



## Espelho - Emenda à Despesa

TIPO AUTOR	TIPO DE EMENDA	EMENDA
Comissão	APROPRIAÇÃO	-----
EMENTA		
Sugestão 01 - Min. da Defesa - Sistema de Defesa Cibernética para a Defesa Nacional - R\$ 300 milhões (Sen. Eduardo Braga)		
MODALIDADE DE EMENDA	SEQUENCIAL	
Comissão	00002660	
ESFERA ORÇAMENTÁRIA		
10 - Orçamento Fiscal		

### ACRÉSCIMOS À PROGRAMAÇÃO

ÓRGÃO ORÇAMENTÁRIO	UNIDADE ORÇAMENTÁRIA
52000 - Ministério da Defesa	52101 - Ministério da Defesa - Administração Direta
FUNCIONAL PROGRAMÁTICA	05.572.6112.147F.0001
FUNÇÃO	SUBFUNÇÃO
05 - Defesa Nacional	572 - Desenvolvimento Tecnológico e Engenharia
PROGRAMA	
6112 - Defesa Nacional	
AÇÃO	
147F - Implantação de Sistema de Defesa Cibernética para a Defesa Nacional	
SUBTÍTULO	
0001 - Nacional	
LOCALIDADE BENEFICIADA	
9000000 - Nacional	

ESPECIFICAÇÃO DO PRODUTO / UNIDADE DE MEDIDA	META	QTD META A ALTERAR
Sistema implantado (% de execução física)	2	27

GND	MODALIDADE DE APLICAÇÃO	RP	em R\$ 1,00	ACRÉSCIMO
3 Outras Despesas Correntes	90 Aplicações Diretas	8	100.000.000	
4 Investimentos	90 Aplicações Diretas	8	200.000.000	
<b>TOTAL:</b>			<b>300.000.000</b>	

### CANCELAMENTOS COMPENSATÓRIOS

SEQUENCIAL	FONTE	GND	MODALIDADE DE APLICAÇÃO	ID	RP	em R\$ 1,00	CANCELAMENTO
000003716	1076	9 Reserva de Contingência	99 A Definir	0	0	300.000.000	
<b>TOTAL:</b>						<b>300.000.000</b>	

### JUSTIFICATIVA

Essa emenda visa desenvolver mecanismos afim de enfrentar as ameaças, aperfeiçoar e atualizar as tecnologias de enfrentamento no combate aos crimes cibernéticos.



## Espelho - Emenda à Despesa

TIPO AUTOR	TIPO DE EMENDA	EMENDA
Comissão	APROPRIAÇÃO	-----

EMENTA  
Sugestão 02 - Exército - Sistema de Defesa Cibernética para a Defesa Nacional - R\$ 20 milhões (Sen. Esperidião Amin)

MODALIDADE DE EMENDA  
Comissão

**SEQUENCIAL**  
**000002719**

ESFERA ORÇAMENTÁRIA  
10 - Orçamento Fiscal

### ACRÉSCIMOS À PROGRAMAÇÃO

ÓRGÃO ORÇAMENTÁRIO  
52000 - Ministério da Defesa

UNIDADE ORÇAMENTÁRIA  
52121 - Comando do Exército

**FUNCIONAL PROGRAMÁTICA**      **05.572.6112.147F.0001**

FUNÇÃO  
05 - Defesa Nacional

SUBFUNÇÃO  
572 - Desenvolvimento Tecnológico e Engenharia

PROGRAMA  
6112 - Defesa Nacional

AÇÃO  
147F - Implantação de Sistema de Defesa Cibernética para a Defesa Nacional

SUBTÍTULO  
0001 - Nacional

LOCALIDADE BENEFICIADA  
9000000 - Nacional

ESPECIFICAÇÃO DO PRODUTO / UNIDADE DE MEDIDA	META	QTD META A ALTERAR
Sistema implantado (% de execução física)	1	1

GND	MODALIDADE DE APLICAÇÃO	RP	em R\$ 1,00 ACRÉSCIMO
4 Investimentos	90 Aplicações Diretas	2	20.000.000
<b>TOTAL:</b>			<b>20.000.000</b>

<b>CANCELAMENTOS COMPENSATÓRIOS</b>			em R\$ 1,00			
SEQUENCIAL	FUNTE	GND	MODALIDADE DE APLICAÇÃO	ID	RP	CANCELAMENTO
000003719	1000	9 Reserva de Contingência	99 A Definir	0	2	20.000.000
<b>TOTAL:</b>						<b>20.000.000</b>

### JUSTIFICATIVA

A integridade operacional das redes elétricas depende da integração perfeita de sistemas cibernéticos e físicos para monitoramento, controle e operação. No entanto, à medida que os Sistemas de Supervisão e Aquisição de Dados (SCADA) se tornam cada vez mais susceptíveis a intrusões cibernéticas devido à adaptação generalizada da Tecnologia da Informação e Comunicação (TIC), os desafios dessa integração e interdependência são amplificados. As subestações, como infraestruturas críticas nas redes elétricas, enfrentam riscos crescentes de potenciais ataques cibernéticos, colocando em risco a estabilidade da rede. Proteger a integridade cibernética e física das subestações é, portanto, imperativo para reforçar e sustentar a elevada resiliência das redes elétricas no cenário em evolução das redes inteligentes.

As subestações, servindo como nós essenciais nas redes elétricas, hospedam componentes importantes, como transformadores, barramentos, disjuntores e Dispositivos Eletrônicos Inteligentes (IEDs). Esses componentes fazem interface com aplicativos de software do Sistema de Gerenciamento de Energia (EMS), necessitando de conectividade ciberfísica robusta. No entanto, embora o acesso remoto simplifique a manutenção, também introduz vulnerabilidades que podem precipitar falhas em cascata e apagões da rede. A urgência em enfrentar estes desafios é evidente. Uma abordagem holística, integrando medidas de segurança cibernética e física, é fundamental para detectar, isolar e mitigar com eficácia invasões cibernéticas ou eventos decorrentes de erros de configuração de protocolos de proteção.

No centro da abordagem proposta está o desenvolvimento de um ambiente de testes ciberfísicos especificamente adaptado para pesquisas de sistemas de controle, proteção e segurança cibernética de subestações. A despeito das restrições no acesso a dados do mundo real, devido aos protocolos de segurança, esse ambiente de teste oferece um caminho prático para simular interações realistas de sistemas cibernéticos e físicos. Ao replicar as complexidades dos equipamentos reais do sistema de energia que fazem interface com ambientes de automação, controle, proteção e TIC, o ambiente de teste mostra sua capacidade em facilitar análises abrangentes da dinâmica de invasões cibernéticas, vulnerabilidades e resiliência do sistema. Além disso, permite a avaliação do desempenho e da confiabilidade das aplicações em diversos cenários, fornecendo estratégias robustas de mitigação.

Na verdade, a implantação de um tal ambiente de testes ciberfísicos representa um catalisador crucial para impulsionar paradigmas de segurança de subestações. A busca por um ambiente que promova a experimentação e a análise abrangentes anuncia uma fronteira



## Espelho - Emenda à Despesa

### JUSTIFICATIVA

inovadora no fortalecimento da resiliência ciberfísica de infraestruturas críticas de energia.

#### Descrição e Benefícios do Projeto:

As novas subestações digitais (SED) representam a inovação das subestações convencionais uma vez que são equipadas por Dispositivos Eletrônicos Inteligentes (IED) que têm a capacidade de compartilhar informações e prover interoperabilidade entre cada um de seus elementos. Os IED usam protocolos de comunicação para troca de dados elétricos digitais, baseados na Norma IEC 61850, em substituição ao método convencional que utiliza sinais analógicos transmitidos por condutores de cobre. A principal vantagem do emprego desses protocolos é a redução significativa do número de condutores dentro da subestação. Por outro lado, essa mudança de paradigma na tecnologia dos sistemas de comunicação mostra-se desafiadora por conta da possibilidade de ataques cibernéticos nos sistemas de proteção e controle das subestações. O objetivo principal é montar um laboratório que consistirá em uma Subestação Digital real e modelada em ambiente de simulação em tempo real, onde IED de proteção serão conectados em Hardware In The Loop (HIL).

A utilização do laboratório possibilitará:

- Analisar o desempenho dos sistemas de proteção das subestações digitais frente a ataques cibernéticos.
- Explorar as possíveis vulnerabilidades nos protocolos de comunicação dos sistemas de proteção das subestações digitais (SED).
- Elaborar estratégias para prevenir possíveis invasões ao sistema de proteção das SED.
- Criar instruções de operação para mitigar os efeitos deletérios de uma ação maliciosa nos sistemas de proteção das SED.

Os benefícios do projeto são:

- Adequar as instalações do laboratório de máquinas elétricas à visão de futuro do setor elétrico, isto é, participar da modernização do sistema elétrico que consiste na digitalização das instalações existentes.
- Ampliar os objetivos do projeto do LaSC na área de segurança cibernética aplicada ao sistema elétrico, ou seja, explorar ataques em equipamentos reais de uma SED.
- Possibilitar a formação/especialização do corpo docente e discente do Instituto, em nível de graduação e pós-graduação.
- Tornar o Instituto uma referência no tema por conta do pioneirismo.

#### Resultado e Alinhamento:

O resultado principal do projeto é a modernização do Laboratório de Máquinas Elétricas do IME, transformando-o em um Laboratório de Sistemas Elétricos de vanguarda para apoio à PD&I em segurança elétrica e cibernética de infraestruturas críticas do Sistema Interligado Nacional (SIN) por meio de ensaios reais e simulados em tempo real com HIL.

Alinhamento Estratégico: Objetivo Estratégico do Exército OEE 3 - Aprimorar a atuação no espaço cibernético, com liberdade de ação; Estratégia 3.1 - Indução à estruturação do Setor Estratégico Cibernético; Ação Estratégica 3.1.2 Implantar o Setor Cibernético no Exército; Iniciativa Estratégica 3.1.2.3 Ampliar a estrutura de pesquisa cibernética; Iniciativa Estratégica 3.1.2.4 Desenvolver soluções tecnológicas de cibernética - Anexo "A" PEEEx 2024- 2027: Item 3. Áreas de Interesse Operacional - Guerra cibernética - Tecnologia de Interesse: Sistemas de informação, Projeto LaSC.



## Espelho - Emenda à Despesa

TIPO AUTOR	TIPO DE EMENDA	EMENDA
Comissão	APROPRIAÇÃO	-----
EMENTA		
Sugestão 03 - ABIN - Ações de Inteligência - R\$ 35 milhões (Sen. Esperidião Amin)		
MODALIDADE DE EMENDA	SEQUENCIAL	
Comissão	00000855	
ESFERA ORÇAMENTÁRIA		
10 - Orçamento Fiscal		

### ACRÉSCIMOS À PROGRAMAÇÃO

ÓRGÃO ORÇAMENTÁRIO	UNIDADE ORÇAMENTÁRIA
20000 - Presidência da República	20118 - Agência Brasileira de Inteligência - ABIN
<b>FUNCIONAL PROGRAMÁTICA</b>	<b>04.183.0032.2684.0001</b>

FUNÇÃO	SUBFUNÇÃO
04 - Administração	183 - Informação e Inteligência
PROGRAMA	
0032 - Programa de Gestão e Manutenção do Poder Executivo	
AÇÃO	
2684 - Ações de Inteligência	
SUBTÍTULO	
0001 - Nacional	
LOCALIDADE BENEFICIADA	
9000000 - Nacional	

ESPECIFICAÇÃO DO PRODUTO / UNIDADE DE MEDIDA	META	QTD META A ALTERAR

GND	MODALIDADE DE APLICAÇÃO	RP	em R\$ 1,00	ACRÉSCIMO
3 Outras Despesas Correntes	90 Aplicações Diretas	8		30.000.000
4 Investimentos	90 Aplicações Diretas	8		5.000.000
<b>TOTAL:</b>				<b>35.000.000</b>

### CANCELAMENTOS COMPENSATÓRIOS

SEQUENCIAL	FONTE	GND	MODALIDADE DE APLICAÇÃO	ID	RP	em R\$ 1,00	CANCELAMENTO
000003719	1000	4 Investimentos	99 A Definir	0	2		35.000.000
<b>TOTAL:</b>							<b>35.000.000</b>

### JUSTIFICATIVA

A Agência Brasileira de Inteligência - ABIN, órgão central do Sistema Brasileiro de Inteligência - Sisbin, está desenvolvendo projeto estratégico para reestruturar o referido SISBIN, com fundamento no Decreto nº 11.693, de 6 de setembro de 2023, e com a finalidade de criar de plataforma digital de produção e compartilhamento de Inteligência e de comunicação segura, com emprego de criptografia de Estado, com solução estruturante para garantir o intercâmbio seguro de dados e conhecimentos entre o órgãos do sistema. Dando cumprimento à Lei n.º 9.883/1999 e a sua regulamentação, o projeto visa maior eficiência, eficácia e e efetividade para integrar, analisar e disseminar dados, informações e conhecimentos para subsidiar o processo decisório do Poder Executivo na execução de políticas públicas e na contraposição de ameaças, sobretudo ações contrárias ao Estado democrático, o extremismo violento e a interferência externa. Além disso, pretende dotar a Administração Pública Federal de solução de comunicação segura com criptografia de Estado, de forma a salvaguardar o conhecimento sensível de ações de espionagem estrangeira. Os resultados do projeto terão impacto relevante na execução das ações de inteligência e contrainteligência, fortalecendo o Sisbin como sistema em defesa das instituições e do Estado Democrático de Direito.



## Espelho - Emenda à Despesa

TIPO AUTOR	TIPO DE EMENDA	EMENDA
Comissão	APROPRIAÇÃO	-----
EMENTA		
Sugestão 04 - Aeronáutica - Ações de Caráter Sigiloso - R\$ 10 milhões (Sen. Esperidião Amin)		
MODALIDADE DE EMENDA	SEQUENCIAL	
Comissão	00002687	
ESFERA ORÇAMENTÁRIA		
10 - Orçamento Fiscal		

### ACRÉSCIMOS À PROGRAMAÇÃO

ÓRGÃO ORÇAMENTÁRIO	UNIDADE ORÇAMENTÁRIA
52000 - Ministério da Defesa	52111 - Comando da Aeronáutica
<b>FUNCIONAL PROGRAMÁTICA</b>	<b>05.183.6112.2866.0001</b>

FUNÇÃO	SUBFUNÇÃO
05 - Defesa Nacional	183 - Informação e Inteligência
PROGRAMA	
6112 - Defesa Nacional	
AÇÃO	
2866 - Ações de Caráter Sigiloso	
SUBTÍTULO	
0001 - Nacional	
LOCALIDADE BENEFICIADA	
9000000 - Nacional	

ESPECIFICAÇÃO DO PRODUTO / UNIDADE DE MEDIDA	META	QTD META A ALTERAR
		<i>em R\$ 1,00</i>
GND	MODALIDADE DE APLICAÇÃO	RP ACRÉSCIMO
3 Outras Despesas Correntes	90 Aplicações Diretas	8 10.000.000
		<b>TOTAL: 10.000.000</b>

SEQUENCIAL	FUNTE	GND	MODALIDADE DE APLICAÇÃO	ID	RP	CANCELAMENTO
000003719	1000	4 Investimentos	99 A Definir	0	2	10.000.000
						<b>TOTAL: 10.000.000</b>

### JUSTIFICATIVA

A partir das diretrizes estabelecidas na Estratégia Nacional de Defesa (END), o Ministério da Defesa (MD) definiu os projetos estratégicos que permitirão ao país desenvolver capacidade para defender, com eficiência, sua soberania e seus interesses. Essas iniciativas são prioritárias e contam com aportes financeiros que garantem sua execução continuada. Dentre os principais projetos, destacam-se três sob responsabilidade da FAB: Aeronaves de Caça F-X2 GRIPEN NG; Aeronaves Cargueiro KC-390 MILLENNIUM; e Programa Estratégico de Sistemas Espaciais (PESE).

Em paralelo, a Política Nacional de Inteligência (PNI), fixada pelo Decreto nº 8.793, de 29 de junho de 2016, prioriza ameaças com potencial capacidade de por em perigo a integridade da sociedade e do Estado e a segurança nacional do Brasil, dentre as quais destacam-se: espionagem, sabotagem, interferência externa, ações contrárias à soberania nacional, ataques cibernéticos, terrorismo e atividades ilegais envolvendo bens de uso dual e tecnologias sensíveis.

Na Aeronáutica, cabe ao Centro de Inteligência da Aeronáutica (CIAER), como elo do Sistema Brasileiro de Inteligência (SISBIN), produzir conhecimentos em atendimento às prescrições dos planos e programas de inteligência, decorrentes da PNI. Ademais, compete ao CIAER fornecer subsídios ao Comandante da Aeronáutica nos assuntos relacionados ao Estado, ao preparo e ao emprego da Força Aérea Brasileira.

Visando o cumprimento das diretrizes da PNI, com dedicada atenção à proteção dos Projetos Estratégicos da Aeronáutica, o CIAER figura como órgão responsável pela salvaguarda das informações vinculadas a tais projetos. Além das ameaças estabelecidas na PNI, as medidas a cargo do CIAER visam, ainda, o cumprimento dos compromissos internacionais de sigilo, dos quais o Brasil é signatário, bem como a proteção da tecnologia adquirida pelo país, nas parcerias decorrentes destes projetos, por meio das cláusulas de compensação



## Espelho - Emenda à Despesa

TIPO AUTOR	TIPO DE EMENDA	EMENDA
Comissão	APROPRIAÇÃO	-----

EMENTA  
Sugestão 05 - Presidência da República - Segurança da Informação e Cibersegurança - R\$ 12 milhões (Sen. Esperidião Amin)

MODALIDADE DE EMENDA  
Comissão

**SEQUENCIAL**  
**00000843**

ESFERA ORÇAMENTÁRIA  
10 - Orçamento Fiscal

### ACRÉSCIMOS À PROGRAMAÇÃO

ÓRGÃO ORÇAMENTÁRIO  
20000 - Presidência da República

UNIDADE ORÇAMENTÁRIA  
20101 - Presidência da República

**FUNCIONAL PROGRAMÁTICA**      **04.126.4102.21AP.0001**

FUNÇÃO  
04 - Administração

SUBFUNÇÃO  
126 - Tecnologia da Informação

PROGRAMA  
4102 - Segurança Institucional

AÇÃO  
21AP - Segurança da Informação e Cibersegurança

SUBTÍTULO  
0001 - Nacional

LOCALIDADE BENEFICIADA  
9000000 - Nacional

ESPECIFICAÇÃO DO PRODUTO / UNIDADE DE MEDIDA	META	QTD META A ALTERAR
Apoio realizado (unidade)	1	1

GND	MODALIDADE DE APLICAÇÃO	RP	em R\$ 1,00 ACRÉSCIMO
3 Outras Despesas Correntes	90 Aplicações Diretas	8	12.000.000
<b>TOTAL:</b>			<b>12.000.000</b>

<b>CANCELAMENTOS COMPENSATÓRIOS</b>				em R\$ 1,00
SEQUENCIAL	FUNTE	GND	MODALIDADE DE APLICAÇÃO	ID RP CANCELAMENTO
000003719	1000	9 Reserva de Contingência	99 A Definir	0 2 12.000.000
<b>TOTAL:</b>				<b>12.000.000</b>

### JUSTIFICATIVA

Da mesma forma que tivemos admiráveis avanços tecnológicos que puderam melhorar nossa conectividade, durante a pandemia da covid 19, e que aceleraram a transformação digital no mundo em que vivemos, também são de admirar os desafios e adversidades que elas nos trouxeram.

E é neste contexto, onde reinam as incertezas do que estará por vir, ao menos uma coisa é bastante certa: a realidade do perigo e do crescimento vertiginoso das ameaças e dos crimes cibernéticos.

Segundo dados do Fórum Econômico Mundial de DAVOS, se hoje o crime cibernético fosse um país, ele seria a terceira maior economia mundial, perdendo apenas para os EUA e China.

E o Brasil, segundo estimativas da FortGuard Labs, foi o segundo País mais atacado da América Latina em 2023, perdendo apenas para o México, sendo neste contexto em que nos encontramos atualmente e que nos desafia a encarar de frente de como estão as nossas vulnerabilidades.

Neste sentido, é urgente que o Gabinete de Segurança Institucional da Presidência da República, através da sua Secretaria da Segurança da Informação e Cibernética disponha de uma ferramenta de inteligência cibernética, preditiva, focada em 'dark web', no intuito de identificar e prever os ataques cibernéticos e por fim otimizar a resiliência cibernética nacional.

Os serviços em questão de solução de tecnologia tem valores estimados na ordem de R\$ 12.000.000,00 (doze milhões de reais) por ano que serão utilizados em favor da defesa cibernética do país.

#### Base Legal:

- LEI Nº 14.600/2023, Art. 8, IV e V
- DECRETO 11676/2023, Arts. 19, 20, e 21
- DECRETO 11856/2023, Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança
- DECRETO 10748/2021, Institui a Rede Federal de Gestão de Incidentes Cibernéticos
- DECRETO 9637/2018, Institui a Política Nacional de Segurança da Informação



## Espelho - Emenda à Despesa

TIPO AUTOR	TIPO DE EMENDA	EMENDA
Comissão	APROPRIAÇÃO	-----

EMENTA  
Sugestão 06 - Marinha - Ações de Caráter Sigiloso - R\$ 2 milhões (Sen. Efraim Filho)

MODALIDADE DE EMENDA  
Comissão

**SEQUENCIAL**  
**000002753**

ESFERA ORÇAMENTÁRIA  
10 - Orçamento Fiscal

### ACRÉSCIMOS À PROGRAMAÇÃO

ÓRGÃO ORÇAMENTÁRIO  
52000 - Ministério da Defesa

UNIDADE ORÇAMENTÁRIA  
52131 - Comando da Marinha

**FUNCIONAL PROGRAMÁTICA**      **05.183.6112.2866.0001**

FUNÇÃO  
05 - Defesa Nacional

SUBFUNÇÃO  
183 - Informação e Inteligência

PROGRAMA  
6112 - Defesa Nacional

AÇÃO  
2866 - Ações de Caráter Sigiloso

SUBTÍTULO  
0001 - Nacional

LOCALIDADE BENEFICIADA  
9000000 - Nacional

ESPECIFICAÇÃO DO PRODUTO / UNIDADE DE MEDIDA	META	QTD META A ALTERAR
----------------------------------------------	------	--------------------

GND	MODALIDADE DE APLICAÇÃO	RP	em R\$ 1,00 ACRÉSCIMO
3 Outras Despesas Correntes	90 Aplicações Diretas	2	2.000.000
<b>TOTAL:</b>			<b>2.000.000</b>

SEQUENCIAL	FUNTE	GND	MODALIDADE DE APLICAÇÃO	ID	RP	em R\$ 1,00 CANCELAMENTO
000003719	1000	9 Reserva de Contingência	99 A Definir	0	2	2.000.000
<b>TOTAL:</b>						<b>2.000.000</b>

### JUSTIFICATIVA

Centro de Inteligência da Marinha - CIM  
CNPJ: 00.394.502/0272-63

Na Marinha do Brasil, cabe ao Centro de Inteligência da Marinha (CIM), como elo do Sistema Brasileiro de Inteligência (SISBIN), produzir conhecimentos em atendimento às prescrições dos planos e programas de inteligência, decorrentes da Política Nacional de inteligência (PNI). Ademais, compete ao CIM fornecer subsídios ao Comandante da Marinha nos assuntos relacionados ao Estado, ao preparo e ao emprego da Marinha do Brasil. Visando o cumprimento das diretrizes da (PNI), com dedicada atenção à proteção dos Projetos Estratégicos da Marinha do Brasil, o CIM figura como Órgão Central e tem a responsabilidade pela salvaguarda das informações vinculadas a tais projetos. Além das ameaças estabelecidas na PNI, as medidas a cargo do CIM, ainda, o cumprimento dos compromissos internacionais de sigilo, dos quais o Brasil é signatário, bem como a proteção da tecnologia adquirida pelo país, nas parcerias decorrentes destes projetos, por meio das cláusulas de compensação das contratadas, por meio de investimentos no Brasil. Assim sendo, faz-se necessário um aporte de recursos na ordem de R\$2.000.000,00 (dois milhões de reais), como Verba para Ações de Caráter Sigiloso.



## Espelho - Emenda à Despesa

TIPO AUTOR	TIPO DE EMENDA	EMENDA
Comissão	APROPRIAÇÃO	-----

EMENTA  
Sugestão 07 - Marinha - Ações de Caráter Sigiloso - R\$ 2 milhões (Sen. Esperidião Amin)

MODALIDADE DE EMENDA  
Comissão

**SEQUENCIAL**  
**000002753**

ESFERA ORÇAMENTÁRIA  
10 - Orçamento Fiscal

### ACRÉSCIMOS À PROGRAMAÇÃO

ÓRGÃO ORÇAMENTÁRIO  
52000 - Ministério da Defesa

UNIDADE ORÇAMENTÁRIA  
52131 - Comando da Marinha

**FUNCIONAL PROGRAMÁTICA**      **05.183.6112.2866.0001**

FUNÇÃO  
05 - Defesa Nacional

SUBFUNÇÃO  
183 - Informação e Inteligência

PROGRAMA  
6112 - Defesa Nacional

AÇÃO  
2866 - Ações de Caráter Sigiloso

SUBTÍTULO  
0001 - Nacional

LOCALIDADE BENEFICIADA  
9000000 - Nacional

ESPECIFICAÇÃO DO PRODUTO / UNIDADE DE MEDIDA	META	QTD META A ALTERAR
----------------------------------------------	------	--------------------

GND	MODALIDADE DE APLICAÇÃO	RP	em R\$ 1,00 ACRÉSCIMO
3 Outras Despesas Correntes	90 Aplicações Diretas	2	2.000.000
<b>TOTAL:</b>			<b>2.000.000</b>

SEQUENCIAL	FUNTE	GND	MODALIDADE DE APLICAÇÃO	ID	RP	em R\$ 1,00 CANCELAMENTO
000003719	1000	9 Reserva de Contingência	99 A Definir	0	2	2.000.000
<b>TOTAL:</b>						<b>2.000.000</b>

### JUSTIFICATIVA

Centro de Inteligência da Marinha - CIM  
CNPJ: 00.394.502/0272-63

Na Marinha do Brasil, cabe ao Centro de Inteligência da Marinha (CIM), como elo do Sistema Brasileiro de Inteligência (SISBIN), produzir conhecimentos em atendimento às prescrições dos planos e programas de inteligência, decorrentes da Política Nacional de inteligência (PNI). Ademais, compete ao CIM fornecer subsídios ao Comandante da Marinha nos assuntos relacionados ao Estado, ao preparo e ao emprego da Marinha do Brasil. Visando o cumprimento das diretrizes da (PNI), com dedicada atenção à proteção dos Projetos Estratégicos da Marinha do Brasil, o CIM figura como Órgão Central e tem a responsabilidade pela salvaguarda das informações vinculadas a tais projetos. Além das ameaças estabelecidas na PNI, as medidas a cargo do CIM, ainda, o cumprimento dos compromissos internacionais de sigilo, dos quais o Brasil é signatário, bem como a proteção da tecnologia adquirida pelo país, nas parcerias decorrentes destes projetos, por meio das cláusulas de compensação das contratadas, por meio de investimentos no Brasil. Assim sendo, faz-se necessário um aporte de recursos na ordem de R\$2.000.000,00 (dois milhões de reais), como Verba para Ações de Caráter Sigiloso.