

DIÁRIO OFICIAL DA UNIÃO

Publicado em: 26/03/2020 | Edição: 59 | Seção: 1 | Página: 15

Órgão: Ministério da Defesa/Gabinete do Ministro

DESPACHO Nº 21/GM-MD, DE 25 DE MARÇO DE 2020

Processo no64535.001865/2020-90

Interessado: Comando do Exército - Base Administrativa do Comando de Comunicações e Guerra Eletrônica do Exército (Ba Adm CCOMGEx).

Assunto: Termo de Licitação Especial nº 01/2019, de 21 de novembro de 2019, do Exército Brasileiro.

Documento vinculado: Nota Técnica nº 2/DEPROD/SEPROD/SG/MD/2020, de 16 de março de 2020.

Submete-se ao MINISTRO DE ESTADO DA DEFESA, o Termo de Licitação Especial nº 01/2019, de 21 de novembro de 2019, do Exército Brasileiro, para autorização do procedimento licitatório, em conformidade com o previsto no § 1º do art. 3º da Lei nº 12.598, de 21 de março de 2012 e nos artigos 12, 13 e 15 do Decreto nº 7.970, de 28 de março de 2013.

Decisão

Autorizo o procedimento licitatório, com base no Termo de Licitação Especial nº 01/2019, de 21 de novembro de 2019, do Comando de Guerra Eletrônica do Exército. Caberá às autoridades competentes do órgão interessado o acompanhamento e a fiscalização dos atos decorrentes.

Publique-se.

Comunique-se o Comando do Exército.

FERNANDO AZEVEDO E SILVA

Ministro da Defesa

Este conteúdo não substitui o publicado na versão certificada.



**MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
COMANDO DE COMUNICAÇÕES E GUERRA ELETRÔNICA DO
EXÉRCITO
COMANDO MARECHAL CÂNDIDO MARIANO DA SILVA RONDON**

TERMO DE LICITAÇÃO ESPECIAL 01/2019

A União, PESSOA JURÍDICA DE DIREITO PÚBLICO INTERNO, por intermédio da Base Administrativa do Comando de Comunicações e Guerra Eletrônica do Exército (Ba Adm/ Cmdo Com GE Ex), organização militar do Exército Brasileiro, inscrita sob o Cadastro Nacional de Pessoas Jurídicas (CNPJ) 00.394.452/0467-82, representada pelo Coronel ADRIANO DE ANDRADE PONTES, Ordenador de Despesas da Ba Adm/ Cmdo Com GE Ex, Cadastro de Pessoa Física (CPF) nº 168.619.488-96, pretende promover PREGÃO ELETRÔNICO, nos termos do Decreto nº 10.024, de 20 de setembro de 2019, da Lei nº 12.598, de 21 de março de 2012 (artigo 3º, § 1º, inciso I), e do Decreto nº 7.970, de 28 de março de 2013, utilizando subsidiariamente a Lei nº 8.666/1993, alinhada com a Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008, e Instrução Normativa ME/ SGD Nº 1, DE 4 DE ABRIL DE 2019, procedimento licitatório destinado à participação de Empresa Estratégica de Defesa (EED) para a manutenção de Produto Estratégico de Defesa (PED), conforme abaixo.

1.1. DO OBJETO

Contratação de Empresa Estratégica de Defesa especializada na área de Tecnologia da Informação para a atualização e inclusão de novos cenários, contemplando manutenções de diversas complexidades em Produto Estratégico de Defesa (Informação), SIMOC - Simulador de Operações de Cibernéticas (Portaria Nº 3.229/MD, de 27 de novembro de 2013), do Exército Brasileiro, compreendendo Inteligência Artificial (Machine Learning), Internet das Coisas - IoT (Internet of Things), dentre outros, a serem executadas por demanda, mediante ordens de serviço incluindo-se todas as migrações de dados, recuperação de dados de logs e afins, atualizações de software, suporte técnico presencial e remoto, além da documentação de acordo com as tecnologias, metodologias e processos de gestão de qualidade especificados no Termo de Referência.



O objeto da referida contratação compreende a descrição abaixo. Conforme a tabela:

Tabela 1: item do objeto.

DESCRIÇÃO
Contratação de serviços técnicos especializados de manutenção de Software para o Simulador de Operações de Guerra Cibernética - SIMOC, compreendendo as seguintes tarefas a serem prestadas, mediante ordens de serviço dimensionadas pela métrica de Unidade de Serviço Técnico (UST): MANUTENÇÃO CORRETIVA , incluindo-se todas as migrações de dados, atualizações de hardware e software, além da documentação e instalações que se fizerem necessárias.
Contratação de serviços técnicos especializados de manutenção de Software para o Simulador de Operações de Guerra Cibernética - SIMOC, compreendendo as seguintes tarefas a serem prestadas, mediante ordens de serviço dimensionadas pela métrica de Unidade de Serviço Técnico (UST): MANUTENÇÃO ADAPTATIVA , incluindo-se todas as migrações de dados, atualizações de hardware e software, além da documentação e instalações que se fizerem necessárias.
Contratação de serviços técnicos especializados de manutenção de Software para o Simulador de Operações de Guerra Cibernética - SIMOC, compreendendo as seguintes tarefas a serem prestadas, mediante ordens de serviço dimensionadas pela métrica de Unidade de Serviço Técnico (UST): MANUTENÇÃO EVOLUTIVA , incluindo-se todas as migrações de dados, atualizações de hardware e software, além da documentação e instalações que se fizerem necessárias.

1.2. RAZÕES DA OPÇÃO DE UTILIZAÇÃO DO PROCEDIMENTO LICITATÓRIO ABRANGIDO PELA LEI Nº 12.598, DE 21 DE MARÇO DE 2012

1.2.1. O Simulador de Operações de Guerra Cibernética é um sistema de aplicação didática de complexa tecnologia, empregado em cursos de capacitação, especialização e extensão, que exige do aluno conhecimentos técnicos na operação de recursos de tecnologia da informação e comunicações em um ambiente de operações cibernéticas.

1.2.2. O Centro de Instrução de Guerra Eletrônica (CIGE) iniciou o projeto de desenvolvimento do SIMOC em 2011. Foram realizadas duas atualizações, em 2014 e 2016. Desde então, a demanda por novos cenários de simulação tornou-se crescente, culminando na necessidade de celebração de contratos de manutenção.

1.2.3. O cenário é o produto do simulador. É uma coleção de objetos pré-cadastrados, eventos, serviços de redes e métricas que ao se comporem, permitem a simulação de eventos e situações que afetam as redes de computadores no mundo real. Assim, há a demanda de atualização dos cenários cibernéticos para que o treinamento do aluno seja o mais real e atual possível.

1.2.4. O simulador emula, fielmente, o comportamento de uma rede típica, (composta de roteadores, switches, firewalls, estações de trabalho, servidores de redes, etc.), além dos serviços de rede, tais como servidor de correio eletrônico, servidor de páginas (servidor Web) servidor de arquivos, além de outras características, como tipos de enlace de dados, perfis de tráfego de redes, dentre outros serviços de

rede existentes no mundo real. Destarte, tal capacidade permite que redes internas de elevada importância possam ser testadas antes de serem implementadas, apresentando o conteúdo sensível de informações que tramita no simulador.

1.2.5. As ações desencadeadas pelos alunos têm reflexo no comportamento do ambiente de simulação, a partir de condições e cenários pré-definidos pelos instrutores, de modo que, por meio do emprego de técnicas de virtualização, é capaz de implementar um ambiente estanque no qual os alunos podem conduzir e reproduzir, de forma segura e controlada, ações e situações encontradas no mundo cibernético real. Dessa forma, o *modus operandi* e as técnicas utilizados pelo Exército na preparação cibernética de seus militares trafega pelo simulador, comprovando a sensibilidade de informações neste software.

1.2.6. O simulador, tal como qualquer software, necessita de manutenção, a qual requer uma equipe técnica dedicada e de tamanho considerável, possuindo conhecimentos específicos e profundos de diversas atividades da área de Tecnologia da Informação. Desse modo, o melhoramento do simulador realizado por uma empresa brasileira possibilita um desenvolvimento de tecnologia na BID, além de fomentar na geração de empregos no Brasil.

1.2.7. Ressalta-se, ainda, o fato de que o SIMOC apresenta demandas evolutivas para atender às necessidades operacionais de treinamento e capacitação. Além disso, a constante evolução tecnológica e o surgimento de novas ameaças cibernéticas impõem a necessidade de inserção de novas funcionalidades e composição de novos cenários.

1.2.8. Tais demandas poderão ser atendidas neste contrato de manutenção pretendido para a criação de novos cenários e o desenvolvimento de novas funcionalidades, permitindo a continuidade do processo de ensino para a formação do “Guerreiro Cibernético” do Exército Brasileiro, bem como o adestramento de servidores públicos e militares das FFAA e a incorporação de tecnologias necessárias à expansão de sua utilização em atendimento às demandas operativas do Ministério da Defesa.

1.2.9. No entanto, o atendimento de tais demandas requer pessoal técnico altamente especializado, em quantidade que excede a disponibilidade do corpo técnico do Exército Brasileiro. Soma-se, ainda, o fato de que existe conteúdo e fluxo de informações de caráter sensível. Com isso, existe a necessidade de contratação de serviço de suporte e manutenção que permita o funcionamento adequado do sistema sem interrupções e sem comprometer as atividades de

instrução ou de capacitação.

1.2.10. Portanto, o objetivo da contratação é garantir o funcionamento do software, preservando a sua integridade e disponibilidade, abrangendo as necessidades de correção que ocorram, levando-se em consideração que é impossível testar todas as possibilidades de execução de um sistema, não se podendo, também, prever as necessidades de evoluções e adaptações, além de novas demandas.

1.2.11. Como o SIMOC é um sistema singular, complexo e sensível, seu desenvolvimento deve ser realizado com o máximo de cautela para atender os interesses da Força.

1.2.12. Atualmente, há a demanda de setores das FFAA e de instituições públicas para treinamento e simulação de redes internas críticas. Assim, o SIMOC adapta-se como instrumento de ensino e de auxílio à prevenção de incidentes cibernéticos à Administração Pública.

1.3. ANÁLISE ENTRE BENEFÍCIO E CUSTO

A análise entre os benefícios e os custos da condução de uma contratação nos moldes da Lei nº 12598/2012, para a contratação de PED, exclusivamente por intermédio de EED, baseia-se nas perspectivas dos benefícios e custos do processo em si e do produto.

1.3.1. DOS BENEFÍCIOS

Tendo em vista o processo licitatório diferenciado, previsto em Lei nº 12598/12, para EED, identificaram-se benefícios relacionados à contratação e ao PED:


1.3.1.1. Do ponto de vista da contratação

a) Garantia de contratação de solução com alto conteúdo nacional.

O desenvolvimento do SIMOC deve ter um alto percentual de conteúdo nacional, principalmente em sua parte de orquestração. No programa irão tramitar o *modus operandi* de ensino de Cibernética e as informações sensíveis de redes emuladas no simulador de diversas instituições brasileiras. Com a possibilidade de aplicar a Lei nº 12598/12 e assegurar uma empresa brasileira para o desenvolvimento do SIMOC, torna-se um benefício a imposição de conteúdo nacional mínimo, sendo extremamente útil neste tipo de sistema estratégico.

b) Garantia de contratação de empresa nacional com experiência na área de Defesa.

A solicitação de contratação de EED pretende estimular a BID nacional. A possibilidade de estipular como condição que a empresa



contratada tenha sede, administração e estabelecimento industrial no Brasil favorece o desenvolvimento nacional. Tais medidas não estão formalmente presentes na Lei nº 8666/93, tornando a utilização do TLE, por meio da Lei nº 12598/12, adequado para o referido caso.

c) Diminuição do risco de solução com falha intencional (*backdoor*).

A contratação de uma solução com alto conteúdo nacional e desenvolvida localmente por uma empresa nacional da área de defesa reduz, sensivelmente, o risco de existência de uma falha do tipo *backdoor* na solução. A existência desse tipo de falha comprometeria a segurança das informações que estariam sendo transmitidas pelo sistema, colocando em risco o tráfego de informações.

d) Geração de emprego e fluxo de investimento na Indústria de Defesa.

A garantia de contratação de empresa nacional traz como benefício adicional a geração de emprego, fomento à Cibernética e renda na indústria de defesa e seus fornecedores. A simples utilização da Lei nº 8666/93 poderia ocasionar a contratação de empresa ou solução estrangeira, dificultando a criação de empregos e renda no Brasil. Destaca-se que a contratação de solução estrangeira incidiria em riscos de segurança da informação.

e) Aumentar a independência do mercado externo com sustentação de parcela dos investimentos na Indústria de Defesa Nacional.

A necessidade das FFAA de se capacitarem e de se adestrarem em cibernética é constante, o que requer a existência permanente de uma base industrial de defesa robusta para atender a essa demanda. Assim, o Estado tem a possibilidade de contribuir com a sustentação e fomento da indústria de defesa nacional de soluções de segurança da informação, mais precisamente, cibernética.

f) Garantia de manutenção da capacidade produtiva da tecnologia adquirida dos produtos e serviços de interesse da Defesa Nacional.

Amparado pela Lei nº 12598/12, caso a empresa contratada seja afastada por motivos quaisquer, fato recorrente em licitações com empresas “aventureiras” pela Lei nº 8666/93, assegura-se a imposição da continuidade produtiva no país. Deste modo, mesmo após o afastamento da empresa, garante-se a passagem de tecnologia e documentação para a continuidade da solução tecnológica no Brasil.

g) Segurança da informação.

Nos termos do edital e do contrato, garantir: o sigilo de assunto de interesse e/ou em quaisquer documentos a que venha a empresa

brasileira contratada tomar conhecimento durante a execução do serviço, a integridade do software, a reprodução customizada, a restrição na comercialização do simulador. Tais necessidades asseguradas sob pena de responsabilidade civil, penal e administrativa, a partir da assinatura do contrato com normas de segurança da informação e de termo de compromisso de manutenção de sigilo.

- h) Garantia da pesquisa e o desenvolvimento de novos produtos e de novas tecnologias a serem aplicadas na indústria de defesa.

Caso seja de interesse da empresa contratada, a utilização do simulador, de forma customizada, e suas tecnologias adjacentes podem resultar em novos produtos para a defesa nacional. A aplicação do simulador pode gerar produtos de verificação de artefatos maliciosos, de análise de *malware* e mais. Desse modo, mesmo após a entrega do simulador, garante-se a continuidade de desenvolvimento tecnológico no Brasil.

1.3.1.2. Do ponto de vista dos Produtos Estratégicos de Defesa

Do ponto de vista do PED, os benefícios identificados são especificados sob o enfoque operacional e estratégico.

1.3.1.2.1. Benefício Operacional

- a) implementação de novas funcionalidades, de acordo com as necessidades das atividades de Instrução e simulação, bem como atualização de hardware, software, repositórios de objetos, criação de cenários e eventos, adequações dos bancos de dados e da documentação do sistema.
- b) ampliação da capacitação e o preparo operacional do pessoal, conduzidos por meio do uso do simulador, aos militares do Exército Brasileiro e das demais Forças Armadas, direcionados às atividades de Guerra Cibernética.
- c) ampliação das possibilidades de uso do simulador, permitindo que outras estruturas das FFAA possam empregá-lo atendendo necessidades como teste de ativos de rede, utilização de cenários para assistir equipamentos e artefatos maliciosos, dentre outras aplicações que podem ser atendidas com a evolução do mesmo.
- d) redução nos custos logísticos de treinamento e de homologação, uma vez que o software virtualiza desde redes simples às estruturas complexas e críticas, dentro de um ambiente controlado, aumentando a produtividade dos instruendos e otimizando a avaliação dos alunos.
- e) implementação de novas tecnologias e capacidades como inserção de

cenários com inteligência artificial, *machine learning* e Internet das Coisas (IoT).

f) gestão baseada em indicadores de produtividade e qualidade.

1.3.1.2.2. Benefício Estratégico

- a) Esta demanda está alinhada ao Plano Estratégico (PEEx) 2020-2023 - objetivo 10: Aumentar a Efetividade na Gestão do Bem Público e 10.1.1: Aperfeiçoar o Sistema de Gestão do Exército; e ao Objetivo estratégico da Estratégia de TI do Exército Brasileiro (PEE/PETI-EB) - OEE nº 04 - "ATUAR NO ESPAÇO CIBERNÉTICO COM LIBERDADE DE AÇÃO. "
- b) Busca atender, ainda, aos seguintes objetivos estratégicos de tecnologia da informação (OETI), constantes da Concepção Estratégica de TI do Exército: - OETI 01 - "APRIMORAR AS SOLUÇÕES E SERVIÇOS DE TI EM ATENDIMENTO ÀS NECESSIDADES DO EXÉRCITO"; "OETI 03 - "AMPLIAR A CAPACIDADE DE ATUAÇÃO NO ESPAÇO CIBERNÉTICO" e OETI 05 - "APRIMORAR A GESTÃO E A CAPACITAÇÃO DO PESSOAL NA ÁREA DE TI".
- c) Proporcionar a segurança da informação aos agentes públicos e às instituições públicas que utilizarem o simulador seja para adestramento ou emulação de rede crítica.

1.3.2. DOS CUSTOS

Ainda com relação à escolha por processo licitatório diferenciado, cabe ressaltar os custos da escolha desse tipo de procedimento.

1.3.2.1. Do ponto de vista da contratação

- a) Diminuição do número de empresas concorrentes
O processo licitatório requerido, devido sua especificidade, reduz o número de participantes. Essa redução eventualmente poderá aumentar o custo da contratação. Contudo, o desenvolvimento e a manutenção do simulador, realizado por empresa nacional poderá gerar empregos e aumento da tecnologia da BID, favorecendo a comercialização deste no simulador no exterior com benefícios à balança comercial e a possibilidade de *royalties* ao Exército.
- b) Especificidade processual sobre a condução do processo licitatório mais diferenciado
Neste momento, há cerca de três a quatro empresas estratégicas de defesa em condições de atender o pleito do desenvolvimento. Com a licitação em modalidade de pregão, pode-se gerar uma competição entre as empresas e a demanda ser atendida com concorrência. Destaca-se que há uma escassez de empresas totalmente brasileiras que trabalham com este produto.

c) Justificativa para o Custo

Apesar de citado anteriormente, o SIMOC é um instrumento de dissuasão de poder. A importação de uma solução estrangeira poderia colocar em risco a segurança da informação das atividades desenvolvidas por intermédio do simulador. Assim, uma solução nacional atende melhor os requisitos propostos, contribuindo para o desenvolvimento das EED.

1.4. OUTROS FATORES DE ANÁLISE

A arquitetura tecnológica utilizada pelo simulador não limitará outros resultados, podendo ser empregada outras tecnologias conforme evolução do Sistema a ser mantido, cabendo ao fornecedor do serviço consultar a equipe técnica do CIGE para homologação das mesmas.

1.4.1. PRINCIPAIS TECNOLOGIAS ASSOCIADAS AO SIMOC

As camadas da arquitetura do sistema representam uma divisão lógica com o intuito de evidenciar a complexidade das interações entre as diversas tecnologias que o compõe. Cada camada é composta por tecnologias relacionadas que definem uma fronteira do sistema. Estas camadas, por sua vez, utilizam alguma tecnologia/protocolo para se comunicarem e compor a solução. A figura 1, abaixo, mostra as principais camadas do sistema e suas principais interações.

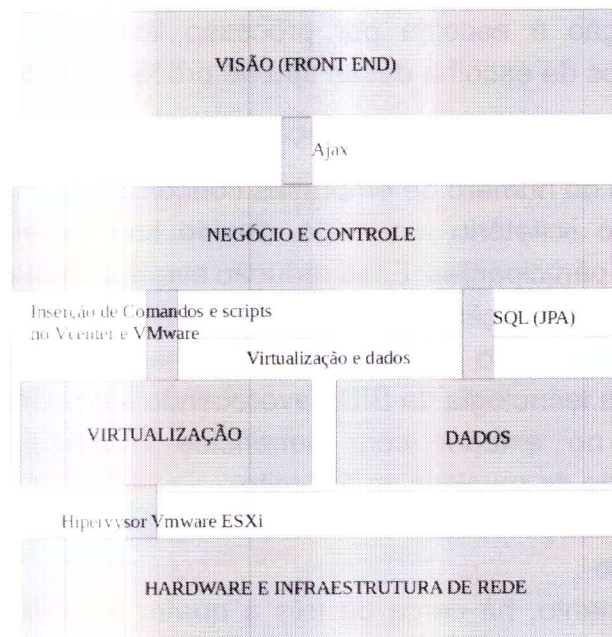


Figura 1: Arquitetura do sistema

a) Visão (*front end*):

- HTML/CSS: Componentes WEB;
- AngularJS(V1): Componente da camada de apresentação para modulo de avaliação, integrado com APIs desenvolvidas com JAX-RS;
- JSP(V1.2): Componente da camada de apresentação;
- DWR: Componente para comunicação assíncrona; e
- JAVASCRIPT: Rotinas e métodos de integração com web-socket.

b) Negócio e Controle:

- TOMCAT: Container WEB para aplicação SimocAPP;
- JAX-RS: Componente para desenvolvimento de API de integração Restful/JSON com AngularJS; e
- SIMOCAPP: Aplicação Java WEB responsável por manter o conteúdo lógico dos cenários. Além de orquestrar as ações que interagem com ambiente virtual.

c) Extração de Dados (*analytics*): basicamente é responsável por capturar tráfego de rede e apresentar resultados estatísticos, alertas, entre outros:

- SURICATA: Captura o fluxo de rede gerado no ambiente virtual para identificar eventos de segurança;
- LOGSTASH: Captura e formata os eventos recebidos pelo Suricata;
- ELASTICSEARCH: Processa um alto volume de dados transformados pelo logstash; e
- KIBANA: Apresenta visualizações customizadas para análise de ataque e defesa cibernética.

d) Desafio (Treinamento Avançado) – CTF: Aplicação WEB em python que interage com o SIMOCAPP a nível de banco de dados (JDBC).

e) Virtualização:

- VCenter: Provê uma API de serviços para gestão do ambiente virtual através do SimocAPP; e
- VSphepe: Hypervisor que virtualiza os objetos e as redes definidos nos cenários no SimocAPP

f) Banco de Dados

- Postgre: Banco de dados relacional para persistência das entidades do SimocAPP; e
- SQLServer.

g) Hardware e infraestrutura de rede:

- Servidor Dell PowerEdge R920;
- Storages HP StorageWorks; e



- HP StorageWorks 8/8 SAN Switch.

h) Segurança:

- NGINX: Proxy reverso para aplicação implementando HTTPS; e
- Firewall Open Source para infraestrutura da aplicação.

1.4.2. PERCENTUAL MÍNIMO DE CONTEÚDO NACIONAL

O SIMOC é um PED 100% nacional, tanto na parte de orquestração dos virtualizadores, como nos eventos criados para comporem os cenários. O conteúdo nacional faz-se necessário 100% na parte de orquestração e código-fonte. Os programas que auxiliam na virtualização dos roteadores, switches, firewalls, estações de trabalho, servidores de redes e demais objetos são softwares proprietários, não cabendo aplicação de conteúdo nacional 100% nesse aspecto.

1.4.3. CAPACIDADE INOVADORA EXIGIDA

O simulador objeto deste TLE detém, por si só, características inovadoras intrínsecas. Seu foco é o desenvolvimento de novas capacidades de simulação às Forças Armadas e ao Setor de Infraestruturas Críticas, como a representação em ambiente virtual de cenários com implementação de novas tecnologias, compreendendo Inteligência Artificial e Internet das Coisas.

A ampliação das possibilidades de uso do simulador permite que outras estruturas das FFAA possam empregá-lo, atendendo necessidades, além de permitir que outros Órgãos da Administração Pública possam se valer do simulador para adestramento e outros fins.

1.4.4. CONTRIBUIÇÃO PARA AUMENTAR A CAPACIDADE TECNOLÓGICA E PRODUTIVA DA BASE INDUSTRIAL DE DEFESA

O simulador possui capacidades tecnológicas que favorecem o uso dual do software. Sua tecnologia pode ser utilizada na certificação e homologação de software e hardware, como teste de ativos de rede, utilização de cenários para verificar comportamento de artefatos maliciosos, dentre outras aplicações que podem ser atendidas com a sua evolução. Deste modo, sua manutenção corrobora para um aumento da capacidade tecnológica, promovendo oportunidade de geração de emprego e atualização tecnológica da BID.

1.4.5. SUSTENTABILIDADE DO CICLO DE VIDA DO PRODE

A manutenção do software pretende estender a utilização do simulador. Tal extensão possibilita gerar royalties ao Exército, com a perspectiva de venda da marca SIMOC, da tecnologia utilizada e do simulador customizado para outras entidades. Dessa forma, o Exército poderá receber com o direito de uso, exploração e comercialização do

bem, servindo de retorno ao investimento realizado.

1.4.6. GARANTIA DE CONTINUIDADE DAS CAPACITAÇÕES TECNOLÓGICAS E PRODUTIVAS A SEREM EXIGIDAS

Com ressalva à propriedade intelectual já pertencente ao Exército, a empresa ganhadora da licitação deverá apresentar garantias no caso de descontinuidade da produção do simulador ou na ocorrência do encerramento da pessoa jurídica, conforme o Art. 9º do Decreto nº 7.970, de 28 de março de 2013.

1.5. OUTRAS INFORMAÇÕES

Outros aspectos abordados pelo art. 12, Parágrafo 2º, do Dec. 9.870/13, não foram citados por se entender que não pertencem ao escopo desse Termo de Licitação Especial.



ADRIANO DE ANDRADE PONTES - Cel
Ordenador de Despesas da Ba Adm/ Cmdo COM GE EX

