MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA

TECNOLOGIA DA INFORMAÇÃO

ICA 7-60

GESTÃO DE INCIDENTES CIBERNÉTICOS NO COMANDO DA AERONÁUTICA

2024

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO DA AERONÁUTICA

TECNOLOGIA DA INFORMAÇÃO

ICA 7-60

GESTÃO DE INCIDENTES CIBERNÉTICOS NO COMANDO DA AERONÁUTICA

2024

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO DA AERONÁUTICA

PORTARIA DTI Nº 78/SNOR, DE17 DE JANEIRO DE 2024.
Protocolo COMAER nº 67131.000099/2024-19

Aprova a ICA7-60 "Gestão de Incidentes Cibernéticos no Comando da Aeronáutica"

O DIRETOR DE TECNOLOGIA DA INFORMAÇÃO DA AERONÁUTICA, no uso das atribuições que lhe conferem o art. 5 da Portaria nº 634/GC3, de 11 de dezembro de2023, e o art. 11 do Regulamento da Diretoria de Tecnologia da Informação da Aeronáutica,aprovado pela Portaria nº 353/GC3, de 10 de agosto de 2022, resolve:

Art. 1º Aprovar a Gestão de Incidentes Cibernéticos (ICA 7-60), nos moldes daNSCA 5-1, conforme o disposto no Parágrafo único do art. 3º da Portaria nº 661/GC3, de 21 dedezembro de 2023.

Art.2º Revoga-se a Portaria EMAER nº41/3SC, de 9 de setembro de 2016, publicada no Boletim do Comando da Aeronáutica nº 158, de 16 de setembro de 2016.

Art. 3º Esta Portaria entra em vigor no dia 1º de fevereiro de 2024.

Maj Brig Eng ELIEZER DE FREITAS CABRAL
Diretor de Tecnologia da Informação da Aeronáutica

(Publicado no BCA nº 021, de 30 de janeiro de 2024)

SUMÁRIO

PREFÁCIO

O Regulamento de Administração da Aeronáutica RCA 12-1/2021, em seu Art. 1º prevê que a "Administração da Aeronáutica é regida pelos Princípios Constitucionais e infraconstitucionais que regulam a Administração Pública Federal".

Conforme a Política Nacional de Segurança da Informação, instituída por meio do Decreto nº 9.637, de 26 de dezembro de 2018, compete aos órgãos e às entidades da administração pública federal, em seu âmbito de atuação, instituir e implementar equipe de prevenção, tratamento e resposta a incidentes cibernéticos, que comporá a Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC). Neste sentido, faz-se necessária a manutenção na Força Aérea Brasileira de uma equipe responsável por prevenir, tratar e responder a incidentes cibernéticos.

Segundo o Decreto nº 10.748, de 16 de julho de 2021, no âmbito do Ministério da Defesa e das Forças Singulares, a articulação com o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov) será feita prioritariamente por meio da equipe de coordenação setorial, operada pelo Comando de Defesa Cibernética (ComDCiber), na condição de órgão central do Sistema Militar de Defesa Cibernética. A Equipe de Coordenação Setorial da Defesa (ECS/Def) foi instituída por meio da Portaria GM-MD N° 4.138, de 14 de agosto de 2023. Nesta mesma portaria ficou definido que o agente responsável da Equipe de Coordenação Setorial da Defesa (ECS/Def) apresentaria o Plano Setorial de Gestão de Incidentes Cibernéticos do Setor Defesa (PSGIC-Def).

O PSGIC-Def foi aprovado por meio da Portaria GM-MD Nº 4.174, de 16 de agosto de 2023. Este Plano tem como objetivo orientar e coordenar as Equipes de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do setor Defesa. Uma das atividades preparatórias previstas no plano consiste na elaboração de documento de constituição da Equipe de Prevenção, Tratamento e Resposta a Incidentes em Redes (ETIR) ou de estrutura equivalente, o qual designará as atribuições e o escopo de atuação.

Neste sentido, a presente instrução tem por objetivo definir o modelo adotado para o tratamento e resposta a incidentes de segurança em redes computacionais no COMAER, bem como as respectivas responsabilidades e atividades a serem desenvolvidas por cada organização.

1 DISPOSIÇÕES PRELIMINARES

1.1 FINALIDADE

Esta Instrução tem por finalidade orientar as Organizações do COMAER quanto à Gestão de Incidentes Cibernéticos no COMAER, realizada pelo Centro de Tratamento de Incidentes de Rede da Força Aérea Brasileira (CTIR.FAB), juntamente com suas Equipes de Tratamento de Incidentes de Segurança em Redes Computacionais (ETIR) distribuídas.

1.2 CONCEITUAÇÃO

Para os efeitos desta Instrução, aplicam-se os termos e expressões com os significados constantes no Glossário das Forças Armadas (MD-35-G-01/2015), no Glossário do COMAER (MCA 10-4/2001), na legislação do STI em vigor e, quando aplicável, na legislação da Administração Pública Federal (APF) em vigor.

1.2.1 AGENTE RESPONSÁVEL

Servidor Público ocupante de cargo efetivo ou militar de carreira de órgão ou entidade da APF, direta ou indireta, incumbido de chefiar e gerenciar a ETIR. (Fonte: Norma Complementar nº 05/IN01/DSIC/GSIPR de 14 de agosto de 2009).

1.2.2 ARTEFATO MALICIOSO

É qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores. (fonte: Norma Complementar nº 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009).

1.2.3 CENTRO DE OPERAÇÕES DE SEGURANÇA (SOC)

Ponto focal para operações de segurança e defesa de redes de computadores de uma organização. O propósito do SOC é defender e monitorar continuamente os sistemas e redes de uma organização (ou seja, infraestrutura cibernética). O SOC também é responsável por detectar, analisar e responder a incidentes de cibersegurança de maneira oportuna.

1.2.4 COMITÊ DE GOVERNANÇA DIGITAL, SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS (CGDSIPD)

Instituído nos termos do Decreto nº 10.332, de 28 de abril de 2020 para deliberar sobre os assuntos relativos à implementação das ações de governo digital e ao uso de recursos de tecnologia da informação e comunicação.

1.2.5 COMUNIDADE OU PÚBLICO ALVO

É o conjunto de pessoas, setores, órgãos ou entidades atendidas por uma ETIR. (fonte: Norma Complementar nº 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009).

1.2.6 CTIR GOV

É o Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores (CTIR) da APF, subordinado ao Departamento de Segurança de Informação e Comunicações (DSIC) do Gabinete de Segurança Institucional da Presidência da República (GSI/PR). (fonte: Norma Complementar nº 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009).

1.2.7 CTIR.FAB

É a sigla designativa para o Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Força Aérea Brasileira, subordinado ao Órgão Central do Sistema de Tecnologia da Informação (STI) do COMAER e mantido pelo Centro de Computação da Aeronáutica de Brasília (CCA-BR). (Conceito adaptado das Normas Complementares: 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009 e 08/IN01/DSIC/GSIPR, de 19 de agosto de 2010).

1.2.8 ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS DO COMAER

O encarregado pelo tratamento de dados pessoais atua como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). (Fonte: Lei Nº 13.709, de 14 de agosto de 2018).

1.2.9 EQUIPE DE COORDENAÇÃO SETORIAL DA DEFESA (ECS/Def)

Equipe de Coordenação Setorial da Defesa (ECS/Def) que 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). (Fonte: Portaria GM-MD N° 4.138, de 14 de agosto de 2023).

1.2.10 EQUIPE DE PREVENÇÃO, TRATAMENTO E RESPOSTA A INCIDENTES EM REDES COMPUTACIONAIS (ETIR)

Grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores. (Fonte: Norma Complementar 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009).

1.2.11 ETIR CENTRAL

Responsável por coordenar, criar as estratégias, gerenciar as atividades e distribuir as tarefas entre as ETIR distribuídas, além de ser responsável, perante toda a organização, pela articulação com a Equipe de Coordenação Setorial da Defesa (ECS/Def), conforme o Plano Setorial de Gestão de Incidentes Cibernéticos do Setor Defesa (PSGIC-Def).

1.2.12 ETIR DISTRIBUÍDA

Todas as ETIR do COMAER que não sejam a ETIR Central.

1.2.13 ETIR DE REFERÊNCIA

Todas as OM do COMAER são atendidas por uma ETIR, chamada de ETIR de Referência. As OM que não estiverem na área de atuação de uma ETIR Distribuída, serão atendidas diretamente pela ETIR Central.

1.2.14 GESTÃO DE INCIDENTES CIBERNÉTICOS

Processo especializado que consiste em detecção, triagem, análise e resposta a eventos anômalos de rede de computadores que possam ser uma ameaça à segurança da informação.

1.2.15 GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

Conjunto de processos que permite identificar e implementar as medidas de proteção necessárias a minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, bem como equilibrá-los com os custos operacionais e financeiros envolvidos. (fonte: Norma Complementar nº 12/IN01/DSIC/GSIPR, de 30 de janeiro de 2012).

1.2.16 INCIDENTEDE SEGURANÇA

Um simples ou uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação. (fonte: NSCA 7-13 de 2022).

1.2.17 PLANO DE GESTÃO DE INCIDENTES CIBERNÉTICOS (PLANGIC)

Plano que orienta as equipes dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional, exceto das agências reguladoras, do Banco Central do Brasil e da Comissão Nacional de Energia Nuclear, sobre a coordenação de atividades referentes à prevenção, ao tratamento e à resposta a incidentes cibernéticos. (fonte: Decreto nº 10.748, de 16 de julho de 2021).

1.2.18 PLANO SETORIAL DE GESTÃO DE INCIDENTES CIBERNÉTICOS DO SETOR DEFESA (PSGIC-Def)

Plano Setorial de Gestão de Incidentes Cibernéticos do Setor Defesa (PSGIC-Def) que tem como objetivo orientar e coordenar as Equipes de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do setor Defesa (ETIR), integrantes da Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC), nas ações referentes à prevenção, ao tratamento e à resposta a incidentes cibernéticos inerentes ao setor Defesa. (fonte: Portaria nº 4.174 de 16 de agosto de 2023).

1.2.19 SERVIÇO

É o conjunto de procedimentos, estruturados em um processo bem definido, oferecido à comunidade da ETIR. (fonte: Norma Complementar nº

05/IN01/DSIC/ GSIPR, de 14 de agosto de 2009).

1.2.20 TRATAMENTO DE INCIDENTES DE SEGURANÇA EM REDES COMPUTACIONAIS

É o serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências. (fonte: Norma Complementar nº 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009). Nesta instrução será referida apenas como "tratamento de incidentes".

1.2.21 REDE FEDERAL DE GESTÃO DE INCIDENTES CIBERNÉTICOS

A Rede Federal de Gestão de Incidentes Cibernéticos - ReGIC instituída pelo Decreto nº 10.748 de 16 de julho de 2021 tem por finalidade aprimorar e manter a coordenação entre órgãos e entidades da administração pública federal direta, autárquica e fundacional para prevenção, tratamento e resposta a incidentes cibernéticos, de modo a elevar o nível de resiliência em segurança cibernética de seus ativos de informação. (fonte: Decreto nº 10.748 de 16 de julho de 2021).

1.2.22 VULNERABILIDADE

É qualquer fragilidade dos sistemas computacionais e redes de computadores que permitam a exploração maliciosa e acessos indesejáveis ou não autorizados. (fonte: Norma Complementar nº 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009).

1.3 ÂMBITO

Esta Instrução se aplica a todas as Organizações do COMAER.

2 RESPONSABILIDADES

2.1 DO ÓRGÃO CENTRAL DO STI

2.1.1 Emitir diretrizes quanto às questões relacionadas ao gerenciamento de incidentes no COMAER.

2.1.2 Coordenar o cumprimento e a evolução da maturidade do processo de gerenciamento de incidentes no COMAER.

2.1.3 Aprovar, em conjunto com os Elos de Coordenação do STI envolvidos, medidas de contenção, correção e erradicação dos incidentes de segurança no COMAER.

2.1.4 Apoiar, incentivar e contribuir para a capacitação nos assuntos afetos ao gerenciamento de incidentes no COMAER.

2.1.5 Acompanhara designação dos Agentes Responsáveis de cada ETIR.

2.1.6 Definir, junto ao EMAER, a criação de novas ETIR, com base nas necessidades identificadas pelos Elos de Coordenação do STI.

2.2 DOS ELOS DE COORDENAÇÃO DO STI

2.2.1 Coordenar a instituição, implementação e manutenção da infraestrutura necessária às ETIR sob sua responsabilidade.

2.2.2 Prover os meios necessários para a capacitação e aperfeiçoamento técnico dos membros das ETIR sob sua responsabilidade.

2.3 DO CTIR.FAB

2.3.1 Coordenar as atividades de tratamento de incidentes no COMAER, atuando como Equipe Central de Prevenção, Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores (ETIR Central).

2.3.2 Relacionar-se externamente com a Equipe de Coordenação Setorial da Defesa (ECS/Def) e outras equipes similares, no que couber.

2.3.3 Criar as estratégias, gerenciar as atividades e distribuir as tarefas entre as ETIR distribuídas, além de ser a única responsável na Força Aérea Brasileira pela comunicação com a Equipe de Coordenação Setorial da Defesa (ECS/Def).

2.3.4 Auxiliar o Órgão Central do STI na geração de indicadores relativos a incidentes cibernéticos no COMAER.

2.3.5 Propor procedimentos a serem adotados quando sistemas de *software* e *hardware* que sejam comprovadamente inseguros sejam identificados em uso no COMAER.

2.3.6 Orientar as ETIR por meio dos normativos técnicos necessários para o tratamento de incidentes no âmbito do COMAER.

2.3.7 Padronizar sistemas a serem empregados por todas as ETIR na atividade de

tratamento de incidentes de segurança em redes de computadores.

2.3.8 Apoiar tecnicamente as demais ETIR nas ações necessárias ao tratamento de incidentes no COMAER.

2.3.9 Manter atualizado o cadastro na Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC), junto ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR GOV), por intermédio do termo de adesão disponibilizado no seu sítio eletrônico.

2.3.10 Disseminar, proativamente ou sob demanda do Elo Central do STI, informações de caráter preventivo, tais como:

a) novos ataques ou tendências de ataques observadas;

b) vulnerabilidades observadas com mais frequência;

c) boas práticas de segurança de aplicação geral; e

d) estatísticas de incidentes cibernéticos.

2.4 DOS ELOS DE SERVIÇO DO STI

2.4.1 Implementar as estratégias e medidas de segurança da informação contidas nas legislações afetas a este assunto em suas respectivas áreas de responsabilidade.

2.4.2 Notificar, em caso de incidente, a ETIR de Referência.

2.4.3 Aplicaras medidas de tratamentos de incidentes cabíveis, de acordo com as orientações emanadas pela ETIR de Referência e pelo CTIR.FAB.

2.4.4 Solicitar à ETIR Central, quando julgado necessário, a identificação de sistemas de *software* e *hardware* vulneráveis.

2.4.5 Apoiar a execução do Plano de Continuidade de Negócios para os ativos críticos no âmbito da respectiva organização.

2.4.6 Implantar a estrutura e as soluções de defesa de perímetro e de monitoramento de incidentes de rede a serem adotadas no âmbito do COMAER, em consonância com as demais orientações emanadas do Órgão Central de TI.

2.4.7 Manter a infraestrutura necessária às ETIR e a infraestrutura para defesa de perímetro no âmbito do COMAER.

2.4.8 Manter um militar de sobreaviso para o tratamento emergencial de incidentes fora do horário de expediente.

2.4.9 Manter e informar ao CTIR.FAB o telefone de contato do militar de sobreaviso.

2.5 DAS ETIR

2.5.1 Implementar as estratégias e medidas de segurança da informação contidas nas legislações afetas a este assunto em suas respectivas áreas de responsabilidade, conforme definidas no **Anexo** a esta Instrução, em alinhamento às orientações recebidas

do CTIR.FAB.

2.5.2 Realizar a gestão de incidentes cibernéticos relacionados aos ativos de informação hospedados na ETIR e bem como nas demais organizações de suas áreas de atuação conforme definidas no **Anexo** a esta Instrução.

2.5.3 Aplicar as ações de tratamento a incidentes, quando necessário, de acordo com as legislações afetas a este tema e com as orientações do CTIR.FAB.

2.5.4 Manter registro de todos os incidentes notificados ou detectados, com a finalidade de assegurar registro histórico das atividades da ETIR.

2.5.5 Monitorar os incidentes de segurança e comunicar ao CTIR.FAB, no menor prazo possível, a ocorrência dos mesmos na estrutura sob sua responsabilidade.

2.5.6 Auxiliar a ETIR Central a identificar sistemas de *software* e *hardware* que sejam comprovadamente inseguros de forma que os mesmos não sejam utilizados nas infraestruturas de TI do COMAER.

2.5.7 Estabelecer regime de trabalho diferenciado para atender demandas específicas, quando solicitado por autoridade competente.

2.5.8 Manter um militar de sobreaviso para o tratamento emergencial de incidentes fora do horário de expediente e informar ao CTIR.FAB os meios de acionamento.

2.6 DO SERVIÇO DE ATENDIMENTO AOS USUÁRIOS DE TI (SAU)

2.6.1 Encaminhar ao CTIR.FAB, por meio do endereço de e-mail abuse@fab.mil.br, os incidentes de segurança eventualmente reportados pelos usuários do COMAER por meio do SAU.

2.7 DOS ELOS USUÁRIOS DO STI

2.7.1 Conhecer, observar e cumprir os normativos gerenciais e técnicos de segurança da informação de acordo com seus níveis de atribuição.

2.7.2 Comunicar os incidentes de segurança por meio do e-mail abuse@fab.mil.br.

2.8 DO AGENTE RESPONSÁVEL

2.8.1 Coordenar as ETIR do COMAER.

2.8.2 Garantir que os incidentes de segurança do COMAER sejam monitorados.

2.8.3 Adotar procedimentos de *feedback* para assegurar que os usuários que comuniquem incidentes de segurança sejam informados dos procedimentos adotados.

2.9 DO GESTOR DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA DO COMAER (GSIC)

2.9.1 Coordenar o Comitê de Governança Digital, Segurança da Informação e Proteção de Dados (CGDSIPD).

2.9.2 Supervisionar o funcionamento do CTIR.FAB.

2.9.3 Atender as demais responsabilidades previstas na Instrução Normativa GSI nº 1, de 27 de maio de 2020 e em suas eventuais normas complementares.

3 ESTRUTURAÇÃO DA GESTÃO DE INCIDENTES CIBERNÉTICOS NO COMAER

3.1 MODELO ADOTADO

3.1.1 O modelo adotado para a estrutura de tratamento e resposta a incidentes de segurança em redes computacionais no COMAER é o modelo combinado ou misto, em conformidade com o item 7.4 da Norma Complementar nº 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009.

3.1.2 O CTIR.FAB atua como a ETIR Central do COMAER e é apoiado por uma rede de ETIR Distribuídas, ativadas de acordo com as necessidades do STI.

3.1.3 O CTIR.FAB atua com autonomia compartilhada, de acordo com o item 9.2 da Norma Complementar nº 05/IN01/DSIC/GSIPR de 14/08/09 e o processo decisório será conduzido pelo Gestor de Segurança da Informação e Cibernética do COMAER.

3.1.4 O processo de tratamento de incidentes no CTIR.FAB é baseado nas orientações da Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC) e em particular da ECS/Def. Estas organizações, por sua vez, adotam as melhores práticas internacionalmente aceitas para a atividade de tratamento de incidentes cibernéticos.

3.2 ESTRUTURA ORGANIZACIONAL

3.2.1 O CTIR.FAB é parte integrante da estrutura orgânica do CCA-BR.

3.2.2 As ETIR distribuídas são partes integrantes da estrutura orgânica das OM designadas pelo Órgão Central do STI e responsáveis pelo serviço de tratamento de incidentes nas áreas definidas por esta Instrução.

3.2.3 Cabe à ETIR designar formalmente o Agente Responsável por intermédio de publicação em Boletim Interno;

3.3 COMPOSIÇÃO DAS ETIR DA AERONÁUTICA

3.3.1 Militares alocados em qualquer uma das ETIR devem ser dedicados exclusivamente à atividade de tratamento de incidentes cibernéticos.

3.3.2 A ETIR Central será composta por, **no mínimo**:

a) 17 oficiais que tenham cumprido a capacitação mínima definida pelo CDCAER;

b) 42 graduados que tenham cumprido a capacitação mínima definida pelo CDCAER.

c) Destes, 3 oficiais e 7 graduados irão compor a equipe fixa que realizará atividades técnicas e administrativas fora do escopo do processo de tratamento de incidentes, enquanto 14 oficiais e 35 graduados, de qualquer OM, irão compor a equipe de serviço de tratamento de incidentes cibernéticos.

3.3.3 As ETIR Distribuídas serão compostas por **no mínimo**:

a) 2 oficiais que tenham cumprido a capacitação mínima definida pelo CDCAER;

b) 4 graduados que tenham cumprido a capacitação mínima definida pelo CDCAER.

3.4 EQUIPE DE TRATAMENTO DE INCIDENTES

3.4.1 A atividade de tratamento de incidente na ETIR Central deverá funcionar sob formato de escala de serviço, publicada diariamente em Boletim Interno. Os militares escalados ficarão indisponíveis para a execução de qualquer outra atividade.

3.4.2 A equipe de serviço designada para a atividade de tratamento de incidente na ETIR Central poderá trabalhar em dois regimes, sendo eles:

a) durante o expediente; ou

b) 24 horas por dia, 7 dias por semana (24x7).

3.4.3 Compete ao Comitê de Governança Digital, Segurança da Informação e Proteção de Dados (CGDSIPD) a decisão sobre qual regime de trabalho será executado pela ETIR Central.

3.4.4 Para a execução do serviço de tratamento de incidente no regime durante o expediente, será necessário atender aos seguintes critérios:

a) composição de 2 equipes de 2 oficiais e 5 graduados para a composição da escala de execução do serviço de tratamento de incidente, totalizando 4 oficiais e 10 graduados.

b) concorrerão à escala militares de qualquer OM que tenham cumprido a capacitação mínima definida pelo CDCAER.

c) composição de um efetivo fixo com 3 oficiais e 7 graduados para execução de atividades técnicas e administrativas como perícias forenses, processos de aquisição, manutenção de sistemas, pesquisa de novas práticas de segurança, provas de conceito de novas ferramentas, edição de normativos, gestão de projetos, gestão de recursos humanos, etc.

3.4.5 Para a execução do serviço de tratamento de incidente no regime 24 horas por dia, 7 dias por semana (24x7), será necessário atender aos seguintes critérios:

a) composição de 7 equipes de 2 oficiais e 5 graduados para a composição da escala de execução do serviço de tratamento de incidente, totalizando 14 oficiais e 35 graduados.

b) concorrerão à escala militares de qualquer OM que tenham cumprido a capacitação mínima definida pelo CDCAER.

c) composição de um efetivo fixo com 3 oficiais e 7 graduados para execução de atividades técnicas e administrativas como perícias forenses, processos de aquisição, manutenção de sistemas, pesquisa de novas práticas de segurança, provas de conceito de novas ferramentas, edição de normativos, gestão de projetos, gestão de recursos humanos, etc.

3.4.6 Na hipótese de regime de trabalho 24x7, as equipes trabalharão em turnos,

conforme Tabela 1.

Turno	Intervalo
1	23h-07h
2	07h-15h
3	15h-23h

Tabela 1: Turnos de serviço

3.4.7 O intervalo mínimo entre dois serviços consecutivos será de 24 horas.

3.4.8 Deverão estar disponíveis, ao menos, 7 equipes completas para a adoção do regime 24x7.

3.4.9 A equipe deve estar pronta para o turno de serviço pelo menos 15 minutos antes do horário previsto para o seu efetivo início, a fim de receber *briefing* acerca das informações técnicas inerentes. O término do turno deve ser no horário previsto.

3.4.10 Os fatos relevantes ocorridos em cada turno serão registrados pela equipe de serviço, utilizando software adequado para esta tarefa.

3.4.11 Deve haver pelo menos um descanso de 15 minutos para cada três horas de operação contínua no turno de serviço.

3.4.12 O processo de rodízio deve ser realizado em cada turno de serviço de modo a possibilitar a realização das principais refeições.

3.4.13 Independentemente do regime de escala, a carga horária **máxima** mensal deverá ser de 160h e a carga **mínima** mensal de 110h.

3.4.14 Acarga mínima mensal não se aplica ao mês de fevereiro.

4 PROCESSO DE GESTÃO DE INCIDENTES

O processo de gestão de incidentes cibernéticos no COMAER segue as orientações estabelecidas no Plano Setorial de Gestão de Incidentes Cibernéticos do Setor Defesa (PSGIC-Def), baseadas nas melhores práticas nacionais e internacionais em gestão de incidentes cibernéticos. Em algumas organizações, o setor responsável por este tipo de atividade pode ser denominado SOC. Os processos que compõem a gestão de incidentes do COMAER estão descritos abaixo:

4.1 DETECÇÃO DO INCIDENTE

4.1.1 Este processo tem início quando uma ETIR identifica algum evento, confirmado ou sob suspeita, que pode indicar um incidente cibernético. Esta identificação pode ocorrer de forma proativa, a partir de monitoramento de rede ou busca em fontes abertas, ou reativo, quando a equipe recebe uma notificação.Esta notificação pode vir de algum Elo do STI, de usuários do STI, de alguma outra ETIR externa ao COMAER ou gerada por soluções de monitoramento de rede.

4.1.2 A eficácia do monitoramento de rede para a detecção de incidentes depende, entre outros fatores, do estabelecimento de linhas de base que caracterizem o uso normal da rede. As anormalidades são consideradas indícios de incidente e, se identificadas, devem ser investigadas.

4.1.3 Uma vez identificado um evento suspeito, as informações de interesse deverão ser registradas em um sistema informatizado adequado e encaminhadas para o tratamento do incidente cibernético, iniciando pela triagem.

4.2 TRIAGEM

4.2.1 O processo de triagem consiste em:

a) verificar se a informação é um incidente cibernético para aceitação ou descarte;

b) verificar se há correlação com outros incidentes;

c) estabelecer a categoria e prioridade para o tratamento do incidente;

d) registrar o incidente na base de incidentes cibernéticos;

e) complementar as informações presentes no registro do incidente; e

f) atribuir o tratamento do incidente ao analista ou à ETIR de Referência.

4.3 ANÁLISE

4.3.1 O processo de análise consiste em:

a) validar as informações tratadas na triagem, ratificando-as, complementando-as ou retificando-as;

b) identificar e avaliar atividades anômalas em relação à linha de base conhecida;

c) identificar pelo menos uma parte da cadeia de ataque para permitir a definição das atividades de resposta;

d) complementar e adicionar novos dados a partir da colaboração das fontes utilizadas na detecção; e

e) incluir todos os dados coletados na documentação sobre o incidente para viabilizar as ações de pós-incidente.

4.4 RESPOSTA

4.4.1 O processo de resposta compreende a coordenação de ações com a ETIR de referência e com os responsáveis pelos ativos que possam estar envolvidos no incidente, tanto em nível técnico quanto em nível gerencial. Também podem ser enviadas notificações para os provedores de serviço utilizados em possíveis ações maliciosas.

4.4.2 A interação com o Elo Central do STI e com Elos de Coordenação do STI pode ser necessária para a definição de determinadas ações de resposta, principalmente se houver necessidade de indisponibilização de sistemas de TI.

4.4.3 O processo de resposta a um incidente cibernético consiste em ações de:

a) contenção;

b) erradicação; e

c) recuperação.

4.4.4 O objetivo da contenção é limitar os danos causados pelo atual incidente de segurança e evitar outros. Devem ser aplicadas medidas para mitigar o incidente, evitando-se a destruição de provas que possam servir de subsídios para possível processo cível, penal ou administrativo. Além disso, são ativadas as medidas de contingência disponíveis.

4.4.5 A erradicação consiste em remover ou inutilizar artefatos utilizados pelos atacantes e em restaurar o ambiente afetado.

4.4.6 O objetivo da recuperação é restabelecer o pleno funcionamento do ambiente afetado após garantir que as ameaças foram neutralizadas ou removidas.

4.4.7 A efetividade das ações de contenção, erradicação e recuperação será maior caso as OM que hospedam os ativos afetados mantenham um plano de continuidade de negócios atualizado. Este tipo de plano deve, entre outros, esclarecer a criticidade de seus ativos, importância dos sistemas para os processos de negócio relacionados e definir ações específicas de contingência em caso de incidentes.

4.4.8 A comunicação entre os Elos do STI e o CTIR.FAB deve ocorrer através das ETIR de Referência, que dará início ao tratamento do incidente com apoio das soluções de TI disponíveis.

4.4.9 Caso o incidente afete dados pessoais de militares ou de civis, será necessária a coordenação de ações com o Encarregado de Dados do COMAER, que deverá receber informações relevantes sobre o incidente para a tomada de decisões relativas à LGPD.

4.4.10 O CTIR.FAB, ao reportar os incidentes de segurança, deve fazê-lo em acordo com as orientações publicadas pela ECS/Def.

4.4.11 O CTIR.FAB deve coordenar com a ECS/Def os tipos de incidentes que devem ser notificados, o canal a ser utilizado e o formato das notificações.

5 DISPOSIÇÕES GERAIS

5.1 Todos os incidentes detectados devem ser registrados em solução de TI específica para este tipo de atividade, com a finalidade de assegurar registro histórico dos procedimentos adotados e lições aprendidas em cada incidente.

5.2 O tratamento da informação pelas ETIR do COMAER deve ser realizado de forma a viabilizar e assegurar disponibilidade, integridade, confidencialidade e autenticidade da informação, observada a legislação em vigor, naquilo que diz respeito ao estabelecimento de graus de sigilo.

5.3 A atividade de gestão de incidentes cibernéticos deve, em geral, seguir os normativos vigentes sobre preservação de evidências digitais.

6 DISPOSIÇÕES FINAIS

6.1 Casos não previstos nesta Instrução serão submetidos à apreciação do Exmo. Sr. Comandante-Geral de Apoio.

6.2 As competências do CCA-BR citadas nesta norma se tornarão do CDCAER, quando de sua ativação.

REFERÊNCIAS

BRASIL. Comando da Aeronáutica. Comando-Geral de Apoio. Portaria COMGAP nº 42/ADLG, de 02 de maio de 2022. Aprova a reedição da Norma de Segurança da Informação e Defesa Cibernética nas Organizações do Comando da Aeronáutica: NSCA 7-13. **Boletim do Comando da Aeronáutica,** Rio de Janeiro, n. 081, de 03 mai. 2022.

BRASIL. Comando da Aeronáutica. Comando-Geral de Apoio. Portaria GABAER Nº 25/GC3, de 21 de janeiro de 2021. Aprova a edição do RCA 12-1 Regulamento de Administração da Aeronáutica, na forma eletrônica (RADA-e). Boletim do Comando da Aeronáutica, Rio de Janeiro n. 017, de 26 jan. 2021.

BRASIL. Comando da Aeronáutica. Estado-Maior da Aeronáutica. Portaria EMAER n°002/3SC2, de 30 de janeiro de 2001. Aprova a reedição do Manual que dispõe sobre padronização do uso de termos, palavras, vocábulos e expressões de uso corrente no âmbito do Comando da Aeronáutica. Glossário da Aeronáutica: MCA 10-4. Boletim Externo OstensivoEMAER, n. 2, 2001.

BRASIL. Instrução Normativa GSI nº 1, de 27 de maio de 2020. Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal. Diário Oficial da União, Brasília, DF, 28 mai. 2020. Disponível em: https://www.gov.br/gsi/pt-br/dsic/legislacao/copy_of_IN01_consolidada.pdf. Acesso em: 19/10/2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 19 de outubro de 2023.

BRASIL. Ministério da Defesa. Gabinete do Ministro. Portaria nº 9/GAP/MD, de 13 de janeiro de 2016. Aprova o Glossário das Forças Armadas – MD-35-G-01 (5ª Edição/2015). Diário Oficial da União, Brasília, DF, 21 jan. 2016. Disponível em: https://bdex.eb.mil.br/jspui/bitstream/123456789/141/1/MD35_G01.pdf. Acesso em 19 de outubro de 2023.

BRASIL. Ministério da Defesa. Gabinete do Ministro. Portaria GM-MD nº 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). Diário Oficial da União, Brasília, DF, 16 ago. 2023. Disponível em: https://www.in.gov.br/web/dou/-/portaria-gm-md-n-4.138-de-14-de-agosto-de-2023-503286617. Acesso em: 18 de outubro de 2023.

BRASIL. Ministério da Defesa. Gabinete do Ministro. Portaria GM-MD nº 4.174, de 16 de agosto de 2023. Aprova o Plano Setorial de Gestão de Incidentes Cibernéticos do Setor Defesa (PSGIC-Def). Diário Oficial da União, Brasília, DF, 18 ago. 2023. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-gm-md-n-4.174-de-16-de-agosto-de-2023-504533401. Acesso em 16 de outubro de 2023.

BRASIL. Norma Complementar nº 05/IN01/DSIC/GSIPR, e seu anexo, Disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal. Diário Oficial da

União: seção 1, Brasília, DF, n. 156, de 17 ago. 2009.

BRASIL. Norma Complementar nº 08/IN01/DSIC/GSIPR, Estabelece as diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal. Diário Oficial da União: seção 1, Brasília, DF, n. 162, de 24 ago. 2010.

BRASIL. Norma Complementar nº 12/IN01/DSIC/GSIPR, Estabelece diretrizes e orientações básicas para o uso de dispositivos móveis nos aspectos referentes à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. Diário Oficial da União: seção 1, Brasília, DF, nº 30, de 10 fev. 2012.

BRASIL. Presidência da República. Decreto nº 9.637, de 26 de dezembro de 2018. Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. Diário Oficial da União, Brasília, DF, 27 dez. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm. Acesso em: 16 de outubro de 2023.

BRASIL. Presidência da República. Decreto nº 10.332, de 28 de abril de 2020. Institui a Estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional e dá outras providências. Diário Oficial da União, Brasília, DF, 29 abr. 2020. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10332.htm.
Acesso em: 18/10/2023

BRASIL. Presidência da República. Decreto nº 10.748, de 16 de julho de 2021. Institui a Rede Federal de Gestão de Incidentes Cibernéticos. Diário Oficial da União, Brasília, DF, 19 jul. 2021. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/decreto/D10748.htm. Acesso em: 16 de outubro de 2023.

Anexo – Áreas de atuação das ETIR do COMAER