EB20-D-01.038

MINISTÉRIO DA DEFESA

EXÉRCITO BRASILEIRO

COMANDANTE DO EXÉRCITO

DIRETRIZ DE GESTÃO DE INCIDENTES CIBERNÉTICOS NO ÂMBITO DO EXÉRCITO BRASILEIRO

1ª Edição

2022

EB20-D-01.038

MINISTÉRIO DA DEFESA

EXÉRCITO BRASILEIRO

COMANDANTE DO EXÉRCITO

DIRETRIZ DE GESTÃO DE INCIDENTES CIBERNÉTICOS NO ÂMBITO DO EXÉRCITO BRASILEIRO

1ª Edição

2022

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
ESTADO-MAIOR DO EXÉRCITO

PORTARIA – EME/C Ex Nº 903, DE 07 DE NOVEMBRO DE 2022
NUP: 64535.050836/2022-13

Aprova a Diretriz de Gestão de Incidentes cibernéticos no âmbito do Exército (EB20-D-01.038) e dá outras providências.

O CHEFE DO ESTADO-MAIOR DO EXÉRCITO, no uso das atribuições que lhe conferem o art. 5º, incisos I e II, do Anexo I, do Decreto nº 5.751, de 12 de abril de 2006, e de acordo com a delegação de competência que lhe confere o art. 1º, inciso IV, alínea "t", da Portaria do Comandante do Exército nº 1.700, de 8 de dezembro de 2017, o art. 3º, inciso I, da Portaria do Comandante do Exército nº 1.782, de 27 de junho de 2022, e em conformidade com o que prescreve o art. 4º, inciso X, do Regulamento do Estado-Maior do Exército (EB10-R-01.007), aprovado pela Portaria do Comandante do Exército nº 1.780, de 21 de junho de 2022, resolve:

Art. 1º Fica aprovada a Diretriz de Gestão de Incidentes Cibernéticos no âmbito do Exército.

Art. 2º Fica determinado que o Órgão de Direção Geral, o Órgão de Direção Operacional, os órgãos de direção setorial, os órgãos de assistência direta e imediata ao Comandante do Exército, os comandos militares de área e as organizações militares adotem, em suas áreas de competência, as providências decorrentes.

Art. 3º Esta Portaria entrará em vigor e produzirá seus efeitos a partir de 1º de dezembro de 2022.

General de Exército VALÉRIO STUMPF TRINDADE
Chefe do Estado-Maior do Exército

(Publicado no Boletim do Exército nº 46, de 18 de novembro de 2022)

FOLHA DE REGISTRO DE MODIFICAÇÕES

NÚMERO DE ORDEM	ATO DE APROVAÇÃO	PÁGINAS AFETADAS	DATA

ÍNDICE DE ASSUNTOS

Pag

DIRETRIZ DE GESTÃO DE INCIDENTES CIBERNÉTICOS
NO ÂMBITO DO EXÉRCITO BRASILEIRO (EB20-D-01.038)

1. FINALIDADE

Orientar a gestão de incidentes cibernéticos no âmbito do Exército Brasileiro (EB) em consonância com o arcabouço legal, normativo e doutrinário do Governo Federal e do Ministério da Defesa (MD).

2. PREMISSAS

a. Conceitos

1) Espaço cibernético (E Ciber) – espaço virtual, composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam, são processadas e/ou armazenadas, além de todas as ações, humanas ou automatizadas, conduzidas nesse ambiente.

2) Ativos de informação – meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, recursos humanos que a eles têm acesso e conhecimento ou dado que tem valor para um indivíduo ou organização.

3) Evento cibernético – qualquer ocorrência identificada em um sistema, serviço ou rede, que indique uma possível falha da política de segurança, falha das salvaguardas, tentativa de exploração de vulnerabilidade de sistema de informação ou mesmo uma situação até então desconhecida, que possa se tornar relevante em termos de segurança cibernética.

4) Incidente cibernético – ocorrência que comprometa, 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 ser caracterizado pela exploração de vulnerabilidade de sistema de informação que constitua violação de norma, política de segurança, procedimento de segurança ou política de uso.

5) Gestão de incidentes cibernéticos – processo no qual são realizadas ações sobre qualquer evento adverso relacionado à segurança e proteção cibernética dos sistemas ou da infraestrutura de computação.

6) Tratamento de incidentes cibernéticos – consiste nas ações e procedimentos tomados imediatamente após a identificação do incidente, visando garantir a continuidade de operações, preservar evidências e emitir as notificações necessárias.

7) Resposta a incidentes cibernéticos – processo que envolve as atividades técnicas de contenção, erradicação e mitigação de um incidente.

8) Crise cibernética – situação excepcional, caracterizada pela ocorrência de um ou mais incidentes cibernéticos graves, com potencial para comprometer ativos de informação críticos da Instituição, provocar efeitos (cinéticos ou não cinéticos) danosos sobre pessoas, instalações ou instituições e/ou afetar a imagem do EB, impondo a adoção de medidas excepcionais na mitigação de possíveis danos ou o emprego de elementos operacionais.

9) Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) – grupo de agentes públicos com a responsabilidade de prestar serviços relacionados à segurança cibernética para o órgão ou a entidade da Administração Pública Federal (APF), em observância à política de segurança da informação e aos processos de gestão de segurança da informação do órgão ou da entidade.

10) ETIR de coordenação - Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos que coordena e facilita as ações de resposta a incidentes entre diversas Seções de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (STIR).

11) Equipe de coordenação setorial – Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos das agências reguladoras, responsável por coordenar as atividades de segurança cibernética e de centralizar as notificações de incidentes do setor.

b. A gestão de incidentes cibernéticos depende da atuação colaborativa de órgãos e entidades da APF, do setor privado e da academia, em todos os níveis, nos contextos nacional e internacional.

c. A gestão de incidentes cibernéticos se enquadra no escopo da Segurança, da Defesa e da Guerra Cibernética, particularmente no tocante às ações de Proteção Cibernética, contribuindo para a Segurança da

Informação (SI).

d. A gestão de incidentes cibernéticos é desenvolvida em tempo integral, a fim de permitir o tratamento e a resposta oportuna e prevenir a escalada para situações de crise.

e. São incidentes cibernéticos, dentre outros:

1) Obtenção de acesso não autorizado a um sistema ou a dados armazenados;

2) Utilização não autorizada de sistemas para a realização de atividades de processamento ou armazenamento de dados;

3) Mudanças não autorizadas de **firmware, hardware** ou **software** em um ambiente computacional;

4) Ataques de negação de serviço (**Denial of Service** - **DOS** ou **Distributed Denial of Service** - **DDOS**);

5) Violação de direito autoral de arquivos digitais (livros, músicas, **softwares** e outros); e

6) Demais ações que visam afetar a disponibilidade, integridade, confidencialidade e autenticidade dos dados.

f. A equipe de coordenação setorial do MD é operada pelo Comando de Defesa Cibernética (COMDCIBER), nos termos do art. 6º do Decreto nº 10.748, de 16 de julho de 2021, que institui a Rede Federal de Gestão de Incidentes Cibernéticos.

g. As atividades a serem desenvolvidas na gestão de uma crise cibernética seguirão as orientações gerais contidas na Diretriz de Acompanhamento da Conjuntura e Gestão de Crise (EB20-D-02.002), quando aplicáveis.

h. Os controles de segurança da informação a serem empregados no EB serão baseados nos constantes da NBR 27002, do **Center For Internet Security (CIS) Critical Security Controls** ou outros controles empregados no MD.

i. A presente Diretriz não contempla a gestão de incidentes cibernéticos durante as operações militares, que será regulada nos planejamentos específicos.

3. CONCEPÇÃO GERAL

a. Estrutura

1) Compõem a infraestrutura para prevenção, tratamento e resposta a incidentes cibernéticos do Exército Brasileiro:

a) A ETIR/EB, do tipo de coordenação, operada pelo Centro Integrado de Telemática do Exército (CITEX); e

b) As STIR operadas pelos Centros de Telemática (CT) e pelo Centro de Telemática de Área (CTA), coordenadas pela ETIR/EB.

2) A ETIR/EB integra a Rede Federal de Gestão de Incidentes Cibernéticos.

3) A articulação da ETIR/EB com o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR.Gov) normalmente será realizada por intermédio da equipe de coordenação setorial do MD, sendo autorizada a ligação direta, em casos excepcionais.

b. Objetivos

1) São objetivos da gestão de incidentes cibernéticos:

a) Contribuir para efetividade da proteção cibernética dos ativos de informação do EB;

b) Colaborar para que o EB utilize o E Ciber de seu interesse com liberdade de ação;

c) Cooperar com as estruturas de gestão de incidentes cibernéticos de órgãos externos, nos níveis nacional e internacional por meio:

(1) da divulgação de medidas de prevenção, tratamento e resposta a incidentes cibernéticos;

(2) do compartilhamento de alertas sobre ameaças e vulnerabilidades cibernéticas; e

(3) da difusão de informações sobre ataques cibernéticos.

d) Analisar os eventos cibernéticos, que não se constituírem incidentes cibernéticos, a fim de determinar tendências, subsidiar atividades pró-ativas de proteção cibernética e ampliar a consciência sobre o espaço cibernético de interesse.

c. Funcionamento

1) O processo de gestão de incidentes cibernéticos envolve a realização das seguintes atividades básicas:

a) Qualquer organização ou indivíduo, ao identificar a possibilidade de ocorrência de um incidente cibernético, deverá informá-la no mais curto prazo à STIR do CTA/CT de sua área, a qual apoiará o detentor do ativo de informação afetado, sob a coordenação e a orientação da ETIR/EB.

b) A ETIR/EB identificará se há outras ETIR externas à Força envolvida no incidente e, caso positivo, providenciará as devidas notificações e com elas coordenará as ações subsequentes.

c) A ETIR/EB avaliará, de imediato, a possibilidade do incidente cibernético afetar a imagem da Força e/ou demandar o emprego de elementos operacionais para sua resposta. Caso positivo, o Chefe do Departamento de Ciência e Tecnologia (DCT) e o COMDCIBER, este como Órgão Central do Sistema de Defesa Cibernética do Exército (SDCiberEx), serão imediatamente informados.

d) O Ch DCT avaliará a necessidade e a oportunidade em que o Comandante do Exército (Cmt Ex), o Comando de Operações Terrestres (COTER), o Centro de Comunicação Social do Exército (CCOMSEx) e o Centro de Inteligência do Exército (CIE) serão informados sobre o incidente.

e) Em se confirmando a avaliação de risco para a imagem da Força, o DCT determinará a coordenação com o CCOMSEx e CIE nas atividades de gestão do incidente.

f) O DCT irá coordenar com o COTER o apoio à resposta ao incidente em caso de:

(1) necessidade de apoio da Aviação do Exército (AvEx) ou da Força Aérea Brasileira (FAB) para o deslocamento de módulos especializados de cibernética;

(2) necessidade de emprego de outros elementos operacionais; e/ou

(3) possibilidade de agravamento que enseje o acionamento de um Gabinete de Crise.

g) As atividades de coleta de evidências e forense computacional serão realizadas pelas STIR, sob coordenação da ETIR/EB.

h) O DCT coordenará o apoio do órgão central do SDCiberEx à ETIR/EB nas atividades de gestão do incidente cibernético, em especial, na coleta de evidências e na atribuição de sua autoria. Caso o CIE tenha sido acionado, também poderá apoiar a realização dessas atividades, mediante solicitação.

i) Durante o tratamento do incidente, será buscada a identificação do responsável pelo incidente cibernético, com a participação de todos os envolvidos, dentro de suas especialidades. Caso tal identificação seja possível e o autor seja externo à Força, os produtos elaborados serão disponibilizados às agências responsáveis.

j) Após o tratamento do incidente, o serviço será restabelecido. A documentação e as lições aprendidas com o incidente deverão ser registradas após o encerramento, para a melhoria do processo de proteção, tratamento e resposta a incidentes.

2) A ETIR/EB poderá realizar atividades específicas e complementares às atividades supracitadas, a fim de promover a efetiva gestão dos incidentes cibernéticos no âmbito do EB.

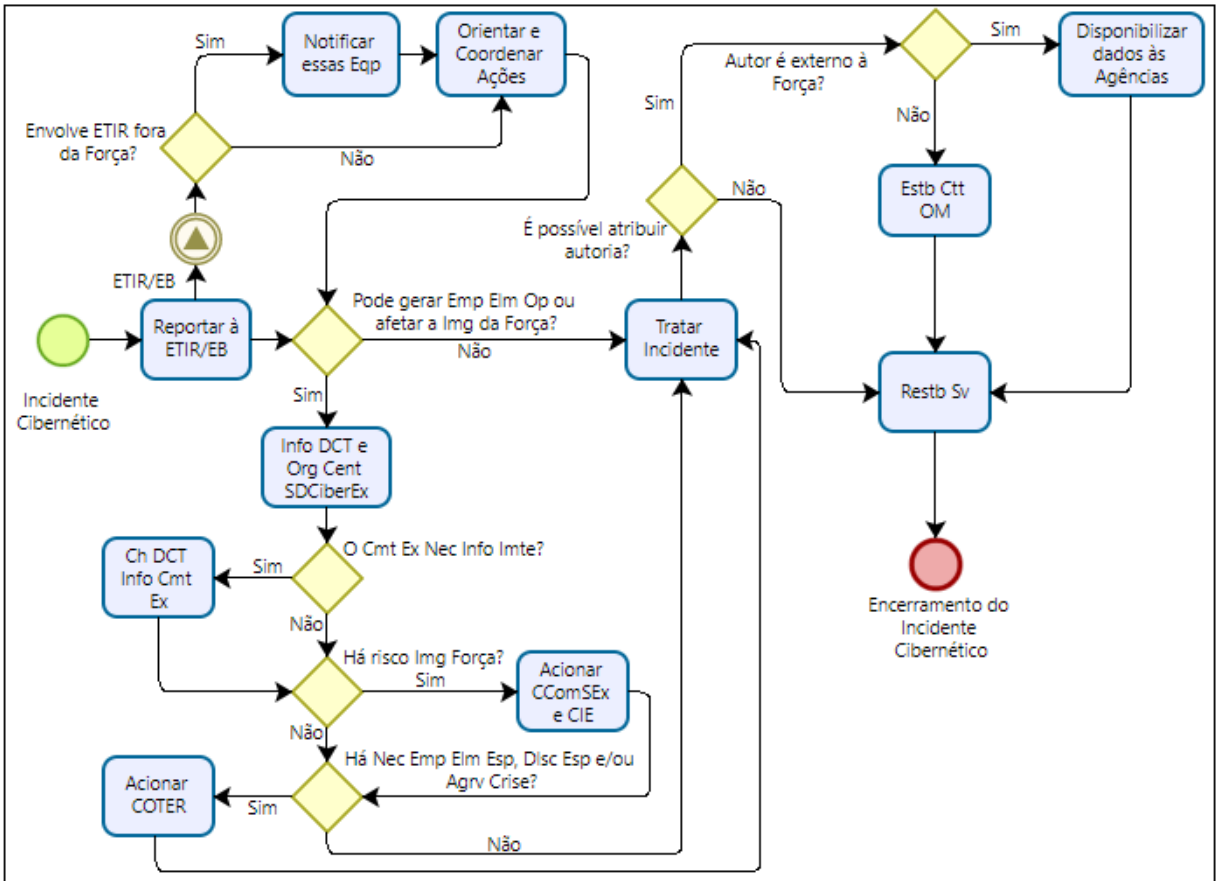

Figura 01: Fluxograma do processo de tratamento de incidentes cibernéticos

4. ATRIBUIÇÕES

a. <u>Estado-Maior do Exército (EME)</u>

1) Orientar, supervisionar, coordenar, controlar e avaliar, no nível de direção geral, a execução das ações previstas nesta Diretriz.

2) Manter atualizadas as normas de gestão de incidentes cibernéticos no âmbito do EB, mediante proposta do DCT.

b. <u>COTER</u>

1) Em coordenação com o DCT, apoiar a gestão de incidentes cibernéticos, nos temas sob sua responsabilidade.

2) Orientar e coordenar o preparo e o emprego da Força Terrestre para o enfrentamento de incidentes e crises cibernéticas.

c. <u>DCT</u>

1) Informar ao Cmt Ex e coordenar as ações com o COTER, CIE e CCOMSEx, em caso de incidentes cibernéticos que possam afetar a imagem da Força, ensejar o emprego de elementos operacionais ou evoluir para crises cibernéticas.

2) Regular a gestão de incidentes cibernéticos no âmbito do EB.

3) Instituir, implementar e operar a ETIR/EB, por intermédio do CITEx, e as STIR por intermédio dos CTA/CT.

4) Prestar orientação técnica ao Órgão de Direção Operacional (ODOp), aos órgãos de direção setorial (ODS), aos comandos militares de área (C Mil A) e órgãos de assistência direta e imediata ao Comandante do Exército (OADI), nos assuntos relativos à gestão de incidentes envolvendo seus ativos de informação.

5) Elaborar, divulgar e atualizar o Plano de Gestão de Incidentes Cibernéticos do EB, em consonância

com o Plano de Gestão de Incidentes Cibernéticos do CTIR.Gov e com o Plano Setorial de Gestão de Incidentes Cibernéticos, que orienta a ETIR/EB e as STIR quanto às atividades referentes à prevenção, ao tratamento e à resposta a incidentes cibernéticos.

6) Fomentar, normatizar, orientar e supervisionar a pesquisa, o desenvolvimento, a inovação e a implementação de sistemas, meios, programas e aplicativos de interesse da gestão de incidentes cibernéticos.

7) Orientar e promover a realização de ações de capacitação dos recursos humanos integrantes da infraestrutura de gestão de incidentes cibernéticos no EB.

8) Fazer gestões para a garantia dos recursos orçamentários necessários para a gestão de incidentes cibernéticos.

9) Propor ao EME a atualização desta Diretriz.

d. <u>Demais ODS, C Mil A e OADI</u>

1) Monitorar os ativos de informação sob sua responsabilidade, a fim de identificar e informar a ocorrência de possíveis incidentes cibernéticos às STIR de sua área.

2) Quando solicitado, apoiar a gestão de incidentes cibernéticos.

e. <u>CCOMSEx</u>

- Quando solicitado, apoiar a gestão de incidentes cibernéticos que possam oferecer risco à imagem da Força.

f. <u>CIE</u>

- Quando solicitado, apoiar a gestão de incidentes cibernéticos.

5. PRESCRIÇÕES DIVERSAS

- Os casos omissos a esta Diretriz serão decididos pelo Chefe do EME.