PROCESSO : 0007345-36.2020.6.12.8000

INTERESSADO : SEÇÃO DE GESTÃO DE ATIVOS DE TECNOLOGIA DA INFORMAÇÃO

ASSUNTO : Decisão de recurso

Decisão nº 8 / 2021 - TRE/PREGOEIRO

Trata-se de procedimento licitatório, na modalidade pregão, em sua forma eletrônica, que tem por objeto contratação de uma solução de software para gerenciamento de eventos e logs de segurança da informação (SIEM - Security Information and Event Management) com suporte e atualização.

DA SESSÃO PÚBLICA

A sessão pública relativa ao Pregão 29/2021, conduzida pela Pregoeira Érika Murackami Duarte da Rosa, teve início em 18/11/2021 e foi operacionalizada no sítio do Portal de Compras do Governo Federal (Comprasnet).

Durante a sessão, foram analisadas as propostas, seguindo a ordem de classificação, e verificada a documentação de habilitação da empresa cuja proposta foi aceita. Ao final da sessão, foi habilitada a empresa ATA COMÉRCIO E SERVIÇOS DE INFORMÁTICA LTDA., conforme registrado na ata da sessão pública e no Resultado por Fornecedor.

Concluída a fase de habilitação e após aberto o prazo, houve interposição de intenção de recurso por parte de duas empresas:

1. NIVA TECNOLOGIA DA INFORMAÇÃO LTDA., nos seguintes termos: "Sr. Pregoeiro, manifestamos intenção de recursos por motivo de vícios no processo que serão abordados detalhadamente na peça recursal apresentada. "

2. TELETEX COMPUTADORES E SISTEMAS LTDA., nos seguintes termos: "Manifestamos intenção de recurso contra a decisão que declarou vencedora a empresa ATA COMÉRCIO, por não atenderem aos subitens 1, 3, 6 e 8 do item 12 - Especificação Técnica da Solução, conforme Termo de Referência. Esta manifestação é realizada com fulcro no Acórdão 339/2010 TCU, o qual recomenda a não rejeição das intenções de recursos."

As mencionadas intenções de recurso foram aceitas pela Pregoeira Erika Murackami Duarte da Rosa, na medida em estavam presentes todos os pressupostos recursais, conforme consta abaixo:

> "Verificada a existência de todos os pressupostos recursais na manifestação registrada (quais sejam: sucumbência, legitimidade, tempestividade, motivo e interesse de agir), aceito a intenção de recurso."

Desta forma, foram abertos os prazos para apresentação das razões/contrarrazões/decisão:

Data limite para registro de recurso: 29/11/2021.

Data limite para registro de contrarrazão: 02/12/2021.

Data limite para registro de decisão: 10/12/2021.

DAS RAZÕES DO RECURSO

Primeiramente, cabe registrar que a empresa NIVA TECNOLOGIA DA INFORMAÇÃO LTDA. não encaminhou as razões do recurso. Considerando que na intenção de recurso, a referida empresa apenas alegou vícios no processo, não trazendo maiores detalhes para análise, esta Pregoeira não tem nada a manifestar acerca da intenção de recurso registrada.

No tocante à empresa TELETEX COMPUTADORES E SISTEMAS LTDA., as razões foram encaminhadas tempestivamente, pelo sistema comprasnet.

Em suas razões (1127273), de forma resumida, a empresa alega que o produto ofertado não atende a todas as especificações do Termo de Referência:

> [...]
>
> 2.1. DA INOBSERVÂNCIA DE REQUISITOS ESSENCIAIS DA PROPOSTA COMERCIAL – VIOLAÇÃO À EXIGÊNCIA DISPOSTA NO ITEM 2. DO CAPÍTULO IV DO TERMO DE REFERÊNCIA. O Item 2, do Capítulo IV, do Termo de Referência, dispõe sobre as especificações técnicas do objeto licitado e exige, segundo subitem 12.1. que a solução de software para gerenciamento de eventos e

> logs de segurança da informação (SIEM – Security Information and Event Management) com suporte e atualização, deva ser capaz de coletar, no mínimo, os logs dos sistemas e ativos Firewalls: Checkpoint R80.x, VMWare NSX, PfSense; Ocorre que a documentação apresentada pela Recorrida não observa, na integralidade, as exigências técnicas previstas no instrumento convocatório, vez que não comprova suporte para NSX e Pfsense. Por sua vez, quanto ao subitem 12.3 do mesmo item, acima mencionado, exige-se que a solução seja capaz de coletar, no mínimo, os logs dos sistemas e ativos de Plataformas de Virtualização: VMware ESX, HyperV, Acropolis/KVM e Oracle VM. Vejamos o que o Termo de Referencia exige: 12. Ser capaz de coletar, no mínimo, os logs dos sistemas e ativos listado abaixo: Firewalls: Checkpoint R80.x, VMWare NSX, PfSense; Switches: HPE e Aruba; Plataformas de Virtualização: VMware ESX, HyperV, Acropolis/KVM e Oracle VM; Sistemas Operacionais: Linux (Debian, RedHat, Ubuntu, CentOs, Oracle Linux), Windows Server (2008, 2012, 2016) e FreeBSD; Antivirus: TrendMicro, Clamav; Servidores de E-mail: Zimbra e Microsoft Exchange; Servidores de Aplicação e Web: Apache2, Squid, Nginx, HAProxy, Apache Tomcat, Jboss e MicroSoft IIS7 (ou superior); VPN: OpenVPN; Porém, de acordo com a documentação apresentada pela Recorrida, não há comprovação sobre o suporte da solução para KVM e Oracle VM, expressamente exigidos no instrumento convocatório. Por fim, quanto ao subitem 12.8 do mesmo item, acima mencionado, exige-se que a solução seja capaz de coletar, no mínimo, os logs dos sistemas e ativos VPN: OpenVPN. Contudo, a documentação apresentada pela Recorrida não comprova que a solução possui suporte para Open VPN. A Recorrida teria comprovado o atendimento a todos os itens apresentando o arquivo "6.3 - ArcSight Connector Supported Products.pdf", referenciando página 2, 4 e 6 que não trazem suporte a KVM, Oracle VM e OpenVPN. Assim sendo, a proposta apresentada pela Recorrida não atende a critérios técnicos mínimos exigidos pelo instrumento convocatório, sendo, portanto, latente a violação aos subitens 12.1, 12.3 e 12.8 do Item 2, Capítulo IV do Termo de Referência, o que torna a classificação da proposta da Recorrida nula e contraria, inclusive, disposição do próprio Edital [...]

Por fim, a Recorrente requer o total provimento das razões apresentadas, e requer seja reformada a decisão que classificou a proposta da empresa Ata Comercio e Serviços de Informática Ltda., a fim de que a mesma seja desclassificada, nos termos da fundamentação

DAS CONTRARRAZÕES DO RECURSO

A recorrida, em suas contrarrazões do recurso alega, em síntese, que:

> [...] é importante indicar alguns equívocos contidos no recurso interposto pela licitante TELETEX COMPUTADORES E SISTEMAS LTDA.. Na análise realizada, a licitante levou em consideração apenas o ponto a ponto e suas referências, quando este documento não é obrigatório segundo o edital, e foi apresentado apenas para servir de roteiro e indicações para análise de todo conteúdo enviado. [..]
>
> Informa ainda, que foram encaminhadas 7 pastas, contendo 266 arquivos, que deveriam ser utilizados na análise das especificações do produto ofertado.

Ao final, requer que seja mantida a decisão que declarou a empresa ATA COMÉRCIO E SERVIÇOS DE INFORMÁTICA LTDA., vencedora da licitação.

DO JULGAMENTO DO MÉRITO DO RECURSO

Antes de analisar o mérito do recurso, cumpre registrar que a unidade demandante ao analisar a proposta da empresa Ata Comércio e Serviços de Informática Ltda., solicitou a complementação das informações, conforme registrado na ata da sessão pública:

> [...] o link encaminhado para conferência dos requisitos não contém a maioria das informações necessárias para análise, trata-se de link genérico, onde, mesmo entrando nos diversos documentos ali constantes, se mostrou inviável a verificação de todas as informações.
>
> Sendo assim, solicito o encaminhamento de documentos complementares, como folders, catálogos, documentos do fabricante ou até mesmo outros links (desde que mais específicos e direcionados para a informação necessária), podendo indicar, inclusive o número da página caso o documento seja muito extenso onde possa ser verificado as especificações técnicas da solução.

Em resposta, a recorrida encaminhou pelo sistema de anexos do comprasnet 07 (sete) pastas contendo arquivos diversos, sobre a especificação do item.

Tais documentos foram enviados a unidade demandante, que após análise, manifestou pelo aceite do produto ofertado.

Cumpre registrar, que tais documentos foram disponibilizados na página deste Tribunal, para consulta pelos interessados.

Posto isto, passaremos a análise do mérito do recurso que, por se tratar de questão técnica, foi analisado pela unidade demandande:

> "Senhora Pregoeira, Sônia!
>
> A empresa TELETEX Computadores e Sistemas Ltda apresentou recurso contra a vencedora do Pregão nº 29/2021 que visa a aquisição de uma ferramenta de SIEM. Seguem abaixo, os itens apontados no recurso e a resposta da empresa ATA Comércio e Serviços de Informática Ltda aos questionamentos:
>
> TELETEX
>
> - 12.1. que a solução de software para gerenciamento de eventos e logs de segurança da informação (SIEM – Security Information and Event Management) com suporte e atualização, deva ser capaz de coletar, no mínimo, os logs dos sistemas e ativos Firewalls: Checkpoint R80.x, VMWare NSX, PfSense;
>
> Ocorre que a documentação apresentada pela Recorrida não observa, na integralidade, as exigências técnicas previstas no instrumento convocatório, vez que não comprova suporte para NSX e Pfsense.
>
> RESPOSTA ATA
>
> 12.1. Firewalls: VMWare NSX
>
> Abaixo estamos apresentando o código do Smart Connectors existente para coleta de VMWare, que se encontra disponível na comunidade do ArcSight um Flex Connector para coleta de eventos do VMWare NSX, e transcrito abaixo:
>
> # FlexAgent Regex Configuration File do.unparsed.events=true
>
> regex=[^bhcorp]*(\w+)\.bhcorp\.ad (dfwpktlogs) [^INET]*(INET|INET6) (\S+) (.*) token.count=5
>
> token[0].name=hostname token[0].type=String
> token[1].name=custString1 token[1].type=String
> token[2].name=custom2 token[2].type=String
> token[3].name=Message token[3].type=String
> token[4].name=message token[4].type=String
> submessage.messageid.token=Message
> submessage.token=message event.name=Message
> event.deviceHostName=hostname
> event.deviceCustomString1=custString1 event.message=message
> event.deviceCustomString2=custom2
>
> event.deviceVendor= stringConstant(VMWare)
> event.deviceProduct= stringConstant(NSX) #l10n.filename.prefix=
>
> submessage.count=2 submessage[0].messageid=match
> submessage[0].pattern.count=3
>
> submessage[0].pattern[0].regex=(\w+) (domain\-\S+) (\w+) (\d+) (\w+) (\d+\.\d+\.\d+\.\d+|[^/]*)\/(\d+)\-
>
> >(\d+\.\d+\.\d+\.\d+|[^/]*)\/(\d+)
> submessage[0].pattern[0].fields=event.deviceAction,event.deviceCustomString4,event.deviceOutboundInterface,event.bytesIn,
> event.transportProtocol,event.sourceAddress,event.sourcePort,event.destinationAddress,event.destinationPort
> submessage[0].pattern[1].regex=(\w+) (domain\-\S+) (\w+) (\d+)
> (\w+) (\d+\.\d+\.\d+\.\d+)\/(\d+)\-
>
> >(\d+\.\d+\.\d+\.\d+)\/(\d+) (\S+)
> submessage[0].pattern[1].fields=event.deviceAction,event.deviceCustomString3,event.deviceOutboundInterface,event.bytesIn,
> event.transportProtocol,event.sourceAddress,event.sourcePort,event.destinationAddress,event.destinationPort,event.deviceCust
> omString4
>
> submessage[0].pattern[2].regex=(\w+) (domain\-\S+) (\w+) (\d+)
> PROTO (\d+) (\d+\.\d+\.\d+\.\d+)\-
>
> >(\d+\.\d+\.\d+\.\d+)
> submessage[0].pattern[2].fields=event.deviceAction,event.deviceCustomString4,event.deviceOutboundInterface,event.bytesIn,
> event.transportProtocol,event.sourceAddress,event.destinationAddress
>
> submessage[1].messageid=TERM
>
> submessage[1].pattern.count=2
>
> submessage[1].pattern[0].regex=(domain\-\S+) (\w+) (\w+) (\d+\.\d+\.\d+\.\d+|[^/]*)\/(\d+)\-
>
> >(\d+\.\d+\.\d+\.\d+|[^/]*)\/(\d+) (\d+\/\d+ \d+\/\d+)
> submessage[1].pattern[0].fields=event.deviceCustomString3,event.deviceOutboundInterface,event.transportProtocol,event.sour
> ceAddress,event.sourcePort,event.destinationAddress,event.destinationPort,event.deviceCustomString4
> submessage[1].pattern[1].regex=(domain\-\S+) (\w+) PROTO
> (\d+) (\d+\.\d+\.\d+\.\d+)\-
>
> >(\d+\.\d+\.\d+\.\d+) (\d+\/\d+) (\d+\/\d+)
> submessage[1].pattern[1].fields=event.deviceCustomString4,event.deviceOutboundInterface,event.transportProtocol,event.sour
> ceAddress,event.destinationAddress,event.deviceCustomString5,event.deviceCustomString6
>
> 12.1. Firewalls: PfSense
>
> O pfSense é um firewall open source, licenciado sob BSD license, baseado no sistema operacional FreeBSD e adaptado para assumir o papel de um firewall e/ou roteador de redes. O nome deriva do fato que o software utiliza a tecnologia packet- filtering.

Como uma variação do Linux FreeBSD, o PfSense não é citado na lista de connectors, pois utiliza mesmo padrão de log do FreeBSD, e a interpretação desses logs para o armazenamento, policiais e Correlacionamento utiliza o flexconnector do Linux.

Como é uma adaptação do sistema operacional FreeBSD, o conector do sistema operacional sobrepõe o do pfSense.

TELETEX

Por sua vez, quanto ao subitem 12.3 do mesmo item, acima mencionado, exige-se que a solução seja capaz de coletar, no mínimo, os logs dos sistemas e ativos de Plataformas de Virtualização: VMware ESX, HyperV, Acropolis/KVM e Oracle VM. Vejamos o que o Termo de Referencia exige:

12. Ser capaz de coletar, no mínimo, os logs dos sistemas e ativos listado abaixo:Firewalls: Checkpoint R80.x, VMWare NSX, PfSense;

Switches: HPE e Aruba;

Plataformas de Virtualização: VMware ESX, HyperV, Acropolis/KVM e Oracle VM;

Sistemas Operacionais: Linux (Debian, RedHat, Ubuntu, CentOs, Oracle Linux), Windows Server (2008, 2012, 2016) e FreeBSD; Antivirus: TrendMicro, Clamav;

Servidores de E-mail: Zimbra e Microsoft Exchange;

Servidores de Aplicação e Web: Apache2, Squid, Nginx, HAProxy, Apache Tomcat, Jboss e MicroSoft IIS7 (ou superior); VPN: OpenVPN;

RESPOSTA ATA

12.3. Plataformas de Virtualização: Acropolis/KVM

Conforme documentação do fabricante Nutanix sobre a solução Acropolis para hiperconvergência a forma de envio de logs para um sistema remoto (syslog) e/ou um SIEM é através da configuração de rsyslog via CLI (link de referência: https://portal.nutanix.com/page/documents/kbs/details?targetId=kA00e0000009CEECA2)

Na base de conhecimento não é citado nenhum tipo específico de SIEM ou solução de syslog para recebimento, assim, apenas um syslog e rsyslog, sendo assim, inferindo que qualquer sistema que coleta eventos via syslog é capaz de interpretar suas mensagens.

O documento também informa que diversos módulos podem ser configurados para envio via syslogs entre eles o módulo ACROPOLIS.

5. Choose a module to forward log information from and specify the level of information to collect.

```
<ncli> rsyslog-config add-module server-name=<remote_server_name> module-name=<module_name> level=<log_level>
```

Replace <module_name> with one of the following:

- ACROPOLIS - The acropolis services are responsible for task scheduling, execution, stat collection, publishing, etc. For more information, see Acropolis Services in the Nutanix Bible.

Por se tratar de mensagens usando o padrão genérico utiliza os níveis padrão de um Syslog: INFO, EMERGENCY, ALERT, CRITICAL, ERROR, WARNING e NOTICE. Também é disponibilizado um exemplo de mensagem que pode ser coletada:

For example, if you set level to INFO, it also covers the levels above it (i.e. EMERGENCY, ALERT, CRITICAL, ERROR, WARNING and NOTICE). If you select INFO for a module, you do not have to select any of the levels above it for the same module.

Note: CVMs send system audit logs to the syslog server by default even when no modules are configured for the server. Below is an example of these audit logs:

```
2021-09-09T08:56:01.353708-05:00 ntnx-xxx-cvm audispd[5307]: node=ntnx-xxx-cvm type=PROCTITLE msg=audit(1631195761.351:193118):
proctitle=2F7573722F62696E2F707974686F6E322E37002D42002F686F6D652F6E7574616E69782F7365727669636565162696C6974792F62696E2F7573696E672D67666C616773002F6
6E7574616E69782F7365727669636565162696C6974792F62696E2F63726F6E5F7365727669636565162696C6974792E7079
```

Sendo assim, por se tratar de um Syslog padrão o Microfocus ArcSight pode utilizar o Smart Connector for Syslog padrão para a coleta de mensagens:

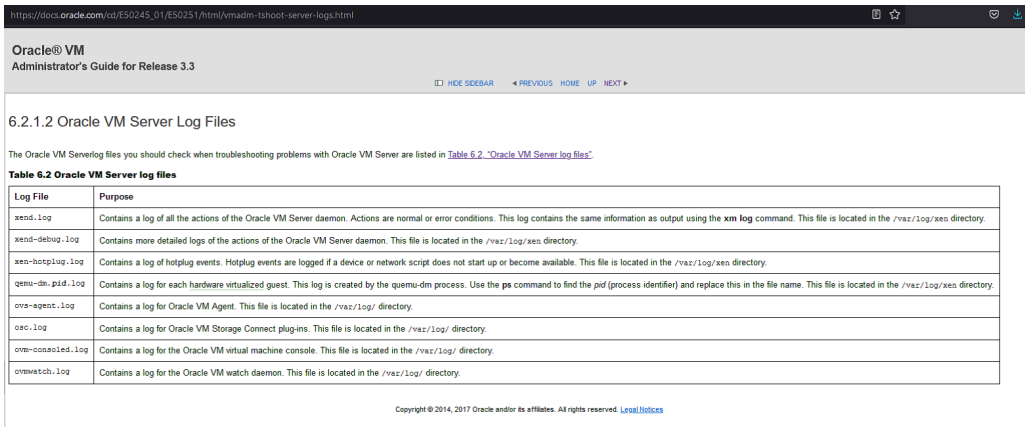
https://www.microfocus.com/documentation/arcsight/arcsight-smartconnectors/pdfdoc/arcsight-cef-syslog/arcsight-cef-syslog.pdf

No documento abaixo são informados os tipos de Syslogs e suas coletas:
https://www.microfocus.com/documentation/arcsight/arcsight-smartconnectors/AS_SmartConn_getstart_HTML/#GettingStarted/smartconn_type_syslog.htm%3FTocPath%3DTypes%2520of%2520SmartConnectors%7C 10

Desta forma, o ponto questionado pela empresa TELETEX como não atendido, na verdade fica demonstrado que sim, é atendido através da coleta padrão do ArcSight através de um SmartConnector para Syslog.

12.3. Plataformas de Virtualização: Oracle VM

Segundo informações do fabricante Oracle os arquivos de logs do Oracle VM são gerados em arquivos de texto (https://docs.oracle.com/cd/E50245_01/E50251/html/vmadm-tshoot-server-logs.html) conforme portal do fabricante Oracle e figura abaixo:



https://docs.oracle.com/cd/E50245_01/E50251/html/vmadm-tshoot-server-logs.html

Oracle® VM
Administrator's Guide for Release 3.3

HIDE SIDEBAR ◂ PREVIOUS HOME UP NEXT ▸

6.2.1.2 Oracle VM Server Log Files

The Oracle VM Serverlog files you should check when troubleshooting problems with Oracle VM Server are listed in Table 6.2 "Oracle VM Server log files".

Table 6.2 Oracle VM Server log files

Log File	Purpose
xend.log	Contains a log of all the actions of the Oracle VM Server daemon. Actions are normal or error conditions. This log contains the same information as output using the **xm log** command. This file is located in the /var/log/xen directory.
xend-debug.log	Contains more detailed logs of the actions of the Oracle VM Server daemon. This file is located in the /var/log/xen directory.
xen-hotplug.log	Contains a log of hotplug events. Hotplug events are logged if a device or network script does not start up or become available. This file is located in the /var/log/xen directory.
qemu-dm.*pid*.log	Contains a log for each hardware virtualized guest. This log is created by the quemu-dm process. Use the **ps** command to find the *pid* (process identifier) and replace this in the file name. This file is located in the /var/log/xen directory.
ovs-agent.log	Contains a log for Oracle VM Agent. This file is located in the /var/log/ directory.
osc.log	Contains a log for Oracle VM Storage Connect plug-ins. This file is located in the /var/log/ directory.
ovm-consoled.log	Contains a log for the Oracle VM virtual machine console. This file is located in the /var/log/ directory.
ovmwatch.log	Contains a log for the Oracle VM watch daemon. This file is located in the /var/log/ directory.

Copyright © 2014, 2017 Oracle and/or its affiliates. All rights reserved. Legal Notices

Assim para isso a MicroFocus disponibiliza conectores do tipo Flex Connector file reader ou folder reader que consistem em ler os arquivos e extrair as informações contida neles. Conforme descrito em documento oficial do fabricante no link abaixo: https://www.microfocus.com/documentation/arcsight/arcsight-smartconnectors/AS_SmartConn_getstart_HTML/#GettingStarted/smartconn_type_file.htm%3FTocPath%3DTypes%2520of%2520SmartConnectors%7C 3

TELETEX

12.8 do mesmo item, acima mencionado, exige-se que a solução seja capaz de coletar, no mínimo, os logs dos sistemas e ativos VPN: OpenVPN. Contudo, a documentação apresentada pela Recorrida não comprova que a solução possui suporte para Open VPN.

RESPOSTA ATA

12.8. VPN: OpenVPN

Abaixo estamos apresentando o código do Smart Connectors existente para coleta de OpenVPN, que se encontra disponível na comunidade do ArcSight um Flex Connector para coleta de eventos do OpenVPN, e transcrito abaixo:

arcsight flexconnector openvpn regex=(openvpn)\[.*\]:\s(.*) token.count=2 token[0].name=type token[0].type=String token[1].name=body token[1].type=String

event.deviceVendor= stringConstant("openvpn") event.deviceProduct= stringConstant("openvpn")

event.sourceUserPrivileges= stringConstant("openvpn") event.deviceProcessName= stringConstant("openvpn") event.flexString2=body

event.name=type event.message=body submessage.messageid.token=type submessage.token=body submessage.count=1 submessage[0].messageid=openvpn submessage[0].pattern.count=3

submessage[0].pattern[0].regex=([^\/]+)\/(\d+.\d+.\d+.\d+):(\d+)\s+(.*)
submessage[0].pattern[0].mappings=$1|$2|$3|$4
submessage[0].pattern[0].fields=event.targetUserName,event.attackerAddress,event.attackerPort,event.message
submessage[0].pattern[1].regex=(\d+.\d+.\d+.\d+):(\d+)\s+(.*)
submessage[0].pattern[1].mappings=$1|$2|$3
submessage[0].pattern[1].fields=event.attackerAddress,event.attackerPort,event.message
submessage[1].pattern.count=1

submessage[1].pattern[0].regex=(.*)
submessage[1].pattern[0].fields=event.message

submessage[1].pattern[0].extramappings=event.reason= stringConstant("unparsed")

Entendo que a empresa ATA Comércio e Serviços de Informática Ltda, demonstrou que a ferramenta ofertada (ArcSight ESM 7.5) atende o solicitado no TR, contrariando o que a empresa TELETEX Computadores e Sistemas apontou em seu recurso.

Sendo assim, sugiro o indeferimento do recurso!

Att.

Marcelo Silva de Novaes

Coordenadoria de Infraestrutura e Suporte Secretaria de Tecnologia da Informação/TRE-MS."

DA DECISÃO

Do exposto, das razões e contrarrazões apresentadas e da manifestação

técnica da unidade demandante, esta Pregoeira **CONHECE** o recurso apresentado pela empresa TELETEX COMPUTADORES E SISTEMAS LTDA., **NEGANDO-LHE PROVIMENTO** quanto ao mérito, pugnando pela **CONTINUIDADE** deste Pregão 29/2021.

A presente decisão será divulgada no COMPRASNET, e no sítio do TRE/MS na internet, para conhecimento dos interessados, e será submetida à autoridade competente do TRE/MS nos termos da legislação aplicável.

Cabe consignar que a Ata da Sessão Pública e o Resultado por Fornecedor já estão disponíveis para consulta no COMPRASNET e no site do TRE/MS.

Após a manifestação da Autoridade Competente quanto ao recurso apresentado, os autos deverão retornar a esta Pregoeira para publicidade e continuidade dos trâmites de praxe.

Sônia Aparecida Granja Anelli

Pregoeira

Documento assinado eletronicamente por **SÔNIA APARECIDA GRANJA ANELLI**, **Pregoeiro**, em 06/12/2021, às 13:52, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://sei.tre-ms.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1128356** e o código CRC **DD847B79**.