RECURSO ADMINISTRATIVO

EDITAL DE LICITAÇÃO

ÓRGÃO LICITANTE: FUNDAÇÃO BUTANTAN – UASG 930829

PREGÃO ELETRÔNICO Nº 90038/2025

SHIELD SECURITY TECNOLOGIA LTDA, inscrita no CNPJ sob o nº 31.746.312/0001-72, com sede na Av. Paulista, nº 37, Conj. 41 e 42, Bela Vista, São Paulo, SP – CEP 01.311-902, neste ato representada pelo Sr. Vitor Villani Correa Fonseca, CPF nº 075.281.866-00 endereço de e-mail: vitor.villani@shieldesc.com.br , vem, muito respeitosamente à presença de Vossas Senhorias, apresentar, com fundamento no subitem 8.7 do edital de licitação, suas **CONTRARRAZÕES** ao Recurso Administrativo interposto pela licitante **TIVIT TERCEIRIZAÇÃO DE PROCESSOS, SERVIÇOS E TECNOLOGIA S.A**. ("TIVIT"), CNPJ/MF nº 07.073.027/0001-53, face da decisão que a declarou inabilitada no certame, pugnando desde já pela manutenção da decisão proferida.

DAS CONTRARRAZÕES DE RECURSO

Insurge a licitante TIVIT - TERCEIRIZAÇÃO DE PROCESSOS, SERVIÇOS E TECNOLOGIA S.A. contra a decisão que lhe declarou inabilitada no certame por não atendimento aos termos do edital, especificações técnicas, com fundamento no relatório de área técnica.

A decisão do pregoeiro, fundamentada na análise da equipe técnica está em completa consonância com o princípio da vinculação ao instrumento convocatório previsto no **caput** do artigo 5º da Lei nº 14.133/2021, que dispõe:

> "Na aplicação desta Lei serão observados os princípios da legalidade, da impessoalidade, da moralidade, da publicidade, da eficiência, do interesse público, da economicidade, do desenvolvimento nacional sustentável, da eficácia, da segregação de funções, da motivação, da razoabilidade, da proporcionalidade, da segurança jurídica, da celeridade, da finalidade, da competitividade, da proporcionalidade, da isonomia, da igualdade, do planejamento, da transparência, da eficácia, da eficácia, da segregação de funções, do julgamento objetivo e da vinculação ao instrumento convocatório."

Portanto, a alteração da decisão proferida de forma acertada, máxima vênia, implicará em violação direta ao texto do edital de licitação, e ao princípio da vinculação ao edital, artigo 5º, caput da Lei 14.133/2021

A vinculação ao edital impõe que tanto a Administração Pública quanto os licitantes estejam estritamente submetidos às regras estabelecidas no instrumento convocatório, impedindo que requisitos sejam desconsiderados ou alterados ao longo do certame, garantindo a previsibilidade e segurança jurídica ao processo.

A inobservância do princípio da vinculação ao edital pode levar à inabilitação do licitante ou à desclassificação de sua proposta, conforme previsto no artigo 59, inciso II, da Lei nº 14.133/2021:

> "Serão desclassificadas as propostas que:
> (...) II - não atenderem às exigências do edital quanto à compatibilidade com as especificações técnicas dos bens ou serviços a serem contratados pela Administração."

Neste contexto, a análise técnica demonstrou que a solução ofertada pelo licitante recorrente não atende aos requisitos exigidos pelo edital, restando absolutamente correta a decisão guerreada. A aceitação de um produto que não atende às exigências previamente estabelecidas configuraria afronta ao princípio da vinculação ao edital, além de comprometer a competitividade e a integridade do certame.

A Administração, ao identificar tal inadequação, tem o dever de agir com observância estrita ao edital, garantindo que somente soluções tecnicamente compatíveis sejam aceitas.

A flexibilização dos critérios estabelecidos, sem fundamentação expressa no edital, poderia ensejar questionamentos administrativos e jurídicos, inclusive com risco de nulidade do certame.

Neste contexto, o princípio da vinculação ao edital desempenha papel essencial na condução dos processos licitatórios, assegurando que as regras estabelecidas no instrumento convocatório sejam cumpridas de forma rigorosa.

Sua observância está diretamente ligada ao princípio da isonomia, evitando favorecimentos indevidos e garantindo a igualdade de condições entre os licitantes.

No caso de processos licitatórios que envolvam softwares ou soluções tecnológicas, a verificação técnica é fundamental para garantir que os produtos atendam integralmente aos requisitos do edital. A inobservância desse princípio, ao admitir soluções que não cumprem as exigências estabelecidas, configura violação ao artigo 59, inciso II, da Lei nº 14.133/2021, restando absolutamente correta a decisão que inabilitou a licitante recorrente por não atendimento aos requisitos técnicos do edital.

DA ANÁLISE TÉCNICA

Objetivando reforçar todas as inconsistências e limitações do software apresentado pela licitante recorrente, que fundamentaram a decisão técnica da equipe deste órgão, submetemos à apreciação a análise técnica elaborada pela equipe da recorrida.

Gestão de vulnerabilidades e exposição centralizada

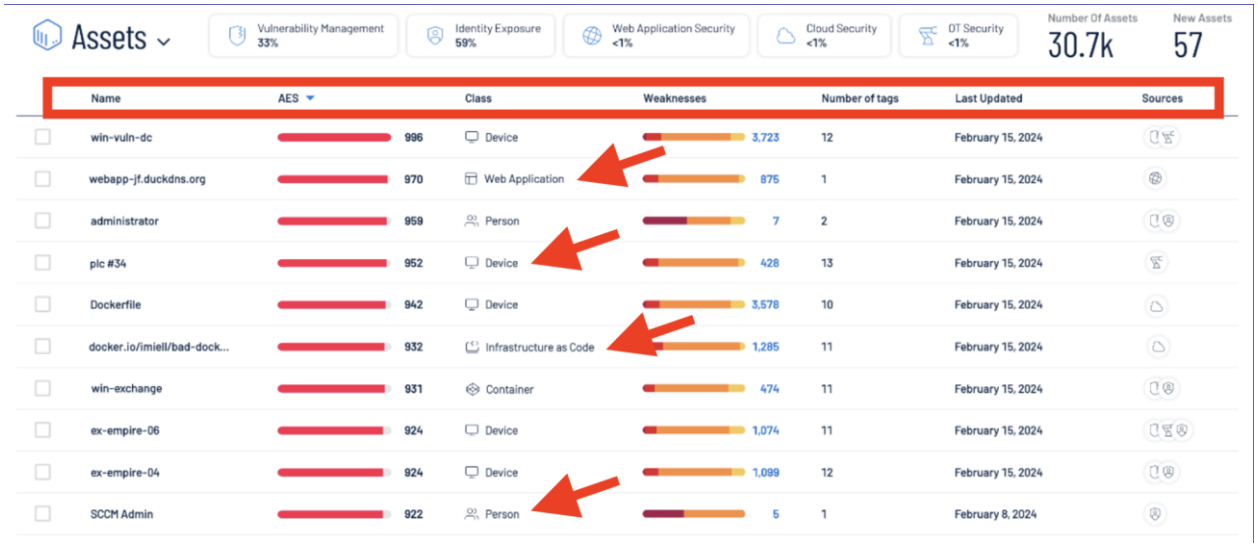
Uma visão unificada e integrada passa por um trabalho de normalização das informações de cada tipo de ativo(OT, IT, Web Application), padronizando métricas, correlacionando informações para que o risco e exposição possa ser medido em um ativo, grupo de ativos, superfície de ataque ou a empresa como um todo utilizando uma mesma métrica para ativos distintos, possibilitando cálculos de exposição e risco por área responsável, segmento de negócio, filiais, datacenter, ambiente em nuvem pública, ambiente on-premise, estratégias corporativas e qualquer outro ambiente onde queira medir o nível de exposição e risco.

A medição de exposição e risco utilizando métricas padronizadas facilita a comunicação e entendimento para todas as áreas da corporação sobre o nível de exposição e risco, seja ela técnica, executiva ou de negócios.

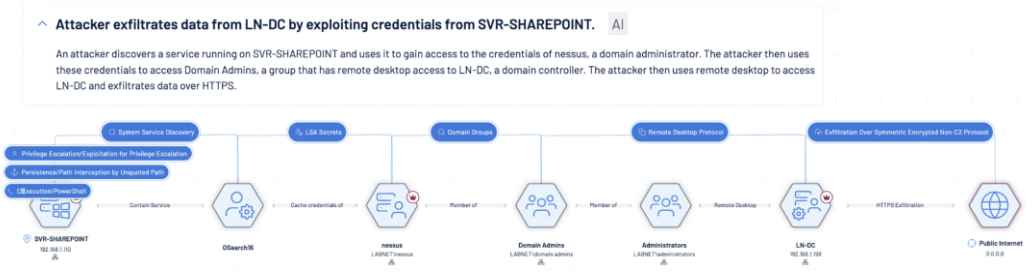
Além disso, após normalização das informações é possível correlacionar as informações de todos os tipos de ativos para mapeamento de possíveis fraquezas a serem exploradas que permitam possíveis caminhos de ataque dentro de um ambiente tecnológico.

As soluções de mercado já utilizam Inteligência Artificial e Ciência de Dados para prover os requisitos dos itens abaixo destacados e presentes no Edital.

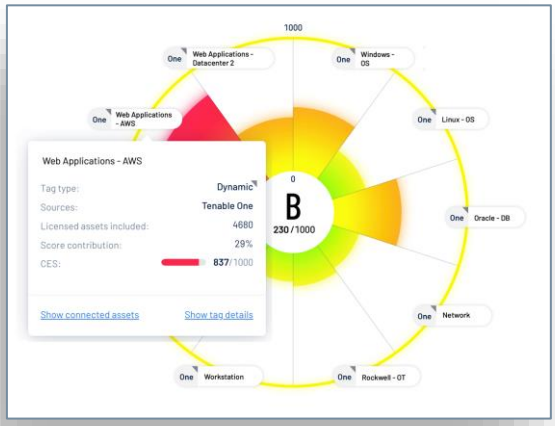
Exemplo 1 - Inventário unificado e com as informações de ativos(Usuário, IT, Web Application, OT, etc) distintos normalizados. Todos possuem uma pontuação(AES) para medir o nível de exposição e risco:



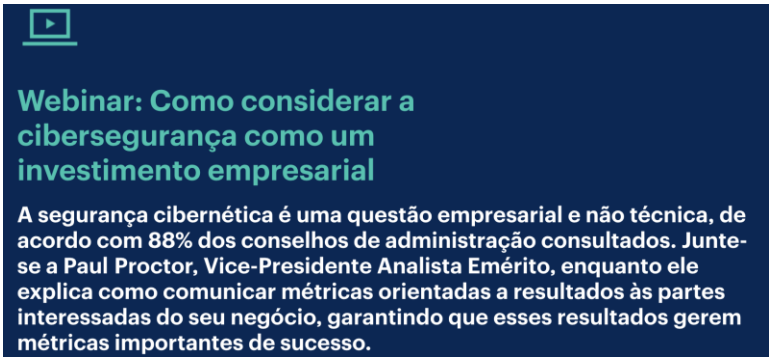
Exemplo 2 – Visualização de possíveis caminhos de ataque de acordo com Inventário unificado e com as informações de ativos(Usuário, IT, Web Application, OT, etc) distintos normalizados:



Exemplo 3 – Cálculo de pontuação de nível de exposição e risco de acordo com Inventário unificado e com as informações de ativos(Usuário, IT, Web Application, OT, etc) distintos normalizados:



Não basta consolidar as informações de produtos e fabricantes distintos em uma única base sem a normalização, contextualização, padronização e correlação. O Instituto Butantan investe em soluções de mercado que possam alinhar tecnologia e a missão da instituição. Trata-se de um conceito de empresas especializadas e sem relação direta com fabricantes de soluções que apontam modelos de gestão que tragam maiores benefícios ao negócio principal da empresa.



Fonte: Gartner Link: https://www.gartner.com.br/pt-br/artigos/como-gerenciar-ameacas-a-ciberseguranca

Alguns itens do Termo de referência deixam claro que uma solução que efetua somente a consolidação de informações de fabricantes distintos, não atende as necessidades atuais de mercado e as necessidades do Instituto Butantan:

> 3.2.2 A adoção de uma plataforma centralizada em nuvem (SAAS), visa gestão do ambiente numa console única, possibilitando eficiência operacional e visão unificada e integrada da exposição, classificação e priorização de vulnerabilidades e riscos dos ambientes tecnológicos de TI, OT, IoT e aplicações Web.
>
> 3.3.1.2 Ganhar eficiência operacional, realizando a gestão das soluções por meio de uma única console, possibilitando uma visão unificada e integrada de riscos e vulnerabilidades e usando métricas padronizadas para as soluções que compõe a plataforma a ser contratada;
>
> 3.3.1.5 Melhorar a comunicação sobre o real risco cibernético. A plataforma fornecerá informações práticas sobre o risco cibernético geral e a capacidade de aprofundamento em unidades operacionais ou departamentos;

Dos requisitos técnicos e funcionais

A Plataforma deve proporcionar uma visão unificada de todos os ativos e vulnerabilidades associadas de software, de configuração e de direitos existentes nestes, contemplando de forma integrada o ambiente de TI, rede industrial (OT e IoT) e aplicações Web.

Os recursos de visualização e priorização das vias de ataque devem fornecer uma resposta focada de forma preventiva para interromper as vias que os invasores podem usar executando essa função de mapeamento dos riscos críticos para a estrutura MITREATT&CK e visualizar continuamente todas as vias de ataque viáveis.

Do não cumprimento aos itens 6.1.1.21, 6.1.1.22 e 6.1.4.8 do Termo de Referência

O edital, em seus subitens 6.1.1.21 e 6.1.1.22, exige que a solução tenha capacidade para scanners ilimitados dentro da infraestrutura. Já o subitem 6.1.4.8 requer a capacidade de realizar scans personalizados por agendamento, além de varreduras com frequência pré-determinada e em horários designados.

Como destacado pela equipe técnica, a proposta do recorrente permite a execução de scans para apenas 600 ativos internos, limitada a quatro vezes ao ano, bem como scans no ambiente para apenas cinco FQDNs externos, também restritos a quatro vezes ao ano.

Dessa forma, a proposta do recorrente não deixou dúvidas à equipe técnica, sendo clara ao apresentar uma execução limitada da solução – em evidente contrariedade ao edital, que exige scanners de forma ilimitada.

Do não atendimento ao item 6.6.4.2 do Termo de Referência

Ao dispor sobre o suporte técnico e manutenção em seu item 6.6, o órgão licitante estabeleceu no subitem 6.6.4.2 que o suporte técnico deverá ser prestado de forma ilimitada.

Nesse aspecto, igualmente não há qualquer dúvida a ser sanada pela equipe técnica, uma vez que a proposta da recorrente é explícita ao limitar a disponibilização de suporte a 12 (doze) horas mensais para abertura de chamados junto ao fabricante - configuração que, evidentemente, descumpre a exigência de suporte ilimitado prevista no edital.

Evidentemente, dispensa-se qualquer esclarecimento adicional, pois a clareza das condições proposta salta aos olhos em qualquer análise técnica mínima. Diante disso, agiu corretamente a equipe técnica do órgão licitante ao concluir que a proposta apresentada não atende ao exigido no Termo de Referência anexo ao edital.

Do não atendimento aos itens 6.1.1.11, 6.7.1 e 6.7.1.1 do Termo de Referência

O edital assim exige no Termo de Referência:

> 6.1.1.11. Possibilitar que os scanners e sensores agentes sejam gerenciados por uma única plataforma, de maneira centralizada;
>
> ...
>
> 6.7.1 As soluções contratadas devem estar consolidadas numa plataforma em nuvem (SAAS) centralizada, de Gerenciamento de Vulnerabilidades baseadas em risco, com única console;
>
> 6.7.1.1. Considerar a visibilidade completa de todos os módulos e ambientes na mesma console de gerenciamento, independentemente do tipo de ativo (TI, OT, IoT ou WAS), incluindo sensores físicos ou virtuais, de forma a possibilitar a eficiência no gerenciamento e obter visão integrada de análise, priorização e gestão de vulnerabilidades e riscos;
>
> ...

A proposta apresentada pela licitante recorrente, Tivit, propõe a utilização de plataformas diferentes para realizar a gestão de vulnerabilidade do sistema, vejamos:

> Para realizar a gestão de vulnerabilidade no ambiente interno a Tivit se propõe a usar a ferramenta Rapid 7
>
> Para realizar a gestão de vulnerabilidade no ambiente Externo a Tivit se propõe a usar a ferramenta Qualys
>
> Para realizar a gestão de vulnerabilidade no ambiente de OT a TIvit se propõe a usar o Claroty CTD

A utilização de ferramentas descentralizadas resulta em um fluxo de trabalho isolado e ineficiente, adicionando complexidade, criando varreduras redundantes, diminuindo drasticamente o processo de correção de riscos

Ao contrário, a visibilidade centralizada pode ajudar a agilizar muito a resolução de vulnerabilidades.

Do não atendimento aos subitens 4.1.1 e 6.5.1 do Termo de Referência

O Termo de Referência estabelece como exigência ao licitante vencedor a realização de treinamento na modalidade remota, com carga horária de até 20 (vinte) horas, turmas limitadas a 10 (dez) participantes, abrangendo operação, manuseio, gerenciamento, configuração e utilização das soluções contratadas, sendo os dias e frações horárias definidos pelo órgão licitante.

A despeito de constar na planilha orçamentária (item 4.1.1), a licitante recorrente omitiu o serviço de treinamento em sua proposta técnica. Mesmo que se conceda - apenas por argumentação - que a proposta faça menção genérica ao treinamento, dela não se extrai qualquer elemento que permita apurar o respectivo custo.

Ante o exposto, resta inequívoco que a equipe técnica atuou com plena correção em sua avaliação

Do não atendimento ao subitem 6.1.1.12 do Termo de Referência

Ao dispor sobre a solução para gestão de vulnerabilidades e auditoria de configuração de ativos para a rede de TI, o órgão licitante exigiu no subitem 6.1.1.12 que o acesso ao console de gerenciamento seja fornecida para pelo menos 10(dez) usuários simultâneos.

Contrariamente, a proposta técnica do licitante recorrente contraria os termos do edital ao dispor que não é concedido acesso ao cliente e, o acesso ao console de gestão do TVM é exclusivo da empresa licitante:

- É reservado à TIVIT o acesso exclusivo à console de gestão do TVM.
- Não é concedido ao Cliente acesso de leitura ou escrita à console do TVM.

Não existe qualquer dúvida a ser sanada nesse tópico, ao contrário, lúcido está que a proposta técnica não atendeu a exigência do Termo de Referência.

Do não atendimento ao subitem 9.1.1 do Termo de Referência

Conforme disposto na tabela de solução de chamados (subitem 9.1.1 do Termo de Referência), os prazos máximos para primeiro contato devem observar os seguintes parâmetros:

- 30 (trinta) minutos para chamados de severidade alta;
- 60 (sessenta) minutos para severidade média;
- 01 (um) dia útil para severidade baixa.

A proposta da licitante recorrente, no entanto, apresenta discrepância flagrante em relação às exigências editalícias nos casos de severidade alta e média, conforme demonstrado a seguir:

Previsão Edital	Tempo de resposta	Proposta Tvit	Tempo de resposta
Severidade alta	Até 30 minutos	Severidade alta	Até 01hora
Severidade média	Até 60 minutos	Severidade média	Até 03horas

Diante do exposto, comprova-se de forma irrefutável a atuação correta e tecnicamente fundamentada da equipe avaliadora. A proposta da recorrente, por sua evidente desconformidade com os requisitos editalícios, não demandava qualquer complementação ou diligência adicional.

Assim, configura-se de maneira cristalina o descumprimento das exigências estabelecidas no instrumento convocatório.

A realização de diligência não se presta à alteração da proposta técnica originalmente apresentada em desconformidade com o edital.

Isso viola não apenas a isonomia do *caput* do artigo 37 da Constituição Federal, como também a igualdade de tratamento de licitantes, do inciso XXI, do mesmo dispositivo constitucional, uma vez que a licitante beneficiada acaba com chance ilícita de ofertar uma segunda proposta, uma dupla chance de competir e isso depois dos alertas nas mensagens de *"chat"* do pregão, no sentido de que o primeiro objeto, pela análise empreendida, não passaria pelo crivo de aceitabilidade.

Isso viola, ainda, a impessoalidade e a legalidade, prestigiadas no artigo 37 da Constituição Federal.

Dos pedidos

Diante do exposto, requer a manutenção da decisão que inabilitou a licitante **TIVIT TERCEIRIZAÇÃO DE PROCESSOS, SERVIÇOS E TECNOLOGIA S.A**. ("TIVIT"), CNPJ/MF nº 07.073.027/0001-53, nos termos da fundamentação apresentada e da análise da equipe técnica deste órgão licitante mantendo-se da habitação da recorrida.

Termos em que pede e espera deferimento.

Belo Horizonte, 23 de abril de 2025

VITOR VILLANI CORREA FONSECA:07528186600

Assinado de forma digital por VITOR VILLANI CORREA FONSECA:07528186600
Dados: 2025.04.23 16:28:57 -03'00'

SHIELD SECURITY TECNOLOGIA LTDA

CNPJ sob o nº 31.746.312/0001-72