrições em Dívida Ativa da União (DAU) junto à Procuradoria-Geral da Fazenda Nacional (PGFN).

Esta certidão é válida para o estabelecimento matriz e suas filiais e, no caso de ente federativo, para todos os órgãos e fundos públicos da administração direta a ele vinculados. Refere-se à situação do sujeito passivo no âmbito da RFB e da PGFN e abrange inclusive as contribuições sociais previstas nas alíneas 'a' a 'd' do parágrafo único do art. 11 da Lei nº 8.212, de 24 de julho de 1991.

A aceitação desta certidão está condicionada à verificação de sua autenticidade na Internet, nos endereços <http://rfb.gov.br> ou <http://www.pgfn.gov.br>.

Certidão emitida gratuitamente com base na Portaria Conjunta RFB/PGFN nº 1.751, de 2/10/2014.
Emitida às 08:55:54 do dia 13/02/2023 <hora e data de Brasília>.
Válida até 12/08/2023.
Código de controle da certidão: **70C5.AC46.EE9E.B4B5**
Qualquer rasura ou emenda invalidará este documento.

Voltar Imprimir

CAIXA ECONÔMICA FEDERAL

Certificado de Regularidade do FGTS - CRF

Inscrição: 09.537.164/0001-27

Razão Social: KARPOUZAS E SOUZA COM REPR LTDA ME

Endereço: AV MARILAND 1135 AP 201 / SAO JOAO / PORTO ALEGRE / RS / 90440-191

A Caixa Econômica Federal, no uso da atribuição que lhe confere o Art. 7, da Lei 8.036, de 11 de maio de 1990, certifica que, nesta data, a empresa acima identificada encontra-se em situação regular perante o Fundo de Garantia do Tempo de Servico - FGTS.

O presente Certificado não servirá de prova contra cobrança de quaisquer débitos referentes a contribuições e/ou encargos devidos, decorrentes das obrigações com o FGTS.

Validade:20/06/2023 a 19/07/2023

Certificação Número: 2023062001121523564800

Informação obtida em 30/06/2023 10:22:36

A utilização deste Certificado para os fins previstos em Lei esta condicionada a verificação de autenticidade no site da Caixa: **www.caixa.gov.br**

Datas e horários baseados em Brasília, Brasil
Sincronizado com o NTP.br e Observatório Nacional (ON) em 04/07/2023 às 08:52:24

Ctr_022023_KSCORP_antivírus

Data e Hora de Criação: 03/07/2023 às 10:07:52

Documentos que originaram esse envelope:

- Ctr_022023_KSCORP_antivírus.pdf (Arquivo PDF) - 29 página(s)
- Contrato Social KSCORP pg 8 a 18.pdf (Arquivo PDF) - 11 página(s)
- CNPJ.pdf (Arquivo PDF) - 1 página(s)
- RG Newton.pdf (Arquivo PDF) - 1 página(s)
- CND tributos Federais e INSS - 30-06-2023.pdf (Arquivo PDF) - 1 página(s)
- CND FGTS - 30-06-2023.pdf (Arquivo PDF) - 1 página(s)

Hashs únicas referente à esse envelope de documentos

[SHA256]: 482d438e7546c4d415ac60b07fad4b0d47d55cfe53998d2c7fe2e9a2a15efc5f
[SHA512]: 5ba70fa521b09255044ecdf3af02fb46c771dc9553aa409c5dff7ee17f53245d91d2b165882e628367393d630747b94dced395db6380642619c02000a5dc717a

Lista de assinaturas solicitadas e associadas à esse envelope

ASSINADO - Leandro Da Silva Félix (leandro.felix@pelotas.rs.gov.br)
Data/Hora: 04/07/2023 - 08:52:24, IP: 187.86.132.227, Geolocalização: [-31.753535, -52.318171]
[SHA256]: 2c4a45f186c19ab71986951b2b7868d17be014451d3e551741c973b26b9f9e87

Leandro Félix

ASSINADO - newton@kscorp.com.br
Data/Hora: 04/07/2023 - 08:38:02, IP: 189.114.107.219, Geolocalização: [-30.024809, -51.193573]
[SHA256]: 3c48997bc779e76bc72615485611dfd7f47458bc8c79a00f6791e534cd54a645

ASSINADO - William Da Cruz Sinotti (william.sinotti@pelotas.rs.gov.br)
Data/Hora: 03/07/2023 - 10:24:28, IP: 187.86.132.227, Geolocalização: [-31.768922, -52.342118]
[SHA256]: 4d0247808d464278c856e047cfb9e277f8e4bc4a9a1e366a22516a9508368517

Histórico de eventos registrados neste envelope

04/07/2023 08:52:54 - Envelope finalizado por leandro.felix@pelotas.rs.gov.br, IP 187.86.132.227
04/07/2023 08:52:24 - Assinatura realizada por leandro.felix@pelotas.rs.gov.br, IP 187.86.132.227
04/07/2023 08:38:02 - Assinatura realizada por newton@kscorp.com.br, IP 189.114.107.219
03/07/2023 10:24:28 - Assinatura realizada por william.sinotti@pelotas.rs.gov.br, IP 187.86.132.227
03/07/2023 10:23:54 - Envelope visualizado por william.sinotti@pelotas.rs.gov.br, IP 187.86.132.227
03/07/2023 10:14:03 - Envelope registrado na Blockchain por cristina.farinha@pelotas.rs.gov.br, IP 187.86.132.227
03/07/2023 10:13:45 - Envelope encaminhado para assinaturas por cristina.farinha@pelotas.rs.gov.br, IP 187.86.132.227
03/07/2023 10:08:01 - Envelope criado por cristina.farinha@pelotas.rs.gov.br, IP 187.86.132.227