I - acompanhar a execução dos acordos de compensação;

II - identificar aspectos de interesse comum para atualização das listas de tecnologias prioritárias para a defesa; e

III - acompanhar as atividades de fomento e fortalecimento dos setores de interesse do Ministério da Defesa.

CAPÍTULO V

DISPOSIÇÕES GERAIS

Art. 12. As negociações de contratos de importação de produtos de interesse da defesa realizadas pelos Comandos das Forças Singulares e pelos órgãos que integram a estrutura do Ministério da Defesa, com valor líquido (preço Free on Board - FOB) igual ou superior a US$ 50.000.000,00 (cinquenta milhões de dólares norte-americanos), ou valor equivalente em outra moeda, em uma única compra ou cumulativamente com um mesmo fornecedor, num período de até doze meses, devem incluir um acordo de compensação, salvo a hipótese prevista no § 2º do art. 14.

Art. 13. As negociações de contratos de importação com valores líquidos (preço Free on Board - FOB) inferiores a US$ 50.000.000,00 (cinquenta milhões de dólares norte-americanos), ou valor equivalente em outra moeda, podem incluir acordos de compensação, desde que sejam do interesse dos Comandos das Forças Singulares e dos órgãos que integram a estrutura do Ministério da Defesa.

Art. 14. O valor a ser compensado deve ser precedido de análise da exequibilidade para exigência de contrapartida e, quando possível, corresponder a cem por cento do valor do contrato de aquisição.

§ 1º Observado o disposto no caput, fica a critério de cada Comando de Força Singular ou dos órgãos que integram a estrutura do Ministério da Defesa, conforme o caso, estabelecer o percentual que julgar adequado.

§ 2º O estudo de exequibilidade da exigência da contrapartida, em relação ao contexto do contrato comercial, poderá ensejar sua dispensa, desde que caracterizada a urgência ou a relevância da operação, após análise do Comando da Força Singular e anuência do Ministério da Defesa, ouvida a Comissão Mista da Indústria de Defesa - CMID.

§ 3º Na hipótese do § 2º, o Ministério da Defesa poderá exigir que a importação de Produto Estratégico de Defesa - PED seja feita com envolvimento de Empresa Estratégica de Defesa - EED capacitada a realizar ou conduzir, em território nacional, no mínimo, uma das atividades previstas na alínea "a" do inciso IV do caput do art. 2º da Lei nº 12.598, de 2012.

Art. 15. O propósito do acordo de compensação deve ser explicitado ao fornecedor desde o início das negociações, bem como em todo e qualquer documento referente ao processo de obtenção.

Art. 16. Em processos de obtenção de produtos de interesse da defesa pelos Comandos das Forças Singulares e por órgãos que integram a estrutura do Ministério da Defesa devem constar explicitamente no instrumento convocatório ou documento equivalente:

I - a exigência de que o contratado promova, em favor de beneficiários, medidas de compensação tecnológica, industrial e comercial como fatores a serem considerados no julgamento das propostas; e

II - que é proibida a transferência de eventuais custos de offset para os valores apresentados no Contrato Comercial.

Parágrafo único. Não serão firmados acordos de compensação sem a associação prévia a um contrato de aquisição, por iniciativa isolada do fornecedor estrangeiro, de empresa brasileira ou na expectativa de realização qualquer processo de aquisição de produtos de interesse da defesa, salvo se autorizado pelo Ministro de Estado da Defesa.

Art. 17. A empresa ofertante é a responsável pela indicação da empresa beneficiária, podendo se utilizar de sistemas do Ministério da Defesa ou outra fonte de informações dos Comandos das Forças Singulares, devendo atestar se a beneficiária possui as necessárias competências e capacidade tecnológica, industrial ou comercial do objeto a ser compensado.

§ 1º Caso haja a necessidade de substituição da empresa beneficiária, ao longo do processo de execução de um projeto do acordo de compensação, a empresa contratada é a responsável pela indicação de uma empresa substituta, observadas as disposições desta Política.

§ 2º A empresa beneficiária poderá ser oportunamente catalogada no Sistema de Cadastramento de Produtos e Empresas de Defesa - SISCAPED do Ministério da Defesa.

Art. 18. Os editais de licitação, os processos de dispensa ou inexigibilidade de licitação nos quais sejam demandadas medidas de compensação tecnológica, industrial e comercial, deverão:

I - estabelecer exigências de compensação tecnológica, industrial e comercial que permitam qualificar, juntamente com os demais critérios de avaliação, a seleção da proposta mais vantajosa para a Administração Pública, a fim da promoção do desenvolvimento da Base Industrial de Defesa - BID;

II - prever o envolvimento, quando aplicável, de instituições de pesquisa e ensino, de nível superior ou técnico, para a retenção e disseminação do conhecimento adquirido;

III - incluir cláusula que obrigue a Contratada a exigir das empresas beneficiadas um programa de Gestão do Conhecimento, visando mitigar o impacto de eventual perda de pessoal capacitado, em virtude de um acordo de compensação; e

IV - incluir cláusulas que obriguem a realização de estudos de avaliação de risco pela empresa contratada, a fim de identificar e mitigar potenciais riscos que possam afetar a continuidade dos benefícios decorrentes das compensações, após findo o prazo do respectivo acordo de compensação.

Art. 19. Os Comandos das Forças Singulares, em suas normas específicas, respeitadas as peculiaridades de seus projetos de compensação, poderão estabelecer formas de incentivo às empresas de interesse de defesa, bem como de meios de incentivo às pequenas e médias empresas como beneficiárias dos projetos, a título de fomento.

Art. 20. A escolha de empresa para ser beneficiária de acordo de compensação deve privilegiar, sempre que possível, empresas que não integrem o mesmo grupo econômico da empresa contratada.

Parágrafo único. Entende-se por grupo econômico, para efeitos desta Portaria, a definição contida na Consolidação da Leis do Trabalho - CLT.

Art. 21. O acordo de compensação será instrumentalizado por meio de um documento específico associado ao contrato principal por um anexo ou por cláusula contratual que definirá as obrigações do fornecedor estrangeiro.

§ 1º O acordo de compensação poderá ser formalizado juntamente com o contrato principal associado ou em prazo definido por cláusula contratual.

§ 2º A delegação de competência para a assinatura do contrato principal deve ser estendida para a assinatura do acordo de compensação correlato.

Art. 22. O prazo de execução e implementação do acordo de compensação deve, sempre que possível, coincidir com a duração do contrato principal associado.

Parágrafo único. O acordo de compensação cujo prazo de implementação seja superior à duração do contrato principal associado será justificado e instruído com medidas que reduzam o risco de inadimplemento por parte do fornecedor estrangeiro, podendo se exigir a prestação de garantias, a critério da autoridade competente, desde que prevista no instrumento convocatório ou documento equivalente.

Art. 23. Os projetos constantes do acordo de compensação deverão atender aos conceitos de causalidade e de adicionalidade com o contrato principal, cabendo ao fornecedor estrangeiro demonstrar a causalidade.

Art. 24. Os benefícios decorrentes dos acordos de compensação devem atender às áreas de interesse, por meio do atingimento de, pelo menos, um dos seguintes termos:

I - capacitar a Base Industrial de Defesa - BID com novas tecnologias;

II - integrar a fabricação de materiais ou equipamentos na Base Industrial de Defesa - BID;

III - capacitar a Base Industrial de Defesa - BID na nacionalização da logística e na manutenção dos produtos de interesse de defesa;

IV - especializar e aperfeiçoar os recursos humanos do setor de defesa; e

V - integrar a Base Industrial de Defesa - BID na cadeia produtiva dos produtos de interesse de defesa, por meio de parcerias internacionais.

Art. 25. Os benefícios a que se refere o art. 24 poderão ser repassados a outros órgãos governamentais ou a entidade privada não integrante da Base Industrial de Defesa - BID, observada a capacidade de absorção do beneficiário do objeto acordado, atestada pela ofertante.

Parágrafo único. O memorando de entendimento firmado entre o fornecedor estrangeiro e o beneficiário deverá ser aprovado pelos Comandos das Forças Singulares ou órgão contratante.

Art. 26. Os acordos de compensação que gerem, eventualmente, excedentes em relação ao valor de compensação pactuado, poderão, a juízo do Comando da Força Singular contratante, ser considerados créditos excedentes de compensação.

Parágrafo único. Os créditos excedentes existentes no banco de crédito de compensação em favor da empresa contratada poderão ser compensados em um prazo máximo de cinco anos, a partir de seu reconhecimento, não podendo comprometer mais de vinte por cento do valor a ser compensado no novo contrato.

CAPÍTULO VI

DISPOSIÇÕES FINAIS

Art. 27. Situações especiais ou casos não previstos nesta Portaria devem ser submetidos ao Ministro de Estado da Defesa.

Art. 28. Os atos administrativos relativos aos acordos de compensação devem observar as disposições da Lei nº 9.784, de 29 de janeiro de 1999, que regula o processo administrativo no âmbito da Administração Pública Federal.

Art. 29. Fica revogada a Portaria GM-MD nº 3.662, de 2 de setembro de 2021, publicada no Diário Oficial da União nº 169, Seção 1, páginas 9 e 10, de 6 de setembro de 2021.

Art. 30. Esta Portaria entra em vigor na data de sua publicação.

JOSÉ MUCIO MONTEIRO FILHO

PORTARIA GM-MD N° 4.138, DE 14 DE AGOSTO DE 2023

Institui a Equipe de Coordenação Setorial da Defesa (ECS/Def) da Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC).

O MINISTRO DE ESTADO DA DEFESA, no uso das atribuições que lhe confere o art. 87, parágrafo único, incisos I e II, da Constituição, tendo em vista o disposto no art. 6º do Decreto nº 10.748, de 16 de julho de 2021, o item 2.3.5 do Anexo ao Decreto nº 10.222, de 5 de fevereiro de 2020, e de acordo com o que consta do Processo Administrativo nº 65364.005385/2023-12, resolve:

CAPÍTULO I

INSTITUIÇÃO DA EQUIPE DE COORDENAÇÃO SETORIAL DA DEFESA (ECS/Def) DA REDE FEDERAL DE GESTÃO DE INCIDENTES CIBERNÉTICOS (ReGIC)

Art. 1º Esta Portaria institui a Equipe de Coordenação Setorial da Defesa (ECS/Def) da Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC), operada pelo Comando de Defesa Cibernética (ComDCiber) do Exército Brasileiro, na condição de órgão central do Sistema Militar de Defesa Cibernética (SMDC).

CAPÍTULO II

ÁREA DE ATUAÇÃO

Art. 2º A Equipe de Coordenação Setorial da Defesa (ECS/Def) de que trata esta Portaria atua na gestão de incidentes cibernéticos no âmbito do Ministério da Defesa (MD), das Forças Singulares (FS) e de outras entidades previstas no Plano Nacional de Segurança de Infraestruturas Críticas (PlanSIC) relacionadas ao setor Defesa que vierem a aderir à Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC).

Art. 3º A Equipe de Coordenação Setorial da Defesa (ECS/Def) tem por missão coordenar as atividades de prevenção, tratamento e resposta a incidentes cibernéticos no âmbito do Setor Defesa, consolidando as notificações dos principais incidentes cibernéticos das equipes centrais do Ministério da Defesa, das Forças Singulares e das demais Equipes de Prevenção, Tratamento e Resposta a Incidentes em Redes (ETIR) públicas ou privadas relacionadas ao setor Defesa.

Art. 4º Cabe à Equipe de Coordenação Setorial da Defesa (ECS/Def) articular-se com o Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR/GOV).

Art. 5º A Equipe de Coordenação Setorial da Defesa (ECS/Def) atenderá ao seguinte público-alvo:

I - obrigatoriamente, todos os órgãos e entidades da Administração Pública Federal (APF) direta, autárquica e fundacional do Ministério da Defesa e Forças Singulares, por intermédio de suas Equipes de Prevenção, Tratamento e Resposta a Incidentes em Redes (ETIR), independente do seu modelo de implementação; e

II - voluntariamente, por adesão à Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC), as empresas públicas, bem como as de sociedade de economia mista federais e as suas subsidiárias, que sejam relacionadas ao setor Defesa como infraestrutura crítica de informação, por intermédio de suas equipes principais.

CAPÍTULO III

TERMOS E DEFINIÇÕES

Art. 6º Para efeito desta Portaria ficam estabelecidos os termos e as principais definições a seguir:

I - agente responsável - servidor público, militar de carreira ou empregado público, ocupantes de cargo efetivo em órgão ou entidade da administração pública federal, direta e indireta, que se enquadre em qualquer das opções seguintes:

a) execute o tratamento de informação classificada;

b) possua credencial de segurança;

c) seja responsável por um posto de controle de um órgão de registro; e

d) utilize dispositivos que tenham embarcado criptografia de Estado.

II - ameaça - conjunto de fatores externos com o potencial de causar em dano para um sistema ou organização;

III - avaliação de riscos - processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco;

IV - público-alvo - conjunto de pessoas, setores, órgãos ou entidades atendidas por uma Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos; e

V - incidente cibernético - ocorrência que pode comprometer, real ou potencialmente, a disponibilidade, a integridade, a confidencialidade ou a autenticidade de sistema de informação ou das informações processadas, armazenadas ou transmitidas por esse sistema. Poderá também ser caracterizada pela tentativa de exploração de vulnerabilidade de sistema de informação que caracterize violação de norma, política de segurança, procedimento de segurança ou política de uso. De maneira geral, os tipos de atividade comumente reconhecidas como incidentes cibernéticos são:

a) tentativas de obter acesso não-autorizado a um sistema ou a dados armazenados;

b) tentativa de utilização não autorizada de sistemas para a realização de atividades de processamento ou armazenamento de dados;

c) mudanças não-autorizadas de firmware, hardware ou software em um ambiente computacional;

d) ataques de negação de serviço (DoS); e

e) demais ações que visem afetar a disponibilidade ou integridade dos dados. Um incidente de segurança cibernética não significa necessariamente que as informações já estão comprometidas; significa apenas que a informação está ameaçada.

Parágrafo único. Em complemento aos termos definidos no art. 6º, deve-se observar as definições e siglas previstas no Glossário de Segurança da Informação (SI), conforme Portaria GSI/PR nº 93, de 18 de outubro de 2021, bem como as Normas Complementares do Gabinete de Segurança Institucional da Presidência (GSI/PR).

CAPÍTULO IV

COMPETÊNCIA

Art. 7º Compete ao Comando de Defesa Cibernética (ComDCiber):

I - designar os integrantes da Equipe de Coordenação Setorial da Defesa (ECS/Def) no prazo de até trinta dias a contar da data de publicação desta Portaria, nos termos do disposto no Decreto nº 10.748, de 2021;

II - supervisionar a atuação da Equipe de Coordenação Setorial da Defesa (ECS/Def) na articulação com as Equipes de Prevenção, Tratamento e Resposta a Incidentes em Redes (ETIR) da Marinha do Brasil (MB), do Exército Brasileiro (EB), da Força Aérea Brasileira (FAB), do Ministério da Defesa e de outros órgãos do setor Defesa que passem a integrar a Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC) e com o Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR/GOV);

III - apoiar as atividades das Equipes de Prevenção, Tratamento e Resposta a Incidentes em Redes (ETIR) relacionadas ao setor Defesa, nos termos do disposto no inciso VII do art. 15 do Decreto nº 9.637, de 26 de dezembro de 2018; e

IV - prover os meios necessários para a capacitação e o aperfeiçoamento técnico dos membros da Equipe de Coordenação Setorial da Defesa (ECS/Def), bem como prover a infraestrutura necessária à sua operação.

Parágrafo único. No âmbito do Ministério da Defesa e das Forças Singulares, compete ao Comando de Defesa Cibernética (ComDCiber) do Exército Brasileiro, na condição de órgão central do Sistema Militar de Defesa Cibernética (SMDC), operar a Equipe de Coordenação Setorial da Defesa (ECS/Def) na coordenação com as Equipes de Prevenção, Tratamento e Resposta a Incidentes em Redes (ETIR) a ela vinculadas e na articulação com o Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR/GOV).

Art. 8º Compete à Equipe de Coordenação Setorial da Defesa (ECS/Def) no âmbito dos órgãos e entidades sob a sua coordenação:

I - divulgar medidas de prevenção, tratamento e resposta a incidentes cibernéticos;

II - compartilhar alertas sobre ameaças e vulnerabilidades cibernéticas;

III - divulgar informações sobre ataques cibernéticos;

IV - promover a cooperação entre os participantes da Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC);

V - promover a celeridade na resposta a incidentes cibernéticos;

VI - comunicar imediatamente o Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR/GOV) sobre a existência de vulnerabilidades ou incidentes cibernéticos mais relevantes e que comprometam, real ou potencialmente, a Disponibilidade, a Integridade, a Confidencialidade e a Autenticidade (DICA) das informações inerentes aos serviços prestados ou contratados, nos termos do disposto no inciso IX do art. 17 do Decreto nº 9.637, de 2018;

VII - requerer às Equipes de Prevenção, Tratamento e Resposta a Incidentes em Redes (ETIR) do setor Defesa informações sobre as vulnerabilidades ou incidentes cibernéticos mais relevantes e que comprometam a Disponibilidade, a Integridade, a Confidencialidade e a Autenticidade (DICA) das informações que transitam pelas redes, a serem definidos pelas próprias instituições que as operam com base na gestão de riscos das suas Infraestruturas Críticas (IC);

VIII - notificar o Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR/GOV) quanto aos incidentes cibernéticos mais relevantes e que impactam a Disponibilidade, a Integridade, a Confidencialidade e a Autenticidade (DICA) das informações que transitam pelas redes, com base nas notificações obtidas das equipes centrais das Forças Singulares e das demais Equipes de Prevenção, Tratamento e Resposta a Incidentes em Redes (ETIR) do setor Defesa;

IX - identificar outras entidades, públicas ou privadas, relevantes para a Gestão de Incidentes Cibernéticos nas áreas prioritárias do setor Defesa;

X - difundir lições aprendidas para a melhoria do processo de prevenção, tratamento e resposta a incidentes cibernéticos no âmbito da Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC);

XI - distribuir sistemas colaborativos (hardware e software) com o objetivo de otimizar a difusão de informações relativas a incidentes cibernéticos, normatizando sua adoção e capacitando pessoal para a sua operação;

XII - identificar proativamente vulnerabilidades cibernéticas existentes nos ativos de informação do Sistema Militar de Defesa Cibernética (SMDC);

XIII - fornecer informações relativas às Equipes de Prevenção, Tratamento e Resposta a Incidentes em Redes (ETIR) dos órgãos e entidades que deverão constar do Plano Setorial da Defesa para a Gestão de Incidentes Cibernéticos; e

XIV - elaborar, atualizar e divulgar o Plano Setorial para Gestão de Incidentes Cibernéticos da Defesa (PSGIC - Def), nos termos do art. 13 do Decreto nº 10.748, de 2021.

Art. 9º Compete ao agente responsável da Equipe de Coordenação Setorial da Defesa (ECS/Def):

I - executar o tratamento de informação classificada;

II - possuir credencial de segurança;

III - zelar pela utilização de dispositivos que tenham criptografia baseada em algoritmo de Estado embarcada, quando disponíveis, nas comunicações com as Equipes de Prevenção, Tratamento e Resposta a Incidentes em Redes (ETIR);

IV - criar os procedimentos internos, gerenciar as atividades e distribuir tarefas para a Equipe de Coordenação Setorial da Defesa (ECS/Def); e

V - assessorar o Comando de Defesa Cibernética (ComDCiber) na gestão de incidentes cibernéticos.

§ 1º Excepcionalmente, as equipes do Ministério da Defesa e das Forças Singulares poderão articular-se diretamente com o Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR/GOV), conforme estabelecido no Plano Setorial de Gestão de Incidentes Cibernéticos da Defesa (PSGIC-Def), hipótese em que deverão informar a Equipe de Coordenação Setorial da Defesa (ECS/Def) tempestivamente.

§ 2º As Equipes de Prevenção, Tratamento e Resposta a Incidentes em Redes (ETIR) centrais das Forças Singulares e as demais Equipes de Prevenção, Tratamento e Resposta a Incidentes em Redes (ETIR) diretamente vinculadas à Equipe de Coordenação Setorial da Defesa (ECS/Def), pelo princípio da oportunidade e de modo colaborativo, podem notificar, em função do tipo e do impacto, o incidente cibernético para o Gestor de Segurança da Informação de órgãos e entidades não integrantes da Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC) ou de outros setores que não o da Defesa.

CAPÍTULO V

MODELO DE IMPLEMENTAÇÃO E COMPOSIÇÃO

Art. 10. A Equipe de Coordenação Setorial da Defesa (ECS/Def) exerce um papel de coordenação com as equipes centrais das Forças Singulares e com as Equipes de Prevenção, Tratamento e Resposta a Incidentes em Redes (ETIR) da Autoridade Certificadora de Defesa (AC-Defesa), da Seção de Comando e Controle do Estado-Maior das Forças Armadas (SC-1/EMCFA), da Escola Superior de Guerra (ESG), da Escola Superior de Defesa (ESD), do Hospital das Forças Armadas (HFA) e das equipes principais das entidades públicas ou privadas relacionadas ao setor Defesa que vierem aderir à Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC).

§ 1º As equipes centrais das Forças Singulares, bem como as demais Equipes de Prevenção, Tratamento e Resposta a Incidentes em Redes (ETIR) do setor Defesa são responsáveis por implementar as estratégias e exercer suas atividades de coordenação em suas respectivas áreas de responsabilidade.

§ 2º O processo de coordenação desenvolvido pela Equipe de Coordenação Setorial da Defesa (ECS/Def) envolve o recebimento de notificações de incidentes cibernéticos oriundas das equipes do setor, sua consolidação e compartilhamento das informações a elas inerentes, bem como o acompanhamento do tratamento e resposta e a geração de indicadores e estatísticas.

§ 3º O Plano Setorial para Gestão de Incidentes Cibernéticos da Defesa (PSGIC-Def) definirá como se dará a coordenação entre a Equipe de Coordenação Setorial da Defesa (ECS/Def) e as demais equipes centrais das Forças Singulares e Equipes de Prevenção, Tratamento e Resposta a Incidentes em Redes (ETIR) vinculadas diretamente, assim como as possibilidades de apoio da Equipe de Coordenação Setorial da Defesa (ECS/Def) à sua constituência para fins de prevenção, tratamento e resposta.

§ 4º A Equipe de Coordenação Setorial da Defesa (ECS/Def) adotará o modelo combinado ou misto, conforme a Norma Complementar nº 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009.

Art. 11. A Equipe de Coordenação Setorial da Defesa (ECS/Def) será composta pelos seguintes membros:

I - um oficial superior, preferencialmente, no último posto, com conhecimento em Gestão de Incidentes Cibernéticos que exercerá a função de agente responsável pela ECS/Def;

II - no mínimo dois oficiais e/ou Sargento (S Ten/Sgt) com conhecimento em Gestão de Incidentes Cibernéticos e gerencial, para compor a Turma Gerencial; e

III - no mínimo quatro oficiais e/ou Sargento (S Ten/Sgt) com perfil técnico adequado às funções de prevenção, tratamento e resposta de incidentes de rede, além de conhecimento em administração de sistema ou de segurança, administração de banco de dados e de rede, para compor a Turma Técnica.

§ 1º O agente responsável Equipe de Coordenação Setorial da Defesa (ECS/Def) pode solicitar que oficiais e/ou Sargento (S Ten/Sgt) do Comando de Defesa Cibernética (ComDCiber) componham a turma de suporte, conforme a situação exigir, composta por militares com conhecimentos nas áreas jurídica, comunicação social, relações institucionais, inteligência e gestão de riscos, formando a Turma de Suporte (ad hoc).

§ 2º A Equipe de Coordenação Setorial da Defesa (ECS/Def) deve ser constituída por militares de carreira do Comando de Defesa Cibernética (ComDCiber), com caráter técnico e gerencial.

§ 3º Os integrantes da Equipe de Coordenação Setorial da Defesa (ECS/Def) devem ser indicados pelo Comandante de Defesa Cibernética (ComDCiber) e designados por meio de Boletim Interno do Comando de Defesa Cibernética (ComDCiber), dando ciência ao Ministério da Defesa.

§ 4º Para cada membro da Equipe de Coordenação Setorial da Defesa (ECS/Def) deve ser designado um suplente que deverá ser qualificado e orientado para a realização das tarefas e atividades de uma Equipe de Prevenção, Tratamento e Resposta a Incidentes em Redes (ETIR).

§ 5º Os trabalhos da Equipe de Coordenação Setorial da Defesa (ECS/Def) são voltados para a Gestão de Incidentes Cibernéticos e desenvolvidos em dedicação integral, a fim de permitir o tratamento e a resposta oportuna e prevenir a escalada para situações de crise.

§ 6º O agente responsável da Equipe de Coordenação Setorial da Defesa (ECS/Def) exerce a função de assessor direto do Comando de Defesa Cibernética (ComDCiber).

CAPÍTULO VI

AUTONOMIA

Art. 12. A Equipe de Coordenação Setorial da Defesa (ECS/Def) opera em regime de autonomia compartilhada com outros órgãos do Comando de Defesa Cibernética (ComDCiber), constituindo órgão de assessoramento no processo decisório relativo à Gestão de Incidentes Cibernéticos, no âmbito do Ministério da Defesa, das Forças Singulares e do Sistema Integrado de Dados de Infraestruturas Críticas (IC) relacionadas ao setor Defesa.

Art. 13. A Equipe de Coordenação Setorial da Defesa (ECS/Def) tem competência para recomendar medidas de prevenção, tratamento, resposta e procedimentos a serem executados ou as medidas de recuperação durante e pós-incidente cibernético no âmbito do Setor Defesa, bem como para discutir as ações a serem tomadas (ou as repercussões, caso as recomendações não sejam seguidas) com os outros órgãos do Comando de Defesa Cibernética (ComDCiber).

Art. 14. A tomada de decisão técnica relacionada a incidentes cibernéticos que não comprometam, real ou potencialmente, a continuidade da Disponibilidade, a Integridade, a Confidencialidade e a Autenticidade (DICA) das informações que transitam pela rede constitui competência do agente responsável da Equipe de Coordenação Setorial da Defesa (ECS/Def).

Art. 15. Cada órgão do setor Defesa tem autonomia para deliberar sobre o nome-fantasia de sua equipe central, bem como das demais Equipes de Prevenção, Tratamento e Resposta a Incidentes em Redes (ETIR) sob sua coordenação, conforme o modelo de capilaridade adotado.

CAPÍTULO VII

DOS CANAIS DE COMUNICAÇÕES

Art. 16. A articulação da Equipe de Coordenação Setorial da Defesa (ECS/Def) com as Equipes de Prevenção, Tratamento e Resposta a Incidentes em Redes (ETIR) para fins de notificações deve ocorrer conforme definido no Plano Setorial para Gestão de Incidentes Cibernéticos da Defesa (PSGIC - Def).

Art. 17. A Equipe de Coordenação Setorial da Defesa (ECS/Def) deve operar em conformidade com as melhores práticas nacionais e internacionais sobre a Gestão de Incidentes Cibernéticos, desde que não conflitem com as normas complementares e legislação previstas no âmbito da Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC).

Art. 18. A Equipe de Coordenação Setorial da Defesa (ECS/Def) deve estar alinhada à prática do Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR/GOV) na Administração Pública Federal (APF) quanto ao uso de taxonomia comum para a identificação e classificação dos incidentes cibernéticos no âmbito do setor Defesa.

Art. 19. A troca de informações relacionadas a incidentes cibernéticos deve ocorrer, preferencialmente, através de correio eletrônico institucional de sua equipe central ou principal com o correio eletrônico institucional da Equipe de Coordenação Setorial da Defesa (ECS/Def) (ecs@comdciber.eb.mil.br).

Art. 20. Havendo indisponibilidade do correio eletrônico constante no art. 19 desta norma, excepcionalmente, poderão ser utilizados outros canais de comunicações, como:

I - voz;

II - Inter-Network Operation Center Dial By Autonomous System Number (INOC-DBA);

III - mensagem instantânea;

IV - reunião por videoconferência; e

V - sítios eletrônicos e mídias sociais institucionais.

Art. 21. A comunicação do incidente cibernético à Equipe de Coordenação Setorial da Defesa (ECS/Def) não exime a responsabilidade de comunicação do fato aos Gestores de Segurança de Informação envolvidos e ao processamento das informações da forma estabelecida por cada instituição, garantindo o respeito à hierarquia da cadeia de comando

CAPÍTULO VIII

DISPOSIÇÕES FINAIS

Art. 22. A Equipe de Coordenação Setorial da Defesa (ECS/Def) deve obedecer ao disposto nas normas de SI estabelecidas pelo Gabinete de Segurança Institucional da Presidência da República (GSI/PR) que dispõem sobre Equipes de Prevenção, Tratamento e Resposta a Incidentes em Redes (ETIR) e padrões para notificação de incidentes cibernéticos ao Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR/GOV).

Art. 23. A eficácia das ações de Gestão de Incidentes Cibernéticos depende, fundamentalmente, da atuação colaborativa dos integrantes da Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC), incluindo não apenas o Ministério da Defesa, mas também a comunidade acadêmica, os setores público e privado e a base industrial de defesa.

Art. 24. O Plano Setorial para Gestão de Incidentes Cibernéticos da Defesa (PSGIC - Def) deverá ser apreciado pelo Comando de Defesa Cibernética (ComDCiber) e estar alinhado ao Plano de Gestão de Incidentes Cibernéticos para a Administração Pública Federal (PlanGIC) e ao Plano Nacional de Segurança de Infraestruturas Críticas (PlanSIC).

Art. 25. A responsabilidade pela Gestão de Incidentes Cibernéticos, bem como das vulnerabilidades de ativos de informação de cada órgão integrante da Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC) é do próprio órgão.

Art. 26. A Equipe de Coordenação Setorial da Defesa (ECS/Def) deve agir como facilitador no processo de recuperação decorrente de incidentes cibernéticos, bem como na troca de informações entre as partes envolvidas e na articulação com o Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR/GOV).

Art. 27. As informações sobre incidentes cibernéticos devem ser utilizadas também para determinar tendências e padrões de atividades de ataques, bem como para recomendar estratégias de prevenção adequadas para todas as instituições do setor Defesa e de toda a Administração Pública Federal (APF).

Art. 28. Todos os integrantes da Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC) no setor Defesa devem zelar pelo cumprimento do previsto na Lei nº 13.709, de 14 de agosto de 2018, que institui a Lei Geral de Proteção de Dados (LGPD).

Art. 29. A Equipe de Coordenação Setorial da Defesa (ECS/Def) deve utilizar o padrão Traffic Light Protocol (TLP), versão mais atualizada, e estimular sua utilização pelas Equipes de Prevenção, Tratamento e Resposta a Incidentes em Redes (ETIR) do setor Defesa, conforme definido pelo Forum of Incident Response and Security Teams (FIRST).

Art. 30. Havendo indícios de ilícitos criminais, inclusive crimes cibernéticos durante o processo de Gestão de Incidentes Cibernéticos, as equipes centrais das Forças Singulares e as demais Equipes de Prevenção, Tratamento e Resposta a Incidentes em Redes (ETIR) do setor Defesa devem, além de comunicar a Equipe de Coordenação Setorial da Defesa (ECS/Def), acionar as autoridades policiais competentes para a adoção dos procedimentos legais necessários. Ademais, devem observar os procedimentos para o registro, coleta e preservação de evidências, exigindo consulta às orientações sobre cadeia de custódia, bem como executar as medidas preliminares para os devidos trabalhos de polícia judiciária militar ou civil e priorizar a continuidade dos serviços da Equipe de Prevenção, Tratamento e Resposta a Incidentes em Redes (ETIR) e da missão institucional da organização.

Art. 31. A Equipe de Coordenação Setorial da Defesa (ECS/Def) não realiza procedimentos de investigação criminal, restringindo-se às atividades de coordenação de Gestão de Incidentes Cibernéticos nas redes de computadores no âmbito do setor Defesa integrante da Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC). Eventuais desdobramentos na esfera policial relacionados a incidentes cibernéticos devem ser encaminhados às autoridades policiais competentes pelo próprio órgão ou entidade que sofreu o incidente.

Art. 32. O agente responsável da Equipe de Coordenação Setorial da Defesa (ECS/Def) tem o prazo de sessenta dias para apresentar o Plano Setorial de Gestão de Incidentes Cibernéticos do Setor Defesa (PSGIC-Def), contado a partir da data de publicação do ato de designação dos integrantes da ECS/Def.

Art. 33. O Plano Setorial para Gestão de Incidentes Cibernéticos da Defesa irá compor, na forma adequada, as Normas Operacionais do Sistema de Defesa Cibernética (NOSDCiber).

Art. 34. Os casos omissos a esta Portaria serão decididos pelo Ministério da Defesa, ouvido o Comando de Defesa Cibernética (ComDCiber).

Art. 35. Esta Portaria entra em vigor na data de sua publicação.

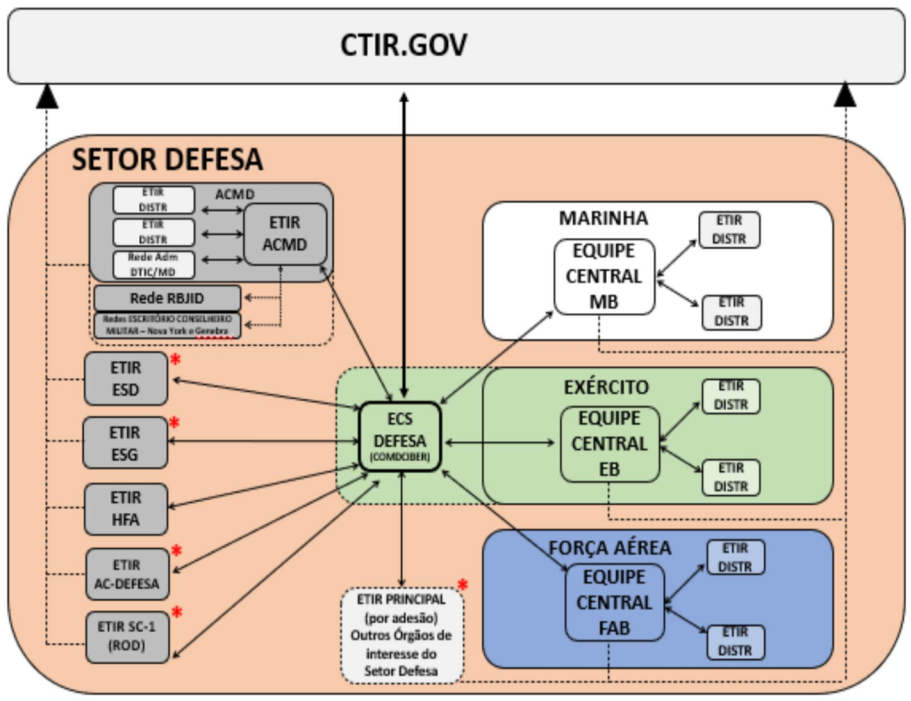
JOSÉ MUCIO MONTEIRO FILHO

ANEXO

ORGANIZAÇÃO DA REDE FEDERAL DE GESTÃO DE INCIDENTES CIBERNÉTICOS (REGIC) NO ÂMBITO DO SETOR DEFESA PARA FINS DE COORDENAÇÃO E CONSCIÊNCIA SITUACIONAL NA GESTÃO DE INCIDENTES CIBERNÉTICOS

LEGENDA	
⟷	Relacionamento primário entre ETIR com a ECS e, esta última, com o CTIR GOV para fins de coordenação na Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC)
-------->	Relacionamento entre ETIR e CTIR GOV, conforme § 1º art. 6º do Decreto nº 10.748, de 16 Jul 21
*	ETIR a serem criadas
ETIR CENTRAL	ETIR responsável por coordenar, criar as estratégias, gerenciar as atividades e distribuir as tarefas entre as equipes descentralizadas (distribuídas). Articula-se com a ECS-Def e exerce um papel de Grupo de Resposta a Incidentes de Segurança em Computadores CSIRT (do inglês "**Computer Security Incident Response Team**")
ETIR DISTR	ETIR responsável por implementar as estratégias e exercer suas atividades em suas respectivas áreas de responsabilidade dentro de um modelo de gestão descentralizado ou misto, devendo reportar à uma equipe central na organização
ETIR PCP	ETIR Principal de uma Área Prioritária
ETIR ACMD	ETIR da Administração Central do Ministério da Defesa (ACMD), responsável pela coordenação de incidentes cibernéticos na rede administrativa do MD e na coordenação com outras ETIR distribuídas
ETIR CENTRAL MB	ETIR da Diretoria de Comunicações e Tecnologia da Informação da Marinha (DCTIM) que opera a Central de Tratamento de Incidentes em Redes de Computadores da MB (CTIR.mar)
ETIR CENTRAL EB	ETIR do Centro Integrado de Telemática do Exército (CITEx) que opera o Centro de Coordenação de Tratamento de Incidentes de Rede do EB (CCTIR/EB)
ETIR CENTRAL FAB	ETIR do Centro de Computação da Aeronáutica de Brasília (CCA-BR) que opera o Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da FAB (CTIR.FAB)

Fluxo de relacionamento entre ETIR para fins de coordenação na ReGIC



Ministério do Desenvolvimento Agrário e Agricultura Familiar

INSTITUTO NACIONAL DE COLONIZAÇÃO E REFORMA AGRÁRIA

PORTARIA Nº 143, DE 14 DE AGOSTO DE 2023

Retifica área de projeto de assentamento.

O PRESIDENTE DO INSTITUTO NACIONAL DE COLONIZAÇÃO E REFORMA AGRÁRIA - INCRA, no uso das atribuições que lhe são conferidas no inciso IV do art. 22 do Decreto nº 11.232, de 10 de outubro 2022, combinado com o inciso VIII do art. 104 do Regimento Interno da Autarquia, aprovado pela Portaria nº 2.541, de 28 de dezembro de 2022, publicada no Diário Oficial da União do dia 30 de dezembro de 2022, e

Considerando os órgãos da Superintendência Regional de São Paulo - SR(SP) e da Diretoria de Desenvolvimento e Consolidação de Projetos de Assentamento - DD, que procederam a análise do processo administrativo nº 54190.001678/1998-07 e decidiram pela regularidade da retificação de informações na Portaria/INCRA/SR-08/Nº 74, de 10 de novembro de 1998, publicada no Diário Oficial da União nº 225, de 24 de novembro de 1998, que criou o Projeto de Assentamento Porto Velho, código SIPRA SP0083000, localizado no município de Presidente Epitácio, no estado de São Paulo.

Considerando a conformidade da alteração da área do Projeto de Assentamento Porto Velho com a base cartográfica da SR(SP), de 1.492,8854 ha para 1.494,1056 ha, segundo a Nota Técnica nº 1727/2023/SR(SP)D1/SR(SP)D/SR(SP)/INCRA (16860338), resolve:

Art. 1º Retificar a área de 1.492,8854 ha (um mil, quatrocentos e noventa e dois hectares, oitenta e oito ares e cinquenta e quatro centiares), constante da Portaria/INCRA/SR-08/Nº 74, de 10 de novembro de 1998, publicada no Diário Oficial da União nº 225, de 24 de novembro de 1998, que criou o Projeto de Assentamento Porto Velho, código SIPRA SP0083000, localizado no município de Presidente Epitácio, no estado de São Paulo, para a área de 1.494,1056 ha (um mil, quatrocentos e noventa e quatro hectares, dez ares e cinquenta e seis centiares), em conformidade com a base cartográfica da SR(SP).

Art. 2º Esta Portaria entra em vigor na data de sua publicação.

CÉSAR FERNANDO SCHIAVON ALDRIGHI

PORTARIA Nº 144, DE 15 DE AGOSTO DE 2023

Delegação de competência ao Superintendente Regional do Incra no Oeste do Pará - SR(PA/O), para celebrar instrumento de Contrato de Constituição de Servidão Administrativa.

O PRESIDENTE DO INSTITUTO NACIONAL DE COLONIZAÇÃO E REFORMA AGRÁRIA - INCRA, no uso das atribuições que lhe são conferidas pelo art. 22, da Estrutura Regimental deste Instituto, aprovada pelo Decreto nº 11.232, de 10 de outubro de 2022, publicado no Diário Oficial da União do dia 11 de outubro de 2022, combinado com o art. 104, incisos IV e V, do Regimento Interno da Autarquia, aprovado pela Portaria nº 2.541, de 28 de dezembro de 2022, publicada no Diário Oficial da União do dia 30 de dezembro de 2022;

Considerando a deliberação ocorrida na 719ª Reunião do Conselho Diretor, realizada em 19 de junho de 2023;

Considerando a decisão emitida por meio da Resolução/INCRA/CD/Nº 41, de 20 de junho de 2020;

Considerando as manifestações prestadas pela Procuradoria Federal Especializada - PFE na Nota n. 00080/2023/EQUAD-AGRÁRIA/PFE-INCRA-SEDE/PGF/AGU (SEI nº 17254822) e no Despacho n. 00203/2023/CGA/PFE-INCRA-SEDE/PGF/AGU (SEI nº 17254901) acolhidos pelo Despacho n. 00341/2023/GAB/PFE/PFE-INCRA-SEDE/PGF/AGU (SEI nº 17254928);

E, por fim, considerando o constante nos autos do processo administrativo nº 54000.005256/2018-70, resolve:

Art. 1º Delegar competência ao Superintendente Regional do Incra no Oeste do Pará - SR(PA/O), assistido pela Procuradoria Federal Especializada - PFE junto a esta Autarquia à celebrar o instrumento de Contrato de Constituição de Servidão Administrativa, em favor da empresa Brazauro Recursos Minerais S.A.

Art. 2º Esta Portaria entra em vigor na data de sua publicação.

CÉSAR FERNANDO SCHIAVON ALDRIGHI