1ª PARTE
LEIS E DECRETOS

Sem alteração.

2ª PARTE
ATOS ADMINISTRATIVOS

COMANDANTE DO EXÉRCITO

PORTARIA Nº 803, DE 30 DE JULHO DE 2014.

Aprova as Instruções Gerais de Segurança da Informação e Comunicações para o Exército Brasileiro (EB10-IG-01.014) e dá outras providências.

O **COMANDANTE DO EXÉRCITO**, no uso das atribuições que lhe conferem o art. 4º da Lei Complementar nº 97, de 9 de junho de 1999, alterada pela Lei Complementar nº 136, de 25 de agosto de 2010, e o inciso I e XIV do art. 20 da Estrutura Regimental do Comando do Exército, aprovada pelo Decreto nº 5.751, de 12 de abril de 2006, de acordo com o que propõe o Estado-Maior do Exército (EME), resolve:

Art. 1º Aprovar as Instruções Gerais de Segurança da Informação e Comunicações para o Exército Brasileiro (EB10-IG-01.014).

Art. 2º Revogar a Portaria do Comandante do Exército nº 483, de 20 de setembro de 2001.

Art. 3º Estabelecer que esta portaria entre em vigor na data de sua publicação.

INSTRUÇÕES GERAIS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES PARA O EXÉRCITO BRASILEIRO (EB10-IG-01.014)

ÍNDICE DOS ASSUNTOS

PREFÁCIO

As Instruções Gerais (IG), descritas neste documento, têm por finalidade orientar o planejamento e a execução das ações relacionadas à Segurança da Informação e Comunicações (SIC) no âmbito do Exército Brasileiro (EB). Foram elaboradas considerando, como referência, documentos normativos sobre SIC vigentes no âmbito do Ministério da Defesa (MD), assim como outras publicações de interesse na esfera da Administração Pública Federal (APF). Desta forma, proporcionando harmonia e alinhamento das ações de SIC a serem adotadas no EB, com as ações consolidadas em outras instituições do Governo Federal, sem perder de vista as particularidades da Força.

As diretrizes gerais, contidas nestas IG, devem nortear as ações de SIC em todas as Organizações Militares (OM) do EB e demais publicações sobre o tema. Para desdobramento destas IG, nos níveis operacional e tático, devem ser consultadas as Instruções Reguladoras (IR) delas decorrentes.

CAPÍTULO I
DA FINALIDADE

Art. 1º Estas IG têm por finalidade orientar as ações de SIC no âmbito do EB, de modo a viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações institucionais.

CAPÍTULO II
DA CONCEITUAÇÃO E REFERÊNCIAS

Seção I
Da Conceituação

Art. 2º Para efeitos destas IG são estabelecidos os seguintes conceitos e definições:

I - Ameaça: conjunto de fatores internos e/ou externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou OM;

II - Ativos de informação: os meios de armazenamento, recepção, transmissão e processamento da informação; os equipamentos necessários a isso; os sistemas utilizados para tal; os locais onde se encontram esses meios; e também os recursos humanos que a eles têm acesso;

III - Autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

IV - Avaliação de riscos: processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco;

V - Capacitação em Segurança da Informação e Comunicações: atividade de ensino que tem como objetivo orientar sobre o que é SIC, fazendo com que os participantes saibam aplicar os conhecimentos em sua rotina pessoal e profissional, além de servirem como multiplicadores sobre o tema, estando aptos para atuar em suas OM como Gestores de SIC;

VI - Comitê de Segurança da Informação e Comunicações (COMSIC): grupo de militares designados com a responsabilidade de assessorar a implementação das ações de SIC no âmbito do EB;

VII - Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;

VIII - Conscientização: atividade destinada à sensibilizar sobre o que é SIC e a sua importância, fazendo com que os participantes internalizem os conhecimentos relativos à SIC e os apliquem conscientemente em sua rotina pessoal e profissional, identificando as ações que precisam ser corrigidas, além de servirem como multiplicadores sobre o tema;

IX - Defesa Cibernética: conjunto de ações ofensivas, defensivas e exploratórias, realizadas no Espaço Cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo MD, com as finalidades de proteger os sistemas de informação de interesse da Defesa Nacional, obter dados para a produção de conhecimento de Inteligência e comprometer os sistemas de informação do oponente;

X - Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

XI - Gestão de Continuidade da Missão: processo abrangente de gestão que identifica ameaças potenciais para uma OM e os possíveis impactos na missão, caso estas ameaças se concretizem. Este processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses e a imagem da Instituição;

XII - Gestão de Riscos de SIC: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;

XIII - Gestão da SIC: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade da missão, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à Tecnologia da Informação e Comunicações (TIC);

XIV - Gestor de SIC: responsável pelas ações de SIC no âmbito de sua OM;

XV - Guerra Cibernética: corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de C² do adversário, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar. Compreende ações que envolvem as ferramentas de Tecnologia da Informação e Comunicações (TIC) para desestabilizar ou tirar proveito dos Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle (STIC²) do oponente e defender os próprios STIC². Abrange, essencialmente, as Ações Cibernéticas. A oportunidade para o emprego dessas ações ou a sua efetiva utilização será proporcional à dependência do oponente em relação à TIC;

XVI - Guerra da Informação: conjunto de ações destinadas a obter a superioridade das informações, afetando as redes de comunicação de um oponente e as informações que servem de base aos processos decisórios do adversário, ao mesmo tempo em que garante as informações e os processos amigos;

XVII - Impacto: tamanho do prejuízo, medido através de propriedades mensuráveis ou abstratas, que a concretização de uma determinada ameaça causará;

XVIII - Incidente de Rede: ocorrência de um evento de violação de segurança da rede, seja de origem intencional ou não, que atinja recursos de infraestrutura física, lógica ou de alimentação elétrica, hardware, meios de armazenamento, protocolos, dados, serviços, software ou qualquer outros recursos de rede cujo comprometimento atinja a integridade, a disponibilidade ou a confidencialidade da informação;

XIX - Informação: estas IG consideram-na em sua acepção genérica, englobando dados, informações e conhecimentos, hierarquizados de acordo com o valor agregado, resultante das suas possibilidades de emprego e dos processos utilizados para a sua obtenção;

XX - Integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XXI - Inventário e Mapeamento de Ativos de Informação: é um processo interativo e evolutivo, composto por 3 (três) etapas:

a) identificação e classificação de ativos de informação;

b) identificação de potenciais ameaças e vulnerabilidades; e

c) avaliação de riscos.

XXII - Sistema de Gestão da Segurança da Informação: parte de um sistema de gestão global, baseado na abordagem de risco à missão da OM, para planejar, implementar, monitorar e manter a SIC;

XXIII - Risco: potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo na OM;

XXIV - Segurança Cibernética: arte de assegurar a existência e a continuidade da sociedade da informação de uma nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infraestruturas críticas;

XXV - Segurança da Informação e Comunicações: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

XXVI - Segurança Orgânica: conjunto de medidas passivas destinadas a prevenir e obstruir ações adversas, de elemento ou grupo de qualquer natureza, e engloba as atividades de segurança ligadas a pessoal, comunicações, informática, documentação e material, áreas e instalações; e

XXVII - Vulnerabilidade: qualquer fragilidade existente em um sistema de informação que, se explorado, pode vir a causar um impacto ao sistema.

Seção II
Das Referências

Art. 3º Referências:

I - Lei nº 8.159, de 8 de janeiro de 1991 - Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências;

II - Medida Provisória nº 2.200-2, de 24 de agosto de 2001 - Institui a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, e dá outras providências;

III - Decreto nº 3.505, de 13 de junho de 2000 - Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;

IV - Decreto nº 3.865, de 13 de julho de 2001 - Estabelece requisito para contratação de serviços de certificação digital pelos Órgãos Públicos Federais e dá outras providências;

V - Decreto nº 3.996, de 31 de outubro de 2001 - Dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal;

VI - Decreto nº 7.845, de 14 de novembro de 2012 - Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento;

VII - Instrução Normativa GSI/PR nº 1, de 18 de junho de 2008 - Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências;

VIII - Instrução Normativa GSI/PR nº 2, de 5 de fevereiro de 2013 - Dispõe sobre o Credenciamento de segurança para o tratamento de informação classificada, em qualquer grau de sigilo, no âmbito do Poder Executivo Federal, e suas Normas Complementares;

IX - Instrução Normativa GSI/PR nº 3, de 6 de março de 2013 - Dispõe sobre os parâmetros e padrões mínimos dos recursos criptográficos baseados em algoritmos de Estado para criptografia da informação classificada no âmbito do Poder Executivo Federal, e suas Normas Complementares;

X - Portaria Normativa nº 0215-MD, de 27 de março de 2001 - Dispõe sobre a Política para o Sistema Militar de Comando e Controle;

XI - Portaria Normativa nº 3.389-MD, de 21 de dezembro de 2012 - Dispõe sobre a Política Cibernética de Defesa;

XII - Portaria do Comandante do Exército nº 11, de 10 de janeiro de 2001 - Aprova as Instruções Gerais para a Salvaguarda de Assuntos Sigilosos no Exército Brasileiro;

XIII - Portaria do Comandante do Exército nº 445, de 14 de junho de 2010 - Aprova a Diretriz Estratégica Organizadora do Sistema de Informação do Exército e dá outras providências;

XIV - Portaria do Comandante do Exército nº 508, de 25 de junho de 2013 - Aprova as Instruções Gerais do Ciclo de Vida de *Software* (EB10-IG-01.006), 1ª Edição, 2013, e dá outras providências;

XV - Manual de Campanha MC 30-3 - Ramo Contrainteligência;

XVI - ABNT NBR ISO/IEC 27001:2013 - Sistemas de gestão de segurança da informação - Requisitos; e

XVII - ABNT NBR ISO/IEC 27002:2013 - Código de prática para controles de segurança da informação.

CAPÍTULO III
DOS OBJETIVOS E PRESSUPOSTOS BÁSICOS

Seção I
Dos Objetivos

Art. 4º São objetivos destas IG no âmbito do EB:

I - estabelecer as referências básicas para a SIC;

II - estabelecer diretrizes para a implementação da SIC; e

III - definir responsabilidades pelas ações relacionadas à SIC.

Seção II
Dos Pressupostos Básicos

Art. 5º As diretrizes gerais descritas nestas IG declaram o comprometimento e a visão do Alto Comando do EB em relação à SIC.

Art. 6º A informação institucional do EB é um patrimônio a ser protegido e preservado.

Art. 7º A eficiência no emprego dos recursos de TIC constitui fator primordial para a eficácia do EB.

Art. 8º A existência de ameaças, vulnerabilidades e riscos é inerente ao emprego e acesso às informações, num contexto de uma crescente informatização de atividades e processos organizacionais.

Art. 9º O sucesso das ações de SIC depende, fundamentalmente, da conscientização do público interno, da capacitação científico-tecnológica dos recursos humanos envolvidos, da qualidade das soluções adotadas e da SIC contra ameaças internas e externas.

CAPÍTULO IV
DAS DIRETRIZES GERAIS

Art. 10. Estas IG devem ser consideradas como o documento norteador para a elaboração de todos os documentos normativos sobre SIC no âmbito do EB.

Art. 11. Procedimentos de SIC que requeiram IR ainda não publicadas, deverão ser baseados nas normas específicas sobre o tema no âmbito do MD ou da APF.

Art. 12. A informação, como um recurso vital para a OM, deve ser tratada como patrimônio a ser protegido e preservado em todo o seu ciclo de vida.

Art. 13. Todas as informações produzidas e manuseadas no âmbito do EB devem ser tratadas para assegurar a disponibilidade, integridade, confidencialidade e autenticidade.

Art. 14. Deverão ser definidos procedimentos formais para o armazenamento, o transporte e o descarte das informações produzidas e armazenadas, de modo a se evitar a perda, o roubo ou a exposição indevida.

Art. 15. A gestão de riscos de SIC deve ser o elemento norteador para a tomada de decisões em relação a todas as ações de SIC.

Art. 16. Os riscos de SIC devem ser continuamente monitorados e tratados, de acordo com as vulnerabilidades associadas aos ativos de informação e respectivos níveis de risco.

Art. 17. Todas as relações formalizadas com partes externas e terceiros devem ser objetos de avaliação de riscos.

Art. 18. Todos os ativos de informação, no âmbito do EB, devem ser objetos de gestão de riscos.

Art. 19. Toda a cadeia hierárquica do EB, empresas prestadoras de serviços, terceiros e partes interessadas deverão ser sensibilizadas a respeito da importância de SIC para a Força e, assim, promover atitudes favoráveis referentes ao tema.

Art. 20. O tema SIC deve ser abordado nas escolas e cursos de formação e aperfeiçoamento militar do EB, de forma a possibilitar a crescente conscientização e o desenvolvimento de atitudes favoráveis à proteção das informações julgadas relevantes para a Força.

Art. 21. Em todas as OM do EB deverão ser realizadas instruções de sensibilização, conscientização e capacitação para formação e fortalecimento da cultura de SIC.

Art. 22. O uso institucional das redes sociais deve ser norteado por diretrizes, critérios, limitações e responsabilidades para seu uso seguro.

Art. 23. A utilização de rede sem fio deverá se restringir às situações nas quais o uso de rede cabeada seja comprovadamente inviável, devendo a mesma ser dotada de todas as boas práticas de segurança, de maneira que sejam mitigados os riscos de acesso indevido ou interceptação das informações transmitidas.

Art. 24. A implementação ou a contratação de tecnologias de computação em nuvem devem ser realizadas somente sob criteriosa avaliação de riscos e em conformidade com as IR específicas sobre o tema.

Art. 25. Deve ser estimulada a eliminação da dependência externa em relação a sistemas, equipamentos, dispositivos e atividades vinculadas à segurança dos sistemas de informação e de comunicações.

Art. 26. O emprego de tecnologias consagradas pelo uso, que não estejam explicitadas nestas IG, assim como, temas normatizados em instâncias superiores do EB, deverão ser disciplinadas em IR específicas.

Art. 27. A cifração e decifração de informações classificadas em qualquer grau de sigilo devem utilizar recurso criptográfico baseado em algoritmo de Estado. Para o cumprimento desta diretriz, incluindo os casos de tratamento excepcional, deverão ser observados os requisitos dispostos nos normativos sobre o tema, publicados por intermédio do Conselho de Defesa Nacional (CDN) e do MD.

Art. 28. O emprego da criptologia no âmbito do EB deverá ser realizado conforme procedimentos definidos em IR específicas.

Art. 29. O uso de sistemas criptográficos de origem estrangeira deve ser evitado ao máximo, devendo ser buscado o desenvolvimento e a adoção de padrões criptográficos de Estado, respeitada a necessidade de interoperabilidade com os sistemas criptográficos adotados no âmbito do MD e da APF.

Art. 30. O uso de dispositivos móveis para acesso aos recursos computacionais no âmbito do EB deve ser controlado conforme procedimentos de segurança definidos em IR específicas sobre o tema.

Art. 31. A interoperabilidade e a integração dos sistemas de informação, não só no âmbito do EB, mas também junto às demais Forças Armadas e aos demais órgãos da APF, devem ser promovidas, quando julgado necessário, sempre respeitando as diretrizes e normas de segurança aplicáveis.

Art. 32. A remoção, a reutilização e o descarte dos discos rígidos dos servidores e estações de trabalho deverão ser regulados por meio de Diretriz de Segurança ou Norma Geral de Ação de cada OM, de modo que seja evitada a recuperação, a perda, o roubo ou a exposição indevida das informações armazenadas nos dispositivos.

Art. 33. O controle de acesso físico e lógico deve ser implementado considerando, no mínimo, a identificação, a autenticação, a autorização, o interesse do serviço e a necessidade de conhecer como condicionantes prévias para concessão de acesso.

Art. 34. Todos os usuários, no âmbito do EB, devem reportar vulnerabilidades ou qualquer situação que apresente risco à SIC, logo após sua identificação, para os superiores imediatos e, se aplicável, ao responsável pela SIC da OM.

Art. 35. Os incidentes de rede devem ser reportados para a Seção de Segurança dos Centro de Telemática de Área/Centro de Telemática (CTA/CT) ou Centro Integrado de Telemática do Exército (CITEx)/Infraestrutura de Tratamento de Incidentes de Redes do Exército (ITIREx), quando se tratarem de ativos do domínio eb.mil.br, e Departamento de Educação e Cultura do Exército (DECEx), quando se tratarem de ativos do domínio ensino.eb.br.

Art. 36. A gestão de continuidade da missão no âmbito do EB deve:

I - ser um processo inerente à manutenção dos sistemas de informação da Força; e

II - buscar minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades sobre as atividades da OM, por intermédio de ações de prevenção, resposta e recuperação.

Art. 37. Todos os processos críticos para o EB devem ser contemplados na gestão de continuidade da missão.

Art. 38. O processo de auditoria interna nas OM do EB deverá ser realizado periodicamente, de modo a garantir a manutenção e evolução da maturidade da gestão da SIC na Força.

Art. 39. Todas as redes computacionais do EB deverão ser abrangidas de processos de tratamento e resposta a incidentes em redes computacionais.

Art. 40. Uma metodologia de gestão da SIC deve ser estabelecida para apoiar a implementação da SIC no âmbito do EB.

CAPÍTULO V
DAS RESPONSABILIDADES

Seção I
Do Estado-Maior do Exército

Art. 41. Compete ao Estado-Maior do Exército (EME):

I - coordenar as ações junto às outras Forças e Órgãos da APF nos processos que visem estabelecer normativos conjuntos e integrados de SIC;

II - acompanhar, em âmbito nacional e internacional, a evolução doutrinária das atividades inerentes à SIC;

III - realizar atividades de prospecção visando à melhoria da capacitação do EB em ações inseridas no contexto de Segurança, Defesa e Guerra Cibernéticas e Guerra da Informação;

IV - instituir o COMSIC do EB considerando a representatividade dos diversos setores;

V - designar o Gestor de SIC do EB; e

VI - manter atualizadas as presentes IG.

Seção II
Do Departamento de Ciência e Tecnologia

Art. 42. Compete ao Departamento de Ciência e Tecnologia (DCT):

I - propor ao EME a elaboração e atualização dos documentos normativos de SIC no âmbito do EB;

II - promover a capacitação de pessoal especializado, nos níveis de extensão, especialização, graduação e pós-graduação, nas áreas do conhecimento relativas à SIC, dentro e fora do EB, no país e no exterior;

III - desenvolver pesquisas básicas e aplicadas relacionadas com SIC, que possibilitem ao EB assegurar a inviolabilidade das soluções adotadas e a eliminação da dependência externa;

IV - implementar e adotar soluções de segurança corporativa relativas à plataforma de TIC sob sua responsabilidade, com base em estudos sobre a pertinência, abrangência, confiabilidade, permanência, manutenção e suporte das mesmas;

V - realizar a monitoração permanente e a avaliação da plataforma de TIC no âmbito do EB;

VI - prestar assessoramento técnico às OM do EB, relativo à segurança de sistemas de informação;

VII - realizar a certificação das soluções tecnológicas a serem adotadas no âmbito do EB, com base nas orientações do MD e da Secretaria-Executiva do CDN;

VIII - promover a capacitação continuada dos profissionais da área de SIC das OM do EB, por meio de cursos de extensão e especialização;

IX - participar com pessoal qualificado, junto aos órgãos públicos e privados, da elaboração dos acordos multilaterais, convenções, normas, recomendações e outros atos sobre SIC propostos por organismos nacionais e internacionais;

X - promover a interoperabilidade dos sistemas de informação utilizados internamente pelo EB, bem como promover a adequada integração dos mesmos com os adotados pelas demais Forças, no tocante aos aspectos ligados à SIC, em especial com relação ao Sistema Militar de Comando e Controle e no âmbito da APF, quando pertinente;

XI - acompanhar, em âmbito nacional e internacional, a evolução tecnológica das atividades inerentes à SIC; e

XII - efetivar estudos nos quesitos estrutura e funcionamento de rede, de modo a obter o máximo de eficiência e segurança desde o curto prazo, o máximo de economia a médio e longo prazos, e o mínimo de dependência externa (ação do homem), a qualquer tempo, para a consecução dos objetivos esperados.

Seção III
Do Departamento de Educação e Cultura do Exército

Art. 43. Compete ao DECEx:

I - incluir em todos os currículos nos cursos de formação, de aperfeiçoamento e de Altos Estudos Militares, da linha de ensino bélico, no âmbito do EB, assuntos relacionados à SIC;

II - investir na formação continuada dos profissionais da área de SIC das OM, por meio de cursos de extensão e especialização;

III - gerenciar o processo de tratamento e resposta a incidentes em redes computacionais de sua competência; e

IV - reportar ao Centro de Defesa Cibernética (CDCiber) os incidentes de maior relevância para o EB ocorridos nas redes do DECEx.

Seção IV
Do Centro de Comunicação Social do Exército

Art. 44. Compete ao Centro de Comunicação Social do Exército (CCOMSEx):

I - apoiar a veiculação das campanhas sobre o que é SIC e a sua importância;

II - apoiar as demandas de SIC no que concerne às suas competências institucionais; e

III - gerir o uso institucional das mídias sociais em conformidade com as normas de SIC vigentes no EB ou em instância superior aplicável.

Seção V
Do Centro de Inteligência do Exército

Art. 45. Compete ao Centro de Inteligência do Exército (CIE):

I - propor ao EME as atualizações necessárias para manter a doutrina de Contrainteligência compatível com o arcabouço normativo de SIC vigente no EB;

II - orientar as OM do EB sobre as medidas de Contrainteligência relativas à SIC;

III - realizar a monitoração permanente da execução das medidas de Segurança Orgânica preconizadas pela doutrina de Contrainteligência, no âmbito do EB;

IV - apoiar as demandas de SIC no que concerne às suas competências institucionais; e

V - reportar ao CDCiber os incidentes de rede identificados no sistema de inteligência de relevância para o EB.

Seção VI
Do Centro de Defesa Cibernética

Art. 46. Compete ao CDCiber:

I - propor ao DCT a elaboração e atualização dos documentos normativos de SIC no âmbito do EB;

II - cooperar com o DCT na elaboração de documentos normativos para o setor cibernético, considerando a SIC como base da Defesa Cibernética.

III - acompanhar os incidentes de rede de maior relevância para o EB ocorridos no espaço cibernético de interesse;

IV - propor aos órgãos competentes as atividades de capacitação na área cibernética no âmbito do EB; e

V - promover o desenvolvimento de projetos no setor cibernético em acordo com o Sistema de Ciência e Tecnologia do Exército.

Seção VII
Do Centro Integrado de Telemática do Exército

Art. 47. Compete ao CITEx:

I - proporcionar SIC nas bases física e lógica necessárias para o funcionamento dos sistemas de interesse do Sistema Estratégico de Comando e Controle do Exército;

II - prover SIC na integração dos Sistema Estratégico de Comando e Controle do Exército, Sistema de Comando e Controle da Força Terrestre e Sistema Militar de Comando e Controle;

III - prover o adequado nível de SIC ao Sistema Estratégico de Comunicações do Exército;

IV - gerenciar o processo de tratamento e resposta a incidentes em redes computacionais de sua competência; e

V - reportar ao CDCiber os incidentes de maior relevância para o EB ocorridos nas redes do EB.

Seção VIII
Do Gestor de Segurança da Informação e Comunicações do Exército Brasileiro

Art. 48. Compete ao Gestor de SIC do EB:

I - conduzir o processo de Gestão da SIC no âmbito da Força (Planejamento, Implementação, Monitoramento e Manutenção);

II - propor o planejamento orçamentário necessário às ações de SIC no âmbito do EB;

III - coordenar o COMSIC do EB;

IV - viabilizar a consolidação da visão de futuro estabelecida nestas IG; e

V - propor ao EME atualizações das presentes IG.

Seção IX
Do Comitê de Segurança da Informação e Comunicações

Art. 49. Compete ao COMSIC instituído no seu âmbito de atuação:

I - assessorar o Gestor de SIC sobre as ações necessárias para conduzir o processo de Gestão da SIC; e

II - instituir grupos de trabalho para abordar temas específicos sobre SIC.

Seção X
Das Demais Organizações Militares

Art. 50. Os Comandantes, Chefes e Diretores de OM, em seu âmbito de atuação, devem:

I - assegurar o cumprimento das diretrizes preconizadas nestas IG e nos documentos que lhes são complementares;

II - orientar os subordinados quanto à importância do assunto tratado nestas IG, contribuindo para o aprimoramento da mentalidade de SIC;

III - atribuir ao oficial do Estado-Maior a função de Gestor de SIC;

IV - nos casos em que se fizer necessário e for viável administrativamente, constituir o COMSIC da OM considerando a representatividade dos diversos setores;

V - aplicar as ações corretivas e disciplinares cabíveis nos casos de comprometimento da SIC; e

VI - incluir no planejamento orçamentário da OM os recursos para a implementação da SIC.

Seção XI
Dos Gestores de Segurança da Informação e Comunicações das Organizações Militares do Exército Brasileiro

Art. 51. O Gestor de SIC, em seu âmbito de atuação, deve:

I - conduzir o processo de Gestão da SIC no âmbito da OM (Planejamento, Implementação, Monitoramento e Manutenção);

II - promover a cultura de SIC;

III - disseminar as ações de SIC;

IV - acompanhar as investigações e as avaliações dos danos decorrentes do comprometimento da SIC, assessorando o Comandante de OM sobre as ações necessárias; e

V - coordenar o COMSIC da OM, quando for o caso.

CAPÍTULO VI
DAS PRESCRIÇÕES DIVERSAS

Seção I
Da Violação

Art. 52. A violação ou descumprimento de um ou mais itens destas IG e de suas IR poderá resultar na aplicação de sanções disciplinares.

Seção II
Da Atualização

Art. 53. As propostas de atualização destas IG devem, observada a cadeia de comando, ser encaminhadas pelos Comandantes, Chefes e Diretores de OM ao Gestor de SIC do EB, cabendo a este propor ao EME as alterações julgadas cabíveis.

Art. 54. Estas IG assim como todas as IR decorrentes destas, devem ser analisadas criticamente no período máximo de 3 (três) anos, no intuito de verificar a necessidade de atualização do seu teor.

PORTARIA Nº 852, DE 7 DE AGOSTO DE 2014.

Transforma a 5ª Companhia de Guardas em 15ª Companhia de Polícia do Exército e dá outras providências.

O **COMANDANTE DO EXÉRCITO**, no uso das atribuições que lhe conferem o art. 4º da Lei Complementar nº 97, de 9 de junho de 1999, alterada pela Lei Complementar nº 136, de 25 de agosto de 2010, o inciso V do art. 20 da Estrutura Regimental do Comando do Exército, aprovada pelo Decreto nº 5.751, de 12 de abril de 2006, e de acordo com o que propõe o Estado-Maior do Exército, resolve:

Art. 1º Transformar, a partir de 13 de agosto de 2014, a 5ª Companhia de Guardas em 15ª Companhia de Polícia do Exército, com sede na cidade de Belém-PA, subordinada ao Comando Militar do Norte.

Art. 2º Determinar que o Estado-Maior do Exército, os órgãos de direção setorial e o Comando Militar do Norte adotem, em suas áreas de competência, as providências decorrentes.

Art. 3º Estabelecer que esta portaria entre em vigor na data de sua publicação.