

APÊNDICE I



PRESIDÊNCIA DA REPÚBLICA
GABINETE DE SEGURANÇA INSTITUCIONAL
SECRETARIA DE SEGURANÇA E COORDENAÇÃO PRESIDENCIAL
DEPARTAMENTO DE SEGURANÇA PRESIDENCIAL

DESCRIÇÃO E ESPECIFICAÇÕES TÉCNICAS DOS ITENS

1. SISTEMA DE PROTEÇÃO CONTRA DRONES

O sistema deverá ser capaz de monitorar a área delimitada, detectando possíveis invasões de Drones não autorizados, bem como permitir a neutralização do mesmo.

O sistema deverá ser instalado no Palácio do Planalto, no Palácio da Alvorada e no Palácio do Jaburu.

O sistema de proteção contra drones deverá ser totalmente integrável ao Sistema de Proteção das Instalações Presidenciais (ProPR), em fase de projeto, conforme especificações que constam no Apêndice VII. A comprovação da compatibilidade entre os sistemas se dará por meio de testes de modelagem computacional nas interfaces físicas e lógicas, dos equipamentos adquiridos, em comparação com as especificações projetadas no PRO-PR.

a. Conceito Geral do Sistema

O Sistema de Proteção Contra Drones deverá possuir uma plataforma de comando e controle, um subsistema de monitoração/detecção e outro de neutralização.

A monitoração deverá funcionar de forma integrada, emitindo sinal de alerta, quando detectada a invasão de Drones na área delimitada.

A partir do sinal de alerta, o sistema de comando e controle deverá registrar, classificar, alertar e acionar o subsistema de neutralização que deverá ser capaz de interferir diretamente sobre o Drone, obrigando-o a descer.

O módulo de comando e controle deverá operar de forma 100% automática (24/7) ou manual, conforme a necessidade.

b. Composição do Sistema:

Subsistema de Monitoração;

Subsistema de Neutralização; e

Plataforma de Comando e Controle.

1) Subsistema de Monitoração/Deteccção

O sistema de monitoração/deteccção deve garantir detectar Aeronaves Remotamente Pilotadas (ARP)/Drones independente de modelo, marca ou fabricante a uma distância de 100 metros após o limite delimitado das áreas do Palácio do Planalto, do Palácio da Alvorada e do Palácio do Jaburu. O sistema deverá permitir o ajuste de Potência (RF) da transmissão pela mesma antena, ampliando a distância de deteccção para até 200 metros, quando necessário.

O Sistema de monitoração será composto por Sensor de RF, com as seguintes características:

- Invólucro à prova de intempéries com classificação mínima IP65 resistente ao meio ambiente. Unidade selada sem peças internas móveis;
- Tamanho reduzido para facilidade de configuração e desmontagem;
- Receptor RF de banda larga com faixa de frequência de 400 MHz a 6 GHz;
- Varredura automática de toda largura de banda indicando sinais de não ameaça e ameaça;
- Processar automaticamente: escaneamento, identificação, classificação e alarme, com possibilidade de acionamento automático da neutralização;
- Possuir capacidade de gravação automática em tempo real dos registros (Logs) para auditoria;
- Realizar a identificação dos Drones invasores através de biblioteca de assinaturas eletrônicas (atualizável) de forma a garantir a efetividade do sistema para diversos fabricantes de drones e novos modelos, assim como seus componentes;
- Possuir capacidade de expansão para triangulação e localização dos sinais de drone e pilotos em tempo real; e
- Possuir capacidade de expansão para plotagem da trajetória dos drones em tempo real.

2) Subsistema de Neutralização

Para combater as ameaças de SARP/Drones o subsistema de neutralização deverá ser capaz de interferir em sistemas de comunicações modernos como Aeronaves Remotamente Pilotadas (ARP)/Drones controlados por radiofrequência e orientados por GPS, devendo possuir as seguintes características:

- Operar com alimentação primária de 110~220 VAC e secundário sistema NO-BREAK.
- Possuir capacidade de bloquear e/ou interferir através dos canais disponíveis as ameaças ao longo da faixa de frequência abaixo simultaneamente:

a) GPS L1 (padrão, configurável para faixas de frequência entre 1160 e 1610 MHz);

b) Canal específico para faixa de 2390 a 2510 GHz; e

c) Canal específico para faixa de 5690 a 5810 GHz.

d) Canal específico para expansão futura.

- Deverá permitir a escolha dos canais a serem acionados, ajuste do nível de potência de RF e pela possibilidade de inclusão de novos canais de operação compreendendo faixas entre 20 e 6000 MHz.

- Deverá realizar bloqueios de varreduras específicas conforme as faixas de operação e aplicação configurada. Possuir modulações de interferências especiais que garanta a máxima eficiência, contra Drones/SARP.

- Possuir conexões de rede Ethernet (LAN), podendo ser configurado através de um computador.

- O Subsistema de Neutralização deve garantir o “jameamento” de Aeronaves Remotamente Pilotadas (ARP)/Drones abatendo-os a uma distância de 100 metros após o limite delimitado das áreas do Palácio do Planalto, do Palácio da Alvorada e do Palácio do Jaburu.

- Possuir potências ajustáveis, com indicações de nível de potência de saída dos amplificadores, além de possuir robusto sistema de dissipação de calor e mecanismos de resfriamento/ventilação dos amplificadores do equipamento. Os amplificadores podem ser ligados e desligados por software de IHM (Interface Homem Máquina).

- Deverá operar no modo manual (*stand-alone*) em que o operador pode ativar os canais manualmente, por chaves, ou remotamente pela IHM e no modo automático através do acionamento pelo sistema de comando e controle.

3) **Plataforma de Comando e Controle**

A Plataforma deverá possuir uma IHM (Interface Homem Máquina), que permita ao administrador do sistema criar vários perfis de usuários com diferentes níveis de acesso ao sistema de comando e controle.

Deverá permitir ao usuário definir relatórios, acessar logs dos alarmes e fazer acompanhamento em tempo real do funcionamento do sistema.

Deverá permitir o envio de alertas e alarmes automaticamente via meio eletrônico (e-mail, SMS).

Deverá permitir integração com sistemas de terceiros.

Deverá monitorar o funcionamento dos sensores emitindo alertas em caso de falhas.

Deverá ter capacidade de diagnóstico dos seus sensores.

Deverá permitir ao administrador realizar remotamente o escaneamento prévio de frequências em cada posição geográfica dos sensores (no momento da instalação) de forma a permitir a otimização do sistema de forma a realizar uma melhor análise e definição do local de instalação do equipamento sensor e cobertura.

A Plataforma de Comando e controle deverá possuir mecanismo de auditoria para garantir a operação segura e evitar qualquer intervenção não registrada no sistema.

A Plataforma de Comando deverá possuir biblioteca de assinaturas de drones de consumo, com atualização permanente, durante a vigência do contrato.

A Plataforma de Comando deverá ser fornecida com licença permanente incorporando todas as melhorias e atualizações, durante a vigência do contrato.

A Plataforma de Comando deverá ser atualizável tanto online como offline.

A Plataforma de Comando deverá permitir instalação local ou virtualizada.

A Plataforma de Comando deverá permitir monitoramento local e remoto simultaneamente.

2. CAPACITAÇÃO DE OPERADORES DO SISTEMA DE PROTEÇÃO CONTRA DRONES

O Treinamento de Instalação, Configuração e Operação será fornecido na sede do Departamento de Segurança Presidencial (DSEG), em Brasília/DF, com duração mínima de 8 horas para 9 alunos.

O objetivo do treinamento será capacitar a equipe técnica do DSEG para instalar, configurar, operar e manter os sistemas de proteção contra drones.

A empresa Contratada deverá fornecer treinamentos de instalação, configuração e operação, com carga horária mínima de 8 horas aula, em até 3 dias.

Deverão ser disponibilizadas no mínimo 6 vagas para técnicos e/ou engenheiros do Departamento de Segurança Presidencial.

A empresa ganhadora do certame deverá emitir certificados de conclusão do curso para os alunos do treinamento.

Todo e qualquer material didático deverá ser fornecido pela Contratada.

Caso o sistema venha a sofrer atualização (*upgrade*) durante o período de garantia, e havendo necessidade, a Contratada deverá ofertar treinamento, sem custos adicionais para a Contratante, nos mesmos moldes do treinamento inicial. Caberá a Contratada definir a necessidade de atualização da capacitação de operadores, garantindo assim, o pleno emprego das capacidades dos equipamentos.

APÊNDICE II



PRESIDÊNCIA DA REPÚBLICA
GABINETE DE SEGURANÇA INSTITUCIONAL
SECRETARIA DE SEGURANÇA E COORDENAÇÃO PRESIDENCIAL
DEPARTAMENTO DE SEGURANÇA PRESIDENCIAL

ORDEM DE FORNECIMENTO Nº _____/20_____.

(MODELO)

Fornecedor: _____

CNPJ nº: _____._____._____/_____-____.

Fax: _____

Anexo: 2019NE_____, de ____ de _____ de 20____

Solicitamos a entrega dos materiais constantes da Nota de Empenho, em anexo, no Departamento de Segurança Presidencial, Via N-2 NORTE, Fundo do Palácio do Planalto, observadas as especificações e demais condições estabelecidas no Edital do respectivo processo de aquisição.

Prazo de entrega: ____ de _____ de 20____.

Horário de recebimento do material: Manhã: 08:00 às 12:00h / Tarde: 14:00 às 18:00h

Brasília/DF, ____ de _____ de 20____

Nome:

Departamento de Segurança Presidencial /GSIPR

Recebi a presente Ordem de Fornecimento, ciente das condições estabelecidas.

(Local), ____ de _____ de 20____

Nome:

Empresa

Obs: Favor datar, assinar e enviar via e-mail para (

@presidencia.gov.br).

APÊNDICE III

LIQUIDAÇÃO E PAGAMENTO DE DESPESA CONTRATUAL

TERMO DE RECEBIMENTO PROVISÓRIO - FISCAIS

Número do Contrato:		Contratada/razão social:	
CNPJ:		Vigência:	
Valor do contrato		Data de início da prestação	
Numero do processo de gestão e fiscalização			

Período de adimplemento ou mês da prestação liquidada:	
Nota fiscal/fatura n° (se houver):	

Ocorrências e providências:

1-Fatos positivos da execução

2-Fatos negativos da execução

3 – Abertura de processo de responsabilidade contratual do particular

4- Cálculo e aplicação de glosas

5 – Instrumento de Medição de Resultados

6 – Pesquisa com o público usuário

7 – Outras informações e análises

8 – TI – Prazo para o recebimento definitivo

Ressaltamos que o recebimento definitivo destes serviços e/ou bens ocorrerá em até _____ dias, desde que não ocorram problemas técnicos ou divergências quanto às especificações constantes do Contrato acima identificado.

Conclusão e recomendações:

APÊNDICE IV

LIQUIDAÇÃO E PAGAMENTO DE DESPESA CONTRATUAL TERMO DE RECEBIMENTO DEFINITIVO – ATESTO DO GESTOR

Número do Contrato:		Contratada/razão social:	
CNPJ:		Vigência:	
Valor do contrato:		Data de início da prestação:	
Numero do processo de acomp. e fiscalização:			

Período de adimplemento ou mês da prestação liquidada/OS:	
Número da Nota fiscal/fatura (se houver):	
Valor da Nota Fiscal/fatura (se houver):	

[OPÇÃO 1 – adimplemento total]

Declaro, com base nos relatórios dos fiscais do contrato (SEI n°xxxx e xxxx) [e/ou com fundamento em outro(s) documento], que o serviço foi prestado em conformidade com as especificações do contrato, em razão do que realizo o atesto com o recebimento definitivo da prestação e o encaminhamento do processo para o pagamento da despesa, no montante de R\$ _____ (por extenso).

[OPÇÃO 2 – havendo prestação em quantidade/qualidade menor que a devida]

Declaro, com base nos relatórios dos fiscais do contrato (SEI n°xxxx e xxxx) [e/ou com fundamento em outro(s) documento], que o serviço foi parcialmente prestado em conformidade com as especificações do contrato, em razão do que realizo o atesto parcial com recebimento definitivo apenas da parcela adimplida, fato que recomenda o encaminhamento do processo para o pagamento da despesa apenas na proporção indicada no montante de R\$ _____ (por extenso).

[OPÇÃO 3 – havendo redimensionamento de valores a serem pagos]

Declaro, com base nos relatórios dos fiscais do contrato (SEI n°xxxx e xxxx) [e/ou com fundamento em outro(s) documento], que o serviço foi prestado com relativa conformidade com as especificações do contrato, todavia com incidência de redimensionamento de valor na aplicação do **Instrumento de Medição de Resultados-IMR**, em razão do que realizo o atesto com recebimento definitivo da parcela adimplida, fato que recomenda o encaminhamento do processo para o pagamento da despesa apenas na proporção indicada no montante de R\$ _____ (por extenso).

[OPÇÃO 4 – inadimplemento total]

Declaro, com base nos relatórios dos fiscais do contrato (SEI n°xxxx e xxxx) [e/ou com fundamento em outro(s) documento], que o serviço não foi prestado conforme as especificações do contrato, em razão do que não se poderá realizar o pagamento solicitado pela contratada.

Nota(s) Fiscal(is)

N°	Data de emissão	Valor	Multa	Glosa e redução	Crédito	Liquidação

APÊNDICE V

(MODELO)

(em papel timbrado da empresa)

TERMO DE GARANTIA DOS PRODUTOS FORNECIDOS

A empresa _____, CNPJ _____, por intermédio de seu representante legal o(a) Sr(a) _____ RG _____ e CPF _____, compromete-se a prestar garantia, nos seguintes termos:

I. O objeto terá prazo de garantia de ____ (_____) meses, a contar do recebimento definitivo.

II. Durante o período de garantia, a adjudicatária, independentemente de ser ou não fabricante do objeto, obriga-se a substituir, sem ônus para o GSI/PR, o objeto que apresentar defeitos ou incorreções resultantes da fabricação, no prazo máximo de 60 (sessenta) dias úteis, a contar a notificação.

III. O pedido de substituição do objeto, durante o período de garantia, será formalizado por telefone, *e-mail*, fax ou outro meio hábil de comunicação.

(local), ____ de _____ 20__.

(assinatura do representante legal)

Nome:

Empresa:

APÊNDICE VI

PREGÃO, NA FORMA ELETRÔNICA, Nº /2019
PROCESSO Nº

MODELO DA PLANILHA DE COMPOSIÇÃO DE PREÇOS (Proposta Comercial)

Pregão, na forma eletrônica, nº /2019 - GSI

Data de abertura:/...../2019.

GRUPO	ITEM	DESCRIÇÃO/ ESPECIFICAÇÃO	UNIDADE DE MEDIDA	QTD TOTAL	PREÇO UNITÁRIO ESTIMADO	PREÇO TOTAL ESTIMADO
1	1	Sistema de Proteção Contra Drones	Und	03		
	2	Capacitação de Operadores do Sistema de Proteção Contra Drones	Sv	09		
VALOR TOTAL ESTIMADO R\$						

(*) Os valores que deverão ser cadastrados no sistema Comprasnet é o valor total por item.

1. Observações:

- a) prazo de validade de 60 (sessenta) dias, a contar da data de sua apresentação;
- b) prazo de entrega de até ____ (____) dias a contar do recebimento da Solicitação de Fornecimento;

2. Declarações:

- a) declaração expressa de estarem incluídos nos preços cotados todos os impostos, taxas, fretes, seguros, bem como quaisquer outras despesas, diretas e indiretas, incidentes sobre o objeto deste Pregão, nada mais sendo lícito pleitear a esse título.
- b) Declaro de que tenho pleno conhecimento das condições da licitação, bem como das normas e legislação que tratam do assunto.

3. Dados da empresa:

EMPRESA/RAZÃO SOCIAL:

ENDEREÇO:

CEP:

CNPJ:

INSCRIÇÃO ESTADUAL:

TELEFONE:

FAX:

BANCO:

AGÊNCIA: CONTA-CORRENTE:

E-MAIL:

_____, ____ de _____ de 2019.

(Nome completo do declarante)

(Nº da CI do declarante)

(Assinatura do declarante)

APÊNDICE VII



PRESIDÊNCIA DA REPÚBLICA
GABINETE DE SEGURANÇA INSTITUCIONAL
SECRETARIA DE SEGURANÇA E COORDENAÇÃO PRESIDENCIAL
DEPARTAMENTO DE SEGURANÇA PRESIDENCIAL

SOLUÇÃO ANTI DRONE PREVISTA PARA O SISTEMA DE PROTEÇÃO DAS INSTALAÇÕES PRESIDENCIAIS (PROPR)

1 Solução Anti Drone

A solução anti drone tem sua área de cobertura até 200 metros após a cerca de limite da edificação.

A solução anti drone será capaz de identificar o operador e o drone dentro do limite de 200 metros de perímetro e também será capaz de fazer o jamming das frequências de controle e de GPS.

A solução anti drone deverá possuir um sistema de detecção automático, ou seja, caso entre uma aeronave dentro do raio de ação da solução e fazer sua identificação automaticamente sem a necessidade de ação de operador.

Após a detecção a solução deve fazer o jamming do controle do drone automaticamente, fazendo com que o mesmo retorne para o ponto de origem.

O bloqueio de sinal de GPS do drone será acionado somente pela intervenção do operador do sistema.

Toda a detecção de invasão do perímetro será notificada aos operadores através da solução de integração (Sistema Integrador).

2 Sistema anti drone

O sistema anti drone deve possuir as características abaixo como premissa:

2.1 Detecção de drones

O sistema deve garantir detectar o drone e seu operador a uma distância de 200 metros após o limite dos sítios.

O sistema deve garantir o “jameamento” do drone impedindo que ele entre a uma distância de 200 metros após o limite dos sítios.

O sistema deve garantir o “jameamento” do drone abatendo-o a uma distância de 200 metros após o limite dos sítios.

2.2 Requisitos de software

O software deve ser fornecido com licença permanente por tempo indeterminado;

O software deve ser capaz de rodar em um ambiente totalmente virtualizado com VMware ou Hyper V;

O software deve permitir a seleção dos modos de operação do equipamento (faixas de frequência, parâmetros de varreduras, modulações, etc.);

O software do equipamento deve permitir a análise de cobertura do site, para definição da posição de instalação e operação do equipamento;

O software do equipamento deve fornecer uma biblioteca de antenas, com modelos de irradiação, para definição e análise de cobertura, para cada aplicação;

O software deve apresentar as indicações do sistema e seus Amplificadores (temperatura e potência) e dar avisos se necessário;

O software deve ter a capacidade de ligar/desligar cada canal e/ou seu amplificador de forma independente;

O software deve permitir realizar a configuração de cada equipamento e armazenar a configuração realizada;

O software deve permitir buscar a configuração padrão do equipamento conforme definições de fábrica (“*Factory Default*”);

O software deve manter o cadastro de usuários e suas respectivas permissões de acesso e controle ao sistema;

O cadastro de usuários deve exigir o cadastro de uma senha de acesso para cada usuário, sendo a senha requisitada para qualquer acesso aos módulos do sistema;

O cadastro de usuários deve permitir, minimamente, a configuração do tipo do usuário entre usuário “básico” = operador, e um usuário “avançado” = técnico;

O software deve manter e exibir logs de eventos, relacionados a usuários, de todas as atividades efetuadas no sistema por usuário “básico” = operador, e um usuário “avançado” = técnico;

O software deve manter e exibir logs de eventos operacionais (por exemplo: avisos de temperatura dos amplificadores), por pelo menos um mês de armazenamento;

O software do equipamento deve permitir a análise de cobertura do site, para definição da posição de instalação e operação do equipamento;

O sistema deve possuir capacidade de bloquear e/ou interferir nas ameaças ao longo da faixa de frequência abaixo (as bandas populares dos Drones), mas não se restringindo a tal:

- 433 - 470MHz (ISM);
- 902 - 928MHz (ISM);
- GPS L1 (padrão, configurável para faixas de frequência entre 1160 e 1610 MHz);
- 2390 - 2490MHz (WIFI);
- 5725 - 5875MHz (WIFI);
- Canal específico para expansão futura.

O sistema deve possuir a capacidade de detectar tanto o operador quanto o drone a uma distância de 200 metros após o perímetro de cada edificação.

O software de radar deve prover mapas em alcance e velocidade radial (*Doppler*) da atividade na área a ser protegidas.

O software deve analisar a trajetória ao longo do tempo.

O software deve acionar alertas sobre movimento identificados como suspeitos.

O software deve permitir criar zonas de interesse em sua área de cobertura.

O software deve transmitir posições de alertas para o software de integração.

O software deve permitir repetição de alerta para identificação de possíveis violações de segurança e melhoria da segurança geral do site.

O software deve permitir integração a nível de software através de uma *Application Programming Interface* (API) ou *Software Development Kit* (SDK).

2.3 Requisitos de hardware.

Os servidores devem permitir a sua virtualização e atender as seguintes características mínimas, mas não se restringindo a tal:

Deve possuir 8 vCPU virtualizadas;

Deve possuir 16 GB de capacidade de memória RAM;

Deve possuir capacidade de disco 3200 (GB);

Deve possuir capacidade de 150 Mbps operações de entrada e saída por segundo (IOPS);

Deve possuir uma placa de rede 1 Gigabits virtualizada.