Pregão/Concorrência Eletrônica

- **Visualização de Recursos, Contrarrazões e Decisões**

INTENÇÃO DE RECURSO:

Senhor Pregoeiro, vimos manifestar nossa intenção de recorrer da decisão de declarar Vencedora a empresa HORIZON, em virtude de que a proposta da mesma não atende às exigências do edital, visto que a mesma cotou o Part Number KL4863KAUTS que não contempla todas as exigências, bem como não apresentou Atestado de Capacidade Técnica, conforme exigência. As razões serão melhor explicitadas na peça recursal. Obrigado

Fechar

Pregão/Concorrência Eletrônica

- **Visualização de Recursos, Contrarrazões e Decisões**

INTENÇÃO DE RECURSO:

Senhor Pregoeiro, vimos manifestar nossa intenção de recorrer da decisão de declarar Vencedora a empresa HORIZON, em virtude de que a proposta da mesma não atende às exigências do edital, visto que a mesma cotou o Part Number KL4863KAUTS que não contempla todas as exigências, bem como não apresentou Atestado de Capacidade Técnica, conforme exigência. As razões serão melhor explicitadas na peça recursal. Obrigado

Fechar

Pregão/Concorrência Eletrônica

- **Visualização de Recursos, Contrarrazões e Decisões**

RECURSO :

À ILUSTRISSÍMA SRA. PREGOEIRA DA SUPERINTENDÊNCIA ESTADUAL DE LICITAÇÕES DO ESTADO DE RONDÔNIA – SUPEL/RO

PREGÃO ELETRÔNICO Nº 471/2022/ÔMEGA/SUPEL/RO

MICROHARD INFORMÁTICA LTDA., pessoa jurídica de direito privado, inscrita no CNPJ sob o nº. 42.832.691/0001-30, com sede à Rua República Argentina, nº. 520, Bairro Sion, na cidade de Belo Horizonte/MG, CEP: 30.315-490, vem, respeitosamente, a tempo e modo, pe seu representante legal, apresentar RAZÕES DE RECURSO, com supedâneo nos fundamentos a seguir aduzidos:

I – DA TEMPESTIVIDADE E CABIMENTO.

Nos termos do Edital do Pregão Eletrônico nº 471/2022, item 14 (quatorze), o prazo para apresentação das razões de recurso administrativo será de 03 (três) dias úteis, após a aceitação de intenção de recorrer previamente ofertada.

Assim sendo, para comprovar a admissibilidade recursal, faz-se imperioso aduzir que, no dia 13.10.2022 (quinta-feira), a ora Recorrente manifestou a sua intenção de interpor o presente recurso administrativo, cumprindo a determinação contida no edital.

Verifica-se do procedimento administrativo em tela que a Recorrente teve a sua intenção de recurso devidamente aceita no mesmo dia 13.10.2022, apontando-se ainda que o prazo para a Recorrente apresentar suas razões recursais iniciou-se em 14.10.2022 (sexta-feira 18.10.2022 (terça-feira).

Logo, protocolizadas as razões de recurso na presente data, resta-se evidente a tempestividade das referidas razões recursais.

II – DO BREVE RELATO DOS FATOS. DO DESCUMPRIMENTO DAS PREVISÕES EDITALÍCIAS POR PARTE DA EMPRESA HORIZON INOVAÇÃO E TECNOLOGIA LTDA.

A Superintendência Estadual de Licitações do Estado de Rondônia – SUPEL/RO deu início à licitação em apreço, figurando como interessado o Corpo de Bombeiros Militar – CBM, visando o objeto previsto no edital do pregão eletrônico nº 471/2022, qual seja:

"2.1. Do Objeto: Registro de Preços para futura e eventual contratação de Solução de Segurança Cibernética, incluindo instalação, configuração inicial, integração, treinamento, suporte técnico e garantia.

Após o início do certame na data de 11.10.2022, com a participação de 04 (quatro) licitantes interessadas, verificou-se que a empresa Horizon Inovação e Tecnologia Ltda., ora Recorrida, foi convocada a apresentar documentação exigida em edital e, posteriormente, após declarada, até então, vencedora do certame (itens 01 e 02), senão vejamos:

Item 01:
"Aceite de proposta - 13/10/2022 - 12:45:01
Aceite individual da proposta. Fornecedor: HORIZON INOVACAO E TECNOLOGIA LTDA, CNPJ/CPF: 14.497.724/0001-05, pelo melhor lance de R$ 60.000,0000 e com valor negociado a R$ 59.500,0000. Motivo: Valor negociado, conforme proposta de preços
Habilitação de fornecedor - 13/10/2022 - 12:45:45
Habilitação em grupo de propostas. Fornecedor: HORIZON INOVACAO E TECNOLOGIA LTDA -
CNPJ/CPF: 14.497.724/0001-05"

Item 02:
"Aceite de proposta - 13/10/2022 - 12:45:36
Aceite individual da proposta. Fornecedor: HORIZON INOVACAO E TECNOLOGIA LTDA, CNPJ/CPF: 14.497.724/0001-05, pelo melhor lance de R$ 14.000,0000 e com valor negociado a R$ 13.165,0000. Motivo: Valor negociado, conforme proposta de preços
Habilitação de fornecedor - 13/10/2022 - 12:45:45
Habilitação em grupo de propostas. Fornecedor: HORIZON INOVACAO E TECNOLOGIA LTDA -
CNPJ/CPF: 14.497.724/0001-05"

Contudo, após análise da documentação apresentada pela empresa Horizon Inovação e Tecnologia Ltda. resta claro, aos olhos da Recorrente, que o Ente Licitante não poderia ter aceito a proposta da empresa em comento.

Isto porque se mostra cristalino o descumprimento de diversos itens do edital pela licitante Recorrida, inclusive no tocante à capacidade técnica exigida. Nesta senda, permita-se breve explanação:

Prefacialmente, cumpre destacar que a Recorrida apresentou proposta perante o Ente Licitante, desejando atender as exigências previstas em edital, informando, como solução a ser disponibilizada, aquela do "Part Number" "KL4863KAUTS", senão vejamos trecho da proposta

"Licenciamento, manutenção e suporte de solução de Proteção ENDPOINT e AMBIENTES VIRTUAIS (antivírus) - por 36 meses. Conforme descrições técnicas detalhadas de acordo com o item 4 do Termo de Referência. Part Number KL4863KAUTS"

O referido "Part Number" refere-se à solução Kaspersky Endpoint Security for Business "SELECT", sendo que, notadamente, o produto em comento não atende diversas exigências previstas em edital, especialmente previstas como "Especificações Técnicas das Soluções (Antivírus)", quais sejam:

"1.9. Criptografia
1.9.1. Compatibilidade
1.9.1.1. Microsoft Windows 7 Ultimate SP1 ou superior x86/x64;
1.9.1.2. Microsoft Windows 7 Enterprise SP1 ou superior x86/x64;
1.9.1.3. Microsoft Windows 7 Professional SP1 ou superior x86/x64;
1.9.1.4. Microsoft Windows 8 Enterprise x86/x64;
1.9.1.5. Microsoft Windows 8 Pro x86/x64;
1.9.1.6. Microsoft Windows 8.1 Pro x86/x64;
1.9.1.7. Microsoft Windows 8.1 Enterprise x86/x64;
1.9.1.8. Microsoft Windows 10 Enterprise x86/x64;
1.9.1.9. Microsoft Windows 10 Pro x86/x64;
1.9.2. Características
1.9.2.1. 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;
1.9.2.2. Utilizar, no mínimo, algoritmo AES com chave de 256 bits;
1.9.2.3. Capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de pré-boot para autenticação do usuário;
1.9.2.4. Capacidade de utilizar Single Sign- On para a autenticação de pré-boot;
1.9.2.5. Permitir criar vários usuários de autenticação pré-boot;
1.9.2.6. Capacidade de criar um usuário de autenticação pré-boot comum com uma senha igual para todas as máquinas a partir da console de gerenciamento;
1.9.2.7. Capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções:
1.9.2.7.1. Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes;
1.9.2.7.2. Criptografar todos os arquivos individualmente;
1.9.2.7.3. Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas;
1.9.2.7.4. Criptografar o dispositivo em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha;

1.9.2.8. 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
1.9.2.9. Capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados;
1.9.2.10. Capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados;
1.9.2.11. Verifica compatibilidade de hardware antes de aplicar a criptografia;
1.9.2.12. Possibilita estabelecer parâmetros para a senha de criptografia;
1.9.2.13. Bloqueia o reuso de senhas;
1.9.2.14. Bloqueia a senha após um número de tentativas pré-estabelecidas;
1.9.2.15. Capacidade de permitir o usuário solicitar permissão a determinado arquivo criptografado para o administrador mediante templates customizados;
1.9.2.16. Permite criar exclusões para não criptografar determinados “discos rígidos” através de uma busca por nome do computador ou nome do dispositivo
1.9.2.17. Permite criptografar as seguintes pastas pré-definidas: “meus documentos”, “Favoritos”, “Desktop”, “Arquivos temporários” e “Arquivos do outlook”;
1.9.2.18. Permite utilizar variáveis de ambiente para criptografar pastas customizadas;
1.9.2.19. Capacidade de criptografar arquivos por grupos de extensão, tais como: Documentos do office, Document, arquivos de audio, etc;
1.9.2.20. Permite criar um grupo de extensões de arquivos a serem criptografados;
1.9.2.21. Capacidade de criar regra de criptografia para arquivos gerados por aplicações;
1.9.2.22. Permite criptografia de dispositivos móveis mesmo quando o endpoint não possuir comunicação com a console de gerenciamento.
1.9.2.23. Capacidade de deletar arquivos de forma segura após a criptografia;
1.9.2.24. Capacidade de criptografar somente o espaço em disco utilizado;
1.9.2.25. Deve ter a opção de criptografar arquivos criados a partir de aplicações selecionadas pelo administrador;
1.9.2.26. Capacidade de bloquear aplicações selecionadas pelo administrador de acessarem arquivos criptografados;
1.9.2.27. Deve permitir criptografar somente o espaço utilizado em dispositivos removíveis tais como pendrives, HD externo, etc;
1.9.2.28. Capacidade de criptografar discos utilizando a criptografia BitLocker da Microsoft;
1.9.2.29. Deve ter a opção de utilização de TPM para criptografia através do BitLocker;
1.9.2.30. Capacidade de fazer “Hardware encryption”;
1.10. Gerenciamento de Sistemas
1.10.1. Capacidade de criar imagens de sistema operacional remotamente e distribuir essas imagens para computadores gerenciados pela solução e para computadores bare-metal;
1.10.2. Deve possibilitar a utilização de servidores PXE na rede para deploy de imagens;
1.10.3. Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares vulneráveis;
1.10.4. 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;
1.10.5. Capacidade de gerenciar licenças de softwares de terceiros;
1.10.6. Capacidade de registrar mudanças de hardware nas máquinas gerenciadas;
1.10.7. 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;
1.10.8. Possibilita fazer distribuição de software de forma manual e agendada;
1.10.9. Suporta modo de instalação silenciosa;
1.10.10. Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis;
1.10.11. Possibilita fazer a distribuição através de agentes de atualização;
1.10.12. Utiliza tecnologia multicast para evitar tráfego na rede;
1.10.13. Possibilita criar um inventário centralizado de imagens;
1.10.14. Capacidade de atualizar o sistema operacional direto da imagem mantendo os dados do usuário;
1.10.15. Suporte a WakeOnLan para deploy de imagens;
1.10.16. Capacidade de atuar como servidor de atualização do Windows podendo fazer deploy de patches;
1.10.17. Suporta modo de teste, podendo atribuir alguns computadores para receberem as atualizações de forma automática para avaliação de alterações no comportamento;
1.10.18. Capacidade de gerar relatórios de vulnerabilidades e patches;
1.10.19. Possibilita criar exclusões para aplicação de patch por tipo de sistema operacional, Estação de trabalho e Servidor ou por grupo de administração;
1.10.20. Permite iniciar instalação de patch e correções de vulnerabilidades ao reiniciar ou desligar o computador;
1.10.21. Permite baixar atualizações para o computador sem efetuar a instalação
1.10.22. Permite o administrador instalar somente atualizações aprovadas, instalar todas as atualizações (exceto as bloqueadas) ou instalar todas as atualizações incluindo as bloqueadas;
1.10.23. Capacidade de instalar correções de vulnerabilidades de acordo com a severidade;
1.10.24. Permite selecionar produtos a serem atualizados pela console de gerenciamento;
1.10.25. Permite selecionar categorias de atualizações para serem baixadas e instaladas, tais como: atualizações de segurança, ferramentas, drivers, etc;
1.10.26. Capacidade de adicionar caminhos específicos para procura de vulnerabilidades e updates em arquivos;
1.10.27. Capacidade de instalar atualizações ou correções somente em computadores definidos, em grupos definidos ou em uma porcentagem de computadores conforme selecionado pelo administrador;
1.10.28. Capacidade de configurar o reinicio do computador após a aplicação das atualizações e correções de vulnerabilidades;
1.10.29. Deve permitir selecionar o idioma das aplicações que serão atualizadas;
1.10.30. Permitir agendar o sincronismo entre a console de gerenciamento e os sites da Microsoft para baixar atualizações recentes.
1.11. Software de segurança para ambientes virtuais:
1.11.1. O software de segurança para ambientes virtuais deve incluir:
1.11.1.1. Software antivírus sem agente para ambientes virtuais;
1.11.1.2. Software antivírus baseado em agente para ambientes virtuais;
1.11.1.3. Gerenciamento, monitoramento e atualização de software e vacinas centralizados;
1.11.1.4. Capacidade de atualizar definições de vírus e padrões de ataques;
1.11.1.5. Documentação do administrador;
1.11.1.6. Compatibilidade com a rede a ser protegida.
1.11.2. Solução deve estar de acordo com os requisitos do Regulamento Geral sobre a Proteção de Dados (GDPR) para a proteção de ambientes virtuais.
1.11.3. Solução deve possuir proteção para virtualização privada e pública (AWS e Azure).
1.11.4. Solução deve possuir console de gerenciamento única para virtualização privada e pública.
1.12. Requerimentos para o antivírus sem agente:
1.12.1. O software de antivírus sem agente para ambientes virtualizados deve funcionar com as seguintes versões do VMWARE:
1.12.1.1. Vmware ESXi 6.7 Hypervisor
1.12.1.2. Vmware ESXi 6.5 Hypervisor Update 2
1.12.1.3. VMware ESXi 6.5a Hypervisor
1.12.1.4. Update 3 VMware ESXi 6.0 Hypervisor
1.12.1.5. Update 3b VMware ESXi 5.5 Hypervisor
1.12.1.6. VMware vCenter Server 6.7.0b
1.12.1.7. VMware vCenter Server 6.5 Update 2b
1.12.1.8. VMware vCenter Server 6.5a
1.12.1.9. VMware vCenter Server 6.0 Update 3f
1.12.1.10. VMware vCenter Server 5.5 Update 3e
1.12.1.11. VMware NSX 6.3.1
1.12.1.12. VMware NSX for vSphere 6.4.1
1.12.1.13. VMware NSX para vSphere 6.3.6
1.12.1.14. VMware NSX para vSphere 6.2.6
1.12.2. Software de antivírus sem agente para ambientes virtuais deve proteger os seguintes sistemas operacionais:

1.12.2.1. Windows 10 (32 / 64-bit)
1.12.2.2. Windows 8.1 (32 / 64-bit)
1.12.2.3. Windows 8 (32 / 64-bit)
1.12.2.4. Windows 7 Service Pack 1 (32 / 64- bit)
1.12.2.5. Windows XP SP3 ou superior (32- bit)
1.12.2.6. Windows Server 2012 e 2012 R2 sem suporte a ReFS (Sistemas de Arquivos Resiliente) (64-bit)
1.12.2.7. Windows Server 2008 R2 Service Pack 1 (64-bit)
1.12.2.8. Windows Server 2003 R2 Service Pack 2 (32 / 64-bit)
1.12.2.9. Ubuntu Server 14.04 LTS (64-bit)
1.12.2.10. Red Hat Enterprise Linux Server 7 (64-bit)
1.12.2.11. SUSE Linux Enterprise Server 12 (64-bit)
1.13. O antivírus sem agente para ambientes virtuais deve prover as seguintes funcionalidades:
1.13.1. Proteção contra malware em tempo real e durante a verificação agendada sem a necessidade de qualquer agente instalado no computador convidado;
1.13.2. Integração com a tecnologia Vmware vShield Manager para proteger o sistema de arquivos do computador;
1.13.3. Integração com a tecnologia Vmware Network Extensibility SDK para prover proteção no nível de rede, implementado para monitorar e bloquear atividade maliciosa na rede bem como endereços de URL com a habilidade de notificar o usuário sobre os bloqueios efetuad
1.13.4. Possuir integração com VMware NSX;
1.13.5. Deve possuir IPS e IDS para Vmware NSX;
1.13.6. Possuir integração com as etiquetas de segurança NSX;
1.13.7. Adicionar automaticamente novas máquinas virtuais ao escopo de proteção, sem a necessidade de qualquer instalação adicional;
1.13.8. Deve automatizar a instalação se baseando em políticas de segurança identificadas pelo VMware NSX;
1.13.9. Fazer scan em máquinas virtuais mesmo desligadas;
1.13.10. Verificar os dispositivos removíveis tais como (Pendrive, Cartões, etc);
1.13.11. O produto deve permitir parar o scan após x (minutos) da inicialização da verificação;
1.13.12. O produto deve ser capaz de ser configurado até três níveis de segurança sendo eles: Recomendado, alto ou baixo;
1.13.13. Prover as seguintes opções caso encontre uma ameaça:
1.13.13.1. Escolher a ação automaticamente;
1.13.13.2. Desinfectar ou bloquear caso a desinfecção falhe;
1.13.13.3. Desinfectar ou deletar caso a desinfecção falhe;
1.13.13.4. Deletar ou bloquear caso a deleção falhe;
1.13.13.5. Bloquear;
1.13.14. A solução deve permitir configurar um tamanho máximo de um arquivo para ser verificado. Ex: Caso o arquivo compactado tenha mais de 10 MB não verificar;
1.13.15. Permitir configurar o tempo máximo de scan em um arquivo;
1.13.16. Verificar os malwares do tipo trojans, auto-dialers, adware, etc;
1.13.17. Permitir verificar drives de rede;
1.13.18. Permitir verificar todos os arquivos do sistema com a exceção dos arquivos selecionados pelo administrador;
1.13.19. Fazer a verificação dos arquivos que possuem somente as extensões definidas pelo administrador;
1.13.20. Permitir a criação de exceções por pastas ou arquivos podendo incluir subpastas;
1.13.21. Permitir a criação de perfis de políticas diferentes para cada grupo de máquinas virtuais;
1.13.22. Possuir a integração com SNMP;
1.13.23. Capacidade de bloquear ataques vindos pela rede;
1.13.24. Verificar os endereços da web por possíveis ameaças;
1.13.25. Permitir a criação de exceções para URLs que não devem ser verificadas;
1.13.26. Permitir enviar uma mensagem de bloqueio caso colaborador acesse um site malicioso;
1.13.27. Proteção baseada em nuvem contra novas ameaças, permitindo a aplicação se comunicar com a fabricante do software para poder dar um veredito a um arquivo tanto na proteção em tempo real como na verificação agendada;
1.13.28. Atualizações centralizadas no sistema com a proteção especializada para virtualização sem a necessidade de distribuir atualizações para cada máquina convidada;
1.13.29. Possibilidade de verificação sob demanda ou manual nas máquinas virtuais selecionadas;
1.13.30. Verificação de: arquivos selecionados, pastas ou todo o sistema na verificação agendada de todas as máquinas virtuais;
1.13.31. Capacidade de implementar a solução de segurança sem a necessidade de reiniciar o Hypervisor ou entrar no modo de manutenção;
1.13.32. Tecnologia que previne a verificação do mesmo arquivo mais de uma vez;
1.13.33. Prevenir múltipla verificação em arquivos iguais mesmo que estejam em máquinas virtuais diferentes;
1.13.34. Bloquear, isolar e remover os vírus notificando o usuário e o administrador;
1.13.35. Possuir uma única console de gerenciamento para todos os componentes de proteção;
1.13.36. Uma única console de gerenciamento tanto para o ambiente virtual como para o ambiente físico;
1.13.37. Capacidade de ver a estrutura de administração tanto física como lógica assim como é apresentado no Vmware vCenter;
1.13.38. Informações detalhadas sobre os eventos e tarefas de implementação nas máquinas virtuais;
1.13.39. Capacidade de aplicar configurações de segurança diferentes para cada grupo de máquinas virtuais;
1.13.40. Criar exceções pelo nome do arquivo, pelo endereço dos arquivos e pela máscara dos arquivos;
1.13.41. Permitir exportar e importar listas com exceções;
1.13.42. Crias listas com exceções frequentes de acordo com as recomendações da Microsoft;
1.13.43. Permitir verificar drives de rede conectados na máquina virtual se necessário;
1.13.44. Capacidade de excluir drives de rede do escopo de proteção;
1.13.45. Suporta o Vmware vMotion, se uma máquina é transferida de um ESXi para outro a proteção não é interrompida;
1.13.46. Criar backup de arquivos deletados pela proteção;
1.13.47. Suportar esquema de licenciamento pela quantidade de máquinas virtuais protegidas e de acordo com o número de CPU cores;
1.13.48. Componente dedicado para integração centralizada com o ambiente virtual para evitar carga no Vmware vCenter e impedir chamadas de soluções de antivírus;
1.13.49. Suporte para ativar o software utilizando um código sob subscrição;
1.13.50. Providenciar informações sobre números de objetos verificados;
1.13.51. Providenciar informações sobre detalhes da definição de antivírus;
1.13.52. Suportar verificação de certificados SSL para comunicação entre o mecanismo de antimalware, servidor de gerenciamento e Componentes de infraestrutura do VMware ;
1.13.53. Importar ou exportar a lista de exclusões e verificações nas tarefas de verificação e perfis de proteção.
1.14. Requerimentos para antivírus em ambientes virtualizados baseado em agente (conector);
1.14.1. Para ser instalado em uma infraestrutura virtualizada, um dos seguintes hypervisors devem ser instalados:
1.14.1.1. Microsoft Windows Server 2016 Hyper-V.
1.14.1.2. Microsoft Windows Server 2012 R2 Hyper-V
1.14.1.3. Citrix XenServer 7.
1.14.1.4. Citrix XenServer 7.1 LTSR.
1.14.1.5. VMware ESXi 6.7.
1.14.1.6. VMware ESXi 6.5.
1.14.1.7. VMware ESXi 6.0.
1.14.1.8. VMware ESXi 5.5.
1.14.1.9. KVM (Kernel-based Virtual Machine) com um dos seguintes sistemas operacionais:
1.4.1.9.1. Ubuntu Server 16.04 LTS.

1.4.1.9.2. Ubuntu Server 14.04 LTS.
1.4.1.9.3. Red Hat Enterprise Linux Server 7, patch 4.
1.4.1.9.4. CentOS 7.4.
1.14.1.10. Proxmox 5.0.
1.14.1.11. Proxmox 5.1
1.14.2. O Antivírus baseado em agente deve prover proteção para as máquinas virtuais no Vmware hypervisor nos seguintes sistemas operacionais:
1.14.2.1. Windows 7 Professional / Enterprise Service Pack 1 (32 / 64-bit)
1.14.2.2. Windows 8.1 Update 1 Professional
/ Enterprise (32 / 64-bit)
1.14.2.3. Windows 10 Pro / Enterprise / Enterprise LTSB / RS1 / RS2 / RS3 / RS4 (32 / 64-bit)
1.14.2.4. Windows Server 2008 R2 Service Pack 1 (64-bit)
1.14.2.5. Windows Server 2012 (64-bit)
1.14.2.6. Windows Server 2012 R2 (64-bit)
1.14.2.7. Windows Server 2016 (64-bit)
1.14.2.8. Debian GNU / Linux 8.9 (32 / 64- bit)
1.14.2.9. Debian GNU / Linux 9.1 (64-bit)
1.14.2.10. Ubuntu Server 16.04 LTS (32 / 64- bit)
1.14.2.11. Ubuntu Server 18.04 LTS (64-bit)
1.14.2.12. CentOS 6.9 (64-bit)
1.14.2.13. CentOS 7.4 (64-bit)
1.14.2.14. Red Hat Enterprise Linux Server 6.9 (64-bit)
1.14.2.15. Red Hat Enterprise Linux Server 7.4 (64-bit)
1.14.2.16. SUSE Linux Enterprise Server 12 Service Pack 1 (64-bit)
1.14.3. A Suite VMware tools deve ser instalada para prover integração entre o Hypervisor, máquinas virtuais e o conector;
1.15. O antivírus baseado em agente deve prover as seguintes funcionalidades:
1.15.1. Antivírus e monitoramento residente;
1.15.2. Proteção contra rootkits e auto dialers a sites pagos;
1.15.3. Verificação por heurística para detectar e bloquear malwares desconhecidos;
1.15.4. Transferir a verificação de malware e as tarefas intensivas para uma única máquina virtual responsável pela proteção;
1.15.5. Garantir a continuidade da proteção de arquivos durante pequenas indisponibilidades na máquina de proteção logando todas as operações de arquivos nas máquinas protegidas durante o período de indisponibilidade, e faz a verificação automática de todas alteraç
acesso;
1.15.6. Proteção baseada em nuvem contra ameaças novas, permitindo a aplicação acessar recursos especializados da fabricante para obter vereditos durante a verificação em tempo real ou agendada;
1.15.7. Deve atender HIPPA e SOX;
1.15.8. Proteção de e-mail contra malwares verificando tráfego de entrada e saída nos protocolos IMAP, SMTP, POP3, MAPI e NNTP independente do cliente de e-mail;
1.15.9. Proteção de tráfego Web: verificação de objetos enviados para os computadores dos usuários via HTTP e FTP, com a possibilidade de adicionar sites confiáveis;
1.15.10. Bloqueia banners e pop-ups nas páginas web;
1.15.11. Capacidade de detectar e bloquear sites de phishing;
1.15.12. Proteção contra ameaças não conhecidas baseadas no comportamento;
1.15.13. Capacidade de determinar comportamento anômalo de uma aplicação analisando a sequência de execução. Capacidade de reverter operações de malware durante o tratamento do arquivo;
1.15.14. Capacidade de restringir o privilégio de programas executáveis tal como escrita no registro ou acesso a arquivos e pastas. Detecção automática de nível de detecção baseado na reputação do programa;
1.15.15. O Firewall deve permitir a criação de regras para pacotes de rede em protocolos específicos (TCP, UDP) e portas;
1.15.16. Permitir a criação de regras de rede para programas específicos;
1.15.17. Proteção contra ataques de hackers utilizando o firewall com IDS/IPS e regras de atividade de rede para as aplicações mais conhecidas;
1.15.18. Criação de regras especiais para bloquear a instalação e/ou execução de uma aplicação. Deve ter a capacidade de controlar a aplicação utilizando o caminho, metadado, MD5, checksum, e categorias predefinidas de aplicações providenciadas pelo fabricante;
1.15.19. Não carregar nenhum módulo de segurança na máquina virtual e sim no appliance virtual;
1.15.20. Permitir a verificação em máquinas linux;
1.15.21. Deve ser capaz de usar o "Microsoft System Center Virtual Machine Manager" (SCVMM) para fazer deploy dos appliances virtuais;
1.15.22. Os virtuais appliances responsáveis pela verificação devem ser baseados em Linux;
1.15.23. Deve ser capaz de apresentar uma lista de máquinas virtuais que estão sob proteção de cada virtual appliance seguro.
1.15.24. Capacidade de desativar a interface local na inicialização do sistema para diminuir consumo de memória;
1.15.25. Permitir selecionar a forma de conexão ao appliance virtual de três formas diferentes:
1.5.25.1. Utilizando Multicast;
1.5.25.2. Selecionando Servidor de integração;
1.5.25.3. Utilizando uma lista de appliances virtuais.
1.15.26. Deve ser capaz de verificar vírus, worms, trojans, toolkits, adware, auto-dialers e outros tipos de ameaças em máquinas Linux;
1.15.27. Deve ser capaz de criar exclusões em máquinas linux por nome ou pasta;
1.15.28. Capacidade de verificar arquivos por formato ou extensão em máquinas Linux;
1.15.29. Permitir configurar limite de tempo de verificação em um arquivo tanto para máquinas Linux como Windows;
1.15.30. Permitir alterar o modo de scan para no mínimo três opções diferentes:
1.5.30.1. Verificação automática;
1.5.30.2. Verificar os arquivos no acesso ou na modificação;
1.5.30.3. Somente no acesso;
1.15.31. Monitorar as atividades de I/O do usuário na utilização de dispositivos externos pelo tipo de dispositivo e/ou BUS usado incluindo a capacidade de criar uma lista de dispositivos confiáveis através do ID;
1.15.32. Capacidade de garantir privilégios na utilização de dispositivos externos para usuários específicos do AD;
1.15.33. Monitorar as atividades do usuário na internet incluindo o bloqueio ou a permissão de acesso a certos recursos bem como a capacidade de bloquear certos tipos de informação (audio, video,etc);
1.15.34. Capacidade de controlar acesso na internet por horário e por usuário do AD;
1.15.35. Atualizações centralizadas permitindo que parte do banco de dados de definições seja armazenado na máquina de proteção (SVM);
1.15.36. Habilidade de executar tarefas de detecção de vulnerabilidades em aplicações instaladas nos computadores incluindo opção de submeter um relatório de qualquer vulnerabilidade encontrada;
1.15.37. Integração com o Windows Update para instalar patches de acordo com as vulnerabilidades encontradas;
1.15.38. Capacidade de instalar e distribuir remotamente componentes do antivirus em todas as máquinas protegidas sem utilização de ferramentas de terceiros;
1.15.39. Armazenar as informações de arquivos verificados para evitar um novo scan sobre o arquivo e aumentar consumo de recursos;
1.15.40. Bloquear, neutralizar e remover os malwares com a opção de notificar os administradores;
1.15.41. Console de gerenciamento única para todos os componentes de proteção;
1.15.42. Console de gerenciamento única tanto para ambientes físicos como virtuais;
1.15.43. Console única para administração de máquinas virtuais Linux e Windows
1.15.44. Provê informações detalhadas sobre os eventos e execução de tarefas;
1.15.45. Capacidade de aplicar configurações de segurança diferentes para cada grupo de máquinas virtuais;
1.15.46. Salvar o backup dos arquivos deletados;
1.15.47. Suporta as seguintes tecnologias Vmware: vMotion, Distributed resource Scheduler;
1.15.48. Suporta as seguintes tecnologias Citrix: Virtual User Drive, Citrix Receiver, Multi-stream ICA, XenMotion Live Migration, Automated VM protection and recovery, Dynamic memory control;
1.15.49. Suportar as seguintes tecnologias Hyper- V: Live migration, Cluster shared volumes, Dynamic memory, Live backup;
1.15.50. Suportar rollback do banco de dados de definições;

1.15.51. Suportar o esquema de licença de acordo com o número de máquinas virtuais protegidas e de acordo com o número de hardware CPU cores
1.15.52. Solução de File Integrity Monitoring (FIM) para Linux e Microsoft Windows que garanta a integridade dos arquivos de sistemas, logs e aplicações críticas, monitorando alterações não autorizadas em arquivos e diretórios críticos.
1.15.53. Deve incluir componente de inspeção de logs, que gere regras de inspeção de logs para eventos do Windows e permita configuração do uso de análise heurística.
1.16. Requerimentos para administração centralizada, monitoramento e update do software para ambientes virtualizados:
1.16.1. A administração centralizada, monitoramento e atualização de softwares deve funcionar em computadores executando os seguintes sistemas operacionais:
1.16.1.1. Microsoft Windows 7 Todas as edições (32/64 bits);
1.16.1.2. Microsoft Windows 8
Pro/Enterprise 32/64 bits;
1.16.1.3. Microsoft Windows 8.1
Pro/Enterprise 32/64 bits;
1.16.1.4. Microsoft Windows 10 Education RS1;
1.16.1.5. Microsoft Windows 10 Education 32/64 bits;
1.16.1.6. Microsoft Windows 10 Enterprise RS1 e Professional RS1 32/64 bits;
1.16.1.7. Microsoft Windows 10 Enterprise e Professional 32/64 bits;
1.16.1.8. Microsoft Windows Small Business Server 2008 Standard x64;
1.16.1.9. Microsoft Windows Small Business Server 2008 Premium x64;
1.16.1.10. Microsoft Windows Small Business Server 2011 Essential, Premium e Standard;
1.16.1.11. Microsoft Windows Server 2008
Todas edições 32/64 bits;
1.16.1.12. Microsoft Windows Server 2008 R2 Todas edições 32/64 bits;
1.16.1.13. Microsoft Windows Server 2012
Todas edições 32/64 bits;
1.16.1.14. Microsoft Windows Server 2012 R2 Todas edições 32/64 bits;
1.16.1.15. Microsoft Windows Server 2016
x64Banco de dados Suportados pela console de administração centralizada.
1.16.2. Microsoft SQL Server Express 2008;
1.16.3. Microsoft SQL Server Express 2008 R2;
1.16.4. Microsoft SQL Server Express 2008 R2 Service Pack 2;
1.16.5. Microsoft SQL Server 2005;
1.16.6. Microsoft SQL Server 2008;
1.16.7. Microsoft SQL Server 2008 R2;
1.16.8. Microsoft SQL Server 2012;
1.16.9. Microsoft SQL Server 2014 Todas as edições x64
1.16.10. MySQL Enterprise versions 5.0.67, 5.0.77, 5.0.85, 5.087 Service Pack 1, 5.091;
1.16.11. MySQL Enterprise versions 5.0.60
Service Pack 1, 5.0.70, 5.0.82 Service Pack 1, 5.0.90;
1.17. Requerimentos Console de administração instalada em ambientes virtualizados:
1.17.1. VmwareWorkstation 12.x Pro;
1.17.2. Microsoft Hyper-V: 2008, 2008 R2, 2012, 2012 R2
1.17.3. Microsoft Virtual PC 2007 (6.0.156.0)
1.17.4. Parallels Desktop 7 e 11;
1.17.5. Citrix XenServer 6.2 e 6.5;
1.17.6. Oracle VM VirtualBox 4.0.4-70112
1.18. O console de administração centralizada deve prover as seguintes funcionalidades:
1.18.1. Deve ser compatível com Microsoft SCVMM;
1.18.2. Capacidade de desativar a interface local do agente (conector) para diminuir uso de memória;
1.18.3. Instalação do antivírus a partir de uma única distribuição;
1.18.4. Seleção de instalação dependendo do número de pontos protegidos;
1.18.5. Capacidade de ler informações do AD para obter dados some as contas dos computadores na organização;
1.18.6. Capacidade de fazer a instalação automática através dos grupos gerenciados;
1.18.7. Capacidade de realocar computadores de acordo com endereço IP, tipo do sistema operacional e localização no AD;
1.18.8. Instalação centralizada;
1.18.9. Remoção centralizada (manual ou automática) de aplicações incompatíveis através do servidor de administração;
1.18.10. Capacidade de instalar o antivírus de diferentes formas: RPC, GPO, agente de administração;
1.18.11. Capacidade de atualizar pacotes de instalação com as últimas atualizações;
1.18.12. Atualizar de forma automática a versão do antivírus e as definições;
1.18.13. Procurar automaticamente por vulnerabilidades nas aplicações e sistemas operacionais presentes da rede;
1.18.14. Capacidade de proibir instalação/execução de aplicações;
1.18.15. Capacidade de gerenciar I/O de dispositivos externos;
1.18.16. Gerenciar a atividade do usuário na internet;
1.18.17. Capacidade de testar as atualizações antes de aplicar para o ambiente;
1.18.18. Capacidade de executar instalações automáticas baseado no sistema de proteçãod edicado, tais como: Vmware ESXi, Microsoft Hyper-V, Citrix XenServer virtualization ou hypervisor;
1.18.19. Criar os usuários baseados em RBAC;
1.18.20. Criar a hierarquia dos servidores de administração e tem capacidade de gerenciar cada um deles através de uma única console de gerenciamento;
1.18.21. Capacidade de criar servidores de administração lógicos, sem a necessidade de ter um servidor adicional para gerenciamento;
1.18.22. Distribuir automaticamente licenças nos computadores gerenciados;
1.18.23. Criar o inventário de software e hardware dos computadores gerenciados na rede;
1.18.24. Instalação centralizada de aplicações de terceiros;
1.18.25. Capacidade de eleger um computador na rede para ser responsável por atualizar outros computadores dentro da rede;
1.18.26. Capacidade de gerar relatórios gráficos;
1.18.27. Capacidade de exportar relatórios para PDF, XML e CSV;
1.18.28. Capacidade de criar contas internas para autenticar no console de administração;
1.18.29. Capacidade de criar backup de forma automática ou manual;
1.18.30. Suporta Windows Failover Clustering;
1.18.31. Console WEB para gerenciar a aplicação;
1.18.32. Sistema para controle de virus outbreak.
1.18.33. Capacidade de gerenciar permissões de administradores;
1.18.34. Capacidade de deletar atualizações já baixadas;
1.18.35. Capacidade de distribuir correções de vulnerabilidades em computadores clientes sem instalar atualizações;
1.18.36. Capacidade de eleger automaticamente um agente de atualização de acordo com uma análise de rede.
1.18.37. Capacidade de manter um histórico das alterações feitas nas políticas tanto de Linux como Windows;
1.18.38. Permite comparar alterações feitas no console de administração;

1.18.39. Deve permitir o rollback de alterações feitas nas políticas através de uma única seleção, sem ter a necessidade de restaurar item por item alterado."

Destaca-se que, quanto aos itens 1.11 até 1.18 acimados, referentes às "Especificações Técnicas das Soluções de Segurança Cibernética (Antivírus)", a proposta apresentada pela Recorrida deveria contemplar o produto "Kaspersky Hybrid Cloud" da fabricante Kaspersky, o qu incluído na proposta apresentada pela empresa Horizon Inovação e Tecnologia Ltda.

A necessidade de fornecimento do "Hybrid Cloud" se mostra cristalina, eis que foi determinada tanto pelo descritivo do edital (itens 1.11 até 1.18) quanto pela resposta emitida pelo Ente no processo SEI 0032764839 (código CRC 6F9F10B8), apontando que o Ente Licita (dezesseis) servidores, devendo os mesmos serem atendidos respeitando-se as funcionalidades em comento (https://sei.sistemas.ro.gov.br/se acao=documento_conferir&codigo_verificador=0032764839&codigo_crc=6F9F10B8&hash_download=7a22d7a18f12bdc4f5883750798f2c0dbd2a808a64bb3a2c60a219c5b6018fc34e6ec780294ac754e3d714d4539f0f9e1f3634eb15ae668ceb556cb0e5d12b64&visualizacao=1&id_

"QUESTIONAMENTO - Empresa "A" (0032692930)
"[...]
Questionamento 1: Na página 27 e na página 76 do edital, consta a quantidade de 338 licenças de antivírus. Porém, no descritivo técnico da página 38, item 1.11 (Software de segurança para ambientes virtuais) até a página 51 item 1.18.39, trata de um produto específico pa virtualizados, que requer um licenciamento específico e exige, obrigatoriamente, a informação de quantidade de licenças. Perguntamos: Quantos servidores virtualizados devem ser protegidos pela solução descrita a partir da página 38?
[...]"
RESPOSTA: A FUNESBOM, por meio da CBM-DINF, manifestou-se:
"[...]
informamos que até o exato momento possuímos apenas 16 (dezesseis) máquinas virtualizadas em 03 (três) Lâminas de servidores físicos." (Grifos nossos).

Resta, portanto, cristalino que o produto apresentado pela Recorrida (KESB SELECT Part Number KL4863KAUTS) não atende integralmente às exigências do Edital.

Ademais, Ilustre Julgadora, analisando-se a documentação apresentada pela Recorrida, verifica-se que a mesma não cumpriu o determinado em edital no tocante à capacidade técnica exigida no certame, in verbis:

"14.2.2.1. Entende-se por pertinente e compatível em característica o(s) atestado(s) que sem sua individualidade ou soma, contemplem que a licitante forneceu software antivírus, objeto do presente termo de referência, conforme o(s) item(ns) que o licitante apresentou na p
14.2.2.2. Entende-se por pertinente e compatível em quantidade o(s) atestado(s) que sem sua individualidade ou soma, contemplem que a licitante forneceu software antivírus, objeto do presente termo de referência, no mínimo 5% (cinco por cento) para o(s) item(ns) qu proposta do item 01 das especificação técnica contida neste Termo de Referência;
14.2.2.3. Entende-se por pertinente e compatível em prazo o(s) atestado(s) que sem sua individualidade ou soma de atestados concomitantes no período de execução (tendo sido os serviços atestados prestados no mesmo período) comprove com pelo ao menos 3 (três) mes que a empresa prestou ou presta satisfatoriamente serviços com características semelhantes com o objeto descrito no item 01 das especificação técnica contida neste Termo de Referência."

Nota-se que, apesar de o edital não se mostrar extremamente rigoroso no tocante à quantidade exigida para comprovação da capacidade técnica pelas licitantes interessadas, mesmo assim, a Recorrida não conseguiu comprovar o mínimo exigido no instrumento convo comprovar expertise em fornecimento de sistema de gestão administrativa, o que, notadamente, não atende o exigido em edital, demonstrando-se que a Recorrida não possui capacidade técnica para atendimento do Ente Licitante (software antivírus).

Veja Ilustre Julgadora que não são poucas as previsões editalícias não atendidas pela licitante que se sagrou vencedora do certame, até então, sendo que a ausência de capacidade técnica não pode ser ignorada pelo Ente Licitante.

Logo, apenas por estas breves digressões, já é possível concluir pela necessidade de rejeição da proposta da Recorrida, com base no que determina o princípio da vinculação ao edital, posto que esta não preencheu todos os requisitos previstos em edital.

III – DO DIREITO
III.1 – DO PRINCÍPIO DA VINCULAÇÃO AO EDITAL.

Conforme mencionado na precedência, decidiu-se por sagrar vencedora do certame, até então, a empresa Horizon Inovação e Tecnologia Ltda., em manifesto equívoco, data venia, cometido pela Ilustre Comissão de Licitação, descumprindo o previsto em edital, posto que a as exigências previstas na norma editalícia.

Nos dizeres de assentado Hely Lopes Meirelles, "a vinculação ao edital é princípio básico de toda licitação. Nem se compreenderia que a administração fixasse no edital a forma e o modo de participação dos licitantes e no decorrer do procedimento ou na realização do j estabelecido, ou admitisse documentação e propostas em desacordo com o solicitado. O edital é a lei interna da licitação, e, como tal, vincula a seus termos tantos os licitantes como a Administração que o expeliu (art. 41)." (Direito Administrativo Brasileiro. São Paulo, Malheir

No mesmo sentido é a lição de José dos Santos Carvalho Filho :

"A vinculação ao instrumento convocatório é garantia do administrador e dos administrados. Significa que as regras traçadas para o procedimento devem ser fielmente observadas por todos. Se a regra fixada não é respeitada, o procedimento se torna inválido e sus administrativa ou judicial. O princípio da vinculação tem extrema importância. Por ele, evita-se a alteração de critérios de julgamento, além de dar a certeza aos interessados do que pretende a Administração. E se evita, finalmente, qualquer brecha que provoque violação à m impessoalidade e à probidade administrativa. Se o instrumento de convocação, normalmente o edital tiver falha, pode ser corrigido, desde que oportunamente, mas os licitantes deverão ter conhecimento da alteração e a possibilidade de se amoldarem a ela. Vedado à Admin descumprimento das regras de convocação, deixando de considerar o que nele se exige, como, por exemplo, a dispensa de documento ou a fixação de preço fora dos limites estabelecidos. Em tais hipóteses, deve dar-se a desclassificação do licitante, como, de resto, impõ "(G.n.)

A respeito do princípio da vinculação ao instrumento convocatório, a Lei nº. 8.666/93 é clara ao dispor que as regras traçadas para o procedimento devem ser fielmente observadas por todos. Senão vejamos:

"Art. 41. A Administração não pode descumprir as normas e condições do edital, ao qual se acha estritamente vinculada". (G.n.)

Assim, não pode a Administração Pública simplesmente tomar uma série de medidas infringindo o edital, como no caso em tela, quando declarou como vencedora do certame empresa que, claramente, não atende todos os requisitos previstos em edital, sendo que a mesma nã técnica exigida no instrumento convocatório.

Como cediço, o Edital faz lei entre a Administração Pública e os licitantes, consoante já consolidado pela jurisprudência pátria, a saber:

"licitação – mandado de segurança – INABILITAÇÃO DA IMPETRANTE – REQUISITO EXPRESSAMENTE PREVISTO NO EDITAL – SE O EDITAL ESPECIFICOU A FORMA COMO DEVERIAM SER APRESENTADOS OS DOCUMENTOS E, MAIS, ESTABELECEU CRITÉRIO DE ACEITA EXIGIDO DA ADMINISTRAÇÃO OUTRO MODO DE ATUAÇÃO, SOB PENA DE AFRONTA AOS PRINCÍPIOS DA LEGALIDADE, DA ISONOMIA E DA VINCULAÇÃO AO EDITAL (ART. 41 DA LEI 8.666/93) – RECURSO IMPROVIDO" (Apelação Cível nº 0012683-86-2010.8.26.0562 – TJSP DJ: 01/04/2013)(G.n.)

"AGRAVO DE INSTRUMENTO. LICITAÇÃO. MODALIDADE DE CONCORRÊNCIA. TIPO TÉCNICA E PREÇO. REGIME DE EMPREITADA. LIMINAR EM MANDADO DE SEGURANÇA. PEDIDO DE SUSPENSÃO DA CONCORRÊNCIA PÚBLICA. LIMINAR EM MANDADO DE SEGURANÇA. REQU LEI 12.016/09 NÃO EVIDENCIADOS. DECISÃO AGRAVADA INALTERADA. RECURSO NÃO PROVIDO.
- Considerando que os parâmetros utilizados pela autoridade coatora para atribuição de notas referentes às propostas técnicas apresentadas pelos licitantes, não se verifica motivo que justifique o deferimento da medida liminar pretendida em Mandado de Segurança.
- Nos termos da jurisprudência do Superior Tribunal de Justiça, "princípio da vinculação ao instrumento convocatório se traduz na regra de que o edital faz lei entre as partes, devendo os seus termos serem observados até o final do certame" (REsp 354.977/SC, Rel. Ministro H Primeira Turma, DJ 9.12.2003, p. 213.).
- Ausentes os requisitos autorizadores previstos no artigo 7º, inciso III, da Lei Federal 12.016/09, deve ser indeferida a medida liminar pretendida, objetivando a suspensão da licitação na modalidade de concorrência, pelo tipo técnica e preço, devendo aguardar-se a aná Instrumento nº 1.0000.16.069412-1/001 – TJMG – Rel. Des. Moacyr Lobato, DJ: 04/05/2017)(G.n.)

"ADMINISTRATIVO. LICITAÇÃO TOMADA DE PREÇO. LEI 8.666/93. DESRESPEITO À ORDEM DE CLASSIFICAÇÃO. DESCABIMENTO DA ALEGAÇÃO DE MAIOR QUALIDADE DO SEGUNDO COLOCADO. SENTENÇA CONFIRMADA. O Edital é a lei do certame, cuja vinculação dos p Administração Pública é obrigatória, tendo que se perseguir, por certo, o cumprimento de todas as exigências e disposições nele dispostas". (TJMG. Processo n.º 1.0011.04.005607-6/001. Rel. José Domingues Ferreira Esteves. 02/09/05). (G.n).

"ADMINISTRATIVO. CONCURSO PÚBLICO. PORTADORES DE NECESSIDADES ESPECIAIS. VINCULAÇÃO AO EDITAL. NÃO COMPARECIMENTO À JUNTA MÉDICA. NEGLIGÊNCIA NO ACOMPANHAMENTO DO ANDAMENTO DO CONCURSO. NOVA OPORTUNIDADE - IMPOSSIBILIDADE.
1. A jurisprudência tem entendido que o edital do concurso é instrumento formal que regula o certame, deve ser respeitado em todas as suas regras, não podendo ser desconsiderado, sob pena de invalidação de todo o processo administrativo, especialmente se o candidato n qualquer item do edital, por força do princípio da vinculação ao instrumento convocatório e isonomia (AG 2006.01.00.040726-6, Rel. Desembargadora Federal Selene Maria de Almeida, 5ª Turma, DJ 17/05/07).2. A divulgação ou convocação de candidatos mediante publicaçã os princípios da publicidade, razoabilidade ou impessoalidade.3. Sentença confirmada.4. Apelação desprovida." (Apelação Cível nº 2009.34.00.005104-1/DF – TRF 1ª Região – Rel. Des. Federal José Amilcar Machado, DJ: 27/08/2012) (G.n.)

Na mesma linha veja a posição do STJ sobre o tema:

"RECURSO ESPECIAL. LICITAÇÃO. LEILÃO. EDITAL. PRINCÍPIO DA VINCULAÇÃO DO INSTRUMENTO CONVOCATÓRIO. EDITAL FAZ LEI ENTRE AS PARTES. - O Princípio da Vinculação ao Instrumento Convocatório se traduz na regra de que o edital faz lei entre as partes, deve observados até o final do certame, vez que vinculam as partes". (Superior Tribunal de Justiça. REsp. 354977/SC. 1ª Turma. Min. Humberto Gomes de Barros. 09/12/2003) (G.n).

Logo, com base na fundamentação precedente, pautada no instrumento convocatório e na Lei Maior das Licitações (Lei nº. 8.666/93), requer a Recorrente seja revogada a decisão que declarou vencedora do certame a Recorrida, eis que notadamente a empresa não atendeu d em edital.

IV – DOS PEDIDOS

Desta forma, haja vista os fatos e fundamentos jurídicos colacionados na precedência, pugna a Recorrente seja dado provimento ao seu recurso, para que seja revogada a decisão que declarou vencedora do certame a empresa Horizon Inovação e Tecnologia Ltda. (itens 0 várias ilegalidades verificadas e apontadas na presente peça recursal.

Nestes termos, pede deferimento.

Belo Horizonte/MG, 18 de outubro de 2022.

_____

MICROHARD INFORMÁTICA LTDA.
José Glicério Ruas Alves

Fechar

Pregão/Concorrência Eletrônica

- **Visualização de Recursos, Contrarrazões e Decisões**

CONTRARRAZÃO :

CONTRARRAZÃO : ILUSTRÍSSIMO(A) SENHOR (A) PREGOEIRO(A) DO PREGÃO ELETRÔNICO Nº 4712022 DA SUPERINTEND.ESTAD.DE COMPRAS E LICITAÇÕES/RO

Ref.: Pregão Eletrônico nº 4712022

HORIZON INOVACAO E TECNOLOGIA LTDA, CNPJ nº14.497.724/0001-05, estabelecida na rua Alceu Amoroso Lima, 172, Edf. Salvador Office & Pool, 7º andar, Caminho das Árvores, CEP 41.820-770, vem interpor Contrarrazão, em relação ao pregão acima enumerado na licitação da SUPERINTEND.ESTAD.DE COMPRAS E LICITAÇÕES/RO vem apresentar, tempestivamente, suas CONTRARRAZÕES AO RECURSO ADMINISTRATIVO interposto por MICROHARD INFORMÁTICA LTDA, no Pregão Eletrônico nº 471/2022, mediante as razões de fato e direito a seguir aduzidas:

I – DA TEMPESTIVIDADE
De início, verifica-se que as contrarrazões, ora apresentadas preenchem o requisito da tempestividade, , sendo determinado o prazo de 3 (três) dias úteis para apresentação do recurso.
Assim, esta peça é tempestiva.

II – DOS FATOS Trata-se de Pregão Eletrônico instaurado pela SUPERINTEND.ESTAD.DE COMPRAS E LICITAÇÕES/RO , edital sob o número 471/2022, cujo objeto é "a escolha da proposta mais vantajosa para a Contratação pelo Licenciamento, manutenção e suporte de solução de Proteção ENDPOINT e AMBIENTES VIRTUAIS (antivírus) - por 36 meses , na modalidade de subscrição (assinatura) Conforme descrições técnicas detalhadas de acordo com o item 4 do Termo de Referência. UNIDADE: LICENÇAS. OBSERVAÇÃO: A DESCRIÇÃO DETALHADA DO ITEM ENCONTRA-SE NO TERMO DE REFERÊNCIA E SAMS.
Realizadas as fases de aceitação de proposta e lances, a empresa HORIZON INOVACAO E TECNOLOGIA LTDA restou declarada vencedora. Vale lembrar que a Recorrida venceu o pregão eletrônico com o menor preço, objetivo do sistema de registro de preço em questão, e a diferença de preço da Recorrente para a Recorrida é elevada e não vantajosa para a administração pública.
Registrada a intenção de recurso e acatada referida manifestação, a empresa Microhard informática ltda, ora Recorrente, apresentou suas alegações para ao final pleitear pela desclassificação e inabilitação da empresa HORIZON INOVACAO E TECNOLOGIA LTDA, de agora em diante denominada de Recorrida.
Inconformada com a decisão que admitiu como vencedora a empresa HORIZON INOVACAO E TECNOLOGIA LTDA, a recorrente, alega que a Recorrida não atende aos requisitos do edital.
Contudo, em que pese à indignação da empresa recorrente contra a habilitação da Horizon, o recurso não merece prosperar pelas razões a seguir apresentadas:

III- DO CUMPRIMENTO AOS REQUISITOS DO EDITAL A) Primeiramente, alega

"Isto porque se mostra cristalino o descumprimento de diversos itens do edital pela licitante Recorrida, inclusive no tocante à capacidade técnica exigida. Nesta senda, permita-se breve explanação:

Prefacialmente, cumpre destacar que a Recorrida apresentou proposta perante o Ente Licitante, desejando atender as exigências previstas em edital, informando, como solução a ser disponibilizada, aquela do "Part Number" "KL4863KAUTS","

A Recorrida é empresa idônea no mercado de tecnologia da informação, prestando serviços de implantação e treinamentos informação à aproximadamente 11 anos, e somos revendedora autorizada e certificada do fabricante.
A Recorrida apresentou atestados de capacidade técnica onde prestou serviços em características, quantidades de prazos compatíveis ao objeto desta licitação onde já finalizou a prestação de contrato.

Diante de todos os argumentos acima, resta evidente que o recurso apresentado não encontra embasamento legal ou técnico, pelo que não merece provimento.

Neste compasso a licitante HORIZON INOVACAO E TECNOLOGIA LTDA, ora recorrida, está certa de que sua proposta ofertada atende, de forma cristalina, as condições do edital e está apta a atender aos interesses da administração pública.

Senhor Pregoeiro, Equipe Técnica e demais membros desta Douta Comissão de Licitação, o Princípio da Vinculação ao Instrumento Convocatório consiste em o administrador e o administrado obedecer às regras impostas pelo Edital de Licitação, não podendo, o mesmo agir de forma diversa a estipulada pelo Instrumento Convocatório.
Desta forma, cabe ressaltar que a empresa RECORRENTE comete um equívoco, pois tenta de forma ingênua desqualificar o trabalho de avaliação das especificações técnicas realizada pela Equipe Técnica. Pois a equipe comparou as especificações técnicas do termo de referência com as documentações, enviada pela RECORRENTE e emitiu seu parecer.
Dessa forma, comprova-se mais uma vez, em que pese já haver farta documentação no sistema COMPRASNET para tanto, o pleno atendimento a todas as exigências previstas no edital e que a forma de licenciamento dos itens está em aderência a forma praticada pelo fabricante.
Assim, em sendo livre para as licitantes apresentarem uma solução que atendesse a demanda descrita no Termo de Referência, a Proposta da empresa vencedora da licitação claramente atende a todos os requisitos solicitados.

V- DO PEDIDO Diante dos fatos e fundamentos jurídicos apresentados em comum acordo com o Edital de Licitação, com a Legislação Vigente, e suas alterações, as demais normas que dispõem sobre a matéria, a empresa IMPUGNANTE, passa a requerer:

a) O indeferimento em sua totalidade do RECURSO ADMINISTRATIVO interposto pela empresa Microhard Informática Ltda, por não possuir embasamento plausível de apreciação.
b) O deferimento em sua totalidade das CONTRARRAZÕES apresentadas pela empresa HORIZON INOVACAO E TECNOLOGIA LTDA, para que a mesma seja declarada Adjudicada e Homologada no certame licitatório, garantindo assim os seus reais direitos adquiridos, prosseguindo com a fase cursiva da licitação para contratação.
c) A devida aplicação dos Princípios da Probidade Administrativa, da Legalidade, do Julgamento Objetivo e da Vinculação ao Instrumento Convocatório.

P. deferimento

Salvador 21 de outubro de 2022

HORIZON COMUNICAÇÃO E INTERATIVIDADE – EIRELI
CNPJ nº14.497.724/0001-05

Fechar

Pregão/Concorrência Eletrônica

- **Visualização de Recursos, Contrarrazões e Decisões**

INTENÇÃO DE RECURSO:

Senhor Pregoeiro, vimos manifestar nossa intenção de recorrer da decisão de declarar Vencedora a empresa HORIZON, em virtude de que a proposta da mesma não atende às exigências do edital, visto que a mesma cotou o Part Number KL4863KAUTS que não contempla todas as exigências, bem como não apresentou Atestado de Capacidade Técnica, conforme exigência. As razões serão melhor explicitadas na peça recursal. Obrigado

Fechar

Pregão/Concorrência Eletrônica

- **Visualização de Recursos, Contrarrazões e Decisões**

RECURSO :

À ILUSTRISSÍMA SRA. PREGOEIRA DA SUPERINTENDÊNCIA ESTADUAL DE LICITAÇÕES DO ESTADO DE RONDÔNIA – SUPEL/RO

PREGÃO ELETRÔNICO Nº 471/2022/ÔMEGA/SUPEL/RO

MICROHARD INFORMÁTICA LTDA., pessoa jurídica de direito privado, inscrita no CNPJ sob o nº. 42.832.691/0001-30, com sede à Rua República Argentina, nº. 520, Bairro Sion, na cidade de Belo Horizonte/MG, CEP: 30.315-490, vem, respeitosamente, a tempo e modo, pe seu representante legal, apresentar RAZÕES DE RECURSO, com supedâneo nos fundamentos a seguir aduzidos:

I – DA TEMPESTIVIDADE E CABIMENTO.

Nos termos do Edital do Pregão Eletrônico nº 471/2022, item 14 (quatorze), o prazo para apresentação das razões de recurso administrativo será de 03 (três) dias úteis, após a aceitação de intenção de recorrer previamente ofertada.

Assim sendo, para comprovar a admissibilidade recursal, faz-se imperioso aduzir que, no dia 13.10.2022 (quinta-feira), a ora Recorrente manifestou a sua intenção de interpor o presente recurso administrativo, cumprindo a determinação contida no edital.

Verifica-se do procedimento administrativo em tela que a Recorrente teve a sua intenção de recurso devidamente aceita no mesmo dia 13.10.2022, apontando-se ainda que o prazo para a Recorrente apresentar suas razões recursais iniciou-se em 14.10.2022 (sexta-feira 18.10.2022 (terça-feira).

Logo, protocolizadas as razões de recurso na presente data, resta-se evidente a tempestividade das referidas razões recursais.

II – DO BREVE RELATO DOS FATOS. DO DESCUMPRIMENTO DAS PREVISÕES EDITALÍCIAS POR PARTE DA EMPRESA HORIZON INOVAÇÃO E TECNOLOGIA LTDA.

A Superintendência Estadual de Licitações do Estado de Rondônia – SUPEL/RO deu início à licitação em apreço, figurando como interessado o Corpo de Bombeiros Militar – CBM, visando o objeto previsto no edital do pregão eletrônico nº 471/2022, qual seja:

"2.1. Do Objeto: Registro de Preços para futura e eventual contratação de Solução de Segurança Cibernética, incluindo instalação, configuração inicial, integração, treinamento, suporte técnico e garantia.

Após o início do certame na data de 11.10.2022, com a participação de 04 (quatro) licitantes interessadas, verificou-se que a empresa Horizon Inovação e Tecnologia Ltda., ora Recorrida, foi convocada a apresentar documentação exigida em edital e, posteriormente, após declarada, até então, vencedora do certame (itens 01 e 02), senão vejamos:

Item 01:
"Aceite de proposta - 13/10/2022 - 12:45:01
Aceite individual da proposta. Fornecedor: HORIZON INOVACAO E TECNOLOGIA LTDA, CNPJ/CPF: 14.497.724/0001-05, pelo melhor lance de R$ 60.000,0000 e com valor negociado a R$ 59.500,0000. Motivo: Valor negociado, conforme proposta de preços
Habilitação de fornecedor - 13/10/2022 - 12:45:45
Habilitação em grupo de propostas. Fornecedor: HORIZON INOVACAO E TECNOLOGIA LTDA -
CNPJ/CPF: 14.497.724/0001-05"

Item 02:
"Aceite de proposta - 13/10/2022 - 12:45:36
Aceite individual da proposta. Fornecedor: HORIZON INOVACAO E TECNOLOGIA LTDA, CNPJ/CPF: 14.497.724/0001-05, pelo melhor lance de R$ 14.000,0000 e com valor negociado a R$ 13.165,0000. Motivo: Valor negociado, conforme proposta de preços
Habilitação de fornecedor - 13/10/2022 - 12:45:45
Habilitação em grupo de propostas. Fornecedor: HORIZON INOVACAO E TECNOLOGIA LTDA -
CNPJ/CPF: 14.497.724/0001-05"

Contudo, após análise da documentação apresentada pela empresa Horizon Inovação e Tecnologia Ltda. resta claro, aos olhos da Recorrente, que o Ente Licitante não poderia ter aceito a proposta da empresa em comento.

Isto porque se mostra cristalino o descumprimento de diversos itens do edital pela licitante Recorrida, inclusive no tocante à capacidade técnica exigida. Nesta senda, permita-se breve explanação:

Prefacialmente, cumpre destacar que a Recorrida apresentou proposta perante o Ente Licitante, desejando atender as exigências previstas em edital, informando, como solução a ser disponibilizada, aquela do "Part Number" "KL4863KAUTS", senão vejamos trecho da proposta

"Licenciamento, manutenção e suporte de solução de Proteção ENDPOINT e AMBIENTES VIRTUAIS (antivírus) - por 36 meses. Conforme descrições técnicas detalhadas de acordo com o item 4 do Termo de Referência. Part Number KL4863KAUTS"

O referido "Part Number" refere-se à solução Kaspersky Endpoint Security for Business "SELECT", sendo que, notadamente, o produto em comento não atende diversas exigências previstas em edital, especialmente previstas como "Especificações Técnicas das Soluções (Antivírus)", quais sejam:

"1.9. Criptografia
1.9.1. Compatibilidade
1.9.1.1. Microsoft Windows 7 Ultimate SP1 ou superior x86/x64;
1.9.1.2. Microsoft Windows 7 Enterprise SP1 ou superior x86/x64;
1.9.1.3. Microsoft Windows 7 Professional SP1 ou superior x86/x64;
1.9.1.4. Microsoft Windows 8 Enterprise x86/x64;
1.9.1.5. Microsoft Windows 8 Pro x86/x64;
1.9.1.6. Microsoft Windows 8.1 Pro x86/x64;
1.9.1.7. Microsoft Windows 8.1 Enterprise x86/x64;
1.9.1.8. Microsoft Windows 10 Enterprise x86/x64;
1.9.1.9. Microsoft Windows 10 Pro x86/x64;
1.9.2. Características
1.9.2.1. 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;
1.9.2.2. Utilizar, no mínimo, algoritmo AES com chave de 256 bits;
1.9.2.3. Capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de pré-boot para autenticação do usuário;
1.9.2.4. Capacidade de utilizar Single Sign- On para a autenticação de pré-boot;
1.9.2.5. Permitir criar vários usuários de autenticação pré-boot;
1.9.2.6. Capacidade de criar um usuário de autenticação pré-boot comum com uma senha igual para todas as máquinas a partir da console de gerenciamento;
1.9.2.7. Capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções:
1.9.2.7.1. Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes;
1.9.2.7.2. Criptografar todos os arquivos individualmente;
1.9.2.7.3. Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas;
1.9.2.7.4. Criptografar o dispositivo em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha;

1.9.2.8. 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
1.9.2.9. Capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados;
1.9.2.10. Capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados;
1.9.2.11. Verifica compatibilidade de hardware antes de aplicar a criptografia;
1.9.2.12. Possibilita estabelecer parâmetros para a senha de criptografia;
1.9.2.13. Bloqueia o reuso de senhas;
1.9.2.14. Bloqueia a senha após um número de tentativas pré-estabelecidas;
1.9.2.15. Capacidade de permitir o usuário solicitar permissão a determinado arquivo criptografado para o administrador mediante templates customizados;
1.9.2.16. Permite criar exclusões para não criptografar determinados “discos rígidos” através de uma busca por nome do computador ou nome do dispositivo
1.9.2.17. Permite criptografar as seguintes pastas pré-definidas: “meus documentos”, “Favoritos”, “Desktop”, “Arquivos temporários” e “Arquivos do outlook”;
1.9.2.18. Permite utilizar variáveis de ambiente para criptografar pastas customizadas;
1.9.2.19. Capacidade de criptografar arquivos por grupos de extensão, tais como: Documentos do office, Document, arquivos de audio, etc;
1.9.2.20. Permite criar um grupo de extensões de arquivos a serem criptografados;
1.9.2.21. Capacidade de criar regra de criptografia para arquivos gerados por aplicações;
1.9.2.22. Permite criptografia de dispositivos móveis mesmo quando o endpoint não possuir comunicação com a console de gerenciamento.
1.9.2.23. Capacidade de deletar arquivos de forma segura após a criptografia;
1.9.2.24. Capacidade de criptografar somente o espaço em disco utilizado;
1.9.2.25. Deve ter a opção de criptografar arquivos criados a partir de aplicações selecionadas pelo administrador;
1.9.2.26. Capacidade de bloquear aplicações selecionadas pelo administrador de acessarem arquivos criptografados;
1.9.2.27. Deve permitir criptografar somente o espaço utilizado em dispositivos removíveis tais como pendrives, HD externo, etc;
1.9.2.28. Capacidade de criptografar discos utilizando a criptografia BitLocker da Microsoft;
1.9.2.29. Deve ter a opção de utilização de TPM para criptografia através do BitLocker;
1.9.2.30. Capacidade de fazer “Hardware encryption”;
1.10. Gerenciamento de Sistemas
1.10.1. Capacidade de criar imagens de sistema operacional remotamente e distribuir essas imagens para computadores gerenciados pela solução e para computadores bare-metal;
1.10.2. Deve possibilitar a utilização de servidores PXE na rede para deploy de imagens;
1.10.3. Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares vulneráveis;
1.10.4. 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;
1.10.5. Capacidade de gerenciar licenças de softwares de terceiros;
1.10.6. Capacidade de registrar mudanças de hardware nas máquinas gerenciadas;
1.10.7. 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;
1.10.8. Possibilita fazer distribuição de software de forma manual e agendada;
1.10.9. Suporta modo de instalação silenciosa;
1.10.10. Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis;
1.10.11. Possibilita fazer a distribuição através de agentes de atualização;
1.10.12. Utiliza tecnologia multicast para evitar tráfego na rede;
1.10.13. Possibilita criar um inventário centralizado de imagens;
1.10.14. Capacidade de atualizar o sistema operacional direto da imagem mantendo os dados do usuário;
1.10.15. Suporte a WakeOnLan para deploy de imagens;
1.10.16. Capacidade de atuar como servidor de atualização do Windows podendo fazer deploy de patches;
1.10.17. Suporta modo de teste, podendo atribuir alguns computadores para receberem as atualizações de forma automática para avaliação de alterações no comportamento;
1.10.18. Capacidade de gerar relatórios de vulnerabilidades e patches;
1.10.19. Possibilita criar exclusões para aplicação de patch por tipo de sistema operacional, Estação de trabalho e Servidor ou por grupo de administração;
1.10.20. Permite iniciar instalação de patch e correções de vulnerabilidades ao reiniciar ou desligar o computador;
1.10.21. Permite baixar atualizações para o computador sem efetuar a instalação
1.10.22. Permite o administrador instalar somente atualizações aprovadas, instalar todas as atualizações (exceto as bloqueadas) ou instalar todas as atualizações incluindo as bloqueadas;
1.10.23. Capacidade de instalar correções de vulnerabilidades de acordo com a severidade;
1.10.24. Permite selecionar produtos a serem atualizados pela console de gerenciamento;
1.10.25. Permite selecionar categorias de atualizações para serem baixadas e instaladas, tais como: atualizações de segurança, ferramentas, drivers, etc;
1.10.26. Capacidade de adicionar caminhos específicos para procura de vulnerabilidades e updates em arquivos;
1.10.27. Capacidade de instalar atualizações ou correções somente em computadores definidos, em grupos definidos ou em uma porcentagem de computadores conforme selecionado pelo administrador;
1.10.28. Capacidade de configurar o reinicio do computador após a aplicação das atualizações e correções de vulnerabilidades;
1.10.29. Deve permitir selecionar o idioma das aplicações que serão atualizadas;
1.10.30. Permitir agendar o sincronismo entre a console de gerenciamento e os sites da Microsoft para baixar atualizações recentes.
1.11. Software de segurança para ambientes virtuais:
1.11.1. O software de segurança para ambientes virtuais deve incluir:
1.11.1.1. Software antivírus sem agente para ambientes virtuais;
1.11.1.2. Software antivírus baseado em agente para ambientes virtuais;
1.11.1.3. Gerenciamento, monitoramento e atualização de software e vacinas centralizados;
1.11.1.4. Capacidade de atualizar definições de vírus e padrões de ataques;
1.11.1.5. Documentação do administrador;
1.11.1.6. Compatibilidade com a rede a ser protegida.
1.11.2. Solução deve estar de acordo com os requisitos do Regulamento Geral sobre a Proteção de Dados (GDPR) para a proteção de ambientes virtuais.
1.11.3. Solução deve possuir proteção para virtualização privada e pública (AWS e Azure).
1.11.4. Solução deve possuir console de gerenciamento única para virtualização privada e pública.
1.12. Requerimentos para o antivírus sem agente:
1.12.1. O software de antivírus sem agente para ambientes virtualizados deve funcionar com as seguintes versões do VMWARE:
1.12.1.1. Vmware ESXi 6.7 Hypervisor
1.12.1.2. Vmware ESXi 6.5 Hypervisor Update 2
1.12.1.3. VMware ESXi 6.5a Hypervisor
1.12.1.4. Update 3 VMware ESXi 6.0 Hypervisor
1.12.1.5. Update 3b VMware ESXi 5.5 Hypervisor
1.12.1.6. VMware vCenter Server 6.7.0b
1.12.1.7. VMware vCenter Server 6.5 Update 2b
1.12.1.8. VMware vCenter Server 6.5a
1.12.1.9. VMware vCenter Server 6.0 Update 3f
1.12.1.10. VMware vCenter Server 5.5 Update 3e
1.12.1.11. VMware NSX 6.3.1
1.12.1.12. VMware NSX for vSphere 6.4.1
1.12.1.13. VMware NSX para vSphere 6.3.6
1.12.1.14. VMware NSX para vSphere 6.2.6
1.12.2. Software de antivírus sem agente para ambientes virtuais deve proteger os seguintes sistemas operacionais:

1.12.2.1. Windows 10 (32 / 64-bit)
1.12.2.2. Windows 8.1 (32 / 64-bit)
1.12.2.3. Windows 8 (32 / 64-bit)
1.12.2.4. Windows 7 Service Pack 1 (32 / 64- bit)
1.12.2.5. Windows XP SP3 ou superior (32- bit)
1.12.2.6. Windows Server 2012 e 2012 R2 sem suporte a ReFS (Sistemas de Arquivos Resiliente) (64-bit)
1.12.2.7. Windows Server 2008 R2 Service Pack 1 (64-bit)
1.12.2.8. Windows Server 2003 R2 Service Pack 2 (32 / 64-bit)
1.12.2.9. Ubuntu Server 14.04 LTS (64-bit)
1.12.2.10. Red Hat Enterprise Linux Server 7 (64-bit)
1.12.2.11. SUSE Linux Enterprise Server 12 (64-bit)
1.13. O antivírus sem agente para ambientes virtuais deve prover as seguintes funcionalidades:
1.13.1. Proteção contra malware em tempo real e durante a verificação agendada sem a necessidade de qualquer agente instalado no computador convidado;
1.13.2. Integração com a tecnologia Vmware vShield Manager para proteger o sistema de arquivos do computador;
1.13.3. Integração com a tecnologia Vmware Network Extensibility SDK para prover proteção no nível de rede, implementado para monitorar e bloquear atividade maliciosa na rede bem como endereços de URL com a habilidade de notificar o usuário sobre os bloqueios efetuad
1.13.4. Possuir integração com VMware NSX;
1.13.5. Deve possuir IPS e IDS para Vmware NSX;
1.13.6. Possuir integração com as etiquetas de segurança NSX;
1.13.7. Adicionar automaticamente novas máquinas virtuais ao escopo de proteção, sem a necessidade de qualquer instalação adicional;
1.13.8. Deve automatizar a instalação se baseando em políticas de segurança identificadas pelo VMware NSX;
1.13.9. Fazer scan em máquinas virtuais mesmo desligadas;
1.13.10. Verificar os dispositivos removíveis tais como (Pendrive, Cartões, etc);
1.13.11. O produto deve permitir parar o scan após x (minutos) da inicialização da verificação;
1.13.12. O produto deve ser capaz de ser configurado até três níveis de segurança sendo eles: Recomendado, alto ou baixo;
1.13.13. Prover as seguintes opções caso encontre uma ameaça:
1.13.13.1. Escolher a ação automaticamente;
1.13.13.2. Desinfectar ou bloquear caso a desinfecção falhe;
1.13.13.3. Desinfectar ou deletar caso a desinfecção falhe;
1.13.13.4. Deletar ou bloquear caso a deleção falhe;
1.13.13.5. Bloquear;
1.13.14. A solução deve permitir configurar um tamanho máximo de um arquivo para ser verificado. Ex: Caso o arquivo compactado tenha mais de 10 MB não verificar;
1.13.15. Permitir configurar o tempo máximo de scan em um arquivo;
1.13.16. Verificar os malwares do tipo trojans, auto-dialers, adware, etc;
1.13.17. Permitir verificar drives de rede;
1.13.18. Permitir verificar todos os arquivos do sistema com a exceção dos arquivos selecionados pelo administrador;
1.13.19. Fazer a verificação dos arquivos que possuem somente as extensões definidas pelo administrador;
1.13.20. Permitir a criação de exceções por pastas ou arquivos podendo incluir subpastas;
1.13.21. Permitir a criação de perfis de políticas diferentes para cada grupo de máquinas virtuais;
1.13.22. Possuir a integração com SNMP;
1.13.23. Capacidade de bloquear ataques vindos pela rede;
1.13.24. Verificar os endereços da web por possíveis ameaças;
1.13.25. Permitir a criação de exceções para URLs que não devem ser verificadas;
1.13.26. Permitir enviar uma mensagem de bloqueio caso colaborador acesse um site malicioso;
1.13.27. Proteção baseada em nuvem contra novas ameaças, permitindo a aplicação se comunicar com a fabricante do software para poder dar um veredito a um arquivo tanto na proteção em tempo real como na verificação agendada;
1.13.28. Atualizações centralizadas no sistema com a proteção especializada para virtualização sem a necessidade de distribuir atualizações para cada máquina convidada;
1.13.29. Possibilidade de verificação sob demanda ou manual nas máquinas virtuais selecionadas;
1.13.30. Verificação de: arquivos selecionados, pastas ou todo o sistema na verificação agendada de todas as máquinas virtuais;
1.13.31. Capacidade de implementar a solução de segurança sem a necessidade de reiniciar o Hypervisor ou entrar no modo de manutenção;
1.13.32. Tecnologia que previne a verificação do mesmo arquivo mais de uma vez;
1.13.33. Prevenir múltipla verificação em arquivos iguais mesmo que estejam em máquinas virtuais diferentes;
1.13.34. Bloquear, isolar e remover os vírus notificando o usuário e o administrador;
1.13.35. Possuir uma única console de gerenciamento para todos os componentes de proteção;
1.13.36. Uma única console de gerenciamento tanto para o ambiente virtual como para o ambiente físico;
1.13.37. Capacidade de ver a estrutura de administração tanto física como lógica assim como é apresentado no Vmware vCenter;
1.13.38. Informações detalhadas sobre os eventos e tarefas de implementação nas máquinas virtuais;
1.13.39. Capacidade de aplicar configurações de segurança diferentes para cada grupo de máquinas virtuais;
1.13.40. Criar exceções pelo nome do arquivo, pelo endereço dos arquivos e pela máscara dos arquivos;
1.13.41. Permitir exportar e importar listas com exceções;
1.13.42. Crias listas com exceções frequentes de acordo com as recomendações da Microsoft;
1.13.43. Permitir verificar drives de rede conectados na máquina virtual se necessário;
1.13.44. Capacidade de excluir drives de rede do escopo de proteção;
1.13.45. Suporta o Vmware vMotion, se uma máquina é transferida de um ESXi para outro a proteção não é interrompida;
1.13.46. Criar backup de arquivos deletados pela proteção;
1.13.47. Suportar esquema de licenciamento pela quantidade de máquinas virtuais protegidas e de acordo com o número de CPU cores;
1.13.48. Componente dedicado para integração centralizada com o ambiente virtual para evitar carga no Vmware vCenter e impedir chamadas de soluções de antivírus;
1.13.49. Suporte para ativar o software utilizando um código sob subscrição;
1.13.50. Providenciar informações sobre números de objetos verificados;
1.13.51. Providenciar informações sobre detalhes da definição de antivírus;
1.13.52. Suportar verificação de certificados SSL para comunicação entre o mecanismo de antimalware, servidor de gerenciamento e Componentes de infraestrutura do VMware ;
1.13.53. Importar ou exportar a lista de exclusões e verificações nas tarefas de verificação e perfis de proteção.
1.14. Requerimentos para antivírus em ambientes virtualizados baseado em agente (conector);
1.14.1. Para ser instalado em uma infraestrutura virtualizada, um dos seguintes hypervisors devem ser instalados:
1.14.1.1. Microsoft Windows Server 2016 Hyper-V.
1.14.1.2. Microsoft Windows Server 2012 R2 Hyper-V
1.14.1.3. Citrix XenServer 7.
1.14.1.4. Citrix XenServer 7.1 LTSR.
1.14.1.5. VMware ESXi 6.7.
1.14.1.6. VMware ESXi 6.5.
1.14.1.7. VMware ESXi 6.0.
1.14.1.8. VMware ESXi 5.5.
1.14.1.9. KVM (Kernel-based Virtual Machine) com um dos seguintes sistemas operacionais:
1.4.1.9.1. Ubuntu Server 16.04 LTS.

1.4.1.9.2. Ubuntu Server 14.04 LTS.
1.4.1.9.3. Red Hat Enterprise Linux Server 7, patch 4.
1.4.1.9.4. CentOS 7.4.
1.14.1.10. Proxmox 5.0.
1.14.1.11. Proxmox 5.1
1.14.2. O Antivírus baseado em agente deve prover proteção para as máquinas virtuais no Vmware hypervisor nos seguintes sistemas operacionais:
1.14.2.1. Windows 7 Professional / Enterprise Service Pack 1 (32 / 64-bit)
1.14.2.2. Windows 8.1 Update 1 Professional
/ Enterprise (32 / 64-bit)
1.14.2.3. Windows 10 Pro / Enterprise / Enterprise LTSB / RS1 / RS2 / RS3 / RS4 (32 / 64-bit)
1.14.2.4. Windows Server 2008 R2 Service Pack 1 (64-bit)
1.14.2.5. Windows Server 2012 (64-bit)
1.14.2.6. Windows Server 2012 R2 (64-bit)
1.14.2.7. Windows Server 2016 (64-bit)
1.14.2.8. Debian GNU / Linux 8.9 (32 / 64- bit)
1.14.2.9. Debian GNU / Linux 9.1 (64-bit)
1.14.2.10. Ubuntu Server 16.04 LTS (32 / 64- bit)
1.14.2.11. Ubuntu Server 18.04 LTS (64-bit)
1.14.2.12. CentOS 6.9 (64-bit)
1.14.2.13. CentOS 7.4 (64-bit)
1.14.2.14. Red Hat Enterprise Linux Server 6.9 (64-bit)
1.14.2.15. Red Hat Enterprise Linux Server 7.4 (64-bit)
1.14.2.16. SUSE Linux Enterprise Server 12 Service Pack 1 (64-bit)
1.14.3. A Suite VMware tools deve ser instalada para prover integração entre o Hypervisor, máquinas virtuais e o conector;
1.15. O antivírus baseado em agente deve prover as seguintes funcionalidades:
1.15.1. Antivírus e monitoramento residente;
1.15.2. Proteção contra rootkits e auto dialers a sites pagos;
1.15.3. Verificação por heurística para detectar e bloquear malwares desconhecidos;
1.15.4. Transferir a verificação de malware e as tarefas intensivas para uma única máquina virtual responsável pela proteção;
1.15.5. Garantir a continuidade da proteção de arquivos durante pequenas indisponibilidades na máquina de proteção logando todas as operações de arquivos nas máquinas protegidas durante o período de indisponibilidade, e faz a verificação automática de todas alteraç
acesso;
1.15.6. Proteção baseada em nuvem contra ameaças novas, permitindo a aplicação acessar recursos especializados da fabricante para obter vereditos durante a verificação em tempo real ou agendada;
1.15.7. Deve atender HIPPA e SOX;
1.15.8. Proteção de e-mail contra malwares verificando tráfego de entrada e saída nos protocolos IMAP, SMTP, POP3, MAPI e NNTP independente do cliente de e-mail;
1.15.9. Proteção de tráfego Web: verificação de objetos enviados para os computadores dos usuários via HTTP e FTP, com a possibilidade de adicionar sites confiáveis;
1.15.10. Bloqueia banners e pop-ups nas páginas web;
1.15.11. Capacidade de detectar e bloquear sites de phishing;
1.15.12. Proteção contra ameaças não conhecidas baseadas no comportamento;
1.15.13. Capacidade de determinar comportamento anômalo de uma aplicação analisando a sequência de execução. Capacidade de reverter operações de malware durante o tratamento do arquivo;
1.15.14. Capacidade de restringir o privilégio de programas executáveis tal como escrita no registro ou acesso a arquivos e pastas. Detecção automática de nível de detecção baseado na reputação do programa;
1.15.15. O Firewall deve permitir a criação de regras para pacotes de rede em protocolos específicos (TCP, UDP) e portas;
1.15.16. Permitir a criação de regras de rede para programas específicos;
1.15.17. Proteção contra ataques de hackers utilizando o firewall com IDS/IPS e regras de atividade de rede para as aplicações mais conhecidas;
1.15.18. Criação de regras especiais para bloquear a instalação e/ou execução de uma aplicação. Deve ter a capacidade de controlar a aplicação utilizando o caminho, metadado, MD5, checksum, e categorias predefinidas de aplicações providenciadas pelo fabricante;
1.15.19. Não carregar nenhum módulo de segurança na máquina virtual e sim no appliance virtual;
1.15.20. Permitir a verificação em máquinas linux;
1.15.21. Deve ser capaz de usar o "Microsoft System Center Virtual Machine Manager" (SCVMM) para fazer deploy dos appliances virtuais;
1.15.22. Os virtuais appliances responsáveis pela verificação devem ser baseados em Linux;
1.15.23. Deve ser capaz de apresentar uma lista de máquinas virtuais que estão sob proteção de cada virtual appliance seguro.
1.15.24. Capacidade de desativar a interface local na inicialização do sistema para diminuir consumo de memória;
1.15.25. Permitir selecionar a forma de conexão ao appliance virtual de três formas diferentes:
1.5.25.1. Utilizando Multicast;
1.5.25.2. Selecionando Servidor de integração;
1.5.25.3. Utilizando uma lista de appliances virtuais.
1.15.26. Deve ser capaz de verificar vírus, worms, trojans, toolkits, adware, auto-dialers e outros tipos de ameaças em máquinas Linux;
1.15.27. Deve ser capaz de criar exclusões em máquinas linux por nome ou pasta;
1.15.28. Capacidade de verificar arquivos por formato ou extensão em máquinas Linux;
1.15.29. Permitir configurar limite de tempo de verificação em um arquivo tanto para máquinas Linux como Windows;
1.15.30. Permitir alterar o modo de scan para no mínimo três opções diferentes:
1.5.30.1. Verificação automática;
1.5.30.2. Verificar os arquivos no acesso ou na modificação;
1.5.30.3. Somente no acesso;
1.15.31. Monitorar as atividades de I/O do usuário na utilização de dispositivos externos pelo tipo de dispositivo e/ou BUS usado incluindo a capacidade de criar uma lista de dispositivos confiáveis através do ID;
1.15.32. Capacidade de garantir privilégios na utilização de dispositivos externos para usuários específicos do AD;
1.15.33. Monitorar as atividades do usuário na internet incluindo o bloqueio ou a permissão de acesso a certos recursos bem como a capacidade de bloquear certos tipos de informação (audio, video,etc);
1.15.34. Capacidade de controlar acesso na internet por horário e por usuário do AD;
1.15.35. Atualizações centralizadas permitindo que parte do banco de dados de definições seja armazenado na máquina de proteção (SVM);
1.15.36. Habilidade de executar tarefas de detecção de vulnerabilidades em aplicações instaladas nos computadores incluindo opção de submeter um relatório de qualquer vulnerabilidade encontrada;
1.15.37. Integração com o Windows Update para instalar patches de acordo com as vulnerabilidades encontradas;
1.15.38. Capacidade de instalar e distribuir remotamente componentes do antivirus em todas as máquinas protegidas sem utilização de ferramentas de terceiros;
1.15.39. Armazenar as informações de arquivos verificados para evitar um novo scan sobre o arquivo e aumentar consumo de recursos;
1.15.40. Bloquear, neutralizar e remover os malwares com a opção de notificar os administradores;
1.15.41. Console de gerenciamento única para todos os componentes de proteção;
1.15.42. Console de gerenciamento única tanto para ambientes físicos como virtuais;
1.15.43. Console única para administração de máquinas virtuais Linux e Windows
1.15.44. Provê informações detalhadas sobre os eventos e execução de tarefas;
1.15.45. Capacidade de aplicar configurações de segurança diferentes para cada grupo de máquinas virtuais;
1.15.46. Salvar o backup dos arquivos deletados;
1.15.47. Suporta as seguintes tecnologias Vmware: vMotion, Distributed resource Scheduler;
1.15.48. Suporta as seguintes tecnologias Citrix: Virtual User Drive, Citrix Receiver, Multi-stream ICA, XenMotion Live Migration, Automated VM protection and recovery, Dynamic memory control;
1.15.49. Suportar as seguintes tecnologias Hyper- V: Live migration, Cluster shared volumes, Dynamic memory, Live backup;
1.15.50. Suportar rollback do banco de dados de definições;

1.15.51. Suportar o esquema de licença de acordo com o número de máquinas virtuais protegidas e de acordo com o número de hardware CPU cores
1.15.52. Solução de File Integrity Monitoring (FIM) para Linux e Microsoft Windows que garanta a integridade dos arquivos de sistemas, logs e aplicações críticas, monitorando alterações não autorizadas em arquivos e diretórios críticos.
1.15.53. Deve incluir componente de inspeção de logs, que gere regras de inspeção de logs para eventos do Windows e permita configuração do uso de análise heurística.
1.16. Requerimentos para administração centralizada, monitoramento e update do software para ambientes virtualizados:
1.16.1. A administração centralizada, monitoramento e atualização de softwares deve funcionar em computadores executando os seguintes sistemas operacionais:
1.16.1.1. Microsoft Windows 7 Todas as edições (32/64 bits);
1.16.1.2. Microsoft Windows 8
Pro/Enterprise 32/64 bits;
1.16.1.3. Microsoft Windows 8.1
Pro/Enterprise 32/64 bits;
1.16.1.4. Microsoft Windows 10 Education RS1;
1.16.1.5. Microsoft Windows 10 Education 32/64 bits;
1.16.1.6. Microsoft Windows 10 Enterprise RS1 e Professional RS1 32/64 bits;
1.16.1.7. Microsoft Windows 10 Enterprise e Professional 32/64 bits;
1.16.1.8. Microsoft Windows Small Business Server 2008 Standard x64;
1.16.1.9. Microsoft Windows Small Business Server 2008 Premium x64;
1.16.1.10. Microsoft Windows Small Business Server 2011 Essential, Premium e Standard;
1.16.1.11. Microsoft Windows Server 2008
Todas edições 32/64 bits;
1.16.1.12. Microsoft Windows Server 2008 R2 Todas edições 32/64 bits;
1.16.1.13. Microsoft Windows Server 2012
Todas edições 32/64 bits;
1.16.1.14. Microsoft Windows Server 2012 R2 Todas edições 32/64 bits;
1.16.1.15. Microsoft Windows Server 2016
x64Banco de dados Suportados pela console de administração centralizada.
1.16.2. Microsoft SQL Server Express 2008;
1.16.3. Microsoft SQL Server Express 2008 R2;
1.16.4. Microsoft SQL Server Express 2008 R2 Service Pack 2;
1.16.5. Microsoft SQL Server 2005;
1.16.6. Microsoft SQL Server 2008;
1.16.7. Microsoft SQL Server 2008 R2;
1.16.8. Microsoft SQL Server 2012;
1.16.9. Microsoft SQL Server 2014 Todas as edições x64
1.16.10. MySQL Enterprise versions 5.0.67, 5.0.77, 5.0.85, 5.087 Service Pack 1, 5.091;
1.16.11. MySQL Enterprise versions 5.0.60
Service Pack 1, 5.0.70, 5.0.82 Service Pack 1, 5.0.90;
1.17. Requerimentos Console de administração instalada em ambientes virtualizados:
1.17.1. VmwareWorkstation 12.x Pro;
1.17.2. Microsoft Hyper-V: 2008, 2008 R2, 2012, 2012 R2
1.17.3. Microsoft Virtual PC 2007 (6.0.156.0)
1.17.4. Parallels Desktop 7 e 11;
1.17.5. Citrix XenServer 6.2 e 6.5;
1.17.6. Oracle VM VirtualBox 4.0.4-70112
1.18. O console de administração centralizada deve prover as seguintes funcionalidades:
1.18.1. Deve ser compatível com Microsoft SCVMM;
1.18.2. Capacidade de desativar a interface local do agente (conector) para diminuir uso de memória;
1.18.3. Instalação do antivírus a partir de uma única distribuição;
1.18.4. Seleção de instalação dependendo do número de pontos protegidos;
1.18.5. Capacidade de ler informações do AD para obter dados some as contas dos computadores na organização;
1.18.6. Capacidade de fazer a instalação automática através dos grupos gerenciados;
1.18.7. Capacidade de realocar computadores de acordo com endereço IP, tipo do sistema operacional e localização no AD;
1.18.8. Instalação centralizada;
1.18.9. Remoção centralizada (manual ou automática) de aplicações incompatíveis através do servidor de administração;
1.18.10. Capacidade de instalar o antivírus de diferentes formas: RPC, GPO, agente de administração;
1.18.11. Capacidade de atualizar pacotes de instalação com as últimas atualizações;
1.18.12. Atualizar de forma automática a versão do antivírus e as definições;
1.18.13. Procurar automaticamente por vulnerabilidades nas aplicações e sistemas operacionais presentes da rede;
1.18.14. Capacidade de proibir instalação/execução de aplicações;
1.18.15. Capacidade de gerenciar I/O de dispositivos externos;
1.18.16. Gerenciar a atividade do usuário na internet;
1.18.17. Capacidade de testar as atualizações antes de aplicar para o ambiente;
1.18.18. Capacidade de executar instalações automáticas baseado no sistema de proteçãod edicado, tais como: Vmware ESXi, Microsoft Hyper-V, Citrix XenServer virtualization ou hypervisor;
1.18.19. Criar os usuários baseados em RBAC;
1.18.20. Criar a hierarquia dos servidores de administração e tem capacidade de gerenciar cada um deles através de uma única console de gerenciamento;
1.18.21. Capacidade de criar servidores de administração lógicos, sem a necessidade de ter um servidor adicional para gerenciamento;
1.18.22. Distribuir automaticamente licenças nos computadores gerenciados;
1.18.23. Criar o inventário de software e hardware dos computadores gerenciados na rede;
1.18.24. Instalação centralizada de aplicações de terceiros;
1.18.25. Capacidade de eleger um computador na rede para ser responsável por atualizar outros computadores dentro da rede;
1.18.26. Capacidade de gerar relatórios gráficos;
1.18.27. Capacidade de exportar relatórios para PDF, XML e CSV;
1.18.28. Capacidade de criar contas internas para autenticar no console de administração;
1.18.29. Capacidade de criar backup de forma automática ou manual;
1.18.30. Suporta Windows Failover Clustering;
1.18.31. Console WEB para gerenciar a aplicação;
1.18.32. Sistema para controle de virus outbreak.
1.18.33. Capacidade de gerenciar permissões de administradores;
1.18.34. Capacidade de deletar atualizações já baixadas;
1.18.35. Capacidade de distribuir correções de vulnerabilidades em computadores clientes sem instalar atualizações;
1.18.36. Capacidade de eleger automaticamente um agente de atualização de acordo com uma análise de rede.
1.18.37. Capacidade de manter um histórico das alterações feitas nas políticas tanto de Linux como Windows;
1.18.38. Permite comparar alterações feitas no console de administração;

1.18.39. Deve permitir o rollback de alterações feitas nas políticas através de uma única seleção, sem ter a necessidade de restaurar item por item alterado."

Destaca-se que, quanto aos itens 1.11 até 1.18 acimados, referentes às "Especificações Técnicas das Soluções de Segurança Cibernética (Antivírus)", a proposta apresentada pela Recorrida deveria contemplar o produto "Kaspersky Hybrid Cloud" da fabricante Kaspersky, o qu incluído na proposta apresentada pela empresa Horizon Inovação e Tecnologia Ltda.

A necessidade de fornecimento do "Hybrid Cloud" se mostra cristalina, eis que foi determinada tanto pelo descritivo do edital (itens 1.11 até 1.18) quanto pela resposta emitida pelo Ente no processo SEI 0032764839 (código CRC 6F9F10B8), apontando que o Ente Licita (dezesseis) servidores, devendo os mesmos serem atendidos respeitando-se as funcionalidades em comento (https://sei.sistemas.ro.gov.br/se acao=documento_conferir&codigo_verificador=0032764839&codigo_crc=6F9F10B8&hash_download=7a22d7a18f12bdc4f5883750798f2c0dbd2a808a64bb3a2c60a219c5b6018fc34e6ec780294ac754e3d714d4539f0f9e1f3634eb15ae668ceb556cb0e5d12b64&visualizacao=1&id_

"QUESTIONAMENTO - Empresa "A" (0032692930)
"[...]
Questionamento 1: Na página 27 e na página 76 do edital, consta a quantidade de 338 licenças de antivírus. Porém, no descritivo técnico da página 38, item 1.11 (Software de segurança para ambientes virtuais) até a página 51 item 1.18.39, trata de um produto específico pa virtualizados, que requer um licenciamento específico e exige, obrigatoriamente, a informação de quantidade de licenças. Perguntamos: Quantos servidores virtualizados devem ser protegidos pela solução descrita a partir da página 38?
[...]"
RESPOSTA: A FUNESBOM, por meio da CBM-DINF, manifestou-se:
"[...]
informamos que até o exato momento possuímos apenas 16 (dezesseis) máquinas virtualizadas em 03 (três) Lâminas de servidores físicos." (Grifos nossos).

Resta, portanto, cristalino que o produto apresentado pela Recorrida (KESB SELECT Part Number KL4863KAUTS) não atende integralmente às exigências do Edital.

Ademais, Ilustre Julgadora, analisando-se a documentação apresentada pela Recorrida, verifica-se que a mesma não cumpriu o determinado em edital no tocante à capacidade técnica exigida no certame, in verbis:

"14.2.2.1. Entende-se por pertinente e compatível em característica o(s) atestado(s) que sem sua individualidade ou soma, contemplem que a licitante forneceu software antivírus, objeto do presente termo de referência, conforme o(s) item(ns) que o licitante apresentou na p
14.2.2.2. Entende-se por pertinente e compatível em quantidade o(s) atestado(s) que sem sua individualidade ou soma, contemplem que a licitante forneceu software antivírus, objeto do presente termo de referência, no mínimo 5% (cinco por cento) para o(s) item(ns) qu proposta do item 01 das especificação técnica contida neste Termo de Referência;
14.2.2.3. Entende-se por pertinente e compatível em prazo o(s) atestado(s) que sem sua individualidade ou soma de atestados concomitantes no período de execução (tendo sido os serviços atestados prestados no mesmo período) comprove com pelo ao menos 3 (três) mes que a empresa prestou ou presta satisfatoriamente serviços com características semelhantes com o objeto descrito no item 01 das especificação técnica contida neste Termo de Referência."

Nota-se que, apesar de o edital não se mostrar extremamente rigoroso no tocante à quantidade exigida para comprovação da capacidade técnica pelas licitantes interessadas, mesmo assim, a Recorrida não conseguiu comprovar o mínimo exigido no instrumento convo comprovar expertise em fornecimento de sistema de gestão administrativa, o que, notadamente, não atende o exigido em edital, demonstrando-se que a Recorrida não possui capacidade técnica para atendimento do Ente Licitante (software antivírus).

Veja Ilustre Julgadora que não são poucas as previsões editalícias não atendidas pela licitante que se sagrou vencedora do certame, até então, sendo que a ausência de capacidade técnica não pode ser ignorada pelo Ente Licitante.

Logo, apenas por estas breves digressões, já é possível concluir pela necessidade de rejeição da proposta da Recorrida, com base no que determina o princípio da vinculação ao edital, posto que esta não preencheu todos os requisitos previstos em edital.

III – DO DIREITO
III.1 – DO PRINCÍPIO DA VINCULAÇÃO AO EDITAL.

Conforme mencionado na precedência, decidiu-se por sagrar vencedora do certame, até então, a empresa Horizon Inovação e Tecnologia Ltda., em manifesto equívoco, data venia, cometido pela Ilustre Comissão de Licitação, descumprindo o previsto em edital, posto que a as exigências previstas na norma editalícia.

Nos dizeres de assentado Hely Lopes Meirelles, "a vinculação ao edital é princípio básico de toda licitação. Nem se compreenderia que a administração fixasse no edital a forma e o modo de participação dos licitantes e no decorrer do procedimento ou na realização do j estabelecido, ou admitisse documentação e propostas em desacordo com o solicitado. O edital é a lei interna da licitação, e, como tal, vincula a seus termos tantos os licitantes como a Administração que o expeliu (art. 41)." (Direito Administrativo Brasileiro. São Paulo, Malheir

No mesmo sentido é a lição de José dos Santos Carvalho Filho :

"A vinculação ao instrumento convocatório é garantia do administrador e dos administrados. Significa que as regras traçadas para o procedimento devem ser fielmente observadas por todos. Se a regra fixada não é respeitada, o procedimento se torna inválido e sus administrativa ou judicial. O princípio da vinculação tem extrema importância. Por ele, evita-se a alteração de critérios de julgamento, além de dar a certeza aos interessados do que pretende a Administração. E se evita, finalmente, qualquer brecha que provoque violação à m impessoalidade e à probidade administrativa. Se o instrumento de convocação, normalmente o edital tiver falha, pode ser corrigido, desde que oportunamente, mas os licitantes deverão ter conhecimento da alteração e a possibilidade de se amoldarem a ela. Vedado à Admin descumprimento das regras de convocação, deixando de considerar o que nele se exige, como, por exemplo, a dispensa de documento ou a fixação de preço fora dos limites estabelecidos. Em tais hipóteses, deve dar-se a desclassificação do licitante, como, de resto, impõ "(G.n.)

A respeito do princípio da vinculação ao instrumento convocatório, a Lei nº. 8.666/93 é clara ao dispor que as regras traçadas para o procedimento devem ser fielmente observadas por todos. Senão vejamos:

"Art. 41. A Administração não pode descumprir as normas e condições do edital, ao qual se acha estritamente vinculada". (G.n.)

Assim, não pode a Administração Pública simplesmente tomar uma série de medidas infringindo o edital, como no caso em tela, quando declarou como vencedora do certame empresa que, claramente, não atende todos os requisitos previstos em edital, sendo que a mesma nã técnica exigida no instrumento convocatório.

Como cediço, o Edital faz lei entre a Administração Pública e os licitantes, consoante já consolidado pela jurisprudência pátria, a saber:

"licitação – mandado de segurança – INABILITAÇÃO DA IMPETRANTE – REQUISITO EXPRESSAMENTE PREVISTO NO EDITAL – SE O EDITAL ESPECIFICOU A FORMA COMO DEVERIAM SER APRESENTADOS OS DOCUMENTOS E, MAIS, ESTABELECEU CRITÉRIO DE ACEITA EXIGIDO DA ADMINISTRAÇÃO OUTRO MODO DE ATUAÇÃO, SOB PENA DE AFRONTA AOS PRINCÍPIOS DA LEGALIDADE, DA ISONOMIA E DA VINCULAÇÃO AO EDITAL (ART. 41 DA LEI 8.666/93) – RECURSO IMPROVIDO" (Apelação Cível nº 0012683-86-2010.8.26.0562 – TJSP DJ: 01/04/2013)(G.n.)

"AGRAVO DE INSTRUMENTO. LICITAÇÃO. MODALIDADE DE CONCORRÊNCIA. TIPO TÉCNICA E PREÇO. REGIME DE EMPREITADA. LIMINAR EM MANDADO DE SEGURANÇA. PEDIDO DE SUSPENSÃO DA CONCORRÊNCIA PÚBLICA. LIMINAR EM MANDADO DE SEGURANÇA. REQU LEI 12.016/09 NÃO EVIDENCIADOS. DECISÃO AGRAVADA INALTERADA. RECURSO NÃO PROVIDO.
- Considerando que os parâmetros utilizados pela autoridade coatora para atribuição de notas referentes às propostas técnicas apresentadas pelos licitantes, não se verifica motivo que justifique o deferimento da medida liminar pretendida em Mandado de Segurança.
- Nos termos da jurisprudência do Superior Tribunal de Justiça, "princípio da vinculação ao instrumento convocatório se traduz na regra de que o edital faz lei entre as partes, devendo os seus termos serem observados até o final do certame" (REsp 354.977/SC, Rel. Ministro H Primeira Turma, DJ 9.12.2003, p. 213.).
- Ausentes os requisitos autorizadores previstos no artigo 7º, inciso III, da Lei Federal 12.016/09, deve ser indeferida a medida liminar pretendida, objetivando a suspensão da licitação na modalidade de concorrência, pelo tipo técnica e preço, devendo aguardar-se a aná Instrumento nº 1.0000.16.069412-1/001 – TJMG – Rel. Des. Moacyr Lobato, DJ: 04/05/2017)(G.n.)

"ADMINISTRATIVO. LICITAÇÃO TOMADA DE PREÇO. LEI 8.666/93. DESRESPEITO À ORDEM DE CLASSIFICAÇÃO. DESCABIMENTO DA ALEGAÇÃO DE MAIOR QUALIDADE DO SEGUNDO COLOCADO. SENTENÇA CONFIRMADA. O Edital é a lei do certame, cuja vinculação dos p Administração Pública é obrigatória, tendo que se perseguir, por certo, o cumprimento de todas as exigências e disposições nele dispostas". (TJMG. Processo n.º 1.0011.04.005607-6/001. Rel. José Domingues Ferreira Esteves. 02/09/05). (G.n).

"ADMINISTRATIVO. CONCURSO PÚBLICO. PORTADORES DE NECESSIDADES ESPECIAIS. VINCULAÇÃO AO EDITAL. NÃO COMPARECIMENTO À JUNTA MÉDICA. NEGLIGÊNCIA NO ACOMPANHAMENTO DO ANDAMENTO DO CONCURSO. NOVA OPORTUNIDADE - IMPOSSIBILIDADE.
1. A jurisprudência tem entendido que o edital do concurso é instrumento formal que regula o certame, deve ser respeitado em todas as suas regras, não podendo ser desconsiderado, sob pena de invalidação de todo o processo administrativo, especialmente se o candidato n qualquer item do edital, por força do princípio da vinculação ao instrumento convocatório e isonomia (AG 2006.01.00.040726-6, Rel. Desembargadora Federal Selene Maria de Almeida, 5ª Turma, DJ 17/05/07).2. A divulgação ou convocação de candidatos mediante publicaçã os princípios da publicidade, razoabilidade ou impessoalidade.3. Sentença confirmada.4. Apelação desprovida." (Apelação Cível nº 2009.34.00.005104-1/DF – TRF 1ª Região – Rel. Des. Federal José Amilcar Machado, DJ: 27/08/2012) (G.n.)

Na mesma linha veja a posição do STJ sobre o tema:

"RECURSO ESPECIAL. LICITAÇÃO. LEILÃO. EDITAL. PRINCÍPIO DA VINCULAÇÃO DO INSTRUMENTO CONVOCATÓRIO. EDITAL FAZ LEI ENTRE AS PARTES. - O Princípio da Vinculação ao Instrumento Convocatório se traduz na regra de que o edital faz lei entre as partes, deve observados até o final do certame, vez que vinculam as partes". (Superior Tribunal de Justiça. REsp. 354977/SC. 1ª Turma. Min. Humberto Gomes de Barros. 09/12/2003) (G.n).

Logo, com base na fundamentação precedente, pautada no instrumento convocatório e na Lei Maior das Licitações (Lei nº. 8.666/93), requer a Recorrente seja revogada a decisão que declarou vencedora do certame a Recorrida, eis que notadamente a empresa não atendeu d em edital.

IV – DOS PEDIDOS

Desta forma, haja vista os fatos e fundamentos jurídicos colacionados na precedência, pugna a Recorrente seja dado provimento ao seu recurso, para que seja revogada a decisão que declarou vencedora do certame a empresa Horizon Inovação e Tecnologia Ltda. (itens 0 várias ilegalidades verificadas e apontadas na presente peça recursal.

Nestes termos, pede deferimento.

Belo Horizonte/MG, 18 de outubro de 2022.

_____

MICROHARD INFORMÁTICA LTDA.
José Glicério Ruas Alves

Fechar

Pregão/Concorrência Eletrônica

- **Visualização de Recursos, Contrarrazões e Decisões**

CONTRARRAZÃO :

CONTRARRAZÃO : ILUSTRÍSSIMO(A) SENHOR (A) PREGOEIRO(A) DO PREGÃO ELETRÔNICO Nº 4712022 DA SUPERINTEND.ESTAD.DE COMPRAS E LICITAÇÕES/RO

Ref.: Pregão Eletrônico nº 4712022

HORIZON INOVACAO E TECNOLOGIA LTDA, CNPJ nº14.497.724/0001-05, estabelecida na rua Alceu Amoroso Lima, 172, Edf. Salvador Office & Pool, 7º andar, Caminho das Árvores, CEP 41.820-770, vem interpor Contrarrazão, em relação ao pregão acima enumerado na licitação da SUPERINTEND.ESTAD.DE COMPRAS E LICITAÇÕES/RO vem apresentar, tempestivamente, suas CONTRARRAZÕES AO RECURSO ADMINISTRATIVO interposto por MICROHARD INFORMÁTICA LTDA, no Pregão Eletrônico nº 471/2022, mediante as razões de fato e direito a seguir aduzidas:

I – DA TEMPESTIVIDADE
De início, verifica-se que as contrarrazões, ora apresentadas preenchem o requisito da tempestividade, , sendo determinado o prazo de 3 (três) dias úteis para apresentação do recurso.
Assim, esta peça é tempestiva.

II – DOS FATOS Trata-se de Pregão Eletrônico instaurado pela SUPERINTEND.ESTAD.DE COMPRAS E LICITAÇÕES/RO , edital sob o número 471/2022, cujo objeto é "a escolha da proposta mais vantajosa para a Contratação pelo Licenciamento, manutenção e suporte de solução de Proteção ENDPOINT e AMBIENTES VIRTUAIS (antivírus) - por 36 meses , na modalidade de subscrição (assinatura) Conforme descrições técnicas detalhadas de acordo com o item 4 do Termo de Referência. UNIDADE: LICENÇAS. OBSERVAÇÃO: A DESCRIÇÃO DETALHADA DO ITEM ENCONTRA-SE NO TERMO DE REFERÊNCIA E SAMS.
Realizadas as fases de aceitação de proposta e lances, a empresa HORIZON INOVACAO E TECNOLOGIA LTDA restou declarada vencedora. Vale lembrar que a Recorrida venceu o pregão eletrônico com o menor preço, objetivo do sistema de registro de preço em questão, e a diferença de preço da Recorrente para a Recorrida é elevada e não vantajosa para a administração pública.
Registrada a intenção de recurso e acatada referida manifestação, a empresa Microhard informática ltda, ora Recorrente, apresentou suas alegações para ao final pleitear pela desclassificação e inabilitação da empresa HORIZON INOVACAO E TECNOLOGIA LTDA, de agora em diante denominada de Recorrida.
Inconformada com a decisão que admitiu como vencedora a empresa HORIZON INOVACAO E TECNOLOGIA LTDA, a recorrente, alega que a Recorrida não atende aos requisitos do edital.
Contudo, em que pese à indignação da empresa recorrente contra a habilitação da Horizon, o recurso não merece prosperar pelas razões a seguir apresentadas:

III- DO CUMPRIMENTO AOS REQUISITOS DO EDITAL A) Primeiramente, alega

"Isto porque se mostra cristalino o descumprimento de diversos itens do edital pela licitante Recorrida, inclusive no tocante à capacidade técnica exigida. Nesta senda, permita-se breve explanação:

Prefacialmente, cumpre destacar que a Recorrida apresentou proposta perante o Ente Licitante, desejando atender as exigências previstas em edital, informando, como solução a ser disponibilizada, aquela do "Part Number" "KL4863KAUTS","

A Recorrida é empresa idônea no mercado de tecnologia da informação, prestando serviços de implantação e treinamentos informação à aproximadamente 11 anos, e somos revendedora autorizada e certificada do fabricante.
A Recorrida apresentou atestados de capacidade técnica onde prestou serviços em características, quantidades de prazos compatíveis ao objeto desta licitação onde já finalizou a prestação de contrato.

Diante de todos os argumentos acima, resta evidente que o recurso apresentado não encontra embasamento legal ou técnico, pelo que não merece provimento.

Neste compasso a licitante HORIZON INOVACAO E TECNOLOGIA LTDA, ora recorrida, está certa de que sua proposta ofertada atende, de forma cristalina, as condições do edital e está apta a atender aos interesses da administração pública.

Senhor Pregoeiro, Equipe Técnica e demais membros desta Douta Comissão de Licitação, o Princípio da Vinculação ao Instrumento Convocatório consiste em o administrador e o administrado obedecer às regras impostas pelo Edital de Licitação, não podendo, o mesmo agir de forma diversa a estipulada pelo Instrumento Convocatório.
Desta forma, cabe ressaltar que a empresa RECORRENTE comete um equívoco, pois tenta de forma ingênua desqualificar o trabalho de avaliação das especificações técnicas realizada pela Equipe Técnica. Pois a equipe comparou as especificações técnicas do termo de referência com as documentações, enviada pela RECORRENTE e emitiu seu parecer.
Dessa forma, comprova-se mais uma vez, em que pese já haver farta documentação no sistema COMPRASNET para tanto, o pleno atendimento a todas as exigências previstas no edital e que a forma de licenciamento dos itens está em aderência a forma praticada pelo fabricante.
Assim, em sendo livre para as licitantes apresentarem uma solução que atendesse a demanda descrita no Termo de Referência, a Proposta da empresa vencedora da licitação claramente atende a todos os requisitos solicitados.

V- DO PEDIDO Diante dos fatos e fundamentos jurídicos apresentados em comum acordo com o Edital de Licitação, com a Legislação Vigente, e suas alterações, as demais normas que dispõem sobre a matéria, a empresa IMPUGNANTE, passa a requerer:

a) O indeferimento em sua totalidade do RECURSO ADMINISTRATIVO interposto pela empresa Microhard Informática Ltda, por não possuir embasamento plausível de apreciação.
b) O deferimento em sua totalidade das CONTRARRAZÕES apresentadas pela empresa HORIZON INOVACAO E TECNOLOGIA LTDA, para que a mesma seja declarada Adjudicada e Homologada no certame licitatório, garantindo assim os seus reais direitos adquiridos, prosseguindo com a fase cursiva da licitação para contratação.
c) A devida aplicação dos Princípios da Probidade Administrativa, da Legalidade, do Julgamento Objetivo e da Vinculação ao Instrumento Convocatório.

P. deferimento

Salvador 21 de outubro de 2022

HORIZON COMUNICAÇÃO E INTERATIVIDADE – EIRELI
CNPJ nº14.497.724/0001-05

Fechar

Pregão/Concorrência Eletrônica

- **Visualização de Recursos, Contrarrazões e Decisões**

RECURSO :

À ILUSTRISSÍMA SRA. PREGOEIRA DA SUPERINTENDÊNCIA ESTADUAL DE LICITAÇÕES DO ESTADO DE RONDÔNIA – SUPEL/RO

PREGÃO ELETRÔNICO Nº 471/2022/ÔMEGA/SUPEL/RO

MICROHARD INFORMÁTICA LTDA., pessoa jurídica de direito privado, inscrita no CNPJ sob o nº. 42.832.691/0001-30, com sede à Rua República Argentina, nº. 520, Bairro Sion, na cidade de Belo Horizonte/MG, CEP: 30.315-490, vem, respeitosamente, a tempo e modo, pe seu representante legal, apresentar RAZÕES DE RECURSO, com supedâneo nos fundamentos a seguir aduzidos:

I – DA TEMPESTIVIDADE E CABIMENTO.

Nos termos do Edital do Pregão Eletrônico nº 471/2022, item 14 (quatorze), o prazo para apresentação das razões de recurso administrativo será de 03 (três) dias úteis, após a aceitação de intenção de recorrer previamente ofertada.

Assim sendo, para comprovar a admissibilidade recursal, faz-se imperioso aduzir que, no dia 13.10.2022 (quinta-feira), a ora Recorrente manifestou a sua intenção de interpor o presente recurso administrativo, cumprindo a determinação contida no edital.

Verifica-se do procedimento administrativo em tela que a Recorrente teve a sua intenção de recurso devidamente aceita no mesmo dia 13.10.2022, apontando-se ainda que o prazo para a Recorrente apresentar suas razões recursais iniciou-se em 14.10.2022 (sexta-feira 18.10.2022 (terça-feira).

Logo, protocolizadas as razões de recurso na presente data, resta-se evidente a tempestividade das referidas razões recursais.

II – DO BREVE RELATO DOS FATOS. DO DESCUMPRIMENTO DAS PREVISÕES EDITALÍCIAS POR PARTE DA EMPRESA HORIZON INOVAÇÃO E TECNOLOGIA LTDA.

A Superintendência Estadual de Licitações do Estado de Rondônia – SUPEL/RO deu início à licitação em apreço, figurando como interessado o Corpo de Bombeiros Militar – CBM, visando o objeto previsto no edital do pregão eletrônico nº 471/2022, qual seja:

"2.1. Do Objeto: Registro de Preços para futura e eventual contratação de Solução de Segurança Cibernética, incluindo instalação, configuração inicial, integração, treinamento, suporte técnico e garantia.

Após o início do certame na data de 11.10.2022, com a participação de 04 (quatro) licitantes interessadas, verificou-se que a empresa Horizon Inovação e Tecnologia Ltda., ora Recorrida, foi convocada a apresentar documentação exigida em edital e, posteriormente, após declarada, até então, vencedora do certame (itens 01 e 02), senão vejamos:

Item 01:
"Aceite de proposta - 13/10/2022 - 12:45:01
Aceite individual da proposta. Fornecedor: HORIZON INOVACAO E TECNOLOGIA LTDA, CNPJ/CPF: 14.497.724/0001-05, pelo melhor lance de R$ 60.000,0000 e com valor negociado a R$ 59.500,0000. Motivo: Valor negociado, conforme proposta de preços
Habilitação de fornecedor - 13/10/2022 - 12:45:45
Habilitação em grupo de propostas. Fornecedor: HORIZON INOVACAO E TECNOLOGIA LTDA -
CNPJ/CPF: 14.497.724/0001-05"

Item 02:
"Aceite de proposta - 13/10/2022 - 12:45:36
Aceite individual da proposta. Fornecedor: HORIZON INOVACAO E TECNOLOGIA LTDA, CNPJ/CPF: 14.497.724/0001-05, pelo melhor lance de R$ 14.000,0000 e com valor negociado a R$ 13.165,0000. Motivo: Valor negociado, conforme proposta de preços
Habilitação de fornecedor - 13/10/2022 - 12:45:45
Habilitação em grupo de propostas. Fornecedor: HORIZON INOVACAO E TECNOLOGIA LTDA -
CNPJ/CPF: 14.497.724/0001-05"

Contudo, após análise da documentação apresentada pela empresa Horizon Inovação e Tecnologia Ltda. resta claro, aos olhos da Recorrente, que o Ente Licitante não poderia ter aceito a proposta da empresa em comento.

Isto porque se mostra cristalino o descumprimento de diversos itens do edital pela licitante Recorrida, inclusive no tocante à capacidade técnica exigida. Nesta senda, permita-se breve explanação:

Prefacialmente, cumpre destacar que a Recorrida apresentou proposta perante o Ente Licitante, desejando atender as exigências previstas em edital, informando, como solução a ser disponibilizada, aquela do "Part Number" "KL4863KAUTS", senão vejamos trecho da proposta

"Licenciamento, manutenção e suporte de solução de Proteção ENDPOINT e AMBIENTES VIRTUAIS (antivírus) - por 36 meses. Conforme descrições técnicas detalhadas de acordo com o item 4 do Termo de Referência. Part Number KL4863KAUTS"

O referido "Part Number" refere-se à solução Kaspersky Endpoint Security for Business "SELECT", sendo que, notadamente, o produto em comento não atende diversas exigências previstas em edital, especialmente previstas como "Especificações Técnicas das Soluções (Antivírus)", quais sejam:

"1.9. Criptografia
1.9.1. Compatibilidade
1.9.1.1. Microsoft Windows 7 Ultimate SP1 ou superior x86/x64;
1.9.1.2. Microsoft Windows 7 Enterprise SP1 ou superior x86/x64;
1.9.1.3. Microsoft Windows 7 Professional SP1 ou superior x86/x64;
1.9.1.4. Microsoft Windows 8 Enterprise x86/x64;
1.9.1.5. Microsoft Windows 8 Pro x86/x64;
1.9.1.6. Microsoft Windows 8.1 Pro x86/x64;
1.9.1.7. Microsoft Windows 8.1 Enterprise x86/x64;
1.9.1.8. Microsoft Windows 10 Enterprise x86/x64;
1.9.1.9. Microsoft Windows 10 Pro x86/x64;
1.9.2. Características
1.9.2.1. 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;
1.9.2.2. Utilizar, no mínimo, algoritmo AES com chave de 256 bits;
1.9.2.3. Capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de pré-boot para autenticação do usuário;
1.9.2.4. Capacidade de utilizar Single Sign- On para a autenticação de pré-boot;
1.9.2.5. Permitir criar vários usuários de autenticação pré-boot;
1.9.2.6. Capacidade de criar um usuário de autenticação pré-boot comum com uma senha igual para todas as máquinas a partir da console de gerenciamento;
1.9.2.7. Capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções:
1.9.2.7.1. Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes;
1.9.2.7.2. Criptografar todos os arquivos individualmente;
1.9.2.7.3. Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas;
1.9.2.7.4. Criptografar o dispositivo em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha;

1.9.2.8. 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
1.9.2.9. Capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados;
1.9.2.10. Capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados;
1.9.2.11. Verifica compatibilidade de hardware antes de aplicar a criptografia;
1.9.2.12. Possibilita estabelecer parâmetros para a senha de criptografia;
1.9.2.13. Bloqueia o reuso de senhas;
1.9.2.14. Bloqueia a senha após um número de tentativas pré-estabelecidas;
1.9.2.15. Capacidade de permitir o usuário solicitar permissão a determinado arquivo criptografado para o administrador mediante templates customizados;
1.9.2.16. Permite criar exclusões para não criptografar determinados “discos rígidos” através de uma busca por nome do computador ou nome do dispositivo
1.9.2.17. Permite criptografar as seguintes pastas pré-definidas: “meus documentos”, “Favoritos”, “Desktop”, “Arquivos temporários” e “Arquivos do outlook”;
1.9.2.18. Permite utilizar variáveis de ambiente para criptografar pastas customizadas;
1.9.2.19. Capacidade de criptografar arquivos por grupos de extensão, tais como: Documentos do office, Document, arquivos de audio, etc;
1.9.2.20. Permite criar um grupo de extensões de arquivos a serem criptografados;
1.9.2.21. Capacidade de criar regra de criptografia para arquivos gerados por aplicações;
1.9.2.22. Permite criptografia de dispositivos móveis mesmo quando o endpoint não possuir comunicação com a console de gerenciamento.
1.9.2.23. Capacidade de deletar arquivos de forma segura após a criptografia;
1.9.2.24. Capacidade de criptografar somente o espaço em disco utilizado;
1.9.2.25. Deve ter a opção de criptografar arquivos criados a partir de aplicações selecionadas pelo administrador;
1.9.2.26. Capacidade de bloquear aplicações selecionadas pelo administrador de acessarem arquivos criptografados;
1.9.2.27. Deve permitir criptografar somente o espaço utilizado em dispositivos removíveis tais como pendrives, HD externo, etc;
1.9.2.28. Capacidade de criptografar discos utilizando a criptografia BitLocker da Microsoft;
1.9.2.29. Deve ter a opção de utilização de TPM para criptografia através do BitLocker;
1.9.2.30. Capacidade de fazer “Hardware encryption”;
1.10. Gerenciamento de Sistemas
1.10.1. Capacidade de criar imagens de sistema operacional remotamente e distribuir essas imagens para computadores gerenciados pela solução e para computadores bare-metal;
1.10.2. Deve possibilitar a utilização de servidores PXE na rede para deploy de imagens;
1.10.3. Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares vulneráveis;
1.10.4. 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;
1.10.5. Capacidade de gerenciar licenças de softwares de terceiros;
1.10.6. Capacidade de registrar mudanças de hardware nas máquinas gerenciadas;
1.10.7. 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;
1.10.8. Possibilita fazer distribuição de software de forma manual e agendada;
1.10.9. Suporta modo de instalação silenciosa;
1.10.10. Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis;
1.10.11. Possibilita fazer a distribuição através de agentes de atualização;
1.10.12. Utiliza tecnologia multicast para evitar tráfego na rede;
1.10.13. Possibilita criar um inventário centralizado de imagens;
1.10.14. Capacidade de atualizar o sistema operacional direto da imagem mantendo os dados do usuário;
1.10.15. Suporte a WakeOnLan para deploy de imagens;
1.10.16. Capacidade de atuar como servidor de atualização do Windows podendo fazer deploy de patches;
1.10.17. Suporta modo de teste, podendo atribuir alguns computadores para receberem as atualizações de forma automática para avaliação de alterações no comportamento;
1.10.18. Capacidade de gerar relatórios de vulnerabilidades e patches;
1.10.19. Possibilita criar exclusões para aplicação de patch por tipo de sistema operacional, Estação de trabalho e Servidor ou por grupo de administração;
1.10.20. Permite iniciar instalação de patch e correções de vulnerabilidades ao reiniciar ou desligar o computador;
1.10.21. Permite baixar atualizações para o computador sem efetuar a instalação
1.10.22. Permite o administrador instalar somente atualizações aprovadas, instalar todas as atualizações (exceto as bloqueadas) ou instalar todas as atualizações incluindo as bloqueadas;
1.10.23. Capacidade de instalar correções de vulnerabilidades de acordo com a severidade;
1.10.24. Permite selecionar produtos a serem atualizados pela console de gerenciamento;
1.10.25. Permite selecionar categorias de atualizações para serem baixadas e instaladas, tais como: atualizações de segurança, ferramentas, drivers, etc;
1.10.26. Capacidade de adicionar caminhos específicos para procura de vulnerabilidades e updates em arquivos;
1.10.27. Capacidade de instalar atualizações ou correções somente em computadores definidos, em grupos definidos ou em uma porcentagem de computadores conforme selecionado pelo administrador;
1.10.28. Capacidade de configurar o reinicio do computador após a aplicação das atualizações e correções de vulnerabilidades;
1.10.29. Deve permitir selecionar o idioma das aplicações que serão atualizadas;
1.10.30. Permitir agendar o sincronismo entre a console de gerenciamento e os sites da Microsoft para baixar atualizações recentes.
1.11. Software de segurança para ambientes virtuais:
1.11.1. O software de segurança para ambientes virtuais deve incluir:
1.11.1.1. Software antivírus sem agente para ambientes virtuais;
1.11.1.2. Software antivírus baseado em agente para ambientes virtuais;
1.11.1.3. Gerenciamento, monitoramento e atualização de software e vacinas centralizados;
1.11.1.4. Capacidade de atualizar definições de vírus e padrões de ataques;
1.11.1.5. Documentação do administrador;
1.11.1.6. Compatibilidade com a rede a ser protegida.
1.11.2. Solução deve estar de acordo com os requisitos do Regulamento Geral sobre a Proteção de Dados (GDPR) para a proteção de ambientes virtuais.
1.11.3. Solução deve possuir proteção para virtualização privada e pública (AWS e Azure).
1.11.4. Solução deve possuir console de gerenciamento única para virtualização privada e pública.
1.12. Requerimentos para o antivírus sem agente:
1.12.1. O software de antivírus sem agente para ambientes virtualizados deve funcionar com as seguintes versões do VMWARE:
1.12.1.1. Vmware ESXi 6.7 Hypervisor
1.12.1.2. Vmware ESXi 6.5 Hypervisor Update 2
1.12.1.3. VMware ESXi 6.5a Hypervisor
1.12.1.4. Update 3 VMware ESXi 6.0 Hypervisor
1.12.1.5. Update 3b VMware ESXi 5.5 Hypervisor
1.12.1.6. VMware vCenter Server 6.7.0b
1.12.1.7. VMware vCenter Server 6.5 Update 2b
1.12.1.8. VMware vCenter Server 6.5a
1.12.1.9. VMware vCenter Server 6.0 Update 3f
1.12.1.10. VMware vCenter Server 5.5 Update 3e
1.12.1.11. VMware NSX 6.3.1
1.12.1.12. VMware NSX for vSphere 6.4.1
1.12.1.13. VMware NSX para vSphere 6.3.6
1.12.1.14. VMware NSX para vSphere 6.2.6
1.12.2. Software de antivírus sem agente para ambientes virtuais deve proteger os seguintes sistemas operacionais:

1.12.2.1. Windows 10 (32 / 64-bit)
1.12.2.2. Windows 8.1 (32 / 64-bit)
1.12.2.3. Windows 8 (32 / 64-bit)
1.12.2.4. Windows 7 Service Pack 1 (32 / 64- bit)
1.12.2.5. Windows XP SP3 ou superior (32- bit)
1.12.2.6. Windows Server 2012 e 2012 R2 sem suporte a ReFS (Sistemas de Arquivos Resiliente) (64-bit)
1.12.2.7. Windows Server 2008 R2 Service Pack 1 (64-bit)
1.12.2.8. Windows Server 2003 R2 Service Pack 2 (32 / 64-bit)
1.12.2.9. Ubuntu Server 14.04 LTS (64-bit)
1.12.2.10. Red Hat Enterprise Linux Server 7 (64-bit)
1.12.2.11. SUSE Linux Enterprise Server 12 (64-bit)
1.13. O antivírus sem agente para ambientes virtuais deve prover as seguintes funcionalidades:
1.13.1. Proteção contra malware em tempo real e durante a verificação agendada sem a necessidade de qualquer agente instalado no computador convidado;
1.13.2. Integração com a tecnologia Vmware vShield Manager para proteger o sistema de arquivos do computador;
1.13.3. Integração com a tecnologia Vmware Network Extensibility SDK para prover proteção no nível de rede, implementado para monitorar e bloquear atividade maliciosa na rede bem como endereços de URL com a habilidade de notificar o usuário sobre os bloqueios efetuad
1.13.4. Possuir integração com VMware NSX;
1.13.5. Deve possuir IPS e IDS para Vmware NSX;
1.13.6. Possuir integração com as etiquetas de segurança NSX;
1.13.7. Adicionar automaticamente novas máquinas virtuais ao escopo de proteção, sem a necessidade de qualquer instalação adicional;
1.13.8. Deve automatizar a instalação se baseando em políticas de segurança identificadas pelo VMware NSX;
1.13.9. Fazer scan em máquinas virtuais mesmo desligadas;
1.13.10. Verificar os dispositivos removíveis tais como (Pendrive, Cartões, etc);
1.13.11. O produto deve permitir parar o scan após x (minutos) da inicialização da verificação;
1.13.12. O produto deve ser capaz de ser configurado até três níveis de segurança sendo eles: Recomendado, alto ou baixo;
1.13.13. Prover as seguintes opções caso encontre uma ameaça:
1.13.13.1. Escolher a ação automaticamente;
1.13.13.2. Desinfectar ou bloquear caso a desinfecção falhe;
1.13.13.3. Desinfectar ou deletar caso a desinfecção falhe;
1.13.13.4. Deletar ou bloquear caso a deleção falhe;
1.13.13.5. Bloquear;
1.13.14. A solução deve permitir configurar um tamanho máximo de um arquivo para ser verificado. Ex: Caso o arquivo compactado tenha mais de 10 MB não verificar;
1.13.15. Permitir configurar o tempo máximo de scan em um arquivo;
1.13.16. Verificar os malwares do tipo trojans, auto-dialers, adware, etc;
1.13.17. Permitir verificar drives de rede;
1.13.18. Permitir verificar todos os arquivos do sistema com a exceção dos arquivos selecionados pelo administrador;
1.13.19. Fazer a verificação dos arquivos que possuem somente as extensões definidas pelo administrador;
1.13.20. Permitir a criação de exceções por pastas ou arquivos podendo incluir subpastas;
1.13.21. Permitir a criação de perfis de políticas diferentes para cada grupo de máquinas virtuais;
1.13.22. Possuir a integração com SNMP;
1.13.23. Capacidade de bloquear ataques vindos pela rede;
1.13.24. Verificar os endereços da web por possíveis ameaças;
1.13.25. Permitir a criação de exceções para URLs que não devem ser verificadas;
1.13.26. Permitir enviar uma mensagem de bloqueio caso colaborador acesse um site malicioso;
1.13.27. Proteção baseada em nuvem contra novas ameaças, permitindo a aplicação se comunicar com a fabricante do software para poder dar um veredito a um arquivo tanto na proteção em tempo real como na verificação agendada;
1.13.28. Atualizações centralizadas no sistema com a proteção especializada para virtualização sem a necessidade de distribuir atualizações para cada máquina convidada;
1.13.29. Possibilidade de verificação sob demanda ou manual nas máquinas virtuais selecionadas;
1.13.30. Verificação de: arquivos selecionados, pastas ou todo o sistema na verificação agendada de todas as máquinas virtuais;
1.13.31. Capacidade de implementar a solução de segurança sem a necessidade de reiniciar o Hypervisor ou entrar no modo de manutenção;
1.13.32. Tecnologia que previne a verificação do mesmo arquivo mais de uma vez;
1.13.33. Prevenir múltipla verificação em arquivos iguais mesmo que estejam em máquinas virtuais diferentes;
1.13.34. Bloquear, isolar e remover os vírus notificando o usuário e o administrador;
1.13.35. Possuir uma única console de gerenciamento para todos os componentes de proteção;
1.13.36. Uma única console de gerenciamento tanto para o ambiente virtual como para o ambiente físico;
1.13.37. Capacidade de ver a estrutura de administração tanto física como lógica assim como é apresentado no Vmware vCenter;
1.13.38. Informações detalhadas sobre os eventos e tarefas de implementação nas máquinas virtuais;
1.13.39. Capacidade de aplicar configurações de segurança diferentes para cada grupo de máquinas virtuais;
1.13.40. Criar exceções pelo nome do arquivo, pelo endereço dos arquivos e pela máscara dos arquivos;
1.13.41. Permitir exportar e importar listas com exceções;
1.13.42. Crias listas com exceções frequentes de acordo com as recomendações da Microsoft;
1.13.43. Permitir verificar drives de rede conectados na máquina virtual se necessário;
1.13.44. Capacidade de excluir drives de rede do escopo de proteção;
1.13.45. Suporta o Vmware vMotion, se uma máquina é transferida de um ESXi para outro a proteção não é interrompida;
1.13.46. Criar backup de arquivos deletados pela proteção;
1.13.47. Suportar esquema de licenciamento pela quantidade de máquinas virtuais protegidas e de acordo com o número de CPU cores;
1.13.48. Componente dedicado para integração centralizada com o ambiente virtual para evitar carga no Vmware vCenter e impedir chamadas de soluções de antivírus;
1.13.49. Suporte para ativar o software utilizando um código sob subscrição;
1.13.50. Providenciar informações sobre números de objetos verificados;
1.13.51. Providenciar informações sobre detalhes da definição de antivírus;
1.13.52. Suportar verificação de certificados SSL para comunicação entre o mecanismo de antimalware, servidor de gerenciamento e Componentes de infraestrutura do VMware ;
1.13.53. Importar ou exportar a lista de exclusões e verificações nas tarefas de verificação e perfis de proteção.
1.14. Requerimentos para antivírus em ambientes virtualizados baseado em agente (conector);
1.14.1. Para ser instalado em uma infraestrutura virtualizada, um dos seguintes hypervisors devem ser instalados:
1.14.1.1. Microsoft Windows Server 2016 Hyper-V.
1.14.1.2. Microsoft Windows Server 2012 R2 Hyper-V
1.14.1.3. Citrix XenServer 7.
1.14.1.4. Citrix XenServer 7.1 LTSR.
1.14.1.5. VMware ESXi 6.7.
1.14.1.6. VMware ESXi 6.5.
1.14.1.7. VMware ESXi 6.0.
1.14.1.8. VMware ESXi 5.5.
1.14.1.9. KVM (Kernel-based Virtual Machine) com um dos seguintes sistemas operacionais:
1.4.1.9.1. Ubuntu Server 16.04 LTS.

1.4.1.9.2. Ubuntu Server 14.04 LTS.
1.4.1.9.3. Red Hat Enterprise Linux Server 7, patch 4.
1.4.1.9.4. CentOS 7.4.
1.14.1.10. Proxmox 5.0.
1.14.1.11. Proxmox 5.1
1.14.2. O Antivírus baseado em agente deve prover proteção para as máquinas virtuais no Vmware hypervisor nos seguintes sistemas operacionais:
1.14.2.1. Windows 7 Professional / Enterprise Service Pack 1 (32 / 64-bit)
1.14.2.2. Windows 8.1 Update 1 Professional
/ Enterprise (32 / 64-bit)
1.14.2.3. Windows 10 Pro / Enterprise / Enterprise LTSB / RS1 / RS2 / RS3 / RS4 (32 / 64-bit)
1.14.2.4. Windows Server 2008 R2 Service Pack 1 (64-bit)
1.14.2.5. Windows Server 2012 (64-bit)
1.14.2.6. Windows Server 2012 R2 (64-bit)
1.14.2.7. Windows Server 2016 (64-bit)
1.14.2.8. Debian GNU / Linux 8.9 (32 / 64- bit)
1.14.2.9. Debian GNU / Linux 9.1 (64-bit)
1.14.2.10. Ubuntu Server 16.04 LTS (32 / 64- bit)
1.14.2.11. Ubuntu Server 18.04 LTS (64-bit)
1.14.2.12. CentOS 6.9 (64-bit)
1.14.2.13. CentOS 7.4 (64-bit)
1.14.2.14. Red Hat Enterprise Linux Server 6.9 (64-bit)
1.14.2.15. Red Hat Enterprise Linux Server 7.4 (64-bit)
1.14.2.16. SUSE Linux Enterprise Server 12 Service Pack 1 (64-bit)
1.14.3. A Suite VMware tools deve ser instalada para prover integração entre o Hypervisor, máquinas virtuais e o conector;
1.15. O antivírus baseado em agente deve prover as seguintes funcionalidades:
1.15.1. Antivírus e monitoramento residente;
1.15.2. Proteção contra rootkits e auto dialers a sites pagos;
1.15.3. Verificação por heurística para detectar e bloquear malwares desconhecidos;
1.15.4. Transferir a verificação de malware e as tarefas intensivas para uma única máquina virtual responsável pela proteção;
1.15.5. Garantir a continuidade da proteção de arquivos durante pequenas indisponibilidades na máquina de proteção logando todas as operações de arquivos nas máquinas protegidas durante o período de indisponibilidade, e faz a verificação automática de todas alteraç
acesso;
1.15.6. Proteção baseada em nuvem contra ameaças novas, permitindo a aplicação acessar recursos especializados da fabricante para obter vereditos durante a verificação em tempo real ou agendada;
1.15.7. Deve atender HIPPA e SOX;
1.15.8. Proteção de e-mail contra malwares verificando tráfego de entrada e saída nos protocolos IMAP, SMTP, POP3, MAPI e NNTP independente do cliente de e-mail;
1.15.9. Proteção de tráfego Web: verificação de objetos enviados para os computadores dos usuários via HTTP e FTP, com a possibilidade de adicionar sites confiáveis;
1.15.10. Bloqueia banners e pop-ups nas páginas web;
1.15.11. Capacidade de detectar e bloquear sites de phishing;
1.15.12. Proteção contra ameaças não conhecidas baseadas no comportamento;
1.15.13. Capacidade de determinar comportamento anômalo de uma aplicação analisando a sequência de execução. Capacidade de reverter operações de malware durante o tratamento do arquivo;
1.15.14. Capacidade de restringir o privilégio de programas executáveis tal como escrita no registro ou acesso a arquivos e pastas. Detecção automática de nível de detecção baseado na reputação do programa;
1.15.15. O Firewall deve permitir a criação de regras para pacotes de rede em protocolos específicos (TCP, UDP) e portas;
1.15.16. Permitir a criação de regras de rede para programas específicos;
1.15.17. Proteção contra ataques de hackers utilizando o firewall com IDS/IPS e regras de atividade de rede para as aplicações mais conhecidas;
1.15.18. Criação de regras especiais para bloquear a instalação e/ou execução de uma aplicação. Deve ter a capacidade de controlar a aplicação utilizando o caminho, metadado, MD5, checksum, e categorias predefinidas de aplicações providenciadas pelo fabricante;
1.15.19. Não carregar nenhum módulo de segurança na máquina virtual e sim no appliance virtual;
1.15.20. Permitir a verificação em máquinas linux;
1.15.21. Deve ser capaz de usar o "Microsoft System Center Virtual Machine Manager" (SCVMM) para fazer deploy dos appliances virtuais;
1.15.22. Os virtuais appliances responsáveis pela verificação devem ser baseados em Linux;
1.15.23. Deve ser capaz de apresentar uma lista de máquinas virtuais que estão sob proteção de cada virtual appliance seguro.
1.15.24. Capacidade de desativar a interface local na inicialização do sistema para diminuir consumo de memória;
1.15.25. Permitir selecionar a forma de conexão ao appliance virtual de três formas diferentes:
1.5.25.1. Utilizando Multicast;
1.5.25.2. Selecionando Servidor de integração;
1.5.25.3. Utilizando uma lista de appliances virtuais.
1.15.26. Deve ser capaz de verificar vírus, worms, trojans, toolkits, adware, auto-dialers e outros tipos de ameaças em máquinas Linux;
1.15.27. Deve ser capaz de criar exclusões em máquinas linux por nome ou pasta;
1.15.28. Capacidade de verificar arquivos por formato ou extensão em máquinas Linux;
1.15.29. Permitir configurar limite de tempo de verificação em um arquivo tanto para máquinas Linux como Windows;
1.15.30. Permitir alterar o modo de scan para no mínimo três opções diferentes:
1.5.30.1. Verificação automática;
1.5.30.2. Verificar os arquivos no acesso ou na modificação;
1.5.30.3. Somente no acesso;
1.15.31. Monitorar as atividades de I/O do usuário na utilização de dispositivos externos pelo tipo de dispositivo e/ou BUS usado incluindo a capacidade de criar uma lista de dispositivos confiáveis através do ID;
1.15.32. Capacidade de garantir privilégios na utilização de dispositivos externos para usuários específicos do AD;
1.15.33. Monitorar as atividades do usuário na internet incluindo o bloqueio ou a permissão de acesso a certos recursos bem como a capacidade de bloquear certos tipos de informação (audio, video,etc);
1.15.34. Capacidade de controlar acesso na internet por horário e por usuário do AD;
1.15.35. Atualizações centralizadas permitindo que parte do banco de dados de definições seja armazenado na máquina de proteção (SVM);
1.15.36. Habilidade de executar tarefas de detecção de vulnerabilidades em aplicações instaladas nos computadores incluindo opção de submeter um relatório de qualquer vulnerabilidade encontrada;
1.15.37. Integração com o Windows Update para instalar patches de acordo com as vulnerabilidades encontradas;
1.15.38. Capacidade de instalar e distribuir remotamente componentes do antivirus em todas as máquinas protegidas sem utilização de ferramentas de terceiros;
1.15.39. Armazenar as informações de arquivos verificados para evitar um novo scan sobre o arquivo e aumentar consumo de recursos;
1.15.40. Bloquear, neutralizar e remover os malwares com a opção de notificar os administradores;
1.15.41. Console de gerenciamento única para todos os componentes de proteção;
1.15.42. Console de gerenciamento única tanto para ambientes físicos como virtuais;
1.15.43. Console única para administração de máquinas virtuais Linux e Windows
1.15.44. Provê informações detalhadas sobre os eventos e execução de tarefas;
1.15.45. Capacidade de aplicar configurações de segurança diferentes para cada grupo de máquinas virtuais;
1.15.46. Salvar o backup dos arquivos deletados;
1.15.47. Suporta as seguintes tecnologias Vmware: vMotion, Distributed resource Scheduler;
1.15.48. Suporta as seguintes tecnologias Citrix: Virtual User Drive, Citrix Receiver, Multi-stream ICA, XenMotion Live Migration, Automated VM protection and recovery, Dynamic memory control;
1.15.49. Suportar as seguintes tecnologias Hyper- V: Live migration, Cluster shared volumes, Dynamic memory, Live backup;
1.15.50. Suportar rollback do banco de dados de definições;

1.15.51. Suportar o esquema de licença de acordo com o número de máquinas virtuais protegidas e de acordo com o número de hardware CPU cores
1.15.52. Solução de File Integrity Monitoring (FIM) para Linux e Microsoft Windows que garanta a integridade dos arquivos de sistemas, logs e aplicações críticas, monitorando alterações não autorizadas em arquivos e diretórios críticos.
1.15.53. Deve incluir componente de inspeção de logs, que gere regras de inspeção de logs para eventos do Windows e permita configuração do uso de análise heurística.
1.16. Requerimentos para administração centralizada, monitoramento e update do software para ambientes virtualizados:
1.16.1. A administração centralizada, monitoramento e atualização de softwares deve funcionar em computadores executando os seguintes sistemas operacionais:
1.16.1.1. Microsoft Windows 7 Todas as edições (32/64 bits);
1.16.1.2. Microsoft Windows 8
Pro/Enterprise 32/64 bits;
1.16.1.3. Microsoft Windows 8.1
Pro/Enterprise 32/64 bits;
1.16.1.4. Microsoft Windows 10 Education RS1;
1.16.1.5. Microsoft Windows 10 Education 32/64 bits;
1.16.1.6. Microsoft Windows 10 Enterprise RS1 e Professional RS1 32/64 bits;
1.16.1.7. Microsoft Windows 10 Enterprise e Professional 32/64 bits;
1.16.1.8. Microsoft Windows Small Business Server 2008 Standard x64;
1.16.1.9. Microsoft Windows Small Business Server 2008 Premium x64;
1.16.1.10. Microsoft Windows Small Business Server 2011 Essential, Premium e Standard;
1.16.1.11. Microsoft Windows Server 2008
Todas edições 32/64 bits;
1.16.1.12. Microsoft Windows Server 2008 R2 Todas edições 32/64 bits;
1.16.1.13. Microsoft Windows Server 2012
Todas edições 32/64 bits;
1.16.1.14. Microsoft Windows Server 2012 R2 Todas edições 32/64 bits;
1.16.1.15. Microsoft Windows Server 2016
x64Banco de dados Suportados pela console de administração centralizada.
1.16.2. Microsoft SQL Server Express 2008;
1.16.3. Microsoft SQL Server Express 2008 R2;
1.16.4. Microsoft SQL Server Express 2008 R2 Service Pack 2;
1.16.5. Microsoft SQL Server 2005;
1.16.6. Microsoft SQL Server 2008;
1.16.7. Microsoft SQL Server 2008 R2;
1.16.8. Microsoft SQL Server 2012;
1.16.9. Microsoft SQL Server 2014 Todas as edições x64
1.16.10. MySQL Enterprise versions 5.0.67, 5.0.77, 5.0.85, 5.087 Service Pack 1, 5.091;
1.16.11. MySQL Enterprise versions 5.0.60
Service Pack 1, 5.0.70, 5.0.82 Service Pack 1, 5.0.90;
1.17. Requerimentos Console de administração instalada em ambientes virtualizados:
1.17.1. VmwareWorkstation 12.x Pro;
1.17.2. Microsoft Hyper-V: 2008, 2008 R2, 2012, 2012 R2
1.17.3. Microsoft Virtual PC 2007 (6.0.156.0)
1.17.4. Parallels Desktop 7 e 11;
1.17.5. Citrix XenServer 6.2 e 6.5;
1.17.6. Oracle VM VirtualBox 4.0.4-70112
1.18. O console de administração centralizada deve prover as seguintes funcionalidades:
1.18.1. Deve ser compatível com Microsoft SCVMM;
1.18.2. Capacidade de desativar a interface local do agente (conector) para diminuir uso de memória;
1.18.3. Instalação do antivírus a partir de uma única distribuição;
1.18.4. Seleção de instalação dependendo do número de pontos protegidos;
1.18.5. Capacidade de ler informações do AD para obter dados some as contas dos computadores na organização;
1.18.6. Capacidade de fazer a instalação automática através dos grupos gerenciados;
1.18.7. Capacidade de realocar computadores de acordo com endereço IP, tipo do sistema operacional e localização no AD;
1.18.8. Instalação centralizada;
1.18.9. Remoção centralizada (manual ou automática) de aplicações incompatíveis através do servidor de administração;
1.18.10. Capacidade de instalar o antivírus de diferentes formas: RPC, GPO, agente de administração;
1.18.11. Capacidade de atualizar pacotes de instalação com as últimas atualizações;
1.18.12. Atualizar de forma automática a versão do antivírus e as definições;
1.18.13. Procurar automaticamente por vulnerabilidades nas aplicações e sistemas operacionais presentes da rede;
1.18.14. Capacidade de proibir instalação/execução de aplicações;
1.18.15. Capacidade de gerenciar I/O de dispositivos externos;
1.18.16. Gerenciar a atividade do usuário na internet;
1.18.17. Capacidade de testar as atualizações antes de aplicar para o ambiente;
1.18.18. Capacidade de executar instalações automáticas baseado no sistema de proteçãod edicado, tais como: Vmware ESXi, Microsoft Hyper-V, Citrix XenServer virtualization ou hypervisor;
1.18.19. Criar os usuários baseados em RBAC;
1.18.20. Criar a hierarquia dos servidores de administração e tem capacidade de gerenciar cada um deles através de uma única console de gerenciamento;
1.18.21. Capacidade de criar servidores de administração lógicos, sem a necessidade de ter um servidor adicional para gerenciamento;
1.18.22. Distribuir automaticamente licenças nos computadores gerenciados;
1.18.23. Criar o inventário de software e hardware dos computadores gerenciados na rede;
1.18.24. Instalação centralizada de aplicações de terceiros;
1.18.25. Capacidade de eleger um computador na rede para ser responsável por atualizar outros computadores dentro da rede;
1.18.26. Capacidade de gerar relatórios gráficos;
1.18.27. Capacidade de exportar relatórios para PDF, XML e CSV;
1.18.28. Capacidade de criar contas internas para autenticar no console de administração;
1.18.29. Capacidade de criar backup de forma automática ou manual;
1.18.30. Suporta Windows Failover Clustering;
1.18.31. Console WEB para gerenciar a aplicação;
1.18.32. Sistema para controle de virus outbreak.
1.18.33. Capacidade de gerenciar permissões de administradores;
1.18.34. Capacidade de deletar atualizações já baixadas;
1.18.35. Capacidade de distribuir correções de vulnerabilidades em computadores clientes sem instalar atualizações;
1.18.36. Capacidade de eleger automaticamente um agente de atualização de acordo com uma análise de rede.
1.18.37. Capacidade de manter um histórico das alterações feitas nas políticas tanto de Linux como Windows;
1.18.38. Permite comparar alterações feitas no console de administração;

1.18.39. Deve permitir o rollback de alterações feitas nas políticas através de uma única seleção, sem ter a necessidade de restaurar item por item alterado."

Destaca-se que, quanto aos itens 1.11 até 1.18 acimados, referentes às "Especificações Técnicas das Soluções de Segurança Cibernética (Antivírus)", a proposta apresentada pela Recorrida deveria contemplar o produto "Kaspersky Hybrid Cloud" da fabricante Kaspersky, o qu incluído na proposta apresentada pela empresa Horizon Inovação e Tecnologia Ltda.

A necessidade de fornecimento do "Hybrid Cloud" se mostra cristalina, eis que foi determinada tanto pelo descritivo do edital (itens 1.11 até 1.18) quanto pela resposta emitida pelo Ente no processo SEI 0032764839 (código CRC 6F9F10B8), apontando que o Ente Licita (dezesseis) servidores, devendo os mesmos serem atendidos respeitando-se as funcionalidades em comento (https://sei.sistemas.ro.gov.br/se acao=documento_conferir&codigo_verificador=0032764839&codigo_crc=6F9F10B8&hash_download=7a22d7a18f12bdc4f5883750798f2c0dbd2a808a64bb3a2c60a219c5b6018fc34e6ec780294ac754e3d714d4539f0f9e1f3634eb15ae668ceb556cb0e5d12b64&visualizacao=1&id_

"QUESTIONAMENTO - Empresa "A" (0032692930)
"[...]
Questionamento 1: Na página 27 e na página 76 do edital, consta a quantidade de 338 licenças de antivírus. Porém, no descritivo técnico da página 38, item 1.11 (Software de segurança para ambientes virtuais) até a página 51 item 1.18.39, trata de um produto específico pa virtualizados, que requer um licenciamento específico e exige, obrigatoriamente, a informação de quantidade de licenças. Perguntamos: Quantos servidores virtualizados devem ser protegidos pela solução descrita a partir da página 38?
[...]"
RESPOSTA: A FUNESBOM, por meio da CBM-DINF, manifestou-se:
"[...]
informamos que até o exato momento possuímos apenas 16 (dezesseis) máquinas virtualizadas em 03 (três) Lâminas de servidores físicos." (Grifos nossos).

Resta, portanto, cristalino que o produto apresentado pela Recorrida (KESB SELECT Part Number KL4863KAUTS) não atende integralmente às exigências do Edital.

Ademais, Ilustre Julgadora, analisando-se a documentação apresentada pela Recorrida, verifica-se que a mesma não cumpriu o determinado em edital no tocante à capacidade técnica exigida no certame, in verbis:

"14.2.2.1. Entende-se por pertinente e compatível em característica o(s) atestado(s) que sem sua individualidade ou soma, contemplem que a licitante forneceu software antivírus, objeto do presente termo de referência, conforme o(s) item(ns) que o licitante apresentou na p
14.2.2.2. Entende-se por pertinente e compatível em quantidade o(s) atestado(s) que sem sua individualidade ou soma, contemplem que a licitante forneceu software antivírus, objeto do presente termo de referência, no mínimo 5% (cinco por cento) para o(s) item(ns) qu proposta do item 01 das especificação técnica contida neste Termo de Referência;
14.2.2.3. Entende-se por pertinente e compatível em prazo o(s) atestado(s) que sem sua individualidade ou soma de atestados concomitantes no período de execução (tendo sido os serviços atestados prestados no mesmo período) comprove com pelo ao menos 3 (três) mes que a empresa prestou ou presta satisfatoriamente serviços com características semelhantes com o objeto descrito no item 01 das especificação técnica contida neste Termo de Referência."

Nota-se que, apesar de o edital não se mostrar extremamente rigoroso no tocante à quantidade exigida para comprovação da capacidade técnica pelas licitantes interessadas, mesmo assim, a Recorrida não conseguiu comprovar o mínimo exigido no instrumento convo comprovar expertise em fornecimento de sistema de gestão administrativa, o que, notadamente, não atende o exigido em edital, demonstrando-se que a Recorrida não possui capacidade técnica para atendimento do Ente Licitante (software antivírus).

Veja Ilustre Julgadora que não são poucas as previsões editalícias não atendidas pela licitante que se sagrou vencedora do certame, até então, sendo que a ausência de capacidade técnica não pode ser ignorada pelo Ente Licitante.

Logo, apenas por estas breves digressões, já é possível concluir pela necessidade de rejeição da proposta da Recorrida, com base no que determina o princípio da vinculação ao edital, posto que esta não preencheu todos os requisitos previstos em edital.

III – DO DIREITO
III.1 – DO PRINCÍPIO DA VINCULAÇÃO AO EDITAL.

Conforme mencionado na precedência, decidiu-se por sagrar vencedora do certame, até então, a empresa Horizon Inovação e Tecnologia Ltda., em manifesto equívoco, data venia, cometido pela Ilustre Comissão de Licitação, descumprindo o previsto em edital, posto que a as exigências previstas na norma editalícia.

Nos dizeres de assentado Hely Lopes Meirelles, "a vinculação ao edital é princípio básico de toda licitação. Nem se compreenderia que a administração fixasse no edital a forma e o modo de participação dos licitantes e no decorrer do procedimento ou na realização do j estabelecido, ou admitisse documentação e propostas em desacordo com o solicitado. O edital é a lei interna da licitação, e, como tal, vincula a seus termos tantos os licitantes como a Administração que o expeliu (art. 41)." (Direito Administrativo Brasileiro. São Paulo, Malheir

No mesmo sentido é a lição de José dos Santos Carvalho Filho :

"A vinculação ao instrumento convocatório é garantia do administrador e dos administrados. Significa que as regras traçadas para o procedimento devem ser fielmente observadas por todos. Se a regra fixada não é respeitada, o procedimento se torna inválido e sus administrativa ou judicial. O princípio da vinculação tem extrema importância. Por ele, evita-se a alteração de critérios de julgamento, além de dar a certeza aos interessados do que pretende a Administração. E se evita, finalmente, qualquer brecha que provoque violação à m impessoalidade e à probidade administrativa. Se o instrumento de convocação, normalmente o edital tiver falha, pode ser corrigido, desde que oportunamente, mas os licitantes deverão ter conhecimento da alteração e a possibilidade de se amoldarem a ela. Vedado à Admin descumprimento das regras de convocação, deixando de considerar o que nele se exige, como, por exemplo, a dispensa de documento ou a fixação de preço fora dos limites estabelecidos. Em tais hipóteses, deve dar-se a desclassificação do licitante, como, de resto, impõ "(G.n.)

A respeito do princípio da vinculação ao instrumento convocatório, a Lei nº. 8.666/93 é clara ao dispor que as regras traçadas para o procedimento devem ser fielmente observadas por todos. Senão vejamos:

"Art. 41. A Administração não pode descumprir as normas e condições do edital, ao qual se acha estritamente vinculada". (G.n.)

Assim, não pode a Administração Pública simplesmente tomar uma série de medidas infringindo o edital, como no caso em tela, quando declarou como vencedora do certame empresa que, claramente, não atende todos os requisitos previstos em edital, sendo que a mesma nã técnica exigida no instrumento convocatório.

Como cediço, o Edital faz lei entre a Administração Pública e os licitantes, consoante já consolidado pela jurisprudência pátria, a saber:

"licitação – mandado de segurança – INABILITAÇÃO DA IMPETRANTE – REQUISITO EXPRESSAMENTE PREVISTO NO EDITAL – SE O EDITAL ESPECIFICOU A FORMA COMO DEVERIAM SER APRESENTADOS OS DOCUMENTOS E, MAIS, ESTABELECEU CRITÉRIO DE ACEITA EXIGIDO DA ADMINISTRAÇÃO OUTRO MODO DE ATUAÇÃO, SOB PENA DE AFRONTA AOS PRINCÍPIOS DA LEGALIDADE, DA ISONOMIA E DA VINCULAÇÃO AO EDITAL (ART. 41 DA LEI 8.666/93) – RECURSO IMPROVIDO" (Apelação Cível nº 0012683-86-2010.8.26.0562 – TJSP DJ: 01/04/2013)(G.n.)

"AGRAVO DE INSTRUMENTO. LICITAÇÃO. MODALIDADE DE CONCORRÊNCIA. TIPO TÉCNICA E PREÇO. REGIME DE EMPREITADA. LIMINAR EM MANDADO DE SEGURANÇA. PEDIDO DE SUSPENSÃO DA CONCORRÊNCIA PÚBLICA. LIMINAR EM MANDADO DE SEGURANÇA. REQU LEI 12.016/09 NÃO EVIDENCIADOS. DECISÃO AGRAVADA INALTERADA. RECURSO NÃO PROVIDO.
- Considerando que os parâmetros utilizados pela autoridade coatora para atribuição de notas referentes às propostas técnicas apresentadas pelos licitantes, não se verifica motivo que justifique o deferimento da medida liminar pretendida em Mandado de Segurança.
- Nos termos da jurisprudência do Superior Tribunal de Justiça, "princípio da vinculação ao instrumento convocatório se traduz na regra de que o edital faz lei entre as partes, devendo os seus termos serem observados até o final do certame" (REsp 354.977/SC, Rel. Ministro H Primeira Turma, DJ 9.12.2003, p. 213.).
- Ausentes os requisitos autorizadores previstos no artigo 7º, inciso III, da Lei Federal 12.016/09, deve ser indeferida a medida liminar pretendida, objetivando a suspensão da licitação na modalidade de concorrência, pelo tipo técnica e preço, devendo aguardar-se a aná Instrumento nº 1.0000.16.069412-1/001 – TJMG – Rel. Des. Moacyr Lobato, DJ: 04/05/2017)(G.n.)

"ADMINISTRATIVO. LICITAÇÃO TOMADA DE PREÇO. LEI 8.666/93. DESRESPEITO À ORDEM DE CLASSIFICAÇÃO. DESCABIMENTO DA ALEGAÇÃO DE MAIOR QUALIDADE DO SEGUNDO COLOCADO. SENTENÇA CONFIRMADA. O Edital é a lei do certame, cuja vinculação dos p Administração Pública é obrigatória, tendo que se perseguir, por certo, o cumprimento de todas as exigências e disposições nele dispostas". (TJMG. Processo n.º 1.0011.04.005607-6/001. Rel. José Domingues Ferreira Esteves. 02/09/05). (G.n).

"ADMINISTRATIVO. CONCURSO PÚBLICO. PORTADORES DE NECESSIDADES ESPECIAIS. VINCULAÇÃO AO EDITAL. NÃO COMPARECIMENTO À JUNTA MÉDICA. NEGLIGÊNCIA NO ACOMPANHAMENTO DO ANDAMENTO DO CONCURSO. NOVA OPORTUNIDADE - IMPOSSIBILIDADE.
1. A jurisprudência tem entendido que o edital do concurso é instrumento formal que regula o certame, deve ser respeitado em todas as suas regras, não podendo ser desconsiderado, sob pena de invalidação de todo o processo administrativo, especialmente se o candidato n qualquer item do edital, por força do princípio da vinculação ao instrumento convocatório e isonomia (AG 2006.01.00.040726-6, Rel. Desembargadora Federal Selene Maria de Almeida, 5ª Turma, DJ 17/05/07).2. A divulgação ou convocação de candidatos mediante publicaçã os princípios da publicidade, razoabilidade ou impessoalidade.3. Sentença confirmada.4. Apelação desprovida." (Apelação Cível nº 2009.34.00.005104-1/DF – TRF 1ª Região – Rel. Des. Federal José Amilcar Machado, DJ: 27/08/2012) (G.n.)

Na mesma linha veja a posição do STJ sobre o tema:

"RECURSO ESPECIAL. LICITAÇÃO. LEILÃO. EDITAL. PRINCÍPIO DA VINCULAÇÃO DO INSTRUMENTO CONVOCATÓRIO. EDITAL FAZ LEI ENTRE AS PARTES. - O Princípio da Vinculação ao Instrumento Convocatório se traduz na regra de que o edital faz lei entre as partes, deve observados até o final do certame, vez que vinculam as partes". (Superior Tribunal de Justiça. REsp. 354977/SC. 1ª Turma. Min. Humberto Gomes de Barros. 09/12/2003) (G.n).

Logo, com base na fundamentação precedente, pautada no instrumento convocatório e na Lei Maior das Licitações (Lei nº. 8.666/93), requer a Recorrente seja revogada a decisão que declarou vencedora do certame a Recorrida, eis que notadamente a empresa não atendeu d em edital.

IV – DOS PEDIDOS

Desta forma, haja vista os fatos e fundamentos jurídicos colacionados na precedência, pugna a Recorrente seja dado provimento ao seu recurso, para que seja revogada a decisão que declarou vencedora do certame a empresa Horizon Inovação e Tecnologia Ltda. (itens 0 várias ilegalidades verificadas e apontadas na presente peça recursal.

Nestes termos, pede deferimento.

Belo Horizonte/MG, 18 de outubro de 2022.

_____

MICROHARD INFORMÁTICA LTDA.
José Glicério Ruas Alves

Fechar

Pregão/Concorrência Eletrônica

- **Visualização de Recursos, Contrarrazões e Decisões**

CONTRARRAZÃO :

CONTRARRAZÃO : ILUSTRÍSSIMO(A) SENHOR (A) PREGOEIRO(A) DO PREGÃO ELETRÔNICO Nº 4712022 DA SUPERINTEND.ESTAD.DE COMPRAS E LICITAÇÕES/RO

Ref.: Pregão Eletrônico nº 4712022

HORIZON INOVACAO E TECNOLOGIA LTDA, CNPJ nº14.497.724/0001-05, estabelecida na rua Alceu Amoroso Lima, 172, Edf. Salvador Office & Pool, 7º andar, Caminho das Árvores, CEP 41.820-770, vem interpor Contrarrazão, em relação ao pregão acima enumerado na licitação da SUPERINTEND.ESTAD.DE COMPRAS E LICITAÇÕES/RO vem apresentar, tempestivamente, suas CONTRARRAZÕES AO RECURSO ADMINISTRATIVO interposto por MICROHARD INFORMÁTICA LTDA, no Pregão Eletrônico nº 471/2022, mediante as razões de fato e direito a seguir aduzidas:

I – DA TEMPESTIVIDADE
De início, verifica-se que as contrarrazões, ora apresentadas preenchem o requisito da tempestividade, , sendo determinado o prazo de 3 (três) dias úteis para apresentação do recurso.
Assim, esta peça é tempestiva.

II – DOS FATOS Trata-se de Pregão Eletrônico instaurado pela SUPERINTEND.ESTAD.DE COMPRAS E LICITAÇÕES/RO , edital sob o número 471/2022, cujo objeto é "a escolha da proposta mais vantajosa para a Contratação pelo Licenciamento, manutenção e suporte de solução de Proteção ENDPOINT e AMBIENTES VIRTUAIS (antivírus) - por 36 meses , na modalidade de subscrição (assinatura) Conforme descrições técnicas detalhadas de acordo com o item 4 do Termo de Referência. UNIDADE: LICENÇAS. OBSERVAÇÃO: A DESCRIÇÃO DETALHADA DO ITEM ENCONTRA-SE NO TERMO DE REFERÊNCIA E SAMS.
Realizadas as fases de aceitação de proposta e lances, a empresa HORIZON INOVACAO E TECNOLOGIA LTDA restou declarada vencedora. Vale lembrar que a Recorrida venceu o pregão eletrônico com o menor preço, objetivo do sistema de registro de preço em questão, e a diferença de preço da Recorrente para a Recorrida é elevada e não vantajosa para a administração pública.
Registrada a intenção de recurso e acatada referida manifestação, a empresa Microhard informática ltda, ora Recorrente, apresentou suas alegações para ao final pleitear pela desclassificação e inabilitação da empresa HORIZON INOVACAO E TECNOLOGIA LTDA, de agora em diante denominada de Recorrida.
Inconformada com a decisão que admitiu como vencedora a empresa HORIZON INOVACAO E TECNOLOGIA LTDA, a recorrente, alega que a Recorrida não atende aos requisitos do edital.
Contudo, em que pese à indignação da empresa recorrente contra a habilitação da Horizon, o recurso não merece prosperar pelas razões a seguir apresentadas:

III- DO CUMPRIMENTO AOS REQUISITOS DO EDITAL A) Primeiramente, alega

"Isto porque se mostra cristalino o descumprimento de diversos itens do edital pela licitante Recorrida, inclusive no tocante à capacidade técnica exigida. Nesta senda, permita-se breve explanação:

Prefacialmente, cumpre destacar que a Recorrida apresentou proposta perante o Ente Licitante, desejando atender as exigências previstas em edital, informando, como solução a ser disponibilizada, aquela do "Part Number" "KL4863KAUTS","

A Recorrida é empresa idônea no mercado de tecnologia da informação, prestando serviços de implantação e treinamentos informação à aproximadamente 11 anos, e somos revendedora autorizada e certificada do fabricante.
A Recorrida apresentou atestados de capacidade técnica onde prestou serviços em características, quantidades de prazos compatíveis ao objeto desta licitação onde já finalizou a prestação de contrato.

Diante de todos os argumentos acima, resta evidente que o recurso apresentado não encontra embasamento legal ou técnico, pelo que não merece provimento.

Neste compasso a licitante HORIZON INOVACAO E TECNOLOGIA LTDA, ora recorrida, está certa de que sua proposta ofertada atende, de forma cristalina, as condições do edital e está apta a atender aos interesses da administração pública.

Senhor Pregoeiro, Equipe Técnica e demais membros desta Douta Comissão de Licitação, o Princípio da Vinculação ao Instrumento Convocatório consiste em o administrador e o administrado obedecer às regras impostas pelo Edital de Licitação, não podendo, o mesmo agir de forma diversa a estipulada pelo Instrumento Convocatório.
Desta forma, cabe ressaltar que a empresa RECORRENTE comete um equívoco, pois tenta de forma ingênua desqualificar o trabalho de avaliação das especificações técnicas realizada pela Equipe Técnica. Pois a equipe comparou as especificações técnicas do termo de referência com as documentações, enviada pela RECORRENTE e emitiu seu parecer.
Dessa forma, comprova-se mais uma vez, em que pese já haver farta documentação no sistema COMPRASNET para tanto, o pleno atendimento a todas as exigências previstas no edital e que a forma de licenciamento dos itens está em aderência a forma praticada pelo fabricante.
Assim, em sendo livre para as licitantes apresentarem uma solução que atendesse a demanda descrita no Termo de Referência, a Proposta da empresa vencedora da licitação claramente atende a todos os requisitos solicitados.

V- DO PEDIDO Diante dos fatos e fundamentos jurídicos apresentados em comum acordo com o Edital de Licitação, com a Legislação Vigente, e suas alterações, as demais normas que dispõem sobre a matéria, a empresa IMPUGNANTE, passa a requerer:

a) O indeferimento em sua totalidade do RECURSO ADMINISTRATIVO interposto pela empresa Microhard Informática Ltda, por não possuir embasamento plausível de apreciação.
b) O deferimento em sua totalidade das CONTRARRAZÕES apresentadas pela empresa HORIZON INOVACAO E TECNOLOGIA LTDA, para que a mesma seja declarada Adjudicada e Homologada no certame licitatório, garantindo assim os seus reais direitos adquiridos, prosseguindo com a fase cursiva da licitação para contratação.
c) A devida aplicação dos Princípios da Probidade Administrativa, da Legalidade, do Julgamento Objetivo e da Vinculação ao Instrumento Convocatório.

P. deferimento

Salvador 21 de outubro de 2022

HORIZON COMUNICAÇÃO E INTERATIVIDADE – EIRELI
CNPJ nº14.497.724/0001-05

Fechar